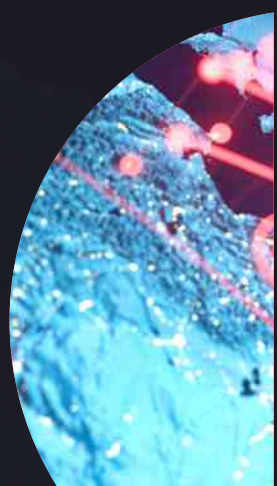**CyberRes** | G A L A X Y

2022 Annual Report
Galaxy Threat Research Program

Table of Contents

SECTION A
Executive Summary

The year 2021 smashed all records in terms of the sheer number of cyberattacks on government entities, private-sector organizations, and individuals. While several new threat actors emerged on the cybersecurity threat landscape in 2021, the existing ones also adopted more advanced tactics, techniques, and procedures (TTPs) to enhance the effectiveness of their operations.

Cyber criminals are motivated by various factors, including espionage, socio-political, criminal, and personal. Cyber espionage campaigns rely on stealth and are usually conducted by sophisticated hacking groups to obtain sensitive or classified information from their targets, such as intellectual property (IP), state secrets, research data, business goals, organizational finances, political strategies, etc. In some cases, cyber espionage is carried out simply to stain the reputation of the targets by leaking dubious business practices or private information.

On the other hand, politically motivated threat actors are more likely to grab public attention via their campaigns commonly known as "hacktivism." The perpetrators of such crusades adopt different strategies, such as defacing the websites of target companies, orchestrating denial of service (DoS) attacks, or exposing questionable information about their targets to promote their cause and beliefs. Government entities, multinational corporations, and powerful individuals have often found themselves at the crosshairs of hacktivists.

Furthermore, the criminally motivated threat actors seek financial gain via information theft, business disruption, or cryptojacking. The attackers employ a variety of attack strategies to infiltrate the target networks to perform various types of nefarious activities such as deploying ransomware or stealing sensitive data that can later be used to extort money from the victims. In some cases, the pilfered information is either leaked or sold to the highest bidder on the underground hacking forums. The adversaries also leverage cryptomining malware that hijacks the resources of infected machines to mine cryptocurrency.

Finally, personally motivated hackers usually carry a personal vendetta against individuals or organizations and try to settle scores by causing disruptions to a business or stealing valuable data or money from the targets. These attackers are usually either employees or ex-employees who have extensive knowledge about an organization's network architecture and defenses.

In this report we provide:
■ An overview of the global cyberthreat landscape.
■ A detailed discussion on the geopolitical, regional, and industry threat landscape for different geographical regions.
■ Insights on industry-specific cyberthreats.

Global Cybersecurity Themes to Watch in 2022

In 2021, organizations across the globe saw how the cyberthreat landscape advanced from its state in previous years, giving way to new and emerging threats. Micro Focus's CyberRes Galaxy threat research program continuously tracks geopolitical and social events. It's clear that they have a direct correlation to changes in cyber activity and how the threat landscape evolves. All businesses are being impacted by cyberattacks, regardless of size and industry.

1. Ransomware: enhanced tactics, new players. Ransomware has become one of the top threats to organizations across industries and no entity is immune. New ransomware groups continue to spring up and their tactics are becoming more advanced. Some of these include Colossus (possibly related to EpsilonRed, BlackCocaine, and REvil), Delta Plus (potential derivative of Babuk ransomware), AtomSilo, and Spook

(potential rebrand of the Prometheus ransomware group).

Keeping on top of the most common and emerging ransomware attack methods and vectors is critical for organizations. Over the last year alone, the tactics used by threat actors have changed, with leak sites being leveraged more commonly. Their scale and intensity have changed, impacting organizations across industries—with government, public sector, and the tech industry being among those most affected. Tabletop exercises are highly encouraged for any organization, in order to effectively prepare for an eventual attack. Several law enforcement agencies, including the Federal Bureau of Investigation (FBI), advise against paying ransoms because it offers an incentive for more cyber criminals to establish or increase their operations.

2. Nation states will continue using cyberattacks and cybercriminal groups for political gain (e.g., Sony attack, SolarWinds). Up to 18,000 of SolarWinds' high-profile clients became vulnerable to hackers, including Fortune 500 companies, Microsoft, Intel, Cisco, the State Department, the Treasury, and the Pentagon. Cyberattacks are entering a new era of lethal impact when state-sponsored threat actors can hack into the software supply chain of a company such as SolarWinds and infect binary code to mimic legitimate protocol traffic and avoid detection.

Nation-state threat actors often gather sensitive information and sabotage the target's assets on behalf of the government. These groups are usually highly funded, well organized, and backed with plenty of resources. Common techniques used by these groups include spear phishing password attacks, social engineering, data exfiltration, Remote Access Trojan, and destructive malware.

3. Service-oriented threat actor groups continue to increase and their tactics are becoming more precise. One of the major changes is the nature of the attacks. They are becoming far more service-oriented ("phishing as a service"), allowing attackers who might not have the required technical abilities to still carry out attacks. While hackers might specialize in one skill, they're able to recruit partners to carry out more sophisticated attacks. This increased sophistication is making attacks more dangerous and tougher to combat. In 2022, the top anticipated targets of cyberattacks are mobile, the Internet of Things, and the cloud.

4. Data privacy laws have a major impact on security operations and cross-functional collaboration is required. New laws are being introduced or updated and enhanced in many parts of the world. While traditionally privacy compliance was strictly in the purview of the legal or privacy teams, stricter regulatory requirements now require a cross-functional approach. For security teams, this means collaborating with the privacy team to document and execute data management and data breach procedures, conduct security breach tabletops, etc. Note that sensitive information must also receive additional security measures. This includes data anonymization and data minimization/deletion.

5. Increase in supply-chain attacks requires stronger protective measures. One of the major cyber-related events in 2021 was the surge in supply-chain attacks. The threat groups became stealthier and better equipped in the wake of the pandemic. The very sophisticated nature of these supply-chain attacks impacted multiple industries. Major supply-chain attacks (such as those on JBS SA, SolarWinds, SITA, and Accellion FTA) disrupted the global supply chain by derailing international trade—thus further increasing the pandemic's impact on the economy. For example, the attack on JBS SA, the largest meat producer globally, resulted in the disruption of the meat trade worldwide and drastically impacted the retail industry. Similarly, the Accellion FTA supply-chain attack significantly affected many industries, such as Singtel, Bombardier, etc. And the SITA supply-chain attack affected air travel. On the other hand, the energy sector (being the most important to any nation) has been a constant attraction for threat groups. Furthermore, the ransomware attack on Colonial Pipeline, the Saudi Aramco data breach, and cyberattacks on Iranian gas stations have

acted as a catalyst to heat up geopolitical tensions. In addition to these, industries such as transportation, manufacturing, real estate, and mining were also impacted by cyberattacks in 2021. Taking all of this into consideration, multilateral cooperation is essential in order to counter the dynamic nature of these attacks. Strong legislation and training on industry-specific cybersecurity measures at respective industries should be adopted to counter these malicious activities.

6. Enhanced threat actor tactics, techniques, and procedures (TTPs). In the 21st century, we are observing significant technological advancements across all industries. Unfortunately, these advancements come with more loose ends to take care of and maintain—meaning that the threat landscape could expand even further without constant monitoring. In 2021 cloud misconfigurations were widely exploited. Several campaigns leveraged vulnerabilities that were discovered during supply-chain attacks. And, triple extortion techniques caused a significant impact due to the threat actors targeting victims, clients, and customers.

7. Vulnerability management programs have become an integral part of IT risk management. Some of the major operating system vendors were affected by a high volume of critical vulnerability disclosures during the last quarter of 2021. Microsoft products endured numerous vulnerability disclosures, including Microsoft Azure flaws and ongoing threats around a remote code execution (RCE) bug, codenamed 'PrintNightmare.' Security researchers also disclosed a critical Apple zero-day zero-click iMessage exploit, named "FORCEDENTRY," which was exploited by the threat actors to install the Pegasus spyware. Furthermore, Apache Java package Log4j was found to be affected by critical vulnerabilities that are being abused by threat actors to compromise organizations worldwide.

8. Public-private partnerships are becoming strategic cybersecurity tools. Cybersecurity-related complaints have tripled during the pandemic. With the increase in threats, governments cannot address all the threats themselves. Instead, they are collaborating with private organizations to help them re-design their cybersecurity posture in order to resolve issues promptly and protect against attacks. In 2021 many governments invested in cyber strategies and collaborated with cybersecurity experts to develop solutions that decrease the chance of cyberattacks. These initiatives aim to increase cyber education across all sectors and improve security programs to ensure better preparedness and response to attacks.

9. Regional and international collaboration increasing to indict cybercriminals. Threat actors such as Winnti group, FIN11, Energetic Bear, and Meteor initially target one certain region, eventually expand their target scope across multiple regions, and then spread across the globe, causing a wide impact. As threat actor groups become more global in nature, enforcement agencies and other private organizations believe they could become more efficient in preventing these attacks through international collaboration. For example, Canada's Ontario Provincial Police (OPP)—in collaboration with the Federal Bureau of Investigation (FBI), the Royal Canadian Mounted Police, and Europol— conducted investigations into numerous ransomware attacks that affected businesses, government agencies, and private individuals throughout Canada.

Intelligence sharing is also set to increase among the Five Eyes group. This elite group of five Anglophonic nations (the United States, the United Kingdom, Australia, New Zealand, and Canada) is focused on intelligence-sharing and cooperation. The changing geopolitical landscape and the impact of the Russian Chinese alliance will leverage a significant threat for this group in the future. Hence, a bill has been proposed in the US Congress to expand the group to nine members. India, Japan, and South Korea are the obvious choices for monitoring Chinese activities, due to their locational advantage. The expansion and alliance will enable the US to enlarge its espionage networks. The coalition will also profoundly benefit organization by strengthening the cyber centers through cooperation and improving the cybersecurity of the supply chains of critical infrastructures. Linguistic diversification, the preparation of the new blueprint of intelligence-sharing, and technology transfer will be major challenges in this expansion.

10. Digital payments landscape. The use of digital payment methods is on the rise as individuals explore convenient ways via the internet to transfer money or process payments in a timely fashion. In addition, banks and other financial institutions are coming up with innovative schemes such as "buy now, pay later," which could also potentially impact the increase in the digital payment landscape. However, even though digital payments offer convenience to the consumer, they pose a higher risk if not secured in the right way. Given the benefits that the digital payment method provides, the usage and advancements could continue, which can help consumers with a fast payment process. We have provided more details on digital payment methods in Section B5 – Preparing for 2022.

Global Constellation Briefing

B1 – Regional/Continental Landscape

As the world continues to be distracted with managing the COVID-19 pandemic, cybercriminals are taking full advantage. Countries worldwide are shifting towards a new normal by enabling swift digitization and managing a remote and virtual workforce. Yet, the rise in cybercrimes is creating an ongoing risk. **In 2021, the North American continent topped the list of most impacted regions by experiencing more than one-third (33.5%) of the total cyber issues reported all over the world.** It is followed by Asia-Pacific (23.5%) and Europe (20%). The United States was affected most by cyberattacks, with a share of 35.14% of the total events. Threat groups such as REvil, Conti, LockBit, Avaddon, Cozy Bear, ShinyHunters, Sprite Spider, Evil Eye, Naikon, Lazarus, etc., were the most active ones in 2021. In addition, the growing motivation for financial gain resulted in a rapid surge of ransomware attacks all over the world. Around 19.3% of the total cyberattacks in 2021 were basically ransomware attacks. The threat actors leveraged popular methods such as malware deployment, spear phishing, social engineering, and distributed denial of service (DDoS) attacks to carry out their malicious activities.

Most Impactful Cyber Events in 2021

Europe
1. SolarWinds Orion supply chain attack
2. Kaseya supply chain (REvil)
3. Accellion FTA supply chain attack
4. Airlines impacted by SITA attack
5. FortiGate VPN (Cring)

Middle East and Africa
1. Israel's Black Shadow breach
2. Supply chain attacks on Israeli firms
3. Vortex Security Team, Unidentied Team
4. Iranian wiper attacks
5. Saudi Aramco data breach

North America
1. Colonial Pipeline attack
2. SolarWinds Orion supply chain attack
3. Accellion FTA supply chain attack
4. Kaseya supply chain (REvil)
5. Sol Oriens ransomware attack (REvil)

Asia
1. Singtel impacted by Accellion attack
2. Air India data breach via SITA attack
3. India power sector targeted by RedEcho
4. Kaseya (REvil)
5. Kimsuky conducts cyber espionage

Latin America
1. Microsoft Exchange servers
2. Porto Seguro S.A.
3. Argentinian government database on Dark Web
4. Eletrobas, Copel ransomware attacks
5. Banking trojan Bizarro expands

Australia and Oceania
1. Kaseya supply chain (REvil)
2. SITA supply chain attack (APT41)
3. Lockbit 2.0 attack on Australian orgs.
4. Reserve Bank of New Zealand compromise via Accellion
5. DDos attacks on New Zealand banks and others

Top Countries Impacted

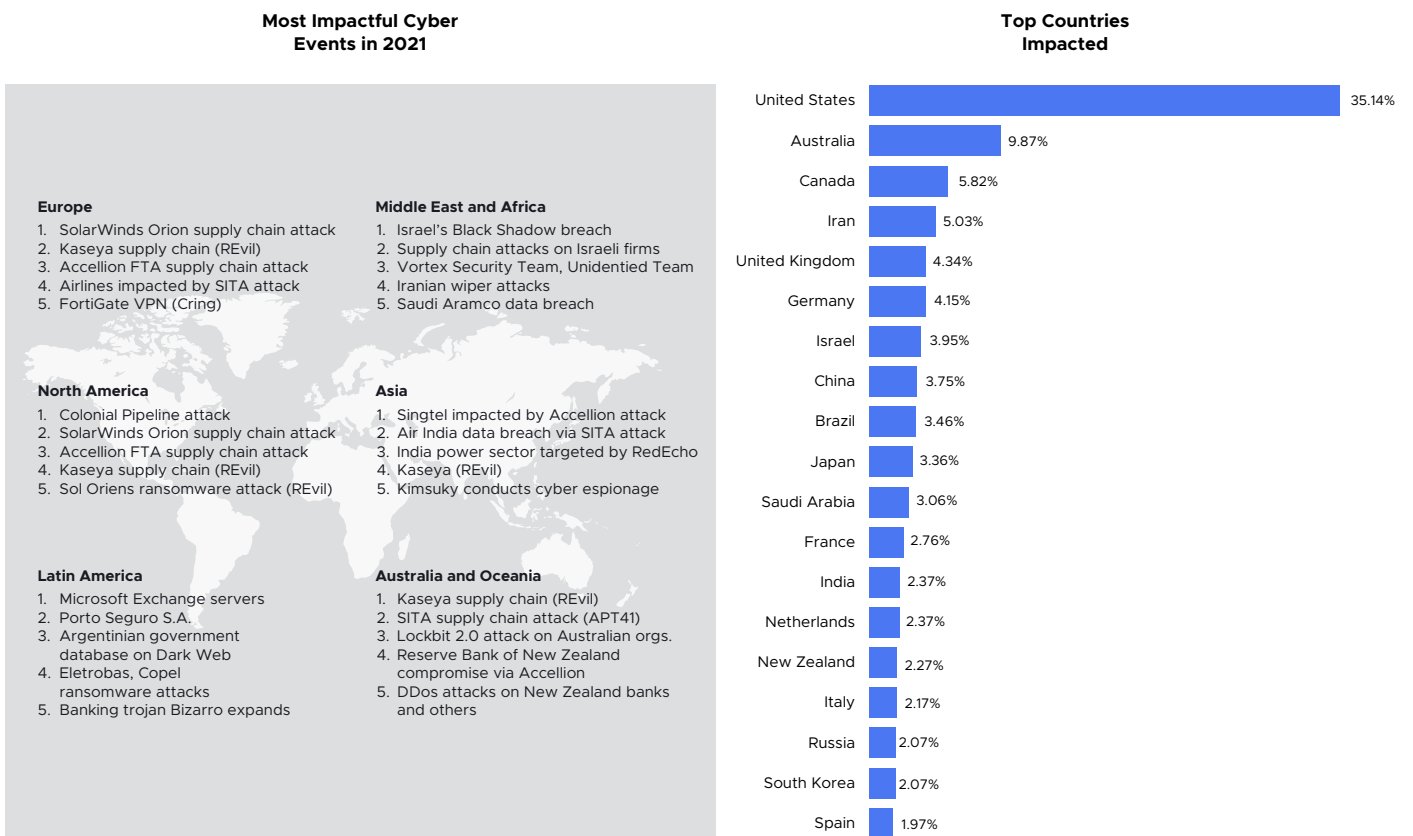| Country	Percentage
United States	35.14%
Australia	9.87%
Canada	5.82%
Iran	5.03%
United Kingdom	4.34%
Germany	4.15%
Israel	3.95%
China	3.75%
Brazil	3.46%
Japan	3.36%
Saudi Arabia	3.06%
France	2.76%
India	2.37%
Netherlands	2.37%
New Zealand	2.27%
Italy	2.17%
Russia	2.07%
South Korea	2.07%
Spain	1.97%

Figure 1 - Top cybersecurity events by region and top countries impacted by cybersecurity events in 2021

The changing global geopolitical landscape and regional disparities have given rise to numerous nation-state attacks across the globe. For example, in the Middle East region, the growing tensions between Iran and Israel have been marked by numerous advanced persistent threat (APT) activities conducted by threat groups such as APT34, APT35, Shamoon, Tracer Kitten, Spectral Kitten, etc. Although these groups have primarily targeted adversary governments and militaries, recently they have shifted their focus towards civilian targets as well. Similarly, the ideological difference between China and the QUAD countries; the mega military technology transfer deal (AUKUS Deal) between Australia, the USA, and the UK; and the South-China Sea conflicts have accelerated the cyberattacks conducted by the APT groups such as Naikon, APT141 (Earth Baku), Microceen, APT10, Lazarus, etc. The primary goals of these APT groups include attacks on national critical infrastructures and running cyber-espionage campaigns against adversary countries. Others, such as the European continent and the United States, have been significantly targeted by nation-state actors suspected of originating from countries such as Russia and China.

The year 2021 was marked by severe and sophisticated cyberattacks, including SolarWinds, Colonial Pipeline, JBS SA, and Accellion FTA—all having significant socio-economic and political impacts worldwide. These incidents show how unpredictable and unprecedented cyberthreats are today. In addition, threat groups are adopting state-of-the-art technologies and some are even shifting their primary focus (e.g., APT27 shifts from its regular cyber-espionage campaigns to ransomware attacks). Organizations need to prepare themselves by implementing multi-layer security measures. The ASEAN countries have set a very good example of how to cooperate in order to tackle cyberthreats. The rest of the international community must work together in technology transfer and intelligence sharing through multilateral collaboration to mitigate the risks posed by cyberattacks.

B2 – Global Sector/Industry Threat Landscape

Each industry faces its own unique attack landscape when it comes to digital risk and facing potential cyberthreats. Different motivations, triggers, geopolitical landscapes, and resources drive the threat actors to target the industries differently. In 2021, cyberthreats highly impacted the public sector, services, finance, retail, healthcare, energy, and transportation industries. With more than one-third (33.7%) of the total attacks, the services sector topped the list, followed by the public sector (21.4%).

The changing global geopolitical landscape, influenced in part by the global pandemic, has brought the public sector under serious threat of cyberattacks

The dynamic behavior of the APT groups all over the world has resulted in significant targeting of adversary governments. The confidential information possessed by the public sector has triggered a surge of cyber-espionage campaigns related to this. Because most governments fail to appropriate sufficient funds to fortify the cyber-infrastructure of their public sector, this gives cybercriminals a tremendous opportunity to exploit the loopholes with ease. Similarly, the defense sectors have been a constant target for APT groups such as APT34, Naikon, Lazarus, etc.

The following graph depicts a global perspective (considering all regions) of how diverse industry sectors were affected by cyber activity during 2021.

Top Sectors Impacted per Continent in 2021

North America
1. Manufacturing
2. Retail
3. Healthcare

Europe
1. Retail
2. Healthcare
3. Finance

Asia
1. Services
2. Finance
3. Retail

Latin America
1. Retail
2. Defense
3. Services

Middle East and Africa
1. Services
2. Defense
3. Energy

Australia and Oceania
1. Finance
2. Manufacturing
3. Defense

Top Industries Impacted Globally in 2021

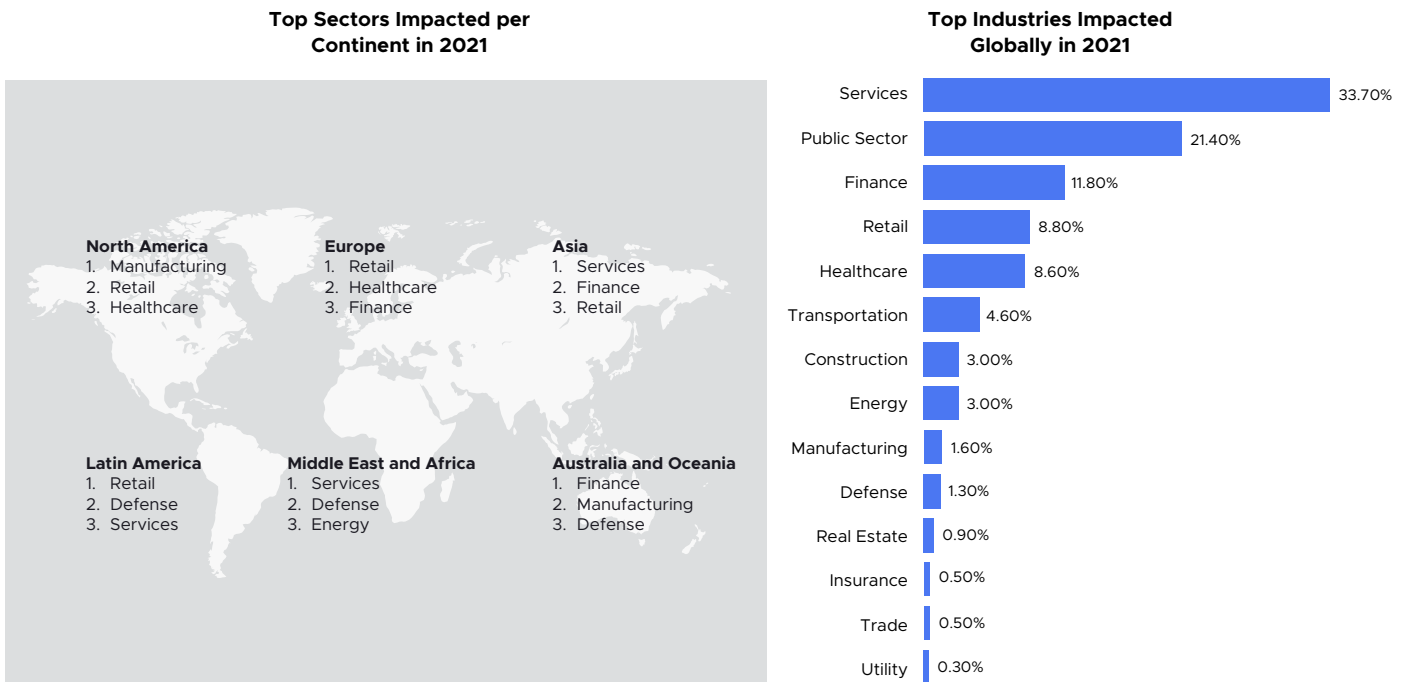| Industry	Percentage
Services	33.70%
Public Sector	21.40%
Finance	11.80%
Retail	8.80%
Healthcare	8.60%
Transportation	4.60%
Construction	3.00%
Energy	3.00%
Manufacturing	1.60%
Defense	1.30%
Real Estate	0.90%
Insurance	0.50%
Trade	0.50%
Utility	0.30%

Figure 2 - Top sectors impacted regionally and globally by cybersecurity events in 2021

The service sector experienced 33.7% of the total cyberattacks in 2021

The service sector is the most diverse and includes a wide range of critical infrastructures. Among all of the sub-industries within the service sector, the telecommunication and technology services experienced more than 62% of the total cyber incidents targeting the service sector. There was also a surge in ransomware attacks targeting the telecommunication sector, given key infrastructure vulnerabilities. For example, the Conti ransomware attack on the SAC Wireless and T-Mobile data breach significantly impacted millions of users. The fact that internet service providers and cloud service providers hold a massive amount of sensitive information is the main reason behind frequent cyberattacks on these companies. The media and entertainment services sector and the education sector have been actively targeted by nation-state actors, primarily for the purpose of cyber espionage. For example, in the Middle East region, APT groups allegedly originating from Iran have been reported for spying on journalists, students, and professors.

In addition, more than 11.8% of cyberattacks targeted the finance sector. The rise in financially motivated threat actors has had a direct impact on this sector, given the high value and sensitivity of the data that financial institutions store (such as credit card details, social security numbers, account credentials, etc.). The enlarging sphere of the digital payment landscape worldwide has invited multiple sophisticated cybercriminals to further exploit the finance sector.

Unfortunately, healthcare institutions are also facing a surge in cyberthreats, with 8.6% of the total cyberattacks in 2021 targeting this sector. US Medical Laboratory and Memorial Health Systems in the United States, Newfoundland and Labrador Healthcare and Humber River Hospital in Canada, Eastern Health in Australia, New Zealand's Waikato DHB, and more were highly impacted by cyberattacks in 2021.

And because the energy sector is one of the most important to any nation, it is a constant attraction for threat groups. The ransomware attack on Colonial Pipeline, the Saudi Aramco data breach, and cyberattacks on Iranian gas stations have acted as a catalyst to further heat up geopolitical tensions. In addition, industries such as transportation, manufacturing, real estate, and mining were also impacted by cyberattacks in 2021. Therefore, multilateral cooperation is essential in order to counter the dynamic nature of these attacks. Strong legislation and training on industry-specific cybersecurity measures at respective industries should be adopted to counter these malicious activities.

B3 – Global Cyberthreat Landscape

In the modern age of cybersecurity, the threat actors have become more drastic, meticulous, and focused with every passing year. Without profoundly monitoring their motivations, tactics, and tools, it is very difficult to create a reliable and robust defense mechanism. The year 2021 was marked by a rapid surge in activities of financially motivated threat actors such as Avaddon, REvil, Carbanak, the LockBit group, Babuk, FIN7, the Conti group, etc., leading to a huge number of ransomware attacks all over the world. On the other hand, the geopolitical conflicts have given rise to multiple cyberespionage campaigns conducted by various state-sponsored advanced persistent threat (APT) groups, including APT41, APT28, Sandworm team, UNC1151, etc. Additionally, threat actors such as Energetic Bear, Agrius, and Hades launch cyberattacks with the aim of sabotage and disruption. Hence, close observation of these threat actors is very important in order to secure the IT infrastructure of any organization. Also, the rapid utilization of different Ransomware-as-a-Service offerings (such as Conti, Blackenergy, PYSA, and the discovery of vulnerabilities such as LOG4J zero-day vulnerability) made 2021 very eventful. This section provides insights on major threats that targeted organizations globally in 2021, analyzed by Micro Focus. The collection includes threat actor groups, vulnerabilities, and ransomware.

Log4j: Apache Vulnerability Likely to Create Ongoing Global Exploits across Industries

Log4j background and patch updates

Critical vulnerabilities found in the widely used Java package Log4j have created a race among threat actors to exploit organizations worldwide. The package is used in numerous Apache frameworks, including Struts2, Druid, Flink, Spark, Tomcat, and Solr. All are used in numerous third-party applications. The initial exploit, which allowed threat actors to perform an unauthenticated remote code execution, is dubbed Log4Shell. It has a critical severity and is tracked as CVE-2021-44228. Although it was patched in version 2.15.0, the patch was deemed incomplete because it allowed threat actors to perform a local DoS attack (tracked as CVE-2021-45046). Consequently, another patch was released in version 2.16.0. Interestingly, a third vulnerability that allows data exfiltration has come to light, the specifics of which are not publicly disclosed. It is determined that the remote code execution in version 2.15.0 is possible.

On December 17, 2021, the Apache Software Foundation released another patch in version 2.17.0. The latest patch addresses a DoS attack tracked as CVE-2021-45105. The vulnerability has a CVSS score of 7.5 and affects Log4j versions from 2.0-beta9 to 2.16.0.

A new remote code execution vulnerability, CVE-2021-44832, with a CVSS score of 6.6, was discovered in Log4j version 2.17.0 on December 29, 2021. A threat actor with edit permission for the configuration file could potentially craft a malicious configuration using a JDBC (Java Database Connectivity) Appender, due to insufficient controls present on JNDI (Java Naming and Directory Interface) access in Log4j. The vulnerability has been addressed in Log4j version 2.17.1.

On January 5, 2022, a newly identified APT group dubbed Aquatic Panda reportedly exploited the Log4Shell (CVE-2021-44228) vulnerability, leveraging a modified version of the Log4j exploit tool to access a vulnerable instance of the VMware Horizon desktop and app virtualization product. The intrusion was identified when the threat group performed DNS lookup connectivity checks for a subdomain running under the Apache Tomcat service on the VMware Horizon instance. The APT group would then execute a series of malicious Linux commands to retrieve the threat actor group's payloads hosted on remote infrastructure.

On January 19, 2022, a new input validation vulnerability was disclosed that affected the SolarWinds Serv-U software versions 15.2.5 and earlier. The vulnerability is tracked as CVE-2021-35247 and has a CVSS score of 5.3. Successful exploitation of this vulnerability can allow the adversaries to build custom queries based on the provided inputs and then send them over the network without proper sanitization. Microsoft has addressed this issue with the release of Serv-U version 15.3.

The vulnerability stems from a Java API JNDI that allows Java software clients to discover and look up data or objects via a name. The objects could be stored in Directory Services, including:

- Lightweight Directory Access Protocol (LDAP)
- Remote Method Invocation (RMI)
- Common Object Request Broker Architecture (CORBA)
- Secure LDAP (LDAPS)
- Domain Name Service (DNS)

Log4j being exploited by botnets and adversaries leveraging the vulnerability to deploy ransomware

Prominent botnets such as Mirai, Muhstik, Tsunami, and Kinsing have begun exploitation attempts of the Log4j vulnerability. Threat actors are attempting to install cryptominers onto the target system, along with exfiltrating sensitive information such as AWS access keys. In addition, they have also deployed Cobalt Strike, which could be used to further compromise the victim network. Several nation-state threat actors such as Nemesis Kitten, Hafnium, and Phosphorus are attempting to leverage the vulnerability. Multiple access brokers have also started targeting the vulnerability for initial access.

After gaining the initial foothold, the access brokers can sell access to various ransomware affiliates, which could potentially increase the exploitation attempts significantly. Ransomware groups such as Khonsari, LockBit, and Conti have targeted organizations leveraging this vulnerability. Numerous software and services are potentially affected and at this time the exact impact of this global incident remains unclear.

A new attack vector that could affect internal systems (not exposed to the internet) running vulnerable versions of Log4j has been discovered, putting them at risk of getting targeted in exploitation attempts. This alternative attack vector leverages JavaScript WebSocket connections to trigger remote code execution. Threat actors are also leveraging the vulnerability in Log4j to deploy the Dridex banking Trojan in Windows devices. The Trojan has evolved to deliver further payloads, including ransomware. Threat actors have also targeted vulnerable Linux devices with Meterpreter.

The Belgian defense ministry is the first known high-profile government entity affected by the vulnerability. Portions of its network were reported to be facing disruption since December 16, 2021. After the exploitation attempts were discovered, the affected network portions were segmented.

Exploitation overview

■ A threat actor sends the malicious string to a target system that is running the vulnerable version of Log4j.

■ The target system logs the string containing the payload.

■ This payload triggers the vulnerability in Log4j2 and the target system sends a request to a domain controlled by the threat actor leveraging the JNDI interface (due to insufficient sanitization of user data).

■ The request, containing a path to a remote Java class file, is injected into the target system's process, triggering the second stage payload.

■ The second stage payload enables the threat actor to perform remote code execution on the target system.

BlackMatter

Industries Targeted	Continents Targeted
Agriculture, Forestry and Fishing, Manufacturing, Transportation, Energy, Finance, Public Sector, HealthCare, Services, and Retail	North America, Asia, Latin America, Europe

BlackMatter is also known as: Carbanak, GOLD NIAGARA, GOLD WATERFALL, FIN7, ITG14

On July 31, 2021, the ransomware threat actors allegedly returned and rebranded DarkSide as BlackMatter ransomware. BlackMatter offers Ransomware-as-a-Service to its affiliates. The encryption algorithm within the decryptor revealed the similarities between DarkSide and BlackMatter, indicating that the threat actors operating the ransomware are identical.

BlackMatter targets multiple device architectures, including Linux, Windows, and ESXi servers. Researchers claimed to have acquired a decryptor from BlackMatter and performed a detailed analysis. Researchers have concluded that BlackMatter adopted the same unique Salsa20 encryption algorithm used by DarkSide in their previous campaigns, including a customized Salsa20 matrix. Additionally, BlackMatter uses an RSA-1024 implementation unique to their encryptor, similar to DarkSide. BlackMatter's TOR leak site shares unique styles with DarkSide's previous leak site. The group stated that they predominantly target large corporations. However, government organizations, defense, non-profit, healthcare, and oil and gas are off limits. The threat actors believe these industries eventually brought forth the downfall of other notorious threat groups.

The BlackMatter group shut down its activities in November 2021. However, given its operating pattern, the group might reappear by rebranding and improving their capabilities and eventually increasing the attack surface.

Pay2Key

Industries Targeted	Continents Targeted
Transportation, Manufacturing, Services, Defense, Finance, Public Sector, Healthcare, Insurance, Retail	North America, Middle East, Africa

Pay2Key is also known as: PARISITE, UNC757, Fox Kitten, Yellow Dev 15

Pay2Key is an Iranian ransomware campaign that began in October 2020. By the end of 2020, the campaign claimed over eight victims. The threat actors operating Pay2Key appear to utilize publicly exposed Remote Desktop Protocol (RDP) as the initial point of compromise inside the victim's network. Pay2Key differs from other common ransomware malware in its operational efficiency and minimal exposure inside the victims' networks. Upon successful infiltration, the malware is allegedly capable of rapid lateral movement inside the targeted network. To reduce the risk of exposure, threat actors identify a pivot device inside the victim's network responsible for communication with Pay2Key's Command and Control (C2) server. Doing so restricts communication with malicious servers to a single node inside the organization's network. Pay2Key utilizes Microsoft's PsExec portable tool to remotely execute ransomware payload files named Cobalt.Client.exe on the targeted devices. Pay2Key leaves the target victim's encrypted networks with a ransom note file named after the organization (i.e., "[ORGANIZATION]_MESSAGE.TXT"). Reports indicate that the ransoms vary from 4 to 9 bitcoins (approximately $62,000 to $140,000).

LockBit

Industries Targeted	Continents Targeted
Agriculture, Forestry and Fishing, Manufacturing, Transportation, Manufacturing, Finance, Energy, Entertainment, Finance, Public Sector, Healthcare, Insurance, Legal, Services, Retail	North America, Asia, Latin America, Europe, Middle East, Africa

LockBit is also known as: LockBitSupp, StealBit

LockBit was first observed during September 2019 and the threat actor group started advertising its Ransomware-as-a- Service program in January 2020. After significant developments with encryption methods and other noticeable improvements (such as a built-in information-stealing function called 'StealBit' and a feature that automatically encrypts devices across Windows domains by leveraging Active Directory group policies), it was introduced as LockBit 2.0 in June 2021. In the initial days, it had heavy ties with Maze and created its own leak site. In the coming days, the threat actor group might continue to target finance and manufacturing industries, as seen in the incident trends observed for 2020 and 2021 in the Middle East and

Africa region. There might also be a possible shift of attacks towards organizations related to Information Technology because of the upward graph in technical advancements.

In most of the ransomware attacks conducted by LockBit, double extortion techniques have been widely used, which refers to exfiltrating data before initiating the encryption process. This allows the attackers to have additional leverage to receive the ransom by threatening to publish the stolen information through data-leak sites. LockBit was the first group to join Maze ransomware's leak site (now deactivated) to benefit from its established platform for double extortion from its targets.

The threat actor group might actively scan for vulnerabilities in firewalls, servers, and other network devices manufactured by well-known network device suppliers. For example, in some of the most significant attacks observed, threat actors exploited a vulnerability in FortiOS SSL Virtual Private Network (VPN) tracked as CVE-2018-13379. On a technical note, the threat actor group might still continue using the multithreaded encryption approach and only encrypt 4KB of data per file. In addition, monitoring is required to detect the abuse of legitimate tools such as process hacker and PC hunter, which are used to terminate processes and services on the victim's system. Also, monitoring of activities in domain controllers will be key, since the ransomware creates new group policies and transfers them to other end nodes in the network. These policies will disable Windows Defender and distribute and execute the ransomware binary to each Windows machine.

PYSA

Industries Targeted	Continents Targeted
Agriculture, Forestry and Fishing, Manufacturing, Transportation, Manufacturing, Finance, Energy, Entertainment, Finance, Public Sector, Healthcare, Insurance, Legal, Services, Retail	North America, Asia, Latin America, Europe, Middle East, Africa

PYSA is also known as: LockBitSupp, StealBit

PYSA ransomware is a variant of Mespinoza observed in 2019. PYSA operates as a Ransomware-as-a-Service model, where it allows the affiliates to modify the code and tools according to their required needs. In this region, the threat actor group might continue to target private organizations in the healthcare and educational industries; similar trends have been observed in recent years. Organizations should be aware that the threat actor group uses brute-force, phishing, and unauthorized RDP as their initial infection vectors. Once the victim's network is compromised, the threat actors use the advanced port and IP scanners and move laterally using PsExec. From past events, it is observed that the ransomware is manually executed and the data is encrypted using AES implemented with RSA-encrypted keys. In addition to healthcare and educational industries, organizations belonging to manufacturing, retail, transportation, and logistics might also be at risk.

Babuk

Industries Targeted	Continents Targeted
Services, Transportation, Retail, Construction, Defense, Manufacturing, Healthcare, Markets, Insurance, Public Sector, Energy, Utility	North America, Asia, Latin America, Europe

Babuk is also known as: DeathKitty, Wacatac, DeathRansom, HelloKitty, HellKitty, FiveHands

Babuk (also known as Babyk) ransomware commenced operating in 2021. The operators behind Babuk specifically target large organizations. Like other prominent ransomware groups, Babuk has adopted a double extortion strategy, threatening to encrypt, exfiltrate, and publish data to Dark Web leak sites.

Security researchers have observed that the code base of Babuk is similar to the Vasa Locker. The operators of this ransomware are active in both English-speaking and Russian-speaking forums. Furthermore, the ransomware does not check for the local language of the target system. Other ransomware groups often avoid systems located in Russia or other former Soviet states by checking the local language settings. As per the group's announcements in the underground forums, they have breached organizations in the transport, healthcare, manufacturing, technology, and agricultural sectors. The operators have initially announced that they will not attack hospitals, non-profit organizations, schools, or companies with less than a specific amount of revenue. However, they have explicitly stated that they will target organizations that support the LGBTQ or BlackLivesMatter causes. Babuk has also posted recruitment advertisements in the Dark Web forums seeking individuals having penetration testing knowledge.

The ransomware leverages ChaCha encryption, Elliptic-curve Diffie–Hellman (ECDH) key generation, and Exchange algorithm to safeguard its keys and employ strong encryption of compromised files. Additionally, Babuk supports command line operation and embeds several built-in functions to spread itself and compromise other systems. Babuk also has the flexibility to encrypt the mounted folders before or after the local disks. The ransomware further has the ability to kill different Windows services and processes that might keep the target files open and thwart the encryption process. The malware also attempts to destroy the shadow volumes by using the native command "vssadmin.exe." Babuk performs this operation twice: initially at the time of execution, as well as post-file encryption.

Babuk ransomware activity was detected in mid-October 2021. The initial infection vector is via exploiting ProxyShell vulnerabilities in the Microsoft Exchange server with the help of the China Chopper web shell. Going forward, we might see the threat actors targeting more Windows devices, considering the number of unpatched Windows assets in the wild.

DarkSide and BlackMatter

Industries Targeted	Continents Targeted
Services, Transportation, Agriculture Forestry and Fishing, Manufacturing, Transportation, Trade, Energy, Finance, Public Sector, Healthcare, Energy, Real Estate, Retail	North America, Asia, Latin America, Europe, Middle East, Oceania

DarkSide is also known as: Carbanak, GOLD NIAGARA, GOLD WATERFALL, FIN7, ITG14

The Colonial Pipeline attack was one of the major attacks of 2021. On May 8, 2021, Colonial Pipeline released a statement announcing that it had been the victim of a ransomware incident and had shut down parts of its pipeline operations in response and to contain the threat. Colonial Pipeline operates infrastructure that delivers diesel fuel, natural gas, and gasoline over a path stretching approximately 5,500 miles between New Jersey and Texas. The DarkSide ransomware adopted the Ransomware-as-a-Service operation model. The threat actor is known for professional operations and significant ransom requests. Based on reports, the threat actor has also developed intricate data leak storage systems with redundancy. Furthermore, DarkSide ransomware operators are known to perform financial analysis on prospective target organizations. Based on the gathered evidence, it is suggested that the threat actors initially compromised the internal network of Colonial Pipeline on April 29, 2021. The compromised VPN account that was used on the attack connection did not use multi-factor authentication (MFA). Therefore, a set of valid credentials were enough for the threat actors to proceed. Within the next eight days from the intrusion, the threat actors allegedly exfiltrated about 100 GB of data from Colonial Pipeline systems and moved laterally within the internal network. Later, the DarkSide threat actor group shut down its operations after pressure from United States law enforcement.

On July 31, 2021, DarkSide threat actors allegedly returned and rebranded DarkSide as BlackMatter ransomware. BlackMatter offers Ransomware-as-a-Service to its affiliates. Researchers have concluded that BlackMatter adopted the same unique Salsa20 encryption algorithm used by DarkSide in their previous campaigns, including a customized Salsa20 matrix. Additionally, BlackMatter uses an RSA-1024 implementation unique to their encryptor, similar to DarkSide. Furthermore, BlackMatter's TOR leak site shares unique styles with DarkSide's previous leak site.

However, the BlackMatter group shut down its activities in November 2021 after performing attacks on several industries. Reports indicate that the threat actors have allegedly shifted their victims to LockBit. Following the trend and seeing the group's activities and targets from the recent past, the group might reappear by rebranding and improving their capabilities and eventually increasing the attack surface.

Avaddon

Industries Targeted	Continents Targeted
Services, Agriculture Forestry and Fishing, Manufacturing, Transportation, Trade, Energy, Finance, Public Sector, Healthcare, Real Estate, Retail	North America, Asia, Latin America, Europe, Middle East, Oceania

Avaddon is also known as: Riddle Spider

When a cyber incident occurs, lessons learned play a significant role in building better security systems, applying security controls, and developing an overall security posture. Avaddon is one of the most prolific ransomware groups, having targeted numerous organizations. Since its shutdown in June 2021, the group has released decryption keys for almost 88 individual organizations. However, these organizations never revealed information about the attacks in the past. From this, it is understood that many of the targeted organizations are not disclosing information about the attack.

Often, after shutting down operations, ransomware groups reappear by rebranding with another name to circumvent law enforcement. As per the analysis, Avaddon can appear after rebranding and continuing its activities and mainly targeting information technology, transport, and healthcare industries. . On a technical note, after reappearing, the threat actors might continue to use credential brute-forcing for initial access and the famous old EternalBlue exploitation to access the target networks and crawl across to locate critical systems.

Conti

Industries Targeted	Continents Targeted
Services, Transportation, Agriculture Forestry and Fishing, Manufacturing, Trade, Finance, Defense, Energy, Mining, Public Sector, Healthcare, Real Estate, Retail, Utility	North America, Asia, Latin America, Europe, Middle East, Oceania

Conti is also known as: Wizard Spider, Grim Spider, TEMP.MixMaster, Gold Blackburn, and Gold Ulrick

On January 21, 2022, Delta Electronics, a Taiwanese electronics manufacturing company, was attacked by the notorious Conti group. The threat actor claimed that it successfully encrypted 1,500 servers and 12,000 computers out of approximately 65,000 devices on Delta Electronics' network. The Conti group reportedly demanded a ransom of $15 million in exchange for the decryptor. The attackers also threatened to release the stolen files if their demands were not met. Interestingly, the perpetrators behind this attack offered to provide a discount if the organization decided to pay the ransom quickly.

On January 20, 2022, Bank Indonesia (BI), the central bank of the Republic of Indonesia, confirmed a ransomware attack on its network. The attack was reportedly carried out by the Conti group in December 2021. The victim organization has acknowledged that the attackers infected over a dozen systems on BI's network. Before initiating the encryption routine, the threat actors also managed to pilfer "non-critical data" belonging to the bank's employees. The Conti ransomware gang has claimed to possess 13.88 GB of data and has threatened to leak it if BI refuses comply with the demands.

In 2021, Conti ransomware was used by many affiliates to conduct attacks on multiple organizations: Sandhills Global, SAC Wireless, Taylor Made Diagnostics, United Parcel Service (UPS), and Norfolk Southern Railway. In North America, 290 organizations were targeted, out of which 16 were healthcare facilities and first responder networks. Conti ransomware is believed to be controlled by a Russian-based cybercrime group known as Wizard Spider. This group might still target critical industries in 2022, with the focus being healthcare systems.

Threat actors might continue to deploy malware such as TrickBot and BazarBackdoor to establish communication with the threat actor, which can later help deploy Conti ransomware. Organization leaders and technical experts should be aware that the threat actors will continue to leverage Server Block Message (SMB) network shares and can also target Remote Desktop Protocol (RDP). Results from the analysis say that the threat actors would leverage existing tools in the system before downloading additional tools such as Mimikatz and Windows Sysinternals, enabling the group to move laterally through the network. It is highly recommended to review RDP and SMB ports, maintain strong password policies, and enable multi-factor authentication whenever it is available.

APT41

Industries Targeted	Continents Targeted
Services, Transportation, Healthcare, Public Sector	North America, Asia, Europe, Australia

The Chinese-speaking APT41 group (aka Barium, Winnti, Wicked Panda, Wicked Spider) has allegedly been involved in multiple sophisticated state-sponsored cybercrimes across the world targeting multiple industries such as services, transportation, healthcare, and the public sector. It is considered to be one of the most prolific nation-state groups that have leveraged a number of custom malware, including a Trojan called Winnti. APT41 is best known for its well-planned supply-chain attacks, with the motive of obtaining access to victims' systems and injecting malicious scripts to perform its cyber-espionage campaigns. From an end user's perspective, these kinds of stealthy attacks are highly difficult to detect. In addition to espionage, the APT41 group is highly motivated by personal financial gain as well.

In 2021, APT41 was actively involved in a three-month cyberattack targeting Air India, beginning in February 2021. A device of the Air India network was connected to the C2 server by deploying Cobalt Strike payloads as a means of initial access. They then exfiltrated sensitive information from Air India's internal servers, compromising more than 20 devices by gaining access to the credentials and moving laterally. In another incident in June 2021, the group targeted at least four state governments of the United States by using three C2 servers, deploying malware, and injecting SQL scripts. This group has already been tagged with the exploitation of several high-sensitive vulnerabilities in Cisco routers, Citrix infrastructure devices, and Zoho

ManageEngine Desktop Central. However, APT41 operators are still using tried-and-tested social engineering and malware deployment tactics to run their spying campaigns. Hence, timely checking of security logs and identification of strange and suspicious domains in network traffic can be a means of curtailing the threats.

DoppelPaymer

Industries Targeted	Continents Targeted
Services, Retail, Manufacturing, Construction, Defense, Finance, Public Sector, Healthcare, Markets, Insurance, Public Sector, Energy, Real Estate, Utility	North America, Asia, Latin America, Europe, Middle East, Oceania

DoppelPaymer is also known as: Doppel Spider, Gold Heron, and Grief

In 2021, DoppelPaymer's activity decreased significantly. The DoppelPaymer leak site remains online, but there has been no activity since May 2021, allegedly because it has rebranded to Grief. According to researchers, although the Grief ransomware code looks cosmetically different, it still leverages the same script with minor code changes. It contains a link that directs the victims to the DoppelPaymer ransom portal, which suggests that the malware developer might still have been developing the Grief ransom portal. So far, the Grief threat actor group is maintaining a low profile. Unlike DoppelPaymer, Grief has switched ransom payment methods to Monero (XMR) instead of Bitcoin (BTC). Grief ransomware has been very active since June 2021 and has recently claimed 41 victims from around the world. This group is still an ongoing threat to this region and organizations belonging to the government, healthcare, technology, and manufacturing sectors continue to be at risk.

REvil

Industries Targeted	Continents Targeted
Services, Retail, Manufacturing, Construction, Defense, Finance, Public Sector, HealthCare, Markets, Insurance, Public Sector, Energy, Real Estate, Utility	North America, Asia, Latin America, Europe, Middle East, Oceania

REvil is also known as: Pinchy Spider, Gold Southfield, Gold Garden, and GandCrab

During 2020 and 2021, REvil (also known as Sodinokibi and Sodin) caused significant disruption and was responsible for many cyberattacks. This included web hosting provider Managed.com, the world's leading beef and poultry producer; JBS Foods; and Sol Oriens, a small US nuclear weapons contractor.

REvil is a Ransomware-as-a-Service operation known for compromising corporate networks. The typical attack vector chosen by the REvil group is either the exploitation of vulnerable network devices or brute-force attacks on Remote Desktop Protocol (RDP) servers, in addition to infection vectors such as phishing and exploit kits. After gaining a foothold on the target's network, the REvil operators attempt to move laterally in the breached network. Threat actors focus on stealing data from servers and workstations and encrypting files on the compromised assets. The main objective is to escalate privilege to the administrator level on domain controllers.

REvil primarily targeted legal, manufacturing, food and beverage, financial services, and healthcare industries. Although the REvil infrastructure was taken down in July 2021, their affiliates might still have contacts with the developer. In addition, there is a high probability that the group might reappear after rebranding and upskilling with more advanced methods and techniques.

B4 – Global Techniques Threat Landscape

Over the years, cybercrime gangs have become more advanced by adopting sophisticated tactics, techniques, and procedures and developing new malicious tools that enable them to enhance the effectiveness of their attacks. Instead of analyzing the final impact of a cyberattack and focusing on the known indicators of compromise (IoCs) associated with the incident, cybersecurity experts prefer to track the indicators of attack (IoAs), tactics, and techniques that potentially indicate an attack in progress. While the tactics represent the objectives of an attack, the techniques demonstrate how threat actors are achieving their tactical objectives.

An in-depth understanding of the common TTPs used by the threat actors in their crusades can enable organizations to develop specific threat models and accordingly deploy a robust and reliable cybersecurity mechanism. This section describes the key techniques from the MITRE ATT&CK framework that were used by active major threat actors in 2021. The MITRE ATT&CK framework is a knowledge database for understanding cyber adversary behavior shown in various phases of an attack lifecycle.

Initial Access

Initial Access includes a series of techniques that adversaries use to gain initial access to a victim's network. The most used and common techniques are phishing and exploiting valid accounts by using compromised credentials. Adversaries lure the victims with spear-phishing attachments and links, which eventually redirect them to download malicious code. This technique is primarily used to target a specific person, group, or company. Compromising credentials is an initial step to exploiting a user account, evading access controls, and reaching certain restricted areas within a network to compromise data and systems.

Adversaries can compromise service accounts related to certain applications, domain accounts, cloud accounts, and local user accounts using the compromised credentials. Enabling MFA, having a robust organization-wide password policy, and frequently auditing the password policy can help prevent exploits by the adversaries. Another often-used initial access vector is the supply chain compromise, in which the adversaries alter the software or the applications before being made available to the public. With this, the adversary will have control of the application on the end-user device and can perform needed actions such as data compromises and password harvesting.

Technique ID	Technique Name	Frequency (technique usage)
T1566.001	Spearphishing Attachment	High
T1566.002	Spearphishing Link	High
T1078.002	Domain Accounts	High
T1195.002	Compromise Software Supply Chain	Medium
T1566.003	Spearphishing Via Service	Low

Execution

The execution tactic consists of techniques that are used after the malicious code is deployed on the victim's system or environment. Prominently used techniques are scheduled tasks, PowerShell execution, and Windows command shell execution. Windows task scheduler is frequently used to schedule the execution of malicious code. Windows task scheduler can be initiated from both the command line and GUI. The PowerShell command-line interface is also often abused for gathering information and executing malicious code. Other techniques include VBScript execution and Python execution.

Technique ID	Technique Name	Frequency (technique usage)
T1053.005	Schtasks Execution	High
T1059.001	PowerShell Execution	High
T1059.003	Windows Command Shell Execution	High
T1204.001	Malicious Link Execution	High
T1204.002	Malicious File Execution	High
T1059.005	VBScript Execution	Medium
T1059.006	Python Execution	Low

Persistence

Persistence is a critical tactic to be aware of because adversaries can be active inside the network without being traced. The tactic consists of techniques that help the adversary maintain a foothold on the victim's system. Frequently used techniques are registry run keys, Web Shell, and shortcut modification. Adversaries usually add a program to a startup folder. Upon the user logging into the system, the program starts running and gives the user permissions defined in the program.

WebShells are used to host scripts on a web server and enable functions that help the adversary use the web server as a medium or a gateway into the victim's network. Other techniques include Bootkit, component firmware, SQL stored procedures, and DLL Side-Loading.

Technique ID	Technique Name	Frequency (technique usage)
T1547.001	Registry Run Keys/Startup Folder	High
T1505.003	Web Shell	Medium
T1547.009	Shortcut Modification	Medium
T1542.003	Bootkit	Low
T1542.002	Component Firmware	Low
T1505.001	SQL Stored Procedures	Low
T1098.001	Additional Azure Service Principal Credentials	Low
T1546.003	Windows Management Instrumentation Event Subscription	Low
T1546.008	Accessibility Features	Low
T1574.002	DLL Side-Loading	Low
T1053.003	Cron Execution	Low
T1137.001	Office Template Macros	Low

Privilege Escalation

Adversaries often use privilege escalation to gain access to certain critical systems that have restricted access and cannot be reached using compromised accounts with low-level permissions. Commonly used techniques are dynamic-link library injection and elevated execution with prompt. Adversaries elevate privileges by injecting dynamic-link libraries (DLLs) into processes. They are also used to evade process-based defenses.

After gaining access to the victim's system, adversaries can use the AuthorizationExecuteWithPrivileges API to display an authentication dialog box on the user's screen (which can be initiated by a third-party installer and piggyback credentials entered in the dialogue box). Later, these privileged credentials exploit critical systems and applications on the victim's networks. Other privilege escalation techniques include component object model hijacking and cloud accounts.

Technique ID	Technique Name	Frequency (technique usage)
T1055.001	Dynamic-link Library Injection	Medium
T1548.004	Elevated Execution with Prompt	Low
T1037.001	Logon Script (Windows)	Low
T1546.015	Component Object Model Hijacking	Low
T1078.004	Cloud Accounts	Low

Defense Evasion

The Defense Evasion tactic consists of techniques used by the adversaries to evade the defenses that are configured in the victim's environment. For example, adversaries frequently use legitimate processes within an operating system to hide the presence of installed malware. Commonly used techniques include match legitimate name or location, file deletion, disable or modify tools, software packaging, masquerade tasks and services, and bypass user access control.

After performing an intrusion, adversaries make sure to delete all of the files that were used in the process, since external files could easily leave traces and can be detected by the security controls. Another prominent technique is impairing defenses where the adversaries disable anti-virus tools, modify firewall rules, disable windows and cloud logs, and abuse windows safe mode. Other techniques include passing the hash, creating a token process, impairing command history logging, and compiling after delivery.

Technique ID	Technique Name	Frequency (technique usage)
T1036.005	Match Legitimate Name or Location	High
T1070.004	File Deletion	High
T1562.001	Disable or Modify Tools	High
T1027.002	Software Packing	High
T1036.004	Masquerade Task or Service	Medium
T1548.002	Bypass User Access Control	Medium
T1564.005	Hidden File System	Low
T1134.001	Token Impersonation/Theft	Low
T1564.003	Hidden Window	Low

T1550.001	Application Access Token	Low
T1550.002	Pass The Hash	Low
T1027.001	Binary Padding	Low
T1550.003	Pass The Ticket	Low
T1550.004	Web Session Cookie	Low
T1134.002	Create Process With Token	Low
T1562.003	Impair Command History Logging	Low
T1027.004	Compile After Delivery	Low

Credential Access

Adversaries use certain techniques such as brute force and network sniffing to compromise accounts. The most commonly used techniques are brute force, keylogging, LSASS memory, kerberoasting, and searching for credentials stored in files on the local system. After obtaining password hashes, adversaries use brute force methods such as password spraying, password guessing, and credential stuffing to obtain the passwords. Other techniques include DCSync, private keys, and LSA secrets.

Technique ID	Technique Name	Frequency (technique usage)
T1110.003	Password Spraying	High
T1056.001	Keylogging	High
T1003.001	LSASS Memory	Medium
T1558.003	Kerberoasting	Medium
T1552.001	Credentials in Files	Medium
T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	Low
T1003.002	Security Account Manager	Low
T1110.001	Password Guessing	Low
T1003.006	DCSync	Low

| T1552.004 | Private Keys | Low |
| T1003.004 | LSA Secrets | Low |

Lateral Movement

During the lateral movement phase, the adversary explores the victim's network to find targets and obtain access to those targets. Adversaries can deploy remote access tools that help the lateral movement. Common techniques used by the adversaries are SMB/Windows Admin shares, remote desktop protocol, and Windows remote management. Service accounts are targeted quite often, enabling the adversary to control actions of that particular service. For example, compromising a service related to a remote connection could allow unauthorized external remote connections such as telnet, SSH, and VNC from the adversary's network.

Technique ID	Technique Name	Frequency (technique usage)
T1021.002	SMB/Windows Admin Shares	High
T1021.001	Remote Desktop Protocol	Medium
T1021.006	Windows Remote Management	Medium

Collection

During collection, the adversary gathers information from multiple assets. Usually, there are two objectives: one is to use that information and exploit more assets within the victim's environment and the other is to exfiltrate the collected sensitive information. Common techniques used during the collection stage are data staging, email collection, and collecting data from information repositories.

Technique ID	Technique Name	Frequency (technique usage)
T1560.001	Archive via Utility	High
T1074.002	Remote Data Staging	Medium
T1114.002	Remote Email Collection	Medium
T1213.002	Sharepoint	Low
T1560.002	Archive via Library	Low

Command and Control

The command and control tactic is used to establish communication between the victim and the adversary network remotely. Common techniques used are bidirectional communication, symmetric cryptography, external proxy, standard encoding, and multi-hop proxy.

Technique ID	Technique Name	Frequency (technique usage)
T1102.002	Bidirectional Communication	High
T1573.001	Symmetric Cryptography	High
T1090.002	External Proxy	High
T1132.001	Standard Encoding	High
T1090.003	Multi-hop Proxy	Medium
T1001.001	Junk Data	Low
T1001.002	Steganography	Low
T1090.001	Internal Proxy	Low
T1090.004	Domain Fronting	Low
T1568.001	Fast Flux DNS	Low
T1001.003	Protocol Impersonation	Low

Exfiltration

After collecting the sensitive information and establishing a connection with the adversary infrastructure, the next step is to exfiltrate the data. Adversaries often compress and encrypt the data to evade detection and enable easy transfers. The collected data is exfiltrated over command-and-control channels. The two main techniques used during exfiltration are Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol and Exfiltration Over Asymmetric Encrypted Non-C2 Protocol.

Technique ID	Technique Name	Frequency (technique usage)
T1048.003	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	High
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	High

Impact

During this phase, the victims could experience down time and access failures to certain systems, due to actions performed by the adversary. These actions could include data destruction, data manipulation, defacement of internal and external systems, disk wipes, firmware corruption, and system shutdown or reboot.

Technique ID	Technique Name	Frequency (technique usage)
T1491.002	External Defacement	High
T1565.001	Stored Data Manipulation	High
T1565.002	Transmitted Data Manipulation	High
T1565.003	Runtime Data Manipulation	High

B5 – Preparing for 2022

Legal, Regulatory, and International Standards Insights

Privacy and Data Protection

Data is at the core of what organizations do. What data do you have? Where is it? Who has access to it? Part of the cost of belonging to the data economy requires effective data protection and data privacy investments. Misuse of private information can be leveraged by malicious actors to extort a victim (for financial gain or other means), as well as to carry out diverse forms of fraud (financial, insurance, identity theft, etc.).

The risks of not properly safeguarding information are severe. Non-compliance can result in large fines under privacy and data protection laws, media scrutiny, and damage to reputation. The consequences often extend to individuals as well, with company executives sharing legal liability for breaches due to perceived negligence. Individuals whose personal information is comprised can also suffer many consequences and lose trust with the organization.

Various governments across the globe are advancing legislation to maintain and protect privacy, leaving companies to deal with cumbersome regulatory requirements. Highlighted below are several jurisdictions that have recently introduced or will soon pass important regulations. All organizations that operate or have ties with these regions will need to assess the impact to their operations.

Figure 3 - Jurisdictions that pose significant privacy and data protection requirements on organizations

North America

Canada's Privacy Reform

Canada's privacy and security regulatory environment is on the brink of a major reform. Bill C-11 proposed a new privacy law: the Consumer Privacy Protection Act (CPPA). Although the Fall 2021 elections erased it from the parliamentary table, the government has committed to reintroducing similar legislation in 2022. Once passed, organizations will face additional compliance requirements and fines that will be among the highest in the world.

Key impacts on business strategy	Key impacts on security operations
- **Cease operations:** Federal Privacy Commissioner can order a company to stop collecting or using personal data. - **Data mobility:** Provide individuals with the right to transfer their personal information to another organization. - **Algorithmic transparency:** New transparency requirements for automated decision-making systems such as algorithms and artificial intelligence. Organizations will also have to explain how a prediction, recommendation, or decision was made. - **Fines:** A maximum fine of 5% of global revenue or $25 million would be levied for serious contraventions.	- **Security safeguards:** The CPPA requires organizations to prove how personal information is protected through physical, organizational, and technological security safeguards. - **Audits:** The Privacy Commissioner's Office (OPC) may audit the personal information management practices of an organization (including its security controls). The OPC can enter an organization's premises to inspect its security requirements. - **Breach reporting:** While organizations are already subject to mandatory data breach reporting requirements under current legislation (including the requirement to keep a record of every breach), the CPPA will now subject organizations to its exorbitant fines—upwards of 5% of companies' global revenue. - **Contracts:** As a result of the additional accountability requirements and potential fines, vendor contracts (and other business data sharing agreements) need to be reviewed to ensure the protection of the information by security safeguards appropriate to the sensitivity of the information.

California Consumer Privacy Act (CCPA) | California Privacy Rights Act (CPRA)

The California Consumer Privacy Act (CCPA) brought a GDPR-like privacy law to the United States. Similar to the GDPR, the CCPA requires organizations to focus on personal information and provide transparency in how they're collecting, sharing, and using such information. The 5 key CCPA requirements noted below are addressed through seven domains. A more comprehensive version of the CCPA, the California Privacy Rights Act (CPRA), provides additional regulatory requirements for organizations to enhance the privacy and security rights of Californians.

Key impacts on business strategy	Key impacts on security operations
- **Data erasure from third parties:** Upon a valid request to delete personal information, a business must direct any service provider to delete the consumer's personal information. Companies have 45 days to respond to a request. - **Private right of action:** Companies could pay US$100-$750 per consumer per incident. - **Fines:** The fine for each violation can be from US$2,500 to $7,500. .	- **Privacy and security assessments:** To keep customer data safe, organizations are required to perform regular audits, assess systems used to manage data, and document a strategic approach to maximizing protection.

European Union (EU)'s General Data Protection Regulation (GDPR)

The GDPR (EU's privacy law introduced in 2018) has often been referred to as a "game changer," introducing significant changes to how organizations manage their privacy and security operations. Although the initial impact (financial, operational, etc.) mostly affected organizations dealing with personal data on European residents, it is now a reference for many countries creating or updating their own privacy laws and regulations. The monetary penalties are steep and many organizations have been fined for non-compliance. Among the highest to date are Amazon (€746), WhatsApp (€225), and Google (€50).

Key impacts on business strategy	Key impacts on security operations
Record keeping: Mandatory data inventorying and record keeping of all internal and third-party data processing of European personal information. **Data erasure:** Comprehensive individual rights to access, correct, port, erase, and object to the processing of their data. **Privacy impact assessments:** Routine data-protection impact assessments for technology and business changes. **Mandatory data protection officers (DPOs)** and an overall rethinking of privacy strategy, governance, and risk management. **Significant fines:** A maximum fine of 4% of global revenue or €20 million would be levied for serious contraventions.	**Mandatory data-breach notification** to regulators (within 72 hours) and to individuals whose information is compromised. **Enhanced security measures:** Requirement to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the digital risk."

Latin America

Brazil's Lei Geral de Proteção de Dados (LGPD)

Brazil is the first country in Latin America to introduce a comprehensive privacy law that applies to both private and public sector entities. Modelled based on the EU's GDPR, the Lei Geral de Proteção de Dados (LGPD) includes administrative sanctions. Both individuals and public prosecutors can bring claims for losses and damages and at least one public civil action has already been filed. LGPD applies when an organization conducts business or processes personal information (PI) in Brazil or processes PI that was collected in Brazil. Most organizations in Brazil are still in the process of aligning their operations with the legal requirements of the LGPD, with smaller organizations struggling the most to comply.

Key impacts on business strategy	Key impacts on security operations
Specific data processing: Data processing can only happen based on a limited list of approved categories. The most common category is gaining valid consent of the data subject. **Extraterritoriality:** The LGPD applies to any individual or legal entity, irrespective of the country in which its headquarters is located or the country in which the data is located. **Extensive data rights:** Must provide individuals with a series of rights, including (but not limited to) data portability, data access and erasure, and the right not to be subject to automated decision making. **Significant fines:** A maximum fine of 2% of sales revenue or 50 Brazilian Real would be levied for serious contraventions.	**Enhanced security measures:** Requirement to implement appropriate technical and organizational measures to ensure a level of security.

Asia Pacific

People's Republic of China's Personal Information Protection Law (PIPL)

China's new comprehensive data law is likely to affect many businesses around the world, not just those operating in China. They will be subject to further scrutiny once the regulations on network data security are introduced, expected in early 2022. These will be introduced by The Cyberspace Administration of China (CAC) to enhance PIPL. Multinationals doing business in China will face significant risks, as they will have to navigate one of the most stringent regulatory regimes.

Key impacts on business strategy	Key impacts on security operations
▪ **Cross-border data transfers:** Requirement to have any cross-border data transfers be submitted first to the Cyberspace Administration of China, which is the cyber and data protection regulator in China. ▪ **Facial recognition:** PIPL regulates the use of facial recognition. ▪ **Personalization:** Organizations using algorithms to personalize their customers' experience require user consent. ▪ **Fines:** Organizations may see fines up to USD$7.7 million or up to 5% of the previous year's business revenue.	▪ **Mandatory assessments:** Risk and impact assessments are required across a broad array of use cases. Companies that automate their data privacy and protection impact assessments for the Americas and EMEA now have a driver to extend this capability to the Asia-Pacific region. ▪ **Incident response:** Data processors must notify multiple business and government stakeholders, as well as affected individuals, about the incidents, risk of data breaches, and remedial actions they've taken within three working days. If the incident involves important data or personal data on more than 100,000 people, companies must report the breach to the appropriate regulators within eight hours. This timeline is among the most stringent globally and will require state-of-the-art detection, response, and resilience capabilities typically seen only in advanced financial and technology companies.

Singapore's Personal Data Protection Act (PDPA)

The Personal Data Protection Act (PDPA) provides a baseline privacy regime and is complementary to sector-specific legislative and regulatory frameworks. It applies to any organization that handles Singaporean personal information. Recent amendments, some of which are still to go into force, have added additional responsibilities and financial risks for organizations.

Key impacts on business strategy	Key impacts on security operations
▪ **Mandatory data breach notification:** Organizations that suffer a data breach are required to notify the privacy authority and affected individuals if it poses a significant harm or impacts more than 500 people. ▪ **Financial penalties:** As a result of recent reforms, organizations will be subject to 10% of annual turnover. ▪ **New individual rights:** Organizations will have to comply with new data portability obligations.	▪ **New criminal offenses:** Mishandling of personal information (knowingly or recklessly) can lead to fines of up to S$5,000 or prison time of up to 2 years. This includes new offenses for dictionary attacks and address-harvesting software. ▪ **Private right of action:** Any individual harmed because of an organization's violation of the PDPA can file a lawsuit for civil damages. A recent court case (Bellingham Alex v Reed Michael [2021] SGHC 125) reveals that what constitutes "harm" may be limited to financial and physical harm.

Middle East and Africa

South Africa's Protection of Personal Information Act (POPIA)

The Protection of Personal Information Act (POPIA) applies to both the public and private sector and provides a detailed framework legislation supporting South Africa's constitutional right to privacy.

Key impacts on business strategy	Key impacts on security operations
• **Offshoring data:** Specific requirements for cross-border data transfers. In response, some global organizations have created local data centers to avoid compliance challenges. • **Fines:** Fines start from ZAR1 -10 million and non-compliant individuals could face one to ten years in jail.	• **Security safeguards:** Must secure the integrity and confidentiality of any personal information in its possession or under its control by taking appropriate and reasonable technical and organizational measures to prevent loss, damage, unauthorized destruction of, and unlawful access to the personal information in its possession. • **Breach reporting:** Requirement to report, as soon as feasible, suspicions of unauthorized access to personal data to the Information Regulator and, in some cases, to the data subjects.

Australia and Oceania

Australia's Privacy Act and other key reforms

Organizations operating in Australia will soon be faced with additional privacy and data protection regulatory requirements. There are a few initiatives happening simultaneously, including an Online Privacy Code and privacy reform discussion paper that will influence the future of privacy in Australia. These are expected to impose significant compliance burdens on companies and public sector organizations. Key changes are highlighted below. Unlike other countries with a comprehensive privacy regulatory regime, such as Canada and the European Union, Australia's current Privacy Act does not apply to smaller organizations (annual turnover of less than A$3M), although this is expected to change in the upcoming reforms.

Key impacts on business strategy	Key impacts on security operations
• **Electronic surveillance law reforms:** A new single Act that better protects personal information and ensures that law enforcement agencies have the appropriate powers to investigate serious crimes and security threats. • **Online platforms:** Social media platforms will need to provide stronger protections for children by verifying their users' age. They must also consider the best interests of the child when handling children's personal information. Parental consent will be required for users under the age of 16. • **Enhanced penalties:** Serious or repeated non-compliance include fines of up to AU$10 million, or three times the value of the benefit obtained from the conduct, or 10% of the domestic annual turnover of the offending entity if the value cannot be determined. • **Increased enforcement powers:** the Australian Information Commissioner will have expanded powers and criminal penalties are to be introduced for reoccurring non-compliance.	• **Scope and application:** Organizations not currently subject to the Privacy Act should start preparing their privacy, security, and compliance teams in anticipation of future legal application.

International Cooperation and New Standards

Cybercrime pays no respect to international borders. Fighting against cyberthreats is a process that has always relied upon multilateral collaboration and information sharing. Some of the significant developments in international collaboration in recent times are listed below.

- The United States has joined the Paris Call for Trust and Security in Cyberspace—along with 80 other countries and hundreds of tech companies, nonprofits, and universities—to improve cybersecurity for citizens and businesses.
- Cybersecurity and digital privacy were designated the highest priority in the 2021 G7 Summit at Carbis Bay in Cornwall.
- In the 2021 Nordic Council Meeting, they agreed on a mutual defense strategy against cyberattacks in the region.
- The European Union, the United States, and Japan organized a week-long online cybersecurity training for Industrial Control Systems Cybersecurity in October 2021.
- The Geneva Summit held between President Biden and President Putin aimed towards diminishing nation-state activities motivated for political gain.
- The United States and Israel have announced the formation of a Joint Task Force on cybersecurity.
- ASEAN countries are leading the global pack in cybersecurity by adopting the ASEAN Regional Action Plan (2021-2025) and forming the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), in order to improve the cybersecurity strategy development, legislation, and research capabilities of the member states.
- India and New Zealand have agreed on close cooperation in cybersecurity and cybercrime.
- The AUKUS Deal signed between Australia, the US, and the UK focuses on cybersecurity, quantum technology, and information sharing.
- Singapore and Estonia have signed an MOU for start-up collaboration, sharing cybersecurity expertise.
- The US and Singapore have signed an agreement to bolster cybersecurity across government agencies.

Strategic Actions for Executives in 2022

1	MAKE CYBERSECURITY AND DATA PROTECTION A KEY PRIORITY WITH A HEALTHY BUDGET	As the frequency and consequences of cyberattacks continue to grow, organizations require more resources dedicated to prevention and response. Cybersecurity, data protection, and privacy teams must be treated as business imperatives and need to be given priority when it comes to resourcing, budgets, and strategic business decisions. While some executives might be inclined to give only the CISOs a seat at the executive table, it's critical to include the privacy and data protection leads as well.
2	ENHANCE BUSINESS AGILITY BY SHIFTING YOUR STRATEGY FROM RISK MANAGEMENT TO ENABLING TRUST	Organizations need to develop a multi-layered strategy to gain a better understanding of their risk profiles and risk appetite. They are advised to deploy agile risk management approaches to predict and counter the dynamic nature of the risk posed by cyberthreats in the changing world. This flexibility of response towards high-velocity risk is essential for handling sophisticated cyberattacks.
3	ESTABLISH AND 1AINTAIN TRUST WITH YOUR CUSTOMERS AND STAKEHOLDERS	In today's rapidly shifting digital landscape, transparent disclosure of information is vital to keeping trust in tact with customers and stakeholders. Emerging technologies can act as a medium to enhance the customer experience, build brand loyalty, and bolster cybersecurity.

4	UNDERSTAND AND ASSESS YOUR THIRD-PARTY PRIVACY AND SECURITY RISKS	Consider implementing formal enterprise-wide assessments for all third-party vendors to better understand and assess the potential risk of data breaches through third parties.
5	ESTABLISH STRATEGIC PUBLIC-PRIVATE PARTNERSHIPS	Companies and federal agencies have benefited from public-private partnership and government responses to recent significant cyber incidents. Timely sharing of information matters for cybersecurity in general. Share knowledge about new threats, approaches, and solutions.

Strategic Actions for Cybersecurity Teams in 2022

1	INVEST IN AND ENHANCE YOUR THREAT INTELLIGENCE PROGRAM AND DARK WEB MONITORING	Having a comprehensive threat intelligence strategy is an important ally in your agile security program. SOC analysts, fraud teams, incident response, and threat hunting and vulnerability management teams all stand to benefit from threat intelligence. They can all leverage it for a variety of use cases, including third-party monitoring and assessing compromised credentials, credit cards, and other personal information. Organizations should consider monitoring for exposure of sensitive details, including account login and credential information posted on paste sites, hacking forums, and Dark Web sites.
2	CREATE A STRONG EMPLOYEE SECURITY TRAINING PROGRAM	Consider investing in employee training on cybersecurity. Regular training sessions should be held to educate users about common issues and attacks. Trained employees are more cautious about unusual behaviors in their systems. If they notice such behaviors, all employees should be advised to raise their concern with the information security team.
3	IMPLEMENT PRIVACY AND DATA PROTECTION MEASURES TO ENSURE LEGAL COMPLIANCE AND MANAGE RISKS	Coordinate with your organization's privacy and data protection teams to identify and assess various risks, including legal and regulatory, financial, and reputational. This collaborative exercise will dictate the additional controls and mitigating measures to be implemented. These might include data inventories, data minimization measures, data classification schemes, privacy impact assessments, etc. Failure to consider and implement such measures could lead to legal and regulatory non-compliance, declining customer trust, and steep fines in many jurisdictions.
4	UPDATE YOUR INCIDENT RESPONSE PLAN AND TEST IT REGULARLY	A cybersecurity incident response (IR) plan is an important tool to help companies prepare for, detect, respond to, and recover from network security incidents. The plan should be tested regularly (at least once per year) and should involve all of the teams that would be involved in the event of a real incident.
5	ENSURE REGULAR BACKUPS OF CRITICAL DATA	Consider regular backups for any critical data or infrastructure. The backups should be tested on a regular basis. Networks should be properly segregated to limit the spread of ransomware.
6	CREATE AND ENFORCE STRONG PASSWORD POLICIES, INCLUDING MULTI-FACTOR AUTHENTICATION	A strong password policy must be enacted for all users, especially for user accounts with privileged access. This password policy must ensure that passwords are of a high complexity, are not commonly used across many accounts, and are changed on a regular basis. A multi-factor authentication scheme is highly recommended.

7	BEHAVIOURAL-BASED PROTECTION	Consider monitoring the existing scheduled tasks for recent updates. Tasks should be watched for executing suspicious or unknown binaries.
8	MONITOR AGAINST UNAUTHORIZED ACCESS TO DIRECTORY SERVICES	Consider establishing a robust event log collection mechanism to allow for active monitoring of the anomalies. Security monitoring of Directory Services enables organizations for a rapid response to potentially malicious activities inside the network.
9	MONITOR SUSPICIOUS PROCESSES	Establish timely monitoring processes for unusual activity (e.g., a process that does not use the network begins to do so), as well as the introduction of new files/programs.
10	AUDIT USER ACCESS CONTROL	Maintain a current User Access Control (UAC) list to evaluate users' level of access to various services inside the network. The access level of each user inside their company-owned machine should also be restricted, in order to avoid the risk of surrendering high privilege to the attackers. This list should be continuously updated to reflect the existing status of each employee. Organizations should consider implementing a formal procedure for user account de-provisioning to avoid misuse and abuse in the future.
11	LOCK-OUT POLICY AND BRUTE-FORCE LOGIN ATTEMPT MONITORING	Implementation of an account lock-out policy must be adopted to prevent users from entering an incorrect password repeatedly. Additionally, organizations should consider deploying use cases for detection and alerting of brute-force login attempts.
12	ENFORCE ANTI-SPAM SOLUTIONS AND PRACTICES	Spam filtering should be enabled as a basic email security practice. It is crucial to deploy anti-spam solutions to prevent the delivery of unsolicited bulk emails to the organization. The deployed anti-spam solutions should support screening of specific types of files (e.g., MS-Office docs, PDFs, RTFs archives, etc.) and detect the presence of binaries/scripts for all incoming emails with attachments.
13	MONITOR AGAINST UNPLANNED CHANGES IN FIREWALL RULES AND THE WINDOWS REGISTRY	Continuous monitoring of any unexpected changes to firewall rules and the Windows registry must be practiced regularly to prevent threat actors from creating persistence.
14	CREATE AND ENFORCE POLICIES ON APPLICATION WHITELISTING	Consider the case for restricting users by only allowing them to consent to specific and trusted applications, such as applications developed by the organization or from verified publishers. In addition, consider implementing an application whitelisting policy to control which programs can be run by users. EDR/EPP solutions are often leveraged to implement application whitelisting and security controls at the enterprise level.
15	AVOID USE OF DEVICE'S DEFAULT CONFIGURATIONS AND CREDENTIALS	Consider changing default settings per manufacturer recommendations and update their assets' firmware before allowing them to access the organization's network.
16	RESTRICT THE USE OF VIRTUAL PLATFORMS	Policies should be adopted to strictly control the deployment of virtual machines in the environment. Only approved software or user accounts should be allowed to create and manage virtual machines.

17	**ASSESS SAFEGUARD MEASURES ON THIRD-PARTY SOFTWARE PLATFORMS**	Open source codes and third-party software might lack a trusted verification process to ensure their safety. Consider performing an assessment of any open source or third-party software before implementing it into their programs.
18	**PROTECT AGAINST RISKS ASSOCIATED WITH REMOVABLE MEDIA**	Limited usage of all removable media must be performed across the network, except for approved users and devices. The removable media should be password-protected, encrypted, and automatically scanned for threats upon connecting to the endpoint.
19	**DDOS PROTECTION AND MONITORING**	DDoS protection and monitoring services should be considered for publicly exposed websites and applications. Ideally, publicly exposed applications should be placed behind a load balancer or content distribution networks. Where feasible, consider having SIEM use cases in place for monitoring, with respect to potential DDoS-related traffic/activity.. In particular, this should be considered for publicly exposed websites and applications.
20	**REVIEW NETWORK SECURITY ARCHITECTURE**	The overall framework that specifies the organizational structure, standards, policies, and functional behavior of a computer network (including security and network features) must be reviewed periodically to address potential loopholes.

Global Theme in Focus: Digital Payments Landscape
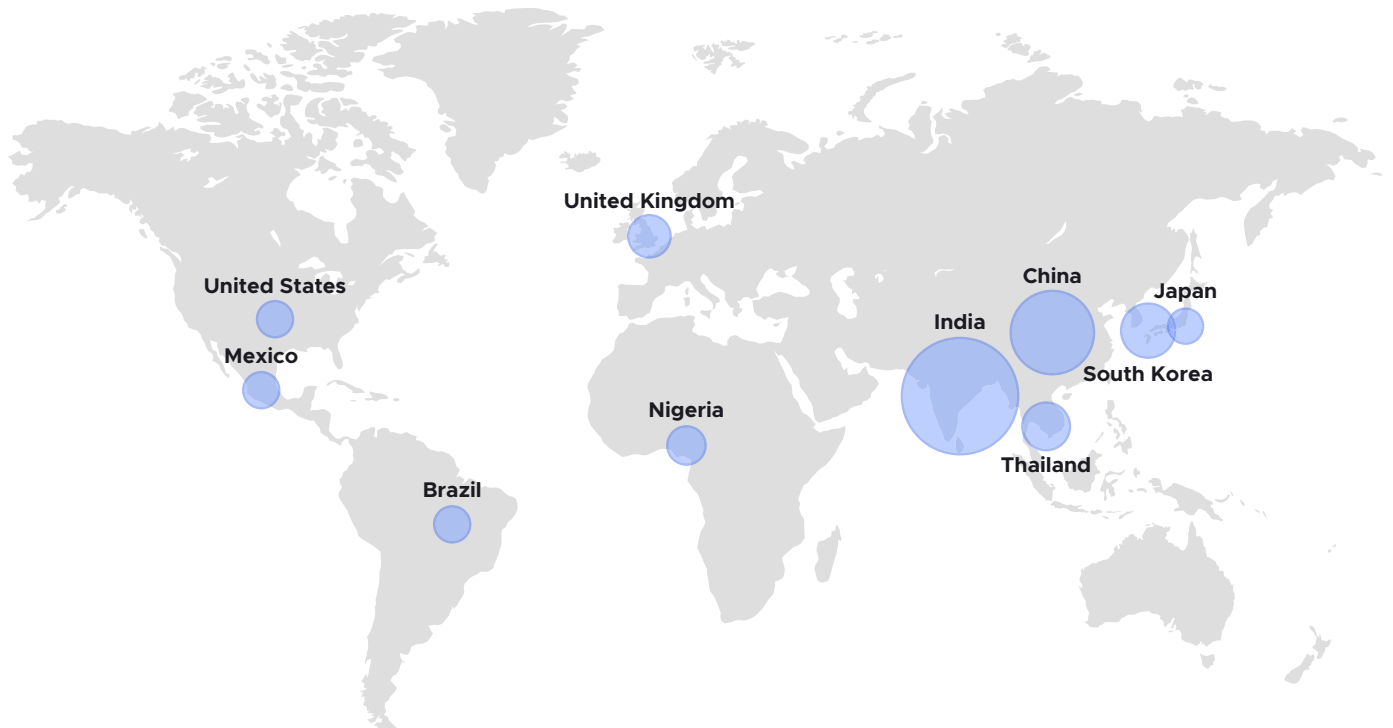
Number of Digital Transactions by Country

Figure 4 - Countries with the highest number of digital transactions in 2021

The transformation in the financial services landscape has been marked by spiraling demand for new, innovative forms of digital payments in different regions in the world. COVID-19 has played a vital role in the acceleration of the mainstream adoption of digital payment methods. Integrated mobile payment applications (such as PayPal, Samsung Pay, Apple Pay, Alipay, and WeChat Pay) are being highly accepted by retail stores and services across the world due to changing lifestyles, daily commerce, and rapid growth in online retailing. Many emerging economies with low rates of bank account ownership have replaced the tradition of cash and cards with smartphones for financial transactions, due to high levels of mobile phone and internet penetration all over the world, especially in the Asia-Pacific region.

Global overview

Online transactions are facilitated through many different systems and services. PayPal's electronic payment system makes financial transactions between two parties streamlined and secure. It keeps the payment information transparent and doesn't require the re-establishment of bank details multiple times. It is free to use and has made wire transfers obsolete. Venmo, introduced in 2009 as the text message-based payment system, transformed in 2012 into a peer-to-peer (P2P) payment application that allows direct fund exchange between individuals. The Chinese payment interface WeChat Pay allows a customer to pay quickly through in-app service; connect to bank accounts; buy movie tickets; and book hotels, flights, and trains. In addition to these, Russia widely uses the YooMoney (formerly Yandex.Money) and Qiwi payment interfaces. Among Europeans, iDEAL is a popular digital wallet in the Netherlands, while Germany mainly uses PayPal, and Sweden prefers Klarna and Swish.

In focus: Asia

In recent years, the highest leap in digital payments has been observed in Asia-Pacific, especially in the South Asian region and the South-East Asian region. In India, the digital payment landscape has been shaped by the introduction of UPI (Unified Payment Interface) by NPCI (National Payments Corporation of India), the umbrella organization monitoring the retail-payment system of India. UPI can facilitate P2P and P2M (peer-to-merchant) transactions. Currently, it has more than 150 million monthly users and aims to have 500 million new users every month by 2025. UPI uses a 4-party model: the issuing bank, the issuing payment service provider (PSP), the beneficiary bank, and the beneficiary PSP. Issuing and beneficiary banks are the accounts where the actual movement of funds occurs. The issuing and beneficiary Payment Service Provider (PSP) is at the front end. A phone application such as Google Pay or Phone Pay is used by the issuing or acquiring PSP to send or obtain the funds. In the UPI ecosystem, although the fund movements happen only between banks, the front end or platform can be provided either by a bank or a non-bank. Other significant parties in the ecosystem are NPCI (which ensures that the information flow is correct between the sending and receiving banks), retailers, and the end consumers.

Similarly, PayNow is a service offered in Singapore. It is enabled by ten participating banks and three participating Non-Bank Financial Institutions (NFIs) that allow peer-to-peer funds transfer. From a privacy perspective, the sender's bank information is kept confidential and only the mobile number, Virtual Payment Address (VPA), or Singapore National Registration Identification Card (NRIC) of the payer can be seen by the payee. Banking details are not required to make a successful payment. The volume (and value) of PayNow transactions has doubled since the start of the pandemic, reaching 125 million in 2020.

Cyberattacks on digital payment systems

The digital payment system has experienced numerous cyberattacks recently. The rise in phishing attacks and online fraud are the biggest threats in this field. The attackers are leveraging malicious links to deploy malware and steal sensitive financial information from the victim system. Nation-state activities are also inevitable in digital payment services. For example, APT38 (originating from North Korea) has been alleged as the perpetrator of attacks on India's Cosmos Bank and several other financial institutions in the South-

East Asian region. Deceptive UPI IDs created by certain websites with the purpose of gaining access to user credentials pose a big risk. Impersonation using fake IDs such as call spoofing, distributed denial of service attacks, and malicious remote screen monitoring tools are also some of the major issues experienced by the digital payment landscape.

International collaboration

Cross-border transactions require specific technology standards between digital economies, mutual regulatory and legal treatments, and trusted cross-border ID systems. Hence, as money crosses borders, multilateral collaboration has become much more important in the era of digital payments. For example, in September 2021, India and Singapore agreed to link their digital payment systems (India's UPI and Singapore's PayNow) to enable instant, low-cost fund transfers. This will enable nationals of both countries to make transactions with each other using one platform. Another international collaboration is the ASEAN-Singapore Cybersecurity Centre of Excellence, which promotes strong international ties for safeguarding the digital economy.

North America Constellation

C1 – Actioning 2022: Regional Themes and Trends

This section provides key regional themes and trends observed throughout 2021. These insights provide valuable insights to organizations on what to expect from a geopolitical and cyberthreat perspective in 2022.

Nation-State Threat Actors Creating Critical Cyber Risks

North America has seen a significant number of cyberattacks in 2021, although most of the threat actors behind the majority of the attacks remain unknown. Even so, threat groups are believed to be of Russian origin have carried out more than 54.8% of attacks. Others, including threat actors originating from China (16.1%) and Iran (9.7%), were also active in North America.

Two threat actors that have been the most actively engaged in malicious activities in North America are LockBit (10.7%) and Conti (10.3%). LockBit ransomware was initially involved in ransomware attacks all over the globe. This group is also known for selling its malicious code to other threat groups. Recently, they have improved and rebranded themselves as LockBit 2.0, a double-extortive Ransomware-as-a-Service operation. On the other hand, Conti has been observed by CISA and the FBI for conducting more than 400 attacks against the US and other international organizations.

The link between nation states and threat actor groups will continue to be a source of political tension. The US Government has accused Russia on several occasions of endorsing several threat groups. The involvement of an infamous Russian actor, DarkSide, in the Colonial Pipeline cyberattack and SolarWinds hacks have further damaged the relationship between the two countries. Considering Russia's alleged interference in the 2016 US Presidential election, the 2022 mid-term Congressional elections will be in the spotlight. Along with this, the growing activities of Iranian advanced persistent threat (APT) groups will be a big concern for the region.

Primary Motivation for Cyberattacks Continues to be Financially Driven

In 2021, almost 69% of the cyberattacks in North America were motivated by financial gain. In addition, vandalism (7%) and espionage (3.4%) were also crucial motivations for the threat groups. Around 18.4% of the attacks were triggered by vulnerabilities in infrastructures or individual accounts, followed by ideological disputes (8%).

Financially motivated cybercrime is anticipated to grow in the region, given that more than 60% of the companies targeted by ransomware attacks show an increased willingness to pay the ransom. As cryptocurrencies become more popular and numerous, they will also be more targeted. This was seen recently in the hacks impacting crypto trading platforms. Blockchain is often praised to be secure and unhackable, but recent events prove otherwise.

Weaknesses in outdated and insecure IT infrastructures enable threat actors to be more successful in their attacks. This was highlighted in several attacks, such as the financially motivated ransomware attack by DarkSide on Colonial Pipeline that was due to some outdated unpatched vulnerabilities in a critical infrastructure. A robust and resilient infrastructure will significantly reduce the risk of cyberthreats and organizations should focus on keeping their IT infrastructure up to date. See Section B for more strategies.

Services and Public Sector among the Most Impacted Industries in the Region

Almost 34% of cyberattacks in 2021 targeted the services sector, followed by the public sector (16.8%). Other sectors impacted were retail (11%), finance (8.6%), and healthcare (6.2%).

Among the services, the technology and telecommunication sectors have been targeted most frequently. Attacks on these sectors comprise 57.7% of the total attacks targeting the services. The increasing use of penetration tools and continuously evolving new techniques are expected to be a major threat to the technology sector going forward. The fragility of legacy technical infrastructures and the growing system complexities make it more challenging to address the probable loopholes in the industry. The consulting services (12.6%) and media (11.2%) sectors have also been increasingly targeted by threat groups.

The rising geopolitical tensions will impact the government and the public sector the most. For example, the forthcoming 2022 US Senate elections will be a major target for the threat groups inside and outside the region. In addition, foreign players' interference in the region's internal politics could drastically affect the government sector.

Growing Ransomware Attacks Require Stronger Security and Business Risk Programs

Ransomware continues to be the most prominent attack method, with more than 30% of the total methods used. Network access (7%) and exploiting vulnerabilities (6.1%) are the two other most frequently used methods. Social engineering and spear-phishing have also been widely used by many threat groups.

The growing financial motivation among the threat actors has caused an alarming rise in ransomware attacks, both in North American and globally. Extortion methods such as big game hunting, double extortion, anonymity-enhanced cryptocurrencies, partnerships, etc., are also advancing rapidly, intensifying the pressure for victims to pay. Several law enforcement agencies, including the Federal Bureau of Investigation, are advising against paying ransoms as it offers an incentive for more cyber criminals to establish or increase their operations.

A "defense-in-depth" strategy with multiple layers of defense is required to mitigate the impacts of these attacks.

PowerShell, Cobalt Strike among Most Frequently Used Tools to Conduct the Attacks

PowerShell (11.7%), Cobalt strike (11.4%), and Remote Desktop Protocol (9%) were the most frequently used tools in the North American region to carry out the cyberattacks in 2021.

PowerShell is one of the most popular tools of choice for many threat groups, as it leverages the attacks as fileless. PowerShell's direct execution in memory and remote access capabilities make it a stealthier weapon to run the malicious scripts. Deploying a security information and event management system (SIEM) and keeping an eye on the Indicators of Compromise (IoCs) can be helpful for organizations to minimize or avoid these attacks.

Cobalt strike is a command-and-control (C2) application itself. It is a commercial threat-emulation and post-exploitation tool commonly used by malicious attackers and penetration testers to compromise and maintain

access to networks. Attacks by Remote Desktop Protocol (RDP) have also become a popular medium among the threat groups to gain initial access to the target systems. The attackers can easily compromise the internet-facing RDP servers with the evolution of automated scanning services and botnet malware tools. Furthermore, due to the use of legitimate administrative credentials by the threat groups, it will be very challenging for traditional security tools to detect the activities.

C2 – Geopolitical Landscape

Geopolitical events often have a great impact and have the potential to influence cybersecurity events. Below are just a few significant geopolitical developments observed in the North American constellation in 2021 that are anticipated to be very relevant to the cybersecurity landscape in 2022.

2022 US Elections Vulnerable to Cyberthreats

The threat of interference by foreign players and ransomware attacks will be a major concern in the US mid-term elections in November 2022. This risk poses a critical challenge to several processes happening simultaneously, including federal, state, and local elections. Federal agencies have already sounded the alarm, given that threat actors with ties to Iran and Russia are thought to have manipulated the 2016 and 2020 US Presidential elections. By revisiting existing policies and laws, educating election officials on security best practices, collaborating with non-governmental cybersecurity experts, and educating voters, the US can mitigate these threats through strategic planning.

Biden's Massive Allocation to Tech and Cyber Set to Improve the Nation's Cybersecurity Posture

Cybersecurity and IT modernization have become key priorities for the Biden administration, including a $9.8 billion investment in cybersecurity to protect the nation's infrastructure; secure federal civilian networks; and support efforts to share information, standards, and best practices. Significant allocations are also provided to the Technology Modernization Fund (TMF) and Cybersecurity and Infrastructure Security Agency (CISA). President Biden's initiative is, in part, a direct reaction to the SolarWinds supply-chain attack. The proposal is marked by the largest-ever Research Development Test and Evaluation (RDT&E) funding as a part of the defense budget. This allocation will enable the country's public sector to reach a real state of cybersecurity readiness. It will also help the country's critical infrastructures (e.g., energy and telecommunication) to be secured and free from large-scale, nation-wide disruption. The Biden administration's biggest challenge will be getting Congress on board with plans to divest the US of legacy platforms in order to fund new capabilities.

US-Israel Partnership in Cybersecurity to Boost Digital Economy

The US and Israel's new partnership in scientific innovation is a direct response to recent security threats, including ransomware, which has become more frequent and impactful. The two nations will enhance their information sharing on cyberthreat intelligence, design better staff training programs, and conduct cross-border cybersecurity exercises. A significant focus on financial crime will enable fintech organizations and innovators to possess more resilient cybersecurity mechanisms to counter money laundering and other malicious activities. With the growing cyberattack risks, especially from Iran-backed threat groups, this innovation-based strategic partnership will fortify the digital economy and security ties between both countries.

Biden-Putin Summit Might Lead to "No-Go" Zones in Nation State Cyber Activities

A summit in Geneva between the leaders of the United States and Russia resulted in a strategic conversation on how to minimize the use of cyberthreat actors for political gain. The cybersecurity attack on Colonial pipeline in May 2021 created a serious concern for how politically motivated cyberattacks can have significant impacts on public safety and critical infrastructure. The latter was specifically identified as a "no-go" zone when it comes to nation-state cyberattacks. The success of this meeting remains to be seen, due to the deteriorating relationship between the two countries. Given the advanced cyber capabilities of each country, however, they are both likely to cooperate on the "no-go" zone discussed.

C3 – Cyberthreat Regional Landscape

North America saw its fair share of cyberattacks in 2021. Among the most prominent organizations targeted were: Colonial Pipeline, JBS, Washington DC Metropolitan Police Department, Discount Car and Truck Company, Home Hardware, and Toronto Transit Commission (TTC). Attacks against these organizations caused a severe impact on critical infrastructure, creating shortages and increasing the cost of goods and services. Additionally, these organizations experienced financial loss due to shutting down operations and paying ransom to the threat actors. Furthermore, ransomware and malware are ever evolving. Initially designed to encrypt files on the victim devices, they can now exfiltrate data and introduce new techniques known as double and triple extortion. During the COVID-19 crisis, many threat actors took advantage of the situation for potential monetary gain.

T-Mobile Data Breach

Industries Targeted	Continents Targeted
Services	United States
T-Mobile threat actor: John Binns	

Threat actors are not only associated with an APT group; a few are also acting on their own, trying to breach large-scale organizations. These threat actors constantly scan for vulnerabilities in the victim's infrastructure to exploit and breach sensitive data and sell it on the Dark Web to the public. An attack on T-Mobile is one example of a data breach allegedly caused by an individual threat actor. A 21-year-old US citizen, John Binns, allegedly claimed that he was the main culprit behind the attack. John Binns first gained access to a data center near East Wenatchee, Washington. From there, he gained access to other company servers. It took him just one week to gain access to the Oracle database server where the sensitive information of millions of T-Mobile's customers was stored. John's primary motivation was to retaliate against the US Government for a kidnapping related to the Satori botnet conspiracy.

T-Mobile explained that the threat actor leveraged their technical systems and specialized tools and capabilities to gain access to its testing environments. Then the threat actor performed brute-force attacks and gained entry into their IT servers that included customer data. Based on this incident, there are two key

takeaways. First, even without sophisticated techniques, threat actors can be successful at performing a large-scale attack on giant organizations. Second, organizations should be prepared and well-equipped with all the security controls needed to detect suspicious behavior within their organization's network.

Equation

Industries Targeted	Continents Targeted
Defense, Public Sector, Energy, Services and Transportation	USA, Mexico

Equation is also known as: Equation group, Tilded Team, Platinum Colony

Equation group is known for its sophisticated global computer attack. It is also among the handful groups with elite capabilities, extraordinary skills, and attack vectors. First observed in 2015, the group is motivated by intelligence gathering and monitoring its victims. Once the target is defined, a sophisticated collection of tools and techniques are leveraged to monitor the victim and exfiltrate valuable information from the network. The group aims to maintain access to the organization's network to collect tactical and general intelligence. Many highly sophisticated malware variants have been linked to the group, including EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, GrayFish, and Fanny. The malware has a self-destructing mechanism built into it and uses virtual file systems. Some of these malwares can stash multiple infected files and encrypt and store them in the victim's computer registry. The group leverages a mix of both zero-day exploits and phishing techniques to lure the victim into opening the link. It then redirects victims to a page that is able to trigger zero-day exploits in both iOS and OS X devices. The Equation group's highly advanced and sophisticated abilities pose a high threat to target organizations and entities within the group's operational remit.

APT28

Industries Targeted	Continents Targeted
Defense, Public Sector, Energy, and Services	USA, Canada

APT28 is also known as: FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake

APT28, also known as Fancy Bear, is a highly sophisticated Russia-based threat actor believed to be associated with the Russian Military. APT28, first observed in 2004, is observed to conduct its cyberespionage operations against NATO (North Atlantic Treaty Organization) member states aligning with the political interests of the Russian government to gain access to sensitive espionage information.

The threat actor group is also known for its capabilities to deploy custom-made tools and exploit zero-day vulnerabilities. Their operations involve malware families that are unique to groups such as X-Agent (also known as CHOPSTICK, Sofacy), WinIDS, Drovorub, Zekapab, and DownRage. X-Agent is believed to be ported to infect both Android and iOS devices, giving the app the ability to record audio and collect sensitive information from the victim device and send it to the threat actor group. Furthermore, the group is witnessed to develop and deploy various new malware such as Drovorub, a Linux RAT, Zekapab, and Acelog. The group has also conducted several highly lucrative spear-phishing campaigns to capture sensitive credentials and deliver malicious payloads. A recent global brute force campaign was observed targeting enterprise and cloud environments (including Kubernetes and Microsoft Office 365), primarily targeting the US and Europe. The group also targeted the Norwegian Parliament and COVID-19 vaccine manufacturers in several countries.

Pioneer Kitten

Industries Targeted	Continents Targeted
Services, HealthCare, Defense, and Finance	United States

Pioneer Kitten is also known as: Parisite, Fox Kitten, Pioneer Kitten, Cobalt Foxglove, UNC757

Pioneer Kitten is an Iran-based threat actor group suspected to be associated with the Iranian government. The group is motivated by gathering intelligence relevant to the Iranian government, such as defense and technology-related intelligence. The group is known to conduct cyber campaigns focusing specifically on persistence to gain sensitive information for a prolonged period. The group leverages web attacks and exploits targeting public-facing infrastructure as the initial attack vector to deliver sensitive payloads and malware. The threat actor group is known to use CVEs such as CVE-2018-13379, CVE-2018-13382, CVE-2018-13383, CVE-2019-11510, CVE-2019-11539, CVE-2019-19781, CVE-2020-0609, CVE-2020-0610, and CVE-2020-5902. The compromised hosts can also be used as a remote access broker for other Iranian state-sponsored APT groups, such as APT33, APT34, and APT39. The APT group has also deployed Pay2key and N3tw0rm ransomware on primarily Israeli targets. In a recent campaign, the APT group was observed exploiting several known vulnerabilities in Pulse Secure VPN, Citrix NetScaler, and F5. Analyzing the recent campaigns, the threat actor can provide network access to other APT groups. Its ability to deploy ransomware on victim machines and the sensitive nature of stolen data pose a high threat to industries.

Energetic Bear

Industries Targeted	Continents Targeted
Services, HealthCare, Defense, and Finance	United States

Energetic Bear is also known as: Havex, Dragonfly, Crouching Yeti

Energetic Bear is a Russian-based, highly active APT (advanced persistent threat) group first observed in 2010. Motivated by espionage activities, the group changed its focus from initially targeting defense, government, and aviation to conducting cyber espionage campaigns—specifically targeting industries related to industrial control of critical infrastructure companies based in the US and Europe in early 2013. The group is known for leveraging web compromise and spear phishing as initial attack vectors. The group also uses vulnerabilities such as CVE-2012-1723, CVE-2012-2034, CVE-2013-1347, CVE-2013-1690, CVE-2013-2729, and CVE-2014-1761. Additionally, common RATs such as Havex and XAML are leveraged by the threat actor group to steal sensitive information from the victim. Cyber-espionage operations are historically observed in countries such as France, the United Kingdom, the United States, Germany, Greece, Israel, Italy, Poland, and Taiwan. Analyzing the previous campaigns by the APT group and its willingness to work with other threat actor groups indicates that it poses a significant threat to organizations involved in critical infrastructure.

Panda Stealer

Industries Targeted	Continents Targeted
Finance (Cryptocurrencies)	Global

Panda Stealer is a cryptocurrency stealer that is being spread globally using spam campaigns and potentially through Discord channels. Researchers found that the malware has been targeting individuals across the United States. The malware begins with phishing emails that lure victims into downloading executables from malicious websites via discord links. These phishing emails are usually disguised as business quote emails that contain .XLSM and .XLS attachments. Once the Panda Stealer is downloaded, it starts to detect keys and addresses related to cryptocurrency wallets holding funds, including Ethereum (ETH), Bytecoin (BCN), Dash (DASH), and Litecoin (LTC). Going forward, Panda Stealers might also be used in campaigns to compromise cryptocurrencies.

C4 – Industry Threat Landscape

Severity Score for Cyber Events Grouped by Industry
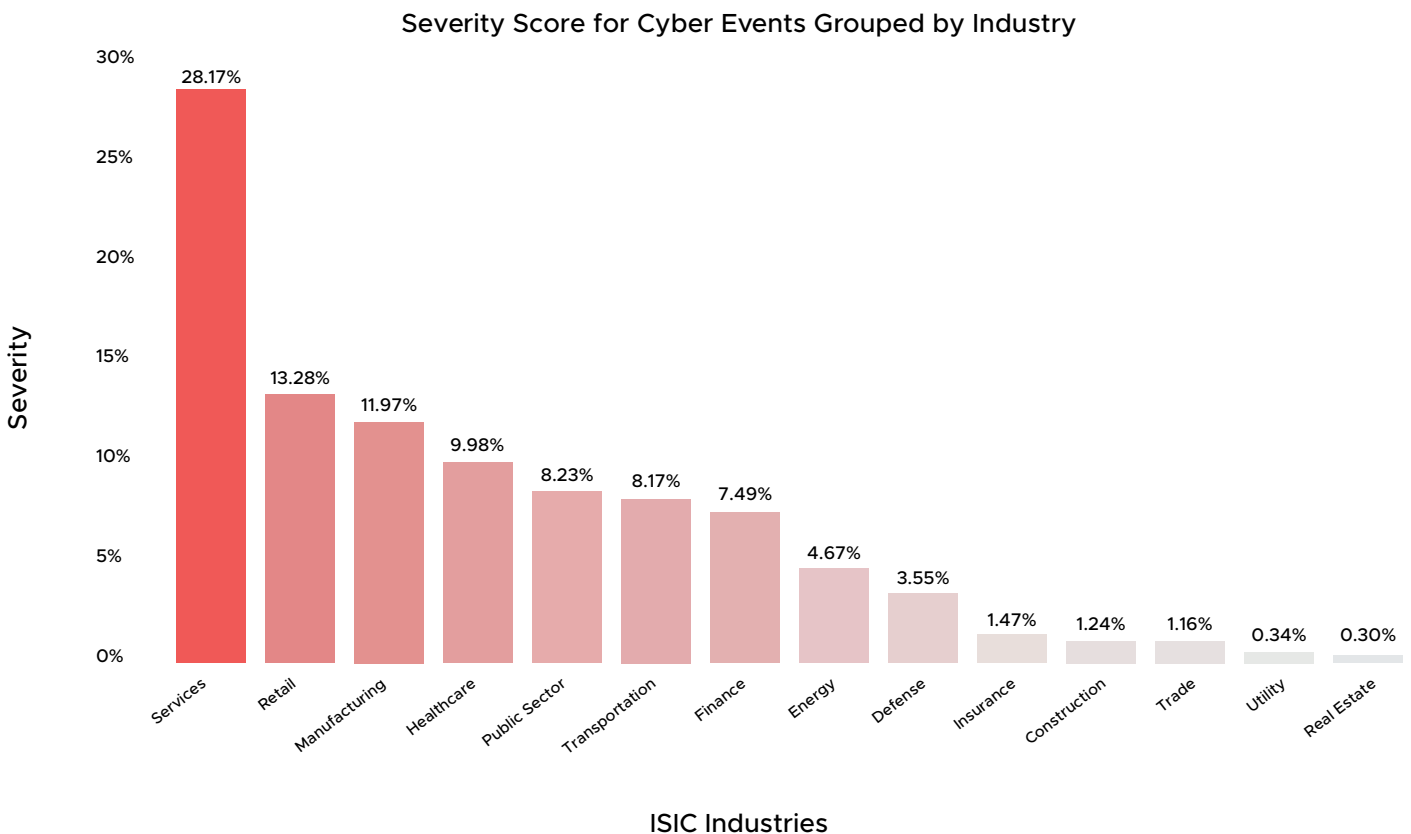
Figure 5 - Industry threat landscape in North America

Telecommunication, Consulting, Media Are the Most Affected Services

The service sector tops the list of industries most affected by cyberattacks in the North American region in 2021. More than one fourth (25.9%) of all cyberattacks performed in the region targeted the service sector. The telecommunication, consulting services, and media sectors were the three most affected services in North America, reporting 56.3%, 12.7%, 11.3% of the attacks, respectively. Although the initial triggers for most of these attacks are unknown, vulnerability in infrastructure and well-known applications seem to be the trigger for many of the events. CozyBear, Avaddon, Grief, Cybermercenary, and FIN7 are the threat actors mainly responsible for the cyberattacks against the telecommunication sector.

The consulting services sector was slammed by Conti and LockBit 2.0 ransomware attacks. Most of the attacks were for the purpose of gaining access to unauthorized data. CoomingProject is behind multiple attacks on the media sector. Ideological disputes is the prime reason behind targeting this sector. The remote desktop protocol (RDP), PowerShell, and Cobalt Strike have been frequently utilized to conduct the attacks on the services.

Cyber-Espionage Campaigns Targeting the Public Sector of the United States

In 2021, 31.2% of the total cyber-espionage campaigns in the US targeted the public sector. There were multiple allegations of threat groups originating from China performing espionage operations. Threat actors such as APT31, Nobelium, UNC2630, and UNC2717 have been observed to target the US public sector.

These groups leveraged social engineering campaigns and deployed malware in the victim organizations to attain their goals. The rising geopolitical tensions worldwide might trigger the advance persistent groups to conduct more government-backed cyber-espionage campaigns against the adversaries of respective governments in the future.

The Healthcare Sector Frequently Exploited by Financially Motivated Threat Actors

Financial gain has been the biggest motivation for the threat actors targeting the healthcare sector. More than 90% of the cyberattacks conducted against the healthcare sector are financially motivated. APT35, Pysa, FIN12, and Hive are the top threat actors to target the healthcare sector, mainly by deploying ransomware. Significant incidents of healthcare organizations being targeted by cyberattacks include the APT35 group targeting US medical personnel credentials, a cyberattack disrupting the Newfoundland and Labrador healthcare system, FIN12 operators targeting US healthcare providers using Ryuk ransomware, etc. The vulnerabilities in the infrastructures of the healthcare sector are the main trigger for these cyberattacks. The FiveEyes group has issued a security warning regarding future cyberattacks to be conducted on the healthcare sector and hospitals in the region.

Data Breach Is More Prevalent in Retail and Telecommunication Industries

Almost half of the total data breach instances in 2021 were meant for the retail (23.3%) and telecommunication (23.3%) industries. A retail data breach includes attackers stealing customer data, which can involve credit card numbers, names, addresses, social security numbers, and even passwords. With the growing e-commerce market in the post-COVID era, data breaches in the retail sector have become more prevalent, heavily impacting the US economy. Threat actors such as Conti, Darkside, and Marketo have been at the top of the list to exploit retail industries through data breaches. However, the telecom industry has also faced multiple data breach incidents. For example, the T-Mobile data breach incident affected more than 40 million users in the US. The main threat actors involved in telecom data breaches include ShinyHunter, FIN7, and CoomingProject. Financial gain is the primary motivation for these data breach activities targeting the retail and telecommunication sectors.

Vulnerabilities in Infrastructure Triggers Huge-Scale Exploitation of Energy Sector

Around 60% of the attacks conducted on the energy sector are triggered by vulnerabilities in infrastructure. Energy companies are basically late adopters of digitization. The delayed implementation of cloud computing and functional software such as business billing and operational software in the energy sector has resulted in a lack of cybersecurity measures, as compared to the corporate world. Several companies in the energy sector depend on outdated control systems that can't be updated easily. They are also vulnerable to the sophisticated nature of many cyberattacks in the current climate. The lack of highly skilled cybersecurity professionals in the core sector paves the way for attackers to exploit these vulnerabilities. REvil, AvosLocker, and Haron are the threat actors responsible for exploiting the infrastructure vulnerabilities in the energy sector. The attack on Colonial Pipeline by DarkSide has caused a significant impact in the region. Most of these attacks are financially motivated. The critical dependence of the energy sector on a nation's economy poses a great attraction for state-sponsored cybercriminals in the future.

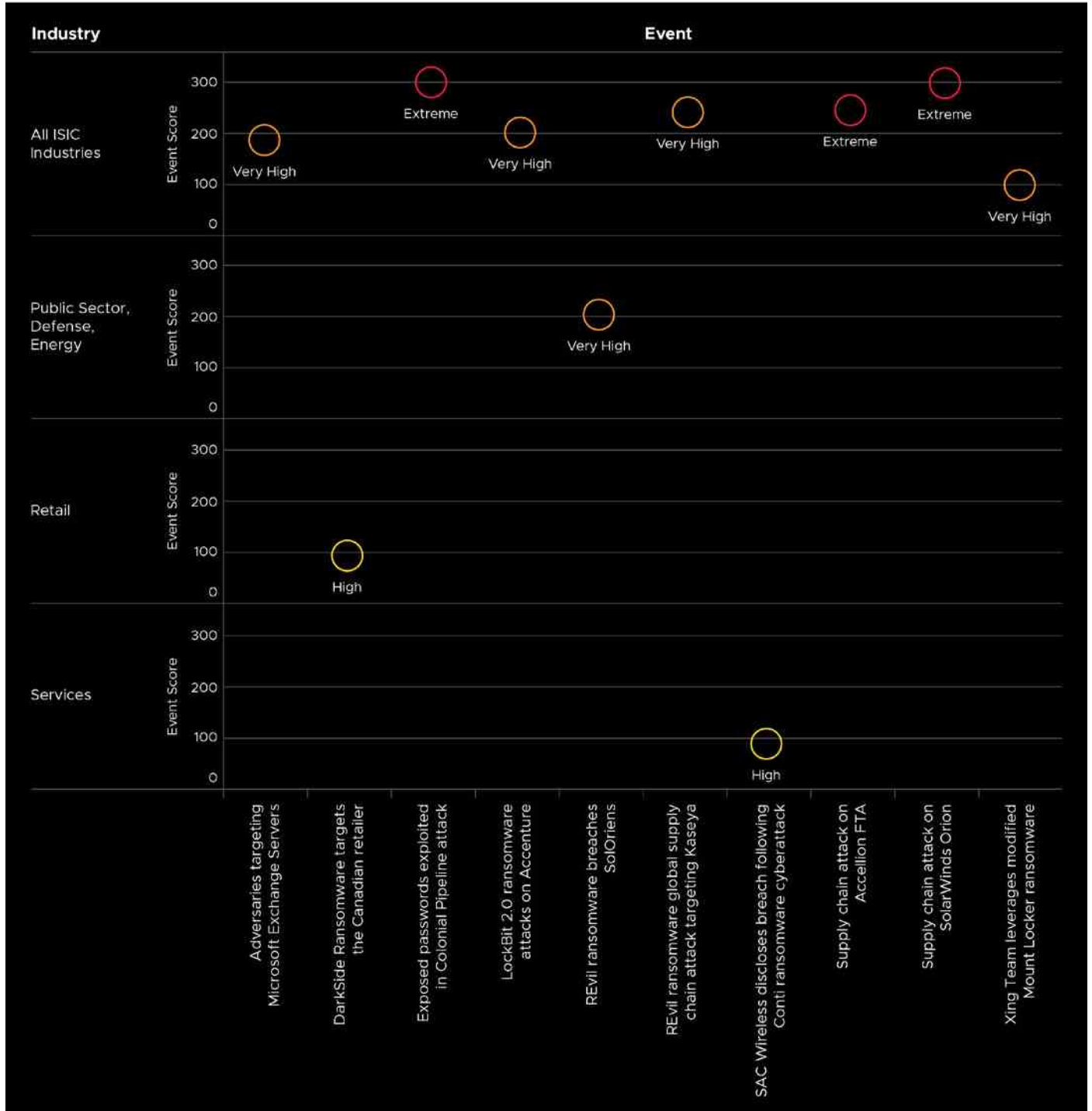# C5 – Key Lessons from the Most Impactful 2021 Attacks

Figure 6 - Top 10 events in North America

#1 Colonial Pipeline attack: exposed password for stale VPN account suspected as initial infection vector

Severity: Extreme

Industries Targeted: All ISIC Industries

Quick Recap: On May 8, 2021, Colonial Pipeline was a victim of a DarkSide ransomware incident and had shut down parts of its pipeline operations to contain the threat. As part of the initial infection vector, an abandoned account was leveraged to reach the internal network via a compromised VPN account without multi-factor authentication (MFA). It is still unclear how the credentials were originally obtained, but the account password was detected on Dark Web credential leaks of other third-party breaches—suggesting that the password might have been used on other accounts as well.

Key Impact: The threat actors allegedly exfiltrated about 100 GB of data from Colonial Pipeline systems and moved laterally within the internal network. Colonial Pipeline was forced to shut down all gasoline transfer pipelines, although there are no indications that any other critical operational technology systems were compromised. The DarkSide operators are using their leak site to publish compromised data that might lead to the disclosure of personally identifiable information (PII), intellectual property, and loss of reputation. DarkSide follows the Ransomware-as-a-Service model, where developers handle coding of the ransomware software and host the payment website. At the same time, affiliates conduct the other phases of the attacks, such as reconnaissance and data exfiltration.

Future Considerations: DarkSide allegedly closed its operations in May 2021, but has allegedly returned and rebranded as BlackMatter ransomware. The encryption algorithm within the decryptor reveals the similarities between DarkSide and BlackMatter, indicating that the threat actors operating the ransomware are identical. Despite the rebranding, the threat group publicly announced in November 2021 that they are shutting down due to increased pressure from the authorities. Given their previous history, the group could reappear in the future, so organizations should be on alert.

DarkSide has mainly targeted publicly traded organizations and has been known to significantly increase initial ransom demands during negotiations. To date, DarkSide is alleged to have compromised over 40 organizations and demands high ransom amounts generally ranging between 200,000 and 2 million USD. The incident affecting Colonial Pipeline highlights the serious threat posed by DarkSide ransomware to critical infrastructure and national security.

#2 Attack on SolarWinds Orion reveals supply-chain vulnerabilities

Severity: Extreme

Industries Targeted: All ISIC Industries

Quick Recap: On December 13, 2020, cybersecurity firm FireEye reported a sophisticated and widespread supply-chain attack targeting the SolarWinds Orion software, a widely used IT monitoring and management tool. The threat actor group responsible, UNC2452 (also known as Nobelium and Dark Halo), was behind the cyber-espionage campaign. They leveraged a Trojan malware in the SolarWinds Orion software update to distribute a malware named SUNBURST. The US Cybersecurity and Infrastructure Security Agency, United Kingdom's National Cybersecurity Centre, the Federal Bureau of Investigation, and the National Security Agency subsequently released a Joint Cybersecurity Advisory on Russian Foreign Intelligence Service (SVR) tactics, techniques, and procedures.

Key Impact: The SolarWinds campaign's primary motive was espionage, leading to sensitive data exfiltration, file execution, forensic and anti-virus services termination, and compromise of email exchange servers. The most impacted organizations were from across industries, but especially Public Sector and Services in North America, Europe, Asia, and the Middle East.

Future Considerations: While not as significant as the SolarWinds cyber incident, the threat actor group remains active, targeting the technology sector. UNC2452 is expected to remain active, possibly leveraging vulnerabilities in outdated software applications to gain unauthorized access. All global industries should remain on alert, especially the technology sector.

Understanding the group's TTPs is critical in helping organizations implement preventive measures. For example, SUNBURST has been observed to deliver different payloads, including an in-memory dropper dubbed TEARDROP that deploys Cobalt Strike BEACON. Once inside the network, the threat actors attempt to elevate their access level. With obtained administrator credentials through the on-premises compromise, the threat actors try to gain access to the organization's global administrator account.

#3 Supply-chain attack on Accellion FTA impacted several organizations

Severity: Extreme | **Industries Targeted:** All ISIC Industries

Quick Recap: In December 2020, Accellion discovered several critical and zero-day vulnerabilities in the organization's File Transfer Appliance (FTA) product, just five months prior to retiring the application. The threat actors implemented a newly discovered web shell dubbed DEWMODE on FTA, leading to many FTA users receiving extortion emails that threatened to exfiltrate data from their environments to the Dark Web leak site belonging to Clop ransomware operators. The vulnerabilities are tracked as CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104.

Key Impact: More than a third of FTA users were affected by the supply-chain attack and less than a quarter of those suffered significant data theft. Accellion provided software patches for all of the known existing vulnerabilities and worked closely with impacted organizations on mitigation efforts.

Future Considerations: Clop ransomware operators were actively involved in cyber incidents throughout 2021 and are expected to continue targeting a wide variety of industries worldwide. Critical vulnerabilities tend to attract attention from ransomware operators, as these exploits could be used to gain a foothold within an organization's network for malicious activities.

#4 REvil ransomware global supply-chain attack targeting Kaseya

Severity: Very High | **Industries Targeted:** All ISIC Industries

Quick Recap: On July 2, 2021, software solutions provider, Kaseya announced that it was the victim of a cybersecurity incident attributed to REvil (also known as Sodinokibi or Sodin), a ransomware group alleged to be of Russian origin. The attack compromised Kaseya's VSA remote IT monitoring and management solution. On July 23, 2021, Kaseya obtained a universal decryptor key for the REvil ransomware through a third-party vendor, Emsisoft, a New Zealand-based anti-virus distributed software company. It remains unknown whether Kaseya paid a ransom.

Key Impact: REvil group allegedly demanded $70 million in Bitcoin (BTC) to provide the decryptor for all systems locked during the Kaseya supply-chain attack. Although public records show that over 200 organizations were affected, it is estimated that thousands of businesses became victims.

Future Considerations: REvil ransomware has been associated with multiple high-profile breaches in the past. REvil is associated with double-extortion attacks and is known for exfiltrating company data in addition to attacking it with malicious ransomware. Recent tactics include using a Linux variant of the encryptor to target VMware ESXi virtual machines, allowing them to encrypt multiple servers at once by targeting the underlying ESXi platform. In July 2021, REvil ceased their operations, which could have been the result of a planned and concurrent shutdown of their infrastructure. Yet, they returned two months later when they made their TOR negotiation and data leak sites accessible again. Organizations across all industry sectors should remain on high alert in 2022.

#5 REvil ransomware breaches US nuclear weapons contractor, Sol Oriens

Severity: Very High

Industries Targeted: Public Sector, Defense, Energy

Quick Recap: In June 2021, REvil struck Sol Oriens, a small US nuclear weapons contractor and subcontractor for the US Department of Energy (DOE). REvil successfully compromised the organization, deployed its ransomware, and then posted this announcement on their blog: "We hereby keep a right (sic) to forward all of the relevant documentation and data to military agencies of our choice (sic)." The threat actors posted the announcement on June 3, 2021, but the attack was likely performed earlier. Sol Oriens did not confirm whether the ransom was paid.

Key Impact: The exfiltrated data included a large amount of the company's payroll dating back September 2020. It exposed sensitive personal information of employees, including quarterly pay, full names, and social security numbers.

Future Considerations: REvil ransomware has been associated with multiple high-profile breaches in the past. The attack against Sol Oriens allegedly provided the threat actor group with classified government documents, which could potentially lead to a series of extortion tactics against government agencies.

#6 Lockbit 2.0 ransomware attacks Accenture

Severity: Very High

Industries Targeted: Public Sector, Defense, Energy

Quick Recap: Ransomware group LockBit 2.0 claimed to have exfiltrated 6 TB of data from Accenture, a multi-national consulting and professional service provider, during a cyber incident in June 2021. The data was published on the threat group's leak site, containing 2,384 items including subfolders. This indicates that Accenture might not have proceeded to pay the ransom.

Key Impact: However, in further development of the incident, Accenture informed that they were able to immediately isolate the affected servers and restore affected systems from backup. Additionally, the organization confirmed that the incident had no impact on operations and client systems.

Future Considerations: LockBit 2.0 is the successor to LockBit ransomware, having enhanced capabilities to capture and automatically encrypt sensitive information. Monitoring outgoing traffic is crucial to identify insider threats, since the group is reported to be recruiting employees from the targeted organizations. The threat actors historically gained initial access into victims' networks by exploiting existing vulnerabilities in the Fortinet FortiOS and FortiProxy products. Based on the malware developments, Lockbit is expected to appear again in the near future.

#7 Targeting Microsoft Exchange Servers

Severity: Very High | **Industries Targeted:** Public Sector, Defense, Energy

Quick Recap: On March 2, 2021, Microsoft published a detailed report addressing four previously unknown or zero-day vulnerabilities in Microsoft Exchange Server used in targeted attacks. Microsoft stated that allegedly state-sponsored threat actor Hafnium exploited Exchange email service to gain access to internal systems. The four exploited vulnerabilities, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, have also been exploited by other threat actors.

According to Microsoft, Hafnium primarily targets US organizations in the services and public sector industries, including infectious disease research, law firms, higher education institutions, defense contractors, policy think tanks, and non-governmental organizations (NGOs). The threat group primarily operates from leased virtual private servers (VPS) in the United States and exfiltrates data to file sharing websites such as MEGA.

Key Impact: Over 30,000 organizations were compromised in the United States as of March 8, 2021, because of the Microsoft Exchange vulnerabilities exploited by Hafnium and various other threat groups.

Future Considerations: The threat actor group appears to be politically motivated. The threat group did not engage in further cyber incidents during 2021, but could re-emerge. Trending exploits such as the Microsoft Exchange Server's vulnerabilities tend to attract attention from ransomware operators as these vulnerabilities could be used to gain a foothold within an organization's network for malicious activities. Organizations should ensure prompt patching of all known vulnerabilities.

#8 Xing Team leverages modified Mount Locker ransomware targeting LineStar Integrity Services

Severity: Very High | **Industries Targeted:** All ISIC Industries

Quick Recap: LineStar Integrity Services was targeted in a ransomware attack in early May 2021. LineStar is Houston's integrated pipeline compliance, technology, and integrity maintenance company. The threat actor, Xing Team, allegedly exfiltrated nearly 70 GB of the corporate entity's internal files and published them on the Dark Web. The exfiltrated data contains 73,500 contracts, emails, accounting files, and other business documents based on available information. Additionally, the file included 19 GB of software data and 10 GB of human resource files, such as copies of employee driver's licenses and Social Security cards. LineStar has claimed that all employees have been notified of the breach of their personal information. Furthermore, the FBI and cybersecurity experts were allegedly notified following this incident.

Key Impact: Although LineStar has stated that the breach caused no disruption to the infrastructure, there is a risk that the leaked data could provide other threat actors with a gateway to further pipeline-based targets, including information on physical equipment or software architecture used by LineStar's clients.

Future Considerations: In the past, Xing Team has leveraged a modified version of the Mount Locker ransomware to encrypt the victim's files and threatened to leak data to increase the pressure on the victim. While not much has been heard about the threat group since the incident, other threat actors could potentially leverage and modify Mount Locker in the coming year.

#9 DarkSide Ransomware targets the Canadian retailer Home Hardware and expands their extortion tactics with a new technique

Severity: High | **Industries Targeted:** Retail

Quick Recap: Home Hardware Stores Ltd., one of Canada's largest hardware retailers, was targeted in a ransomware attack in February 2021. The DarkSide threat actor group is reported to be responsible for gaining access to and exfiltrating part of the corporate data. Additionally, the threat actors started releasing the exfiltrated data from April 2, 2021 onwards. The organization engaged its cybersecurity team to isolate the affected systems and contain the attack.

Key Impact: Home Hardware disclosed that the intrusion had not impacted any consumer transaction or payment data. The threat actors allegedly exfiltrated more than 300 GB of sensitive information. Some of the screenshots provided in the leak site appear to be from a financial report from December 2020. The DarkSide operators claim to have prior experience with other ransomware threat actor groups and are quite successful in their operations. They are also using their leak site to publish compromised data, which could lead to the disclosure of personally identifiable information (PII), intellectual property, and loss of reputation.

Future Considerations: DarkSide was a notorious threat actor that targeted large enterprises and applied extortion tactics. On May 14, 2021, the group allegedly closed its operations, due to losing access to ransomware infrastructure servers. However, on July 31, 2021, the ransomware threat actors allegedly returned and rebranded DarkSide as BlackMatter ransomware. The encryption algorithm within the decryptor reveals similarities between DarkSide and BlackMatter, indicating that the threat actors operating the ransomware are identical. Despite the rebranding, the threat group posted a message on their website on November 01, 2021, announcing that the entire operation would be shutting down within 48 hours, allegedly due to increased pressure from the authorities.

According to the latest updates, the threat actors withdrew four bitcoins (~$250,000) from the exploit hacking forum on November 3, 2021. In addition, they have been editing their posts on platforms and asking moderators to delete them.

DarkSide has previously shut down and returned under a different name and, likely, this could possibly occur again in the near future.

#10 SAC Wireless discloses breach following Conti ransomware cyberattack

Severity: High

Industries Targeted: Services

Quick Recap: On August 23, 2021 a US-based Nokia subsidiary, SAC Wireless, was revealed to have suffered a data breach following a Conti ransomware attack on June 16, 2021. SAC Wireless is an independently operating Nokia company stationed in Chicago, IL, and operates with telecom carriers, Original Equipment Manufacturers (OEMs), and major town owners across the United States. The company identified that personal information on current and former employees, (including details on their health plans' dependents or beneficiaries) was exfiltrated due to the breach confirmed after a forensic investigation was conducted.

Key Impact: The ransomware threat actors disclosed that allegedly 250 GB of sensitive data was exfiltrated on their leak site and threatened to publish all the company's data to the public if SAC Wireless refused to cooperate with the ransom demand.

Future Considerations: The data breach indicates that the ransomware group could claim possession and risk exposure of 250 GB worth of sensitive information (including driver's license, social security number, and medical history of employees). Conti ransomware has previously targeted multiple organizations in the United States and Canada. Prominent past victims include OmniTRAX, University of Vermont Medical Center, Saskatchewan Polytechnic University, Taiwanese industrial manufacturer Advantech, the US criminal court, Canadian technology company Sangoma, and many more. Conti is also suspected of being a potential successor to the Ryuk ransomware group. Therefore, Conti could likely be seen again, targeting a wide range of industry sectors worldwide in 2022.

Europe Constellation

D1 – Actioning 2022: Regional Themes and Trends

The section below provides key regional themes and trends observed throughout 2021. These insights provide valuable insights to organizations on what to expect from a geopolitical and cyberthreat perspective in 2022.

Europe Will Continue to be Targeted by Nation-State Threat Groups

In 2021, threat actors originating from Russia had caused almost 50% of the total cyberattacks in the European region. In addition, North Korean, Romanian, and Belarus threat actors have also actively targeted the region.

Among the wide array of hostile entities, Russia poses unique threats to the Euro-American alliance. Central and Eastern European governments are facing increasing pressure from the threat groups of this hostile nation, disrupting and exploiting European cyberspace continuously. Russian threat groups such as Dmitry Badin, Sodin, REvil, and Primitive Bear are responsible for various cyberattacks in Europe.

Germany, France, and UK to Suffer the Most from the Cyberattacks

Germany (21.6%) and France (18.3%) are the top-most two countries affected most by the cyberattacks in Europe in 2021. The other most impacted countries include the Netherlands (13.3%), the UK (13%), and Ireland (10%). The German General Election of 2021 has faced several state-sponsored cyberattacks. Through spear-phishing campaigns, threat groups have targeted several political leaders, activists, and media. Most of these threat actors have been suspected to be based in Russia. The ideological difference between the European democracies and Russia results in these cyberattacks backed by Russia to manipulate the core democratic functionality of these countries as claimed by the European Union. With many important elections being held in the region in 2022, there is a huge possibility that a series of large-scale cyberattacks will hit Europe soon.

RATs will be the Next Popular Weapon for the Threat Actors

The RATs (Remote Access Trojan) have been used most frequently by the threat groups to conduct their malicious activities. Around 26% of the known tools used by the threat actors in 2021 are some RATs, followed by the Cobalt Strike (19%). In addition, PowerShell scripts (12.5%) have also been used frequently to carry out attacks.

RAT is a malicious example of remote access technology, a form of malware allowing a threat actor to control a device remotely. The most lethal part of the RATs is that they can mimic above-board remote access programs without revealing themselves. Upon being connected to a system, the attackers can acquire login credentials and examine the local files and other personal information. It can also use the connection to download without being noticed by the users. RATs are frequently utilized in spear-phishing campaigns to carry out advanced persistent threat (APT) attacks.

On the other hand, the threat actors have managed to crack the cobalt strike to implant beacons in the target systems. Using beacons, threat actors can do lateral movement in the system and possess access to breached servers to exfiltrate data or deploy further malware payloads. In addition, the PowerShell script has also become a popular tool for threat actors to access the targets remotely.

Telecommunication and Technology Sectors Will be the Prime Targets

The threat actors targeted the telecommunication and technology sector (26%) most during 2021. Other industries affected by cyberattacks include the government and public sector (21%), financial services (14.8%), and the healthcare sector (11.4%).

In recent years, as technology has evolved and the threat landscape has changed, there has been a soaring rise in cyberattacks on the telecommunication sector worldwide. And because this sector is a gateway to critical infrastructure in each region, the effect of cyber operations conducted on it is extensive and significant. And although breaching the core infrastructure of the telecommunication sector is a difficult task, the evolution of highly skilled advanced persistent threat (APT) groups in Europe has turned it into an easy target. In the first half of 2021, the Flubot banking Trojan was utilized frequently to target the sector in Europe. Vulnerabilities in the infrastructure and customer devices are triggering these attacks. Also, telecom operators have been concerned with phishing campaigns, social engineering methods, and malware deployment in remote devices.

The political interference of foreign players in the region is also triggering attacks against the government and public sector. Furthermore, the upcoming significant geopolitical scenarios and the elections in Europe might trigger a series of politically motivated cyberattacks in the region.

Spear-phishing will be the Most Popular Method in the Future

In 2021, more than a quarter of the methods used to conduct cyber-crimes were done by spear-phishing. In addition, ransomware (24%) was also widely used for exploitation.
Spear-phishing is the practice of targeting any specific individual within an organization to distribute malware or exfiltrate data from the individual's system. Here, the threat actors deceive the targets via emails coming from trusted accounts, malicious attachments, or links to deceitful websites. For example, during the German General Election in 2021, a spear-phishing campaign was launched against the members of parliament, government officials, and civil society in an attempt to dilute democratic values. These kinds of campaigns against elections can lead to the dissolution of integrity and transparency of the voters.

D2 – Geopolitical Landscape

Here are some of the significant geopolitical developments observed in the European constellation in 2021.

UK's Plan to Diverge from GDPR after Brexit

Since the dawn of Brexit, there has been a constant occurrence of issues related to cybersecurity decision-making, information-sharing, and policing between the European Union (EU) and the United Kingdom (UK). Although the UK's cybersecurity landscape is mostly independent of the EU constituencies, a lot of EU cybersecurity measures will still remain under the UK's fiat. Post-Brexit, the UK government plans to segregate its data protection regime from that of the EU by diverging from the General Data Protection Regulation (GDPR). This reform can help streamline data flow by reorienting international trade outside the region. This diversion aims to simplify international data transfer and represent the UK as a digital business hub. However, the UK needs to be careful about the EU-UK adequacy decision granted to it by the EU, allowing free flow of personal data from the EU to the UK with the least paperwork. The divergence from GDPR might disrupt the adequacy decision, which can terminate the grant. There has been a strong negative argument that these reforms can take away the protections guaranteed to an individual over fundamental

rights and freedom. These amendments can compromise the principle of accountability, which is the core part of the EU's data protection regime and GDPR. But the goal of this divergence can be achieved by equivalent data protection laws, accompanied by barrierless international cooperation and economic growth led by innovation.

Europe Elections 2022: The Russian Fear Will Impact the EU

In September 2021, ahead of the German General Election, the European Union voiced its concerns by warning about the growing number of Russian cyberattacks conducted against its 27 member countries. And although Russia has consistently denied all of the allegations brought up against it, the EU has frequently called out Moscow's malicious pre-election cyber activities, collectively designated as "Ghostwriters." From the cyberattacks and misinformation campaigns performed by the Russian threat groups during the German General Election, it can be expected that questions will be raised again about the fair conduct of upcoming major elections in Europe. The 2022 European geopolitics will be marked by many important elections, such as the parliamentary elections of Sweden, Hungary, Latvia, Bosnia, and Slovenia and the presidential elections of France, Germany, and Austria. Any cyberattacks conducted against politicians, government entities, civil society, and media personnel of the member states will pose a significant threat to the democratic values, principles, and core functioning of the democracies in the region.

Restricting the US from Accessing EU Data: A Step Leading to Strategic Autonomy

In a changing geopolitical regime, it has been observed that transborder data flow is gaining importance in terms of the socio-economic-political landscape. Federal governments are adopting stricter regulating norms for cross-border data protection. There has been constant pressure on the European Union from France to frame a set of rules restricting the United States from accessing the data in the EU. According to the US Clarifying Lawful Overseas Use of Data Act (aka CLOUD Act), the US Government, with a proper warrant, can compel US companies to disclose the data present in their servers, even if the data is stored in Europe. This restricts the digitization of the European public sectors because of the fears of US surveillance scandals and spying as the data stored in the US cloud service providers becomes vulnerable. There is a high possibility of a breach under various circumstances. Although the EU cybersecurity authorities are developing rules to impose stricter regulations and data protection policies on US cloud service providers, there will still be a need to bring more stringent laws by the EU lawmakers to counter the CLOUD Act. This will help the EU member states to attain strategic autonomy by diminishing their dependence on US cloud services.

A Cyberattack on One Nordic Country Will be an Attack on All Nordic Countries

In the annual Nordic Council meeting held in Copenhagen in November 2021, all eight member states of the council (Denmark, Finland, Iceland, Norway, Sweden, the Faroe Islands, Greenland, and Aland) agreed on a mutual defense strategy against cyberattacks in the region. Because most of these countries are among the most digitized countries in the world, they are becoming more prone to cyberthreats. The recent cyberattacks on the Finnish Parliament and the Norwegian Parliament email system are proof of their vulnerability. Furthermore, state-sponsored cybercrimes from China and Russia will pose a bigger threat in Nordic cyberspace. A cyberattack on any of the Nordic parliaments will be considered an attack on all, and the Nordic democracy, in the future.

The Product Security and Telecommunications Bill: Reinforcing IoT Security of the UK

The introduction of the Product Security and Telecommunications Bill (PSIT Bill) in the UK parliament will strengthen the Internet of Things (IoT) infrastructure against the intrusion of the threat actors, paving the way for new security regulations on connectable consumer products. The connectable consumer products are IoT-based, internet-connected devices. Data from millions of users can be compromised because of the massive use of these insecure consumer connectable devices. The new PSIT Bill includes stricter regulating guidelines and security requirements for these products. The regulations include:

- Banning default passwords.
- Deploying vulnerability disclosure policies for the products.
- Transparent monitoring of security updates.

The manufacturers, importers, and distributors of these products will be bound to follow the regulations. Organizations failing to meet the desired requirements will be fined up to £10 million or four percent of their global turnover. This bill resembles similar bills passed in the EU, Australia, and the US. After being passed, this bill will play a big role in strengthening the security of smart products.

D3 – Cyberthreat Regional Landscape

Sandworm Team

Industries Targeted	Continents Targeted
Energy, Public Sector, Utility, and Services	Poland, Ukraine, France, Georgia

Sandworm Team is also known as: Telebots, Quedagh, Iron Viking, ELECTRUM, Hades, Frozen Barents, SANDFISH

Sandworm team is a highly capable and sophisticated Russia-based advanced persistent threat (APT) group believed to be linked to the General Staff of Russia's Armed Forces. First seen in 2009, the group is historically known to target Energy, Government, Education, and Telecommunication sectors. The APT group leverages customized and obfuscated malware and is also known to conduct sophisticated phishing and well-planned spear-phishing attacks. In addition to these attacks, the threat actor is also observed to use zero-day exploits such as ETERNALBLUE, ETERNALROMANCE, CVE-2014-4114, and CVE-2019-10149. The threat actor has used malware such as BlackEnergy v2 and v3, GreyEnergy, GCat, Telegram-based RAT, DropBear SSH Server, and EmPyre in the past and has capabilities to perform supply-chain attacks. The group used public records and other open-source intelligence for initial reconnaissance of the target victims, which sometimes might also be followed by scanning public-facing server infrastructure to find any vulnerabilities. The group is also observed to deliver payloads using spear-phishing emails and supply-chain attacks by compromising software to abuse the update functionality of the application to deliver malicious payloads. The threat actor group has also leveraged web compromise attacks to deliver malicious payloads to victims. The use of telegram and VPS hosting, usually configured to run as a tor exit node, demonstrates the sophistication of the techniques used by the threat actor group to evade detection.

The effect of the active espionage campaigns of the Sandworm team can be witnessed globally, but specifically targeting countries including the United States, Ukraine, South Korea, and France. One of the campaigns by the threat actor group in France targeted Centreon monitoring software using the CentOS operating system exposed to the public internet. This attack resulted in a breach of several French organizations. It had a major effect on information technology providers, including web-hosting providers, in a four-year cyber espionage campaign. The group is also accused of conducting cyber campaigns against the 2020 Tokyo Olympics and affecting the French and US presidential elections in 2017 and 2016, respectively.

Ghostwriter

Industries Targeted	Continents Targeted
Defense, Services, Public Sector	France, Germany, Ireland, Poland, Switzerland

Equation group is known for its sophisticated global computer attack. It is also among the handful Ghostwriter is a cyber campaign that mainly targets organizations in Lithuania, Latvia, and Poland. The campaign promotes narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe. In addition, the campaign leveraged compromised social media accounts of Polish officials to publish content related to political affairs and create political disruption in Poland. Other activities of this campaign involve website compromises and spoofed emails. A few reports stated that social media accounts were obtained using compromised email accounts. The Ghostwriter campaign also targeted German MPs and, in the past, this group has compromised multiple legitimate websites and has uploaded fabricated content. Researchers allegedly suspect that the group belongs to the Russian state. According to the reports, the group is still active and is an ongoing threat to individuals in government and politics. Considering the upcoming elections in Germany, France, Slovenia, and the United Kingdom, every individual associated with these elections should be mindful and secure all accounts on the internet.

UNC1151

Industries Targeted	Continents Targeted
Defense, Education, Government, Media	France, Germany, Ireland, Poland, Switzerland

UNC1151 group has been active since 2017 and it carries similar activities as the Ghostwriter campaign. According to the reports, UNC1151 is suspected of a state-sponsored cyberespionage actor that heavily performs credential harvesting and multiple malware campaigns. Also, UNC1151 expanded its activity in 2021 and mainly committed credential theft to target German politicians. The UNC1151 campaign might continue

to target individuals associated with European government and media entities, as seen in the past. The technique it might use to spread the malware is through spear-phishing. From past activities, it is observed that UNC1151 uses long subdomains to make phishing domains look legitimate and this group has also targeted thousands of personal and corporate accounts since its rise. One of the incidents was a spear-phishing email sent to a Ukrainian journalist using a spoofed "ukr.net" address. The email was sent via the SMTP2GO service and Gophish framework, which contained a malicious link that led to a spoofed login page that was designed to steal credentials.

Ritchie-Werld & BartSimpson

Industries Targeted	Continents Targeted
Unknown	Unknown

Unpopular individual threat actors also have a more significant role in compromises that occurred in this region. For example, a Russian-speaking threat actor operating under the alias "Ritchie-Werld" offered RDP access to a professional account of a Germany-based stock trader. The actor specified that access has all the administrative privileges and mentioned that Meta Trader and Robo Forex applications are being used. Another threat actor operating under the alias "BartSimpson" advertised the sale of RDP access to the network of a major EU-based manufacturer of software POS terminals. The threat actor also claimed that the compromised network had a revenue of 50M and featured over 450 hosts. Considering the advancements in technology and most of the malware tools being readily available for the threat actors, we might see an increase in the contribution from these individual threat actors to the European threat landscape in the future.

Tortilla

Industries Targeted	Continents Targeted
Unknown	Finland, Germany, UK

The threat actor campaign referred to as Tortilla (based on the filenames seen in the campaign) was infecting organizations in Germany and Finland using Babuk ransomware. In the initial days, the threat actors were using PowerShell-based Netcat clone powercat, which provided the threat actors access to Windows machines in the victim's environment. The campaign was observed targeting Microsoft Exchange servers and was trying to exploit the PowerShell vulnerability to deploy the Babuk ransomware.

The infection starts with deploying a downloader that is in a DLL format on the victim's server. This downloader is a modified version of EfsPotato and is designed to target proxy shell and PetitPotam vulnerabilities. Additionally, the downloader connects with the threat actor's infrastructure to download more tools. The downloader uses a PowerShell command to execute AMSI evade endpoint detection. The

download server on the threat actor's side is hosted using malicious domains fbi[.]fund and xxxs[.]info. In the future, the threat actor might still target organizations with vulnerable servers, so organizations should regularly update their servers. Security controls should constantly look for suspicious service terminations, abnormal high read and write rates for the server drives, shadow copies, and system configuration changes.

FIN11

Industries Targeted	Continents Targeted
Retail, Finance, Services, Manufacturing, Public Sector, Healthcare, Markets	Austria, Canada, Germany, Netherlands, Spain, UK

FIN11 is also known as: TEMP.Warlock

FIN11 was first seen in 2016 and, in the initial years, the threat actor group mainly focused on the financial, retail, and restaurant sectors. Later, the FIN11 group broadened its target scope to other industries such as education, government, energy, and pharmaceuticals. The threat actor group mainly relies on phishing campaigns to gain initial access to the victim networks and later it distributes Clop ransomware. Researchers suspect that the group is based out of the Commonwealth of Independent States, since the files observed were in Russian and there was also a significant decline in the group's activity during Russian holidays. Going forward, the threat actor group might continue to use malicious Microsoft Office files to deliver lures, including invoices, sales orders, and bank statements, as observed in the past.

D4 – Industry Threat Landscape

Severity Score for Cyber Events Grouped by Industry
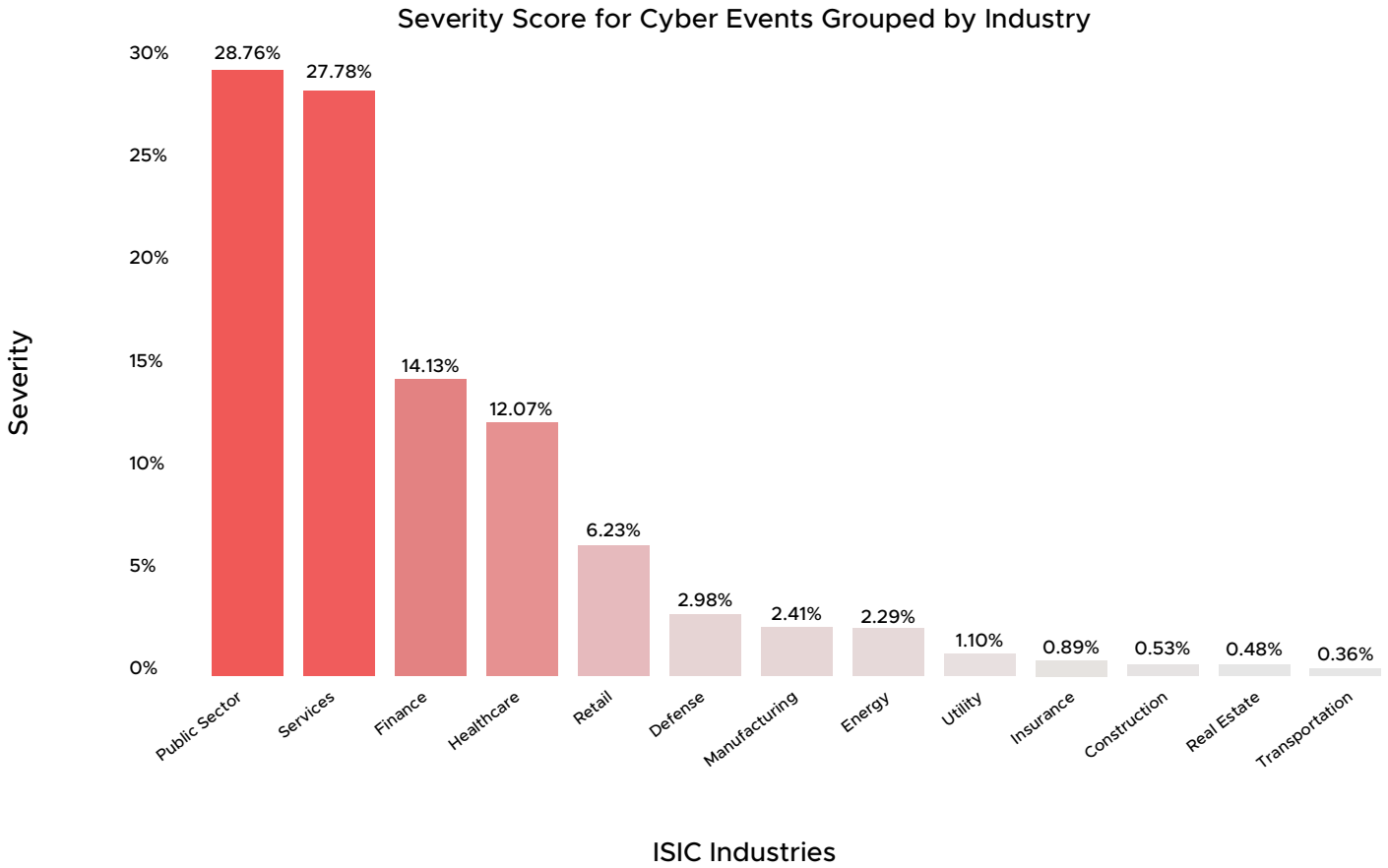
Figure 7 - Industry threat landscape in Europe

Telecommunication, Education, Media Are the Most Affected Services

The services sector exceeds other affected industries by cyber incidents affecting the Europe region in 2021. Around a fourth (23.8%) of all cyberattacks that took place within the region targeted the service sector, of which telecommunications makes up the majority of the affected regions, followed by education and media. While the triggers of most of these attacks remain unknown, vulnerability in infrastructure and well-known applications seem to be the trigger for a lot of events. Furthermore, almost all cyberattacks were financially motivated. Most of the threat actors responsible remain unknown; however, BlackMatter, Sprite Spider, and Hafnium were observed to have targeted the telecommunication sector.

Public Sector in Europe Targeted for Financial Gain and Cyber-espionage

Cyberattacks against public sectors marks the second-most affected industry in Europe in 2021. Approximately 22.4% of the total campaigns conducted in 2021 were reported to target the public sector. Over 78.7% of the cyberattacks were motivated by financial gain and around 6% were cyber-espionage campaigns. While most methods of attack remain unknown, some of those utilized include ransomware deployment (15%), data exfiltration (6%), spear phishing (6%), and credential harvesting (3%). Some of the known threat actors targeting the public sector are REvil, Armagedon, Uknown, APT29, and APT31.

Ransomware Is the Most Common Method of Deployment against Multiple Industries

Financially motivated threat actors target various industries by deploying ransomware in the compromised network infrastructure. The affected industries include services (31.7%), healthcare (12.2%), public sector (12.2%), retail (4.9%), finance (4.9%), and manufacturing (2.4%), among others. While the trigger remains predominantly unknown, compromise due to a vulnerability makes up 34% of the cyberattacks. The known threat groups deploying ransomware include Conti, REvil, BlackMatter, Sprite Spider, TA544, and Sload, most of which were operating within Russia.

The Services Sector Is Constantly Exploited by Financially Motivated Threat Actors

Financial gain is the greatest motivation for the threat actor groups targeting the services sector. Over 78% of the cyberattacks conducted within Europe in 2021 were financially motivated, of which 25.8% of the threat actors targeted the services sector, 19% targeted the public sector, 11.8% targeted finance, 8% targeted healthcare, and 5.9% targeted retail, among others. Hafnium, Sprite Spider, BlackMatter, and Poison Carp are the top threat actors to target the services sector, mainly through ransomware deployment. Significant incidents of services organizations targeted in cyberattacks include BlackMatter ransomware hitting medical technology giant Olympus, Evil Eye campaign targeting Uyghurs on Facebook, and Spanish telecom giant MasMovil being hit by the REvil ransomware gang.

D5 – Key Lessons from the Most Impactful 2021 Attacks
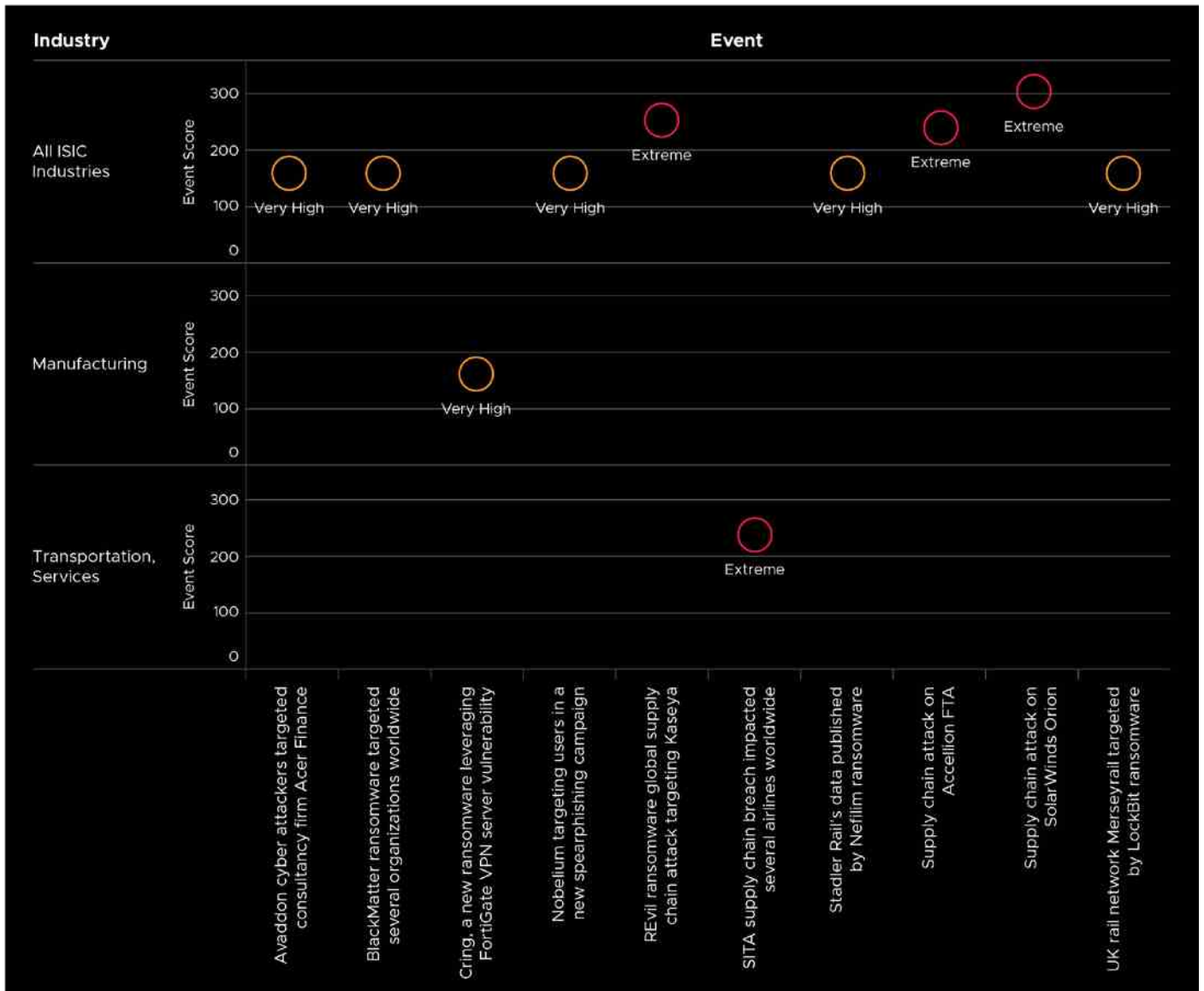
Figure 8 - Top 10 events in Europe

#1 Supply-chain attack on SolarWinds Orion

Severity: Extreme   **Industries Targeted:** All ISIC Industries

Quick Recap: On December 13, 2020, cybersecurity firm FireEye published a report on details of a sophisticated and widespread supply-chain attack targeting SolarWinds Orion software. FireEye is tracking this threat actor as UNC2452—also known as Nobelium and Dark Halo. Orion is a scalable infrastructure monitoring and management platform used by a wide variety of industries. This cyber-espionage campaign commenced by implementing a Trojan malware in the SolarWinds Orion software update, which distributed a malware named SUNBURST.

On March 18, 2021, a new report from Prodaft (a Swiss cybersecurity firm) disclosed another highly technical and sophisticated advanced persistent threat (APT) group dubbed SilverFish. This threat group is suspected of having conducted three waves of attacks. Based on the report, SilverFish has commenced more than 4,720 attacks on prominent private and public organizations while primarily focused on European countries and the United States. Reportedly, the threat actor had targeted a wide range of industries such as the government and public sector, defense, manufacturing, and professional services, while maintaining specific interest in critical infrastructure organizations.

Key Impact: The SolarWinds campaign appears to be primarily focused on espionage. Therefore, the victims should expect malicious activities in their environment, including but not limited to sensitive data exfiltration, file execution, and forensic and anti-virus services termination. Additionally, the threat actors have been observed to compromise email exchange servers. The current list of alleged victims related to this campaign includes victims from government, consulting, technology, telecom, and extractive entities in North America, Europe, Asia, and the Middle East. It is anticipated that there are additional victims in other countries.

Future Considerations: The SolarWinds supply-chain attack has gained significant attraction, as several press reports have focused on identifying the threat actors involved. Additionally, the US government and the cyber community provided detailed information on how the campaign was potentially carried out, along with the malware used. With the aid of MITRE's ATT&CK team, the tactics, techniques, and procedures were mapped to UNC2452.

While not as significant as the SolarWinds cyber incident, the threat actor group remains active, targeting the technology sector. UNC2452 is expected to make an appearance in 2022, possibly leveraging vulnerabilities in the outdated software application to gain unauthorized access.

#2 REvil ransomware global supply-chain attack targeting Kaseya

Severity: Extreme   **Industries Targeted:** All ISIC Industries

Quick Recap: On July 2, 2021, Kaseya, a prominent software solutions provider, announced that it was the victim of a cybersecurity incident. The incident has been attributed to the threat actors operating the REvil (also known as Sodinokibi or Sodin) ransomware group and alleged to be of Russian origin. The attack is believed to have compromised Kaseya's VSA remote IT monitoring and management solution. As a result, at least 1500 organizations were affected. Some prominent affected companies were based in the UK, the Netherlands, Germany, Sweden, Norway, and Italy.

Security researchers stated that Kaseya was initially breached due to a zero-day vulnerability tracked as 'CVE-2021-30116' in its systems, which was already reported to Kaseya. When it was breached, it was working on the patch, resulting in a compromise of its software updates. Additionally, victims of the supply-chain attack were compromised through a Kaseya software update, in which the REvil ransomware infected them.

Impact: REvil demanded $70 million in Bitcoin (BTC) to provide the decryptor for all systems locked during the Kaseya supply-chain attack. One of the affected companies, Coop (a grocery retailer chain in Sweden), was forced to shut down at least 800 stores on July 3, 2021, following the supply-chain attack.

Future Considerations: This attack was one of the most prominent supply-chain attacks of 2021. A supply-chain attack is more cost-effective for threat actors as compromising a single vendor could result in a breach in multiple organizations. Furthermore, the increase in the number of zero-day exploits could also aid the threat actors in supply-chain attacks.

#3 Supply chain attack on Accellion FTA impacted several organizations

Severity: Extreme

Industries Targeted: All ISIC Industries

Quick Recap: In December 2020, Accellion discovered several critical and zero-day vulnerabilities (tracked as CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104) existing in the organization's File Transfer Appliance (FTA) product. FTA is a 20-year-old legacy software designed to allow organizations to securely transfer large files.

Shell, Royal Dutch Shell plc, disclosed unauthorized access to the organizations' file-sharing system due to the zero-day vulnerabilities in Accellion FTA software. Shell is one of the most prominent organizations in the petrochemical and energy industries, with an active presence in more than 70 countries. Shell further stated that there is no evidence suggesting that this attack impacted the organization's core IT systems, as Accellion FTA was reportedly isolated from the rest of Shell's digital infrastructure. Based on the statement, the exfiltrated data includes personal data and data from Shell companies and other stakeholders. The organization has been in the process of contacting the impacted parties. Shell has not provided any further updates on the incident.

Impact: Accellion has provided software patches for all the known existing vulnerabilities and is working closely with impacted organizations on mitigation efforts. Accellion has stated that 300 customers use FTA. Less than 100 of these were impacted by the supply-chain attack and less than 25 appear to have suffered significant data theft. Due to the nature of the supply-chain attack, the details are still emerging. Organizations that specifically use Accellion's FTA software or have third-party vendors using the software as their file-sharing service could also be affected.

Future Considerations: Critical vulnerabilities tend to attract attention from ransomware operators because these exploits could be used to gain a foothold within an organization's network for malicious activities. Additionally, ransomware operators were actively involved in cyber incidents throughout 2021. As a result, the ransomware group is expected to continue targeting a wide variety of industries worldwide in 2022.

#4 SITA supply chain breach impacted several airlines worldwide

Severity: Extreme

Industries Targeted: Transportation, Services

Quick Recap: A supply-chain attack targeting SITA, a global IT organization servicing 90% of the airline industry, resulted in data breaches across multiple airlines. On March 04, 2021, SITA confirmed that customer data was stolen in a breach of its Passenger Service System (PSS). The PSS contains information related to ticket transactions, boarding, and rewards/loyalty program members. Notably, frequent flyer programs have been used as an attack vector to spread quickly across many airlines. One of the notable frequent flyer membership programs affected was Star Alliance. Air India, Lufthansa, Air New Zealand, Singapore Airlines, Scandinavian Airlines, Cathay Pacific, Jeju Air, Malaysia Airlines, and Finnair were some of the major airlines affected. Security researchers have attributed the SITA supply-chain attack to the Chinese state-sponsored threat actor group APT41 (also known as Winnti Umbrella, Wicker Spider, Panda, and Barium). The campaign was dubbed "ColunmTK."

Impact: The SITA breach impacted several airlines and information surrounding frequent flyer programs. The threat actors leveraged Mimikatz and hash dump to obtain victims' credentials. Furthermore, they have used DNS tunneling to exfiltrate data.

Future Considerations: Following the SolarWinds Orion, Accellion FTA, Microsoft Exchange, and Codecov supply-chain attacks, the attack on SITA PSS ranks among the top five highly publicized supply-chain attacks, with global ramifications. A supply-chain attack is more cost-effective for threat actors because compromising a single vendor could result in a breach in multiple organizations. Furthermore, the increase in the number of zero-day exploits could also aid the threat actors in supply-chain attacks.

#5 Cring, a new ransomware leveraging FortiGate VPN server vulnerability

Severity: Very High

Industries Targeted: Manufacturing

Quick Recap: Since at least January 2021, it is suspected that threat actors have been targeting a FortiGate VPN vulnerability (tracked as CVE-2018-13379) to deploy a new variant of ransomware named Cring, also known as Vjiszy1lo, Ghost, and Phantom. This ransomware was initially observed in January 2021 while targeting organizations by exploiting vulnerable FortiGate VPN servers for initial access. Victims of these ransomware attacks include industrial enterprises in European countries, primarily in manufacturing facilities in Italy. In one case, the ransomware attack resulted in temporarily shutting down production at a facility, due to the servers' encryption.

Impact: Attacks by the Cring ransomware have been demonstrated to cause significant disruption to manufacturing facilities. Recently, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint security advisory stating that the threat actors are continuing to exploit Fortinet vulnerabilities to gain initial access to government and corporate networks, which they plan to attack in a future intrusion.

Future Considerations: There is no confirmation of any specific threat actor group utilizing this ransomware. However, the threat actors allegedly performed test connections to the VPN Gateway to identify vulnerable versions of the software used on the device. Cring ransomware activity remained low for the rest of 2021 and is likely to be the case in 2022.

#6 Nobelium targeting users in a new spear-phishing campaign

Severity: Very High

Industries Targeted: All ISIC Industries

Quick Recap: Security researchers have recently uncovered a spear-phishing campaign targeting organizations worldwide. It is believed that the threat actors responsible for the SolarWinds supply-chain attack are behind this recent phishing campaign. The threat actors are referred to as the Nobelium group, also known as APT29, Cozy Bear, CozyDuke, The Dukes, and YTTRIUM. The campaign commenced in January 2021 and evolved through several waves. On May 25, 2021, the threat actors leveraged Constant Contact to distribute malicious URLs to organizations worldwide. Constant Contact is a legitimate mass-mailing service used for email marketing. The Nobelium group used a compromised Constant Contact account to masquerade as USAID.

On June 25, 2021, Microsoft announced a compromise in their customer service systems and attributed this activity to the Nobelium group. Based on available reports, it was observed that the threat actors leveraged password spraying and brute-force. According to the Microsoft Threat Intelligence Center, the attack was mainly unsuccessful and most of the targeted users were not affected. However, all affected customers are being contacted by Microsoft. The organization claims this campaign primarily focused on government agencies, think tanks, IT companies, non-governmental organizations, and financial services. Additionally, 45% of the attacks were targeted in the United Kingdom, Germany, Canada, and the United States.

Impact: Successful deployment of the payloads used in this campaign enabled the Nobelium group to perform data exfiltration, lateral movement, and deliver additional payloads in the target system.

Future Considerations: The Nobelium group was also allegedly behind the SolarWinds supply-chain attack, which affected numerous organizations spanning several industry verticals. Additionally, in the recent phishing campaign, the threat actors leveraged a legitimate mass-mailing service and employed unique infrastructure for every target, enabling them to remain undetected for a longer period.

Considering their activity in 2021, it is expected that Nobelium will make an appearance in 2022.

#7 Avaddon cyberattackers targeted consultancy firm Acer Finance

Severity: Very High

Industries Targeted: All ISIC Industries

Quick Recap: On May 16, 2021, the threat group operating the Avaddon ransomware reportedly compromised the France-based financial consultancy firm Acer Finance. The threat actors threatened Acer Finance with publishing the exfiltrated documents from the organization if they didn't cooperate within ten days. Exfiltrated data is alleged to contain confidential information on clients and employees, including banking, personal correspondence, agreements, forms of payment, licenses, as well as other documents. Similar to other corporations affected by the Avaddon ransomware, the threat actor threatened to target Acer Finance with a DDoS attack if they didn't comply with payment demands.

Impact: The threat actors ensure that there is no way of decrypting data without their decryptor. Furthermore, failure to pay the ransom would result in a DDoS attack and publishing exfiltrated data. The Avaddon ransomware operators supposedly exfiltrated confidential data on clients and employees.

Future Considerations: Avaddon is a ransomware operating in a Ransomware-as-a-Service model and was initially discovered in June 2020. The threat group targets Windows systems and is generally observed to spread via phishing campaigns.

However, on June 11, 2021, Avaddon had allegedly shut down its operation, likely due to the increased pressure by police agencies and United States President Biden's plan to deliberate cyberattacks along with Russian President Vladimir Putin. To support the shutdown claim, Avaddon published a total of 2,934 decryption keys to their victims. Additionally, Avaddon's TOR website was inaccessible, indicating that the threat group likely shut down operations.

While Avaddon supposedly shut down, the operators behind the ransomware could possibly return under a different name. In 2022, Avaddon could still be a threat if they were to return.

#8 BlackMatter ransomware targeted several organizations worldwide

Severity: Very High | **Industries Targeted:** All ISIC Industries

Quick Recap: The BlackMatter ransomware is a Ransomware-as-a-Service tool that aids developers of this ransomware to profit from its affiliates that deploy it against victims. BlackMatter is possibly a re-brand of DarkSide, since it emerged following the disappearance of DarkSide ransomware. This threat group has impacted organizations from the US, UK, Canada, Australia, India, Brazil, Chile, and Thailand. The group has demanded ransom ranging from $80,000 to $15,000,000 in Bitcoin and Monero. On November 1, 2021, the group announced that they would be shutting down their operation.

Impact: The threat group BlackMatter, which was active for four months, has targeted multiple organizations, including the technology company Olympus, which resulted in the shutdown of the company's operation in Europe, Middle East, and Africa.

Future Considerations: The BlackMatter group has communicated instructions for the affiliates to obtain decryption keys for continued extortion of the existing victims. Affiliates allegedly have been redirecting their victims to the LockBit Ransomware TOR page for negotiations. With BlackMatter ransomware ceasing operations, this places LockBit as one of the most powerful and notorious active ransomware operations to date.

#9 UK rail network Merseyrail targeted by LockBit ransomware

Severity: Very High | **Industries Targeted:** All ISIC Industries

Quick Recap: In April 2021, Merseyrail suffered a LockBit ransomware attack on its infrastructure. Merseyrail is a railway network that provides train services to Liverpool, England. In a unique approach, the threat actors operating the LockBit ransomware compromised the Office 365 email account of the organization's managing partner to send a series of emails. Emails titled "LockBit Ransomware Attack and Data Theft" pretended to be sent from the manager to technology news agencies, various U.K. newspapers, and the staff to inform them of the incident and the fact that employee and customer data had been exfiltrated due to this attack. The email also contained an image showing a staff member's personal information. This is the first prominent instance where a threat actor publicly uses the victim's email service to broadcast the incident news.

Impact: LockBit is a relatively new ransomware, but multiple indicators hint that the operators behind it are very devoted to expanding and increasing their outreach. Releasing multiple versions indicates that the threat actors intend to keep up with evolving security controls.

Future Considerations: LockBit ransomware has evolved continuously, adding sophistication to its tactics. Since July 2021, there has been a consistent increase in LockBit 2.0 (enhanced version of LockBit) ransomware attacks worldwide. The latest version supplements a built-in information-stealing function called 'StealBit' and includes a feature that automatically encrypts devices across Windows domains by leveraging Active Directory group policies. The ransomware group targeted some high-profile targets in 2021 and this trend will likely continue.

#10 Stadler Rail's data published by Nefilim ransomware operators on the Dark Web

Severity: Very High	**Industries Targeted:** All ISIC Industries

Quick Recap: On February 11, 2021, Nefilim ransomware operators published exfiltrated information from Stadler Rail on their Dark Web website. The published information appears to be the continuation of the exfiltrated data in an attack conducted in May 2020. Stadler Rail is a Swiss manufacturer and supplier primarily of passenger rail cars and locomotives, including high-speed rail operations.

On May 7, 2020, Stadler Rail reported a cyber incident targeting the organization's IT network, which was suspected of resulting in a data leak. On May 29, 2020, it was reported that the threat actors who stole the data from Stadler Rail had demanded payment of a ransom of 6 million USD in Bitcoin.

Impact: The ransomware group demanded a ransom payment of 6 million USD in Bitcoin after encrypting the data of the affected organization. The threat actors have also threatened to publish the exfiltrated data in their Dark Web leak site.

Future Considerations: The threat actors operating Nefilim have a history of threatening to publish exfiltrated data in the event of a futile negotiation process. In the past, they have committed to publishing sensitive information on their website on the Dark Web. Although the group does not appear to follow a trend in targeting any specific industry, it could pose a significant threat in the coming days.

Asia Pacific Constellation

E1 – Actioning 2022: Regional Themes and Trends

The section below provides key regional themes and trends observed throughout 2021. These insights provide valuable insights to organizations on what to expect from a geopolitical and cyberthreat perspective in 2022.

Japan Will be the Victim of Maximum Cyberattacks in the Indo-Pacific Region

One-fifth of the total cyberattacks conducted in the region in 2021 were against Japanese entities (19.8%). India (14.3%), South Korea (11%), and Taiwan (9.9%) were among the countries affected most by cyberattacks in the Asia-Pacific region.

Many cyber operations targeting Japanese entities have been attributed to advanced persistent threat (APT) groups that have allegedly originated from China and North Korea. Most of the known cyber operations impacting Japan focus on espionage activities such as sensitive data breaches and intellectual property theft. Although the number of cyber campaigns targeting the Tokyo Olympics was huge, not a single large-scale attack was reported, due to the preparedness of the organizers. With its strong international cooperation and technological advancements, Japan has successfully restricted all types of cyber operations that could cause large-scale operational damage to Japanese organizations.

In addition, the long-standing border dispute, growing bilateral ties with Taiwan, and active involvement within the QUAD group are making India a highly targeted victim of the state-sponsored cyber campaigns in the Indo-Pacific region.

The Public Sector Will be the Most Affected Sector in the Future

In 2021, the public sector (27.4%) was impacted the most by cyberattacks in the Asia-Pacific region, followed by the telecommunication sector (17.8%), the transportation sector (8.2%), and the healthcare sector (4.3%).

The growing geopolitical tensions are the main reason behind the public sector being targeted. Most of the cyberattacks conducted in the region are basically for cyber espionage. Confidential, sensitive, or business-critical data is often most targeted in cyber-espionage crusades, as threat actors seek out information that could affect national security, political positioning, and competitive economic advantage. The public sector holds the most sensitive and valuable information related to each nation. Hence, the state-backed threat groups often target the public sector to achieve larger political goals. In addition to this, the large-scale targeting of the telecommunication and transportation sector shows the upcoming threat of disrupting the critical supply-chains in the region by cybercrime groups.

Espionage Is Likely to be the Biggest Motivation for the Threat Groups

Around one-third of the total cyberattacks conducted in the Asia-Pacific region in 2021 were meant for cyber espionage, followed by financial gain. Vulnerability in infrastructures and well-known applications (43.6%) and political disputes (26.4%) triggered the most cyber operations in 2021.

Almost half of the global cyber-espionage campaigns carried out in the Asia-Pacific region are due to geopolitical rivalries in this region. Government entities are being targeted by the threat actors in these espionage campaigns. Most of these incidents are state sponsored. The espionage threat actors include

nation-states, business competitors, and organized criminal groups. Critical private enterprises are also allegedly targeted in various cyber-espionage crusades.

Vulnerabilities in critical infrastructures and well-known applications enable threat groups to conduct their malicious activities with ease to achieve their financial gain. Weakly-secured and outdated infrastructure poses an easy target for the threat actors. Political clashes and disputes also trigger a lot of cyberthreats.

Data Exfiltration Will be the Most Frequently Used Method of Cyberattacks

In more than 24% of the cyberattacks in 2021, threat actors chose to exfiltrate sensitive data from their victims' networks. In addition, spear-phishing and social engineering campaigns were actively used to gain initial access to enterprise networks during cyber operations.

Organizations face data loss from electronic or physical documents or databases, which both insiders and outside elements orchestrate. The Asia-Pacific region has witnessed the highest number of data exfiltration instances in the last few years, followed by North America. 60% of the data exfiltration practices are attained by electronic medium via various web protocols, file transfer, tunneling protocols, or email. Very little exfiltration is conducted physically through USB drives, CDs, DVDs, etc. The expanding cyber-espionage operations in the region and the growing competition among countries to spread global influence triggers the states to follow the data exfiltration method, followed by intelligence gathering against their adversaries. Therefore, organizations need to deploy continuous network monitoring features and data loss prevention (DLP) technologies to mitigate the threat of data exfiltration.

E2 – Geopolitical Landscape

Here are some of the significant geopolitical developments observed in the Asia Pacific constellation in 2021.

Government-backed Chinese Cyber-espionage Groups Are Becoming Stealthier in the Post-COVID World

Threat groups backed by the Chinese government are considered among the most well-resourced and prolific globally. Next to Russia, China has become the most critical threat to the Euro-American alliances over the decade. The telecommunications sector, providers of managed services and broadly used software, and other targets bearing opportunities for intelligence gathering or influence operations have been the prime targets of the Chinese cyber-espionage campaigns. Unlike China's historical smash-and-grab-based cyber-espionage approach, the threat groups follow sophisticated methods such as zero-day exploitation, supply-chain execution, watering-hole attacks, strategic web compromise operations, and custom malware deployment in the post-COVID era. In addition, these state-sponsored threat groups are utilizing social engineering techniques through open-source intelligence (OSINT) followed by spear-phishing to exfiltrate data from the victim's system. PalmerWorm, Axiom (APT72), Elderwood (APT17), Ke3chang (APT15), Deep Panda (APT19), Mustang Panda, menuPass (APT10), and Winnti (APT41) are among the most lethal threat groups with alleged links to the Chinese government. The larger economic goals such as "Made in China 2025" (an industrial policy of the Chinese government to lead China becoming a dominant high-tech manufacturer) and the "Belt and Road Initiative" (a long-term infrastructure development program by China to connect Asia with Africa and Europe for improving regional integration) will be the driving forces to conduct cyber-espionage activities.

New Cybersecurity Strategy Strengthening India's National Security

In the future, Indian cyberspace is likely to see a lot of digital-native, cloud-native, and AI-native platforms, which could become easy targets unless cybersecurity controls are embedded. India's growing digital payments numbers and the lack of cybersecurity knowledge among the rural population who are adapting quickly towards internet penetration could result in many cybercrimes. Hence, the India government is preparing a national cybersecurity strategy that is in the final approval stage. Instead of relying on private players to report malware that is a severe threat to national security, this strategy includes a government-owned malware report portal to overcome the threat. In addition, there will be a national threat intelligence exchange platform, enabling the government to manage all the intelligence sources in one place and distribute them to the concerned bodies. The National Cyber Coordination Center Project, under this strategy, will be very helpful in detecting and restricting the distributed denial-of-service (DDoS) attacks by providing secured gateways for the IPs. The government's focused approach towards cybersecurity preparedness and awareness, their engagement with private organizations in data protection, providing cyber education to the population, and building a legal framework can be a game-changer in securing Indian cyberspace.

ASEAN Revolutionizing the Asia-Pacific Cyberspace

After signing the non-binding UN norms of responsible state behavior in cyberspace, the ASEAN countries lead the global pack in terms of cybersecurity concerns. This group of ten countries is making further progress by adopting the ASEAN Regional Action Plan (2021-2025). By working together in three aspects (cyber strategy, cyber ops-tech collaboration, and cyber capacity building), these countries are taking necessary steps to restrict the threat groups from conducting large-scale cyberattacks in the region. Singapore is actively leading the group by developing the ASEAN Centre to strengthen the regional cybersecurity landscape in this process. This step will benefit the group in research collaboration, knowledge sharing, and training to mitigate the cyberthreats. The ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) also plans to improve the cybersecurity strategy development, legislation, and research capabilities of the member states. The growing tensions with China over the South China Sea will be a leading factor in the ASEAN efforts to prepare for state-sponsored cyberattack threats in the future. With the increasing geopolitical tensions and the rapid expansion in the digital economy, cybersecurity has become of utmost importance for the region. The collaborative measures and the development of state-of-the-art technologies can represent ASEAN leadership as the center for Asia-Pacific cybersecurity.

Indo-Taiwan Cyber Collaboration: A Means to Counter Chinese Cyber-warfare

Cyberattacks are considered the new normal in the current geopolitical ambitions and rivalries scenario. The states employing non-state actors to exploit their adversaries' dependence on information, communication, and digital technologies have blurred the distinction between the state and non-state actors. India and Taiwan have been facing similar cyberthreats from China for years and the post-COVID era of digital technologies has been acting as a catalyst for these events. The cyber-campaign to manipulate the Taiwanese Presidential elections and the APT30 operation against India are alleged to have been performed by China government-backed threat actors. Tackling the threats on their own will be equally challenging for

Taipei and New Delhi. Both parties have a tremendous opportunity to collaborate on these shared threats and develop common synergies to counter these state-sponsored actors. Taiwan has developed a multi-layered secure infrastructure. It includes the origin of the National Information and Communication Security Taskforce (NICST), the Department of Cybersecurity, the Information and Electronic Warfare Command, and

large-scale threat detection systems such as the Hybrid Intrusion Detection System. At the same time, India has also framed the Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC). Working together will enable both to understand how each other functions. Taiwan's long expertise to counter Chinese cyberattacks can help India strengthen its cyberspace further. Institutionalizing the collaboration will foster India's software capabilities and the hardware infrastructure of Taiwan.

Cybersecurity in Tokyo Olympics: An Exemplary Success Story for Future International Sporting Events

Large-scale sporting events such as the World Cups, the World Championships, and the Olympics are frequently the target of cyberthreats for various reasons—such as the huge market size of the events, their modern reliance on digital technology, and their impacts on the geopolitical scenario. It has been observed that the Olympics in Rio de Janeiro, Sochi, Pyeongchang, and London faced some high-impact cyberattacks. For example, during the Olympics in Pyeongchang, South Korea, the Opening Ceremonies were nearly halted due to cyberattack. But at the Tokyo Olympics, the International Olympics Committee (IOC) and the Tokyo Organizing Committee (TOC), learning the lessons from the past, took aggressive preemptive measures, which is the main reason behind zero major cyber issues during the event. Furthermore, the decision to deploy several behavioral specialists and analysts from across the major security agencies of the world catalyzed the process of interpreting intelligence, detecting patterns from that intelligence, and putting together plans for preemptive cyberattacks or counterattacks. In addition, the deployment of Level 1 security operations center analysts was helpful for the real-time analysis of traffic, collecting alerts, filtering out false positives, and escalating abnormal activities to behavioral analysts upon justification of any event. Also, the deployment of private cybersecurity firms was a good move for the uninterrupted conduct of the event. The year 2022 will be marked by various major sporting events such as the Beijing Olympics, World games (Alabama), IAAF World Championships (Eugene), and many more. The respective organizing committees of these events should learn from the Tokyo Olympics. They should go on the offensive and beat the threat actors at their own game by taking preemptive measures and promoting international collaboration in cybersecurity.

E3 – Cyberthreat Regional Landscape

Lazarus APT Group

Industries Targeted	Continents Targeted
Services, Finance, Manufacturing, Defense, Public Sector, HealthCare, Markets, Energy, Utility	China, India, Indonesia, Japan, Philippines, Russia, South Korea, Taiwan, Thailand, Vietnam

Lazarus APT group is also known as: Operation DarkSeoul, Dark Seoul, Hidden Cobra, Hastati Group, Andariel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Group 77, Labyrinth Chollima, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APT-C-26, NICKEL GLADSTONE, COVELLITE.

Lazarus APT group, operating since at least 2009, is among the most active threat actor groups. It is a state-sponsored hacking group from North Korea and is allegedly composed of cyber-operatives from "Bureau 121," the cyber warfare division of North Korea's Reconnaissance General Bureau. Bureau 121 is North Korea's most significant cyber unit that is used for both offensive and defensive operations. Several large-scale campaigns, primarily targeting the defense, energy, government sectors, and crypto markets, have been attributed to this group. For example, in mid-2021, the APT group targeted organizations in the defense industry by using a sophisticated framework capable of targeting three main operating systems (Windows, Linux, and macOS). The framework was named Multi-platform Target (MATA) malware framework. MATA framework incorporates main functions and can act as loader, orchestrator, and plugin.

Lazarus constantly upgrades its technical abilities, including supply-chain attacks, using the BLINDINGCAN malware. Such attacks begin with an email containing a malicious attachment sent to the target victims. Once the malicious attachment is accessed, the malware is installed and reconnaissance is initiated to gather information (especially defense and energy technologies). As a result, Asia has become a key target of Lazarus, with the group being an ongoing threat to all industries, especially those within the defense, government, and energy sectors.

APT 10

Industries Targeted	Continents Targeted
Services, Retail, Defense, Public Sector, HealthCare, Markets, Energy, Manufacturing, Utility	China, India, Indonesia, Japan, Philippines, Russia, South Korea, Taiwan, Thailand, Vietnam

APT10 is also known as: Stone Panda, MenuPass, Happyyongzi, POTASSIUM, DustStorm, Red Apollo, CVNX, HOGFISH, BRONZE RIVERSIDE, DustStorm, CVNX, HOGFISH, Cloud Hopper.

APT10 is an active threat actor speculated as having connections with the People's Republic of China (PRC). The advanced persistent threat (APT) group was first observed in 2006 and is known to have targeted organizations in the healthcare, defense, government, telecommunications, and transportation sectors. APT10 has conducted cyber-espionage operations to retrieve sensitive information from its victims. The threat group is also known for attacks on the supply chain networks of Airbus and several telecom companies.

The APT10 group has attacked southeast Asian telecom companies in one of its latest campaigns, targeting sensitive servers and high-value business assets such as domain controllers, Exchange Server, and web servers. APT10 is also known for using custom malware and exploiting zero-day vulnerabilities as the initial infection vector. Some of the malware and tools used by the group are Poison Ivy, Mimikatz, China Chopper, EvilGrab, RedLeaves, UPPERCUT, ChChes, and PlugX.

Winnti Group

Industries Targeted	Continents Targeted
Services, Manufacturing, Construction, Defense, Public Sector, Healthcare, Markets	China, India, Indonesia, Japan, Philippines, Russia, South Korea, Taiwan, Thailand, Vietnam

Winnti group is also known as: Axiom, Winnti Umbrella, Suckfly, APT41, Group 72, Blackfly, LEAD, WICKED SPIDER, WICKED PANDA, BARIUM, BRONZE ATLAS, BRONZE EXPORT, Red Kelpie.

Winnti group is a People's Republic of China (PRC)-based threat actor that is believed to work under the umbrella of Chinese intelligence. Some speculate that the Winnti group consists of multiple threat actor groups that cooperate and share TTPs among themselves. Winnti group is also known as PassCV, APT17, Axiom, LEAD BARIUM, Wicked Panda, and GREF. The group is motivated by financial gains and espionage and targets diverse industries such as technology, healthcare, government, and defense, while primarily focusing on Southeast Asia countries. Winnti's armory comprises custom-made tools and malware, which can be utilized based on the requirements of each campaign.

Andariel Group

Industries Targeted	Continents Targeted
Construction, Markets, Services	China, India, Japan, Philippines, Russian, Federation, South Korea, Vietnam

Andariel group is also known as: Operation DarkSeoul, Dark Seoul, Hidden Cobra, Hastati Group, Andariel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Subgroup: Bluenoroff, Group 77, Labyrinth Chollima, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APT-C-26, NICKEL GLADSTONE, COVELLITE.

Andariel is a division of the Lazarus APT group, which is associated with North Korea. The Andariel group primarily targets South Korean government entities for financial gains. Threat actors often leverage phishing emails as an initial infection vector by sending a weaponized word document that contains malicious HTML Application (HTA) code. The HTA code installs a secondary payload responsible for communicating with the C2 server and deploying the backdoor, ultimately dropping the ransomware. The custom ransomware is deployed in campaigns used an AES-128 CBC mode algorithm to encrypt all files on the victim machine, except system-critical files with ".exe," ".drv," and ".dll" extensions. Over time, the tools used by this threat group have evolved significantly. More activities are expected from the threat actor going forward. Their main focus is expected to be government entities, manufacturing companies, media houses, and construction industries in the Asia-Pacific region.

DarkHotel

Industries Targeted	Continents Targeted
Defense, Public Sector, Energy, Services	China, India, Japan, Russian, South Korea, Vietnam

DarkHotel APT is also known as: DUBNIUM, Fallout Team, Karba, Luder, Nemim, Nemin, Tapaoux, Pioneer, Shadow Crane, APT-C-06, SIG25, TUNGSTEN BRIDGE, T-APT-02

DarkHotel is an advanced persistent threat (APT) group with operations traced back to 2007. Its primary objective is to gain sensitive information from organizations across government and hospitality sectors and other entities or individuals with access to valuable data by carrying out cyberespionage operations. The group came to light in 2014 in one of its cyber espionage campaigns targeting business travelers and the hospitality sector in Asia, leveraging zero-day exploits. The group is known to target victims using spear-phishing emails or exploiting zero-day vulnerabilities. In one of its recent operations, dubbed 'PowerFall,' DarkHotel APT exploited two Common Vulnerabilities and Exposures (CVEs) in Windows kernel and Internet Explorer, tracked as CVE-2020-0986 and CVE-2020-1380, respectively. The group also uses information-stealing Trojans known as Konni, Nokki, and Pioneer.

Most of the attacks conducted by DarkHotel are towards Japan, Taiwan, China, Russia, and South Korea. The attacks' sophistication resembles that of a state-sponsored APT group. Considering the peer-to-peer spreading tactics of the threat actor group and the ability to use zero-day exploits, it poses an elevated risk to individuals and industries with high-valued proprietary information.

Mikroceen APT Group

Industries Targeted	Continents Targeted
Defense, Public Sector, Energy, Services	Mongolia, Russia, Central Asia

Mikroceen APT is also known as: Vicious Panda

Mikroceen APT group, also known as Vicious Panda, has been active in the cyberthreat landscape since at least 2017. Mikroceen's primary targets are government and education industries in Central Asia, Russia, and Mongolia. The hacking group uses a custom backdoor named Mikroceen RAT to deploy various malicious tools into the victim's environment during an attack.

In March 2021, the threat actors targeted a utility company in Central Asia by compromising Microsoft Exchange servers. After obtaining access to the victim's servers, the threat actors deployed a WebShell to download the Mikroceen RAT backdoor. The backdoor helps deploy required tools such as Mimikatz and Mimikatz_ssp into the victim's system.

APT 27

Industries Targeted	Continents Targeted
HealthCare, Services, Public Sector, Energy	Unavailable

APT27 is also known as: Emissary Panda, TG-3390, APT 27, TEMP.Hippo, Red Phoenix, Budworm, Group 35, ZipToken, Iron Tiger, BRONZE UNION, Lucky Mouse.

APT27 is a People's Republic of China (PRC)-based threat group operating since 2010. Historically, the group has leveraged publicly available tools to access networks to collect political and military intelligence. Although this group has previously prioritized intelligence gathering over monetary gains, in some recent campaigns it has conducted ransomware attacks that are considered a new trend.

In a recent campaign, the threat actors deployed ransomware malware that used Windows BitLocker for encryption. The initial attack vector on this campaign was a compromised third-party service provider. Although ransomware attacks are not the main types of attack attributed to this group, the number of such attacks has increased over time and the threat group was observed to deploy Polar ransomware in at least one instance.

E4 – Industry Threat Landscape

Severity Score for Cyber Events Grouped by Industry
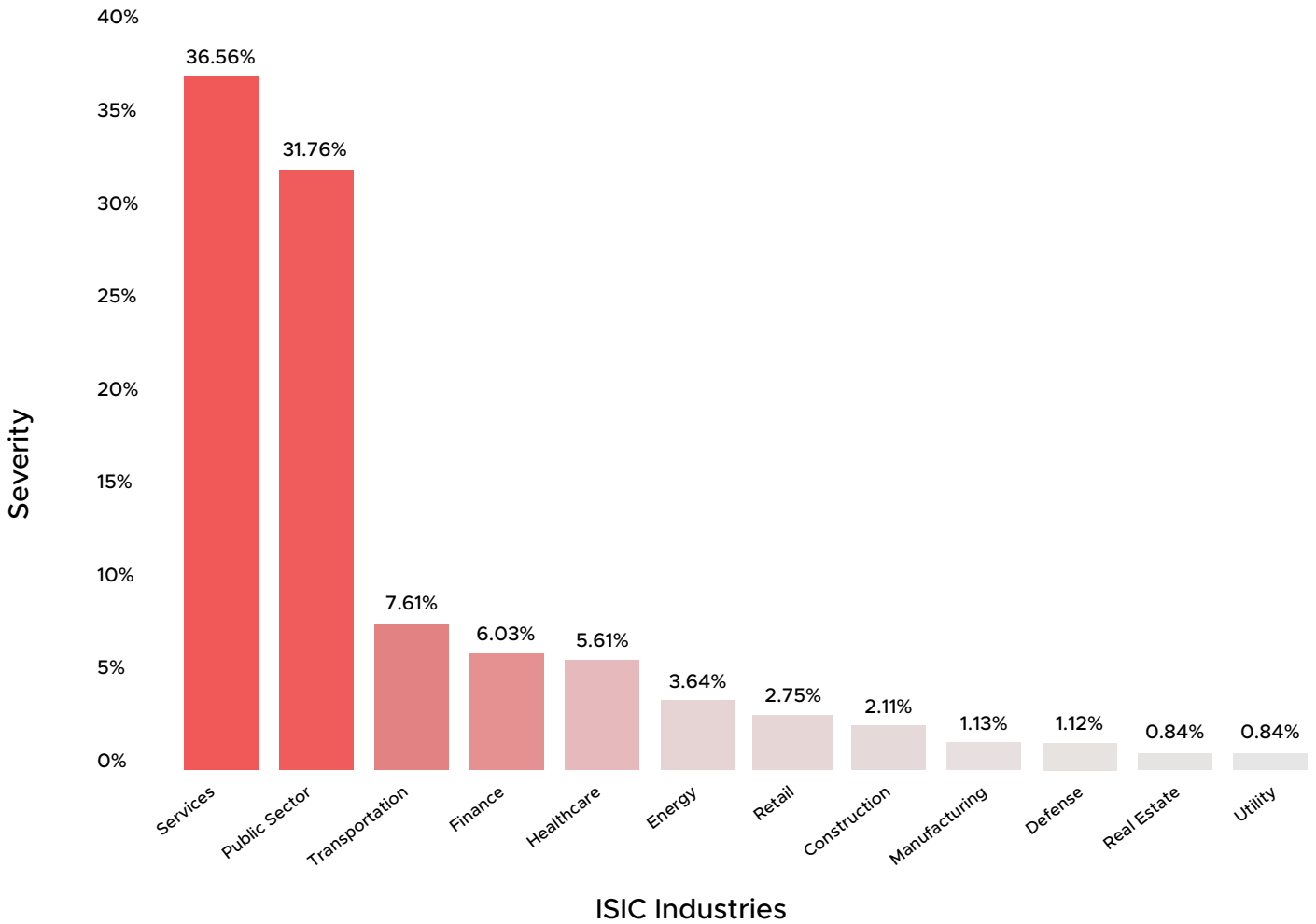
Figure 9 - Industry threat landscape in Asia

Telecommunication Companies Were One of the Prime Targets in Asia

The service sector is one of the most targeted, covering about 20% of the threat landscape in the Asia-Pacific region. Within the sub-sectors, Telecommunication and Technology were the most affected sector, accounting for approximately 76% of the events. Companies from India, Bangladesh, and Nepal were among prominent targets. Ransomware attacks, followed by data exfiltration were among the primary attack vectors for the sector.

Financial gain and espionage were the primary motivation behind the cyberattacks. The prominent threat actors behind the campaigns targeting the telecommunication industry are Gallium, Naikon APT, and Emissary Panda (also known as TG-3390, APT27). Additionally, threat actors attempted to maintain access and compromised high-profile assets such as domain controllers, Microsoft Exchange servers, web servers, and billing servers containing call detail records to collect sensitive information.

Manufacturers Targeted in Ransomware Attacks

targets of ransomware attacks. Japanese manufacturers Yamabiko Corporation and Ito Yogyo were also affected by ransomware campaigns. REvil, AvosLocker, and Babuk ransomware groups were suspected to be behind these attacks. Japanese manufacturers account for approximately 60% of all ransomware attacks.

For all the ransomware campaigns in the region, QBot and TrickBot were among the primarily used malware for initial access. Cobalt Strike and PowerShell Empire were among the prominent tools leveraged for lateral movement. Financial gain appeared to be one of the primary motivations behind these attacks. A common theme behind the ransomware attacks was strained production capabilities due to COVID. For this reason, the manufacturers were possibly more willing to pay the ransom amount.

Retail Sector Targeted with Data Breaches and Ransomware Attacks

Organizations in the retail sector primarily experienced data breaches in the region. As part of the global supply-chain attack in the Codecov code coverage platform, major Japanese retailer Mercari suffered a data breach, while the Indian retailer BigBasket was part of a significant data breach.

Espionage Attack against the Public Sector

Geopolitical tension in the region contributed to the rise of espionage activities against government organizations in the region. Approximately 13% of the cyberattacks attempted to exfiltrate sensitive information. APT groups such as Confucius, SharpPanda, APT10, RedFoxtrot, IndigoZebra, Balikbayan Foxes, Kimsuky, LuminousMoth, and TA406 were primarily active within the region targeting government entities. Around 35% of all cyberattacks against government bodies are done by APT groups. One of the prominent initial access vectors was spear-phishing and a commonly used tool for the lateral movement was Cobalt Strike.

Vulnerabilities in Infrastructure and Applications Were One of the Major Triggers

Considering all of the cyberattacks occurring in the region, vulnerabilities in infrastructure and applications accounted for approximately 31%. Among those events triggered by vulnerabilities, roughly 32% of the affected organizations belong to the services industry. Financial gain was the motivation behind 88% of all the events driven by vulnerabilities.

E5 – Key Lessons from Most Impactful 2021 Attacks

Asia-Pacific: Top 10 Events
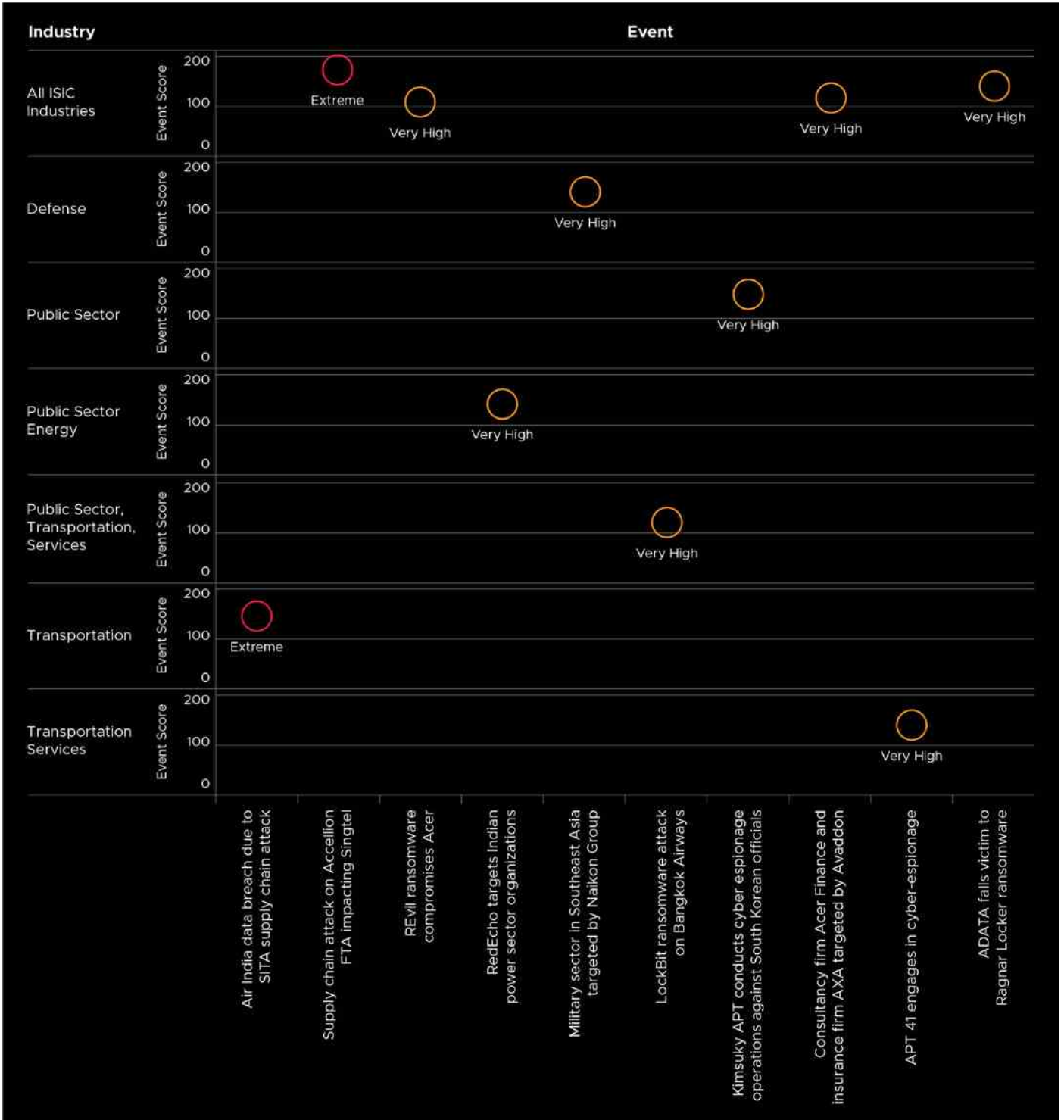
Figure 10 - Top 10 events in Asia

#1 Supply-chain attack on Accellion FTA, impacting Singtel

Severity: Extreme

Industries Targeted: All ISIC Industries

The largest mobile carrier in Singapore released a statement on February 17, 2021, stating the organization was targeted in a cyber incident. Singtel notified clients of this incident caused by the vulnerabilities in the Accellion FTA application. The organization has published a timeline of the incident and the dates that Accellion released patches. The timeline suggests that Accellion had not provided the required patches to Singtel during their internal breach. While Singtel did not provide any information on the enterprises impacted by this incident, the organization mentioned that the affected parties were contacted. Singtel further stated that the exfiltrated information included Personally Identifiable Information (PII) of approximately 129,000 customers, banking details of 28 former employees, credit card details of 45 corporate customers, and information of a total of 23 enterprises, including suppliers, partners, and corporate customers.

Impact: The threat actors managed to exfiltrate approximately 129,000 customers, banking details of 28 former employees, credit card details of 45 corporate customers, and information of a total of 23 enterprises, including suppliers, partners, and corporate customers from Singtel. In addition, organizations that specifically use Accellion's FTA software or have third-party vendors using the software as their file-sharing service might be affected.

Future Considerations: Critical vulnerabilities tend to attract attention from ransomware operators, as these exploits could be used to gain a foothold within an organization's network for malicious activities. Additionally, ransomware operators have been actively involved in cyber incidents throughout 2021. Therefore, the ransomware group is expected to continue targeting various industries worldwide in 2022.

#2 Air India discloses a breach of customers' personal information due to SITA supply chain attack

Severity: Extreme

Industries Targeted: Transportation

Quick Recap: Following the SITA supply-chain attack in late February 2021, Air India announced further information regarding the incident and its impact on airline customers. In March 2021, SITA, a global IT organization servicing 90% of the airline industry, confirmed that customer data was stolen in its Passenger Service System (PSS) breach. Air India had initially notified customers of the SITA breach on March 19, 2021. However, in the light of new developments in the investigation process, the organization disclosed that the personal information of around 4.5 million passengers had been compromised.

The exposed data contained the passengers' personal information from August 26, 2011 to February 3, 2021. The compromised data included ticket and passport details and contact information, name, and date of birth. In addition, Air India's frequent flyer and Star Alliance data were also reportedly impacted. However, the organization has stated that no password or credit card information was compromised.

Impact: The SITA breach impacted several airlines and information surrounding frequent flyer programs. The threat actors leveraged Mimikatz and hash dump to obtain victims' credentials. Furthermore, they used DNS tunneling to exfiltrate data.

Future Considerations: While this attack has not been attributed to any of the known threat actors, the attack on SITA PSS ranks among one of the highly publicized supply-chain attacks, with global consequences. A supply-chain attack is more cost-effective for threat actors because compromising a single vendor could breach multiple organizations. Additionally, the increase in zero-day exploits could aid the threat actors in supply-chain attacks during 2022.

#3 Chinese threat actor, RedEcho, targets Indian power sector organizations

Severity: Very High	**Industries Targeted:** Public Sector, Energy

Quick Recap: Security researchers have observed a significant increase in suspected targeted intrusion attacks against Indian power sector organizations, reportedly from a Chinese state-sponsored group dubbed RedEcho. This increase follows heightened political conflicts between India and China initiated in May 2020.

Based on reports, there has been a rise in threat actor-related infrastructure, which encompasses ShadowPad Command-and-Control (C2) servers to target much of the Indian power sector. ShadowPad is a backdoor malware that beacons to attacker-controlled domains with the infected system's information at regular intervals. It can also execute additional malware and steal data. Ten distinct Indian power-sector organizations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for balancing the regional supply and demand, have been identified as targets. In addition to targeting critical infrastructure organizations in the power utility sector, the threat actors targeted two Indian seaports.

Impact: Throughout the campaign, RedEcho made heavy use of AXIOMATICASYMPTOTE, defined as the term to track infrastructure that comprises ShadowPad C2s shared between several Chinese threat activity groups, including APT41, Tonto team, the Icefog cluster, KeyBoy, and Tick.

Future Considerations: The threat actor shares some similarities in TTPs that indicate a potential connection to other state-sponsored groups such as APT41 and Tonto Team. Not much information is available on the threat actor. However, cyberattacks are expected to rise or fall in conjunction with political tensions between China and India.

#4 North Korean Kimsuky APT conducts cyber espionage operations against South Korean officials

Severity: Very High	**Industries Targeted:** Public Sector

Quick Recap: In mid-May 2021, A North Korean threat actor group, dubbed Kimsuky (also known as Thallium, Black Banshee, and Velvet Chollima) has been involved in a persistent attack on South Korean government entities. This group is suspected of having emerged in 2012 and is widely believed by security agencies in the United States to be tasked with harvesting intelligence by the North Korean regime. The South Korean threat intelligence team within KISA (Korean Internet & Security Agency) detected multiple phishing websites with malicious content intended to target high-profile people within the South Korean government.

The threat actor engages in social engineering tactics through phishing campaigns, sending out phishing emails in bulk and harvesting victims' credentials. In addition, the threat group collects email addresses, which are afterward used to send spear-phishing emails. The threat operators were also observed to monitor their targets through Twitter, harvesting additional information to generate a well-crafted phishing email as part of reconnaissance.

Impact: The operators' tactics mainly rely on social engineering, utilizing phishing and spear-phishing campaigns to harvest intelligence. Kimsuky has a history of targeting the United Nations. For example, in September 2020, 11 United Nations Security Council (UNSC) officials were targeted by Kimsuky using spear-phishing tactics. The threat actors potentially plan on expanding their operations to a wider variety of targets worldwide.

Future Considerations: Kimsuky is a North Korean threat actor targeting South Korean government officials, with the most recent campaign targeting the ministry of foreign affairs. The threat actor is mainly concerned with gathering global intelligence for political espionage. With the continued political tension between South and North Korea, Kimsuky is expected to appear in 2022. Furthermore, Kimsuky might target organizations outside of South Korea.

#5 ADATA falls prey to Ragnar Locker ransomware

Severity: Very High | **Industries Targeted:** All ISIC Industries

Quick Recap: Memory and storage manufacturer ADATA announced that the organization's network was compromised on May 23, 2021. The Taiwan-based company stated that a ransomware attack forced ADATA to take its system offline. However, the organization did not disclose the demanded ransom amount by the threat actor. ADATA mainly manufactures USB Flash drives, memory cards, hard disk drives, solid-state drives, mobile accessories, and DRAM modules.

ADATA notified relevant authorities to aid in their investigation of tracking the threat actor. At the time of writing this advisory, ADATA's business is operational, with additional affected devices reinstated, per their public statement. While ADATA provided no additional information on the name of the ransomware malware, threat actors associated with Ragnar Locker have claimed responsibility. The threat actors started leaking samples of allegedly exfiltrated data from ADATA and claimed to possess approximately 1.5 TB of highly confidential information. The data exfiltrated by the threat operator concerns employees, partners, customers, and clients.

The threat actor published a portion of ADATA's data on their Dark Web leak site to increase pressure towards the corporation. The data leaked so far includes non-disclosure agreements, proprietary files, legal documents, board schematics, contractual agreements, and screen shots of compromised systems.

Impact: While ADATA did not disclose the ransom demands, previous demands range from 200,000 to approximately 600,000 USD. However, in cases similar to EDP, the ransom can go up to over 10 million USD. Failure to cooperate would risk publishing the alleged 1.5 TB of exfiltrated data.

Future Considerations: The threat actors operating the Ragnar Locker ransomware have been actively compromising organizations since 2019. The attackers utilize double extortion techniques similar to various other prominent ransomware gangs. In this technique, the threat actor steals sensitive data from the victim's system before encrypting the files stored on the network. The adversaries then threaten to publish the exfiltrated data in case of a futile negotiation process. Ragnar Locker operators have been quiet lately, with only a few minor cyber incidents in 2021. However, there is no proof of the threat actors shutting operations down. Hence, there could be a possibility of a cyberattack in 2022.

#6 APT41 engages in cyber-espionage

Severity: Very High

Industries Targeted: Transportation, Services

Quick Recap: In August 2021, security researchers observed malicious campaigns attributed to the alleged Chinese state-sponsored threat actor group, APT41, also known as Earth Baku, Winnti Umbrella, Winnti Group, Suckfly, Group72, Blackfly, Lead, Wicked Spider, Wicked Panda, Barium, Bronze Atlas, Bronze Export, and Red Kelpie. This campaign is believed to date back to July 2020 and exploited various vulnerabilities on the targeted victim's infrastructure. Additionally, researchers have found that APT41 has created its malware tools to help with the targeted attacks; they include a backdoor and shellcode loader named StealthVector and StealthMutant. Based on observed improvements, it is suspected that the Earth Baku APT group has likely recruited individuals with experience in low-level programming, software development, and red-team techniques. Targets of APT41's campaign are public and private institutions primarily located in India, Indonesia, Malaysia, Taiwan, Vietnam, and the Philippines.

Threat actors leveraged known vulnerabilities in Microsoft Exchange Server ProxyLogon vulnerability (CVE-2021-26855), Citrix NetScaler/ADC (CVE-2019-10781), Cisco routers (CVE-2019-1653 and CVE-2019-1652), and Zoho ManageEngine Desktop Central (CVE-2020-10189) for exploitation in over 75 organizations located in multiple countries. In the past, a campaign dubbed "ColunmTK" affected significant airlines worldwide and it was attributed to APT41. In addition, the SITA supply-chain attack was also attributed to APT41.

Impact: Organizations with outdated Exchange Server versions are prone to the ProxyLogon vulnerability tracked as CVE-2021-26855 and could be targeted, likely resulting in compromised systems and potentially leading to a data breach.

Future Considerations: This attack has been recently attributed to the Chinese state-sponsored group APT41. The threat actor group is known to carry out Chinese state-sponsored espionage cyber activity and financially motivated attacks. Cyberattacks are expected to rise or fall in conjunction with political tensions between China and other nations following 2022.

#7 Naikon group leverages the Nebulae backdoor malware to target military sector in South East Asia

Severity: Very High

Industries Targeted: Defense

Quick Recap: On April 28, 2021, security researchers published a detailed report on a new Naikon backdoor spanning roughly two years and targeting the military sector in Southeast Asia. The attacks are attributed to the Chinese-speaking threat actor, Naikon group—PLA Unit 78020, Override Panda, Lotus Panda, or Hellsing. Security researchers have attributed this operation to the Naikon group, based on the Command-and-Control (C2) servers and malicious payloads belonging to the Aria-Body loader malware family, utilized in the group's past operations.

Naikon has actively spied on organizations in countries including the Philippines, Malaysia, Indonesia, Singapore, and Thailand, for at least a decade, since 2010. Naikon is likely a state-sponsored threat actor tied to China, mostly known for focusing on high-profile organizations, including government entities and military organizations. According to security researchers, the Naikon group aimed at espionage and data exfiltration, as per the collected evidence.

Impact: The threat actors deployed the Nebulae backdoor, which allowed the threat actors to collect system information, manipulate files and folders, download files from the command-and-control server, and manipulate processes on the target system.

Future Considerations: The Naikon group is a state-sponsored threat actor attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). All historical observations about this threat actor group strongly indicate that they have been focused on executing cyber-espionage operations on countries in the South China Sea, including the Philippines, Malaysia, Indonesia, Singapore, and Thailand, since 2010. Naikon is expected to continue its campaign into 2022.

#8 LockBit ransomware attack on Bangkok Airways

Severity: Very High

Industries Targeted: Public Sector, Transportation, Services

Quick Recap: Based on publicly available reports, on August 25, 2021, the LockBit ransomware group disclosed an attack against Bangkok Airways, allegedly having stolen 103 GB worth of files. Bangkok Airways acknowledged the attack in its press release on August 26, 2021. The affected personal data belonging to passengers include passenger name, family name, nationality, gender, phone number, email address, contact information, passport information, historical travel information, and partial credit card information.

The company also said that the threat actors did not access Bangkok Airways' operational or aeronautical security systems. Moreover, the airline is stated to have notified its customers and other authorities regarding the incident.

Impact: Based on the threat actors' activities, the ransomware attacks could potentially lead to significant loss of sensitive information, disruption in operations, and negatively impact organizations' brand reputations.

Future Considerations: LockBit 2.0 is the successor to LockBit ransomware, with further enhanced capabilities to capture and automatically encrypt sensitive information. LockBit developers have updated the ransomware in multiple instances to upgrade and optimize some of its features, including additional methods for anti-detection capabilities and the ability to circumvent Windows User Access Control (UAC). Additionally, threat actors behind LockBit adopted the double extortion technique (which refers to exfiltrating data before initiating the encryption process), which would allow the threat actors to have additional leverage to receive the ransom by threatening to publish the stolen information through data-leak sites. Based on the malware developments, Lockbit is expected to appear again soon.

#9 REvil ransomware compromises Acer and targets organizations with cyber insurance coverage

Severity: Very High

Industries Targeted: All ISIC Industries

Quick Recap: The Taiwanese electronics organization Acer was targeted by REvil ransomware. Acer is a Taiwanese electronics and computer maker known for monitors, laptops, and desktops. Acer earned $7.8 billion in 2019 and employed approximately 7,000 employees. On March 18, 2021, the ransomware operators announced on their data leak site that they had successfully breached Acer's network and shared images of the allegedly stolen files as proof of compromise. The leaked images were documents, including financial spreadsheets, bank balances, and bank communications.

Impact: The cyberattack against Acer proves that the operators are capable of targeting large corporations. The attack on Acer is part of a trend in which the threat actors targeted organizations with cyber insurance. Furthermore, the threat actor group is focusing on the cyber insurance companies to target their customer base.

Future Considerations: On July 13, 2021, REvil's websites became inaccessible at approximately 1:00 AM EST. Just days before the alleged cease in operation, United States President Biden demanded the Russian President Putin to terminate Russian ransomware threat groups. In the morning of July 13, 2021, the LockBit ransomware representative posted on a Russian hacking forum and claimed that REvil received a legal request from the government, forcing the ransomware group to close their server infrastructure. Security researchers claim that the evidence indicates REvil suffered a planned and concurrent shutdown of their infrastructure.

However, on September 7, 2021, REvil returned with their TOR negotiation and data leak sites becoming accessible. All victims listed had their timers reset and their ransom demands were left as they were when the ransomware group supposedly shut down in July 2021. REvil is expected to continue targeting institutes in various industry sectors in 2022.

#10 Avaddon ransomware targets consultancy firm Acer Finance and insurance firm AXA

Severity: Very High

Industries Targeted: All ISIC Industries

Quick Recap: On May 16, 2021, Avaddon ransomware operators targeted several branches of AXA insurance in Asia. Avaddon's leak site allegedly exfiltrated 3TB of sensitive information stolen collectively from Thailand, Malaysia, the Philippines, and Hong Kong branches. The threat actors noted that the compromised data include sensitive information such as customers' medical reports, ID cards, bank statements, payment records, claim forms, and more. On May 15, 2021, AXA's website was targeted in a series of DDoS (distributed Denial of Service) attacks, which caused intermittent access issues. The threat actors leverage the DDoS attack attempts to increase the pressure on the targeted victims and force them to initiate the negotiation process. Avaddon ransomware operators were first observed to utilize DDoS attacks in October 2020 to gain further leverage on their victims. Avaddon provided the insurance company approximately ten days to cooperate, after which the hacker group would publish AXA's sensitive documents.

Impact: The threat actors allegedly claimed 3 TB of sensitive information from Thailand, Malaysia, the Philippines, and Hong Kong branches. The exposed data allegedly contains customers' medical reports, ID cards, bank statements, payment records, claim forms, and more. A week before the attack on May 9, 2021, AXA claimed to have dropped support for organizations that pay the requested ransom. This public announcement might have provided the Avaddon group incentive to target the organization.

Future Considerations: Avaddon is a ransomware operating in a Ransomware-as-a-Service model and was initially discovered in June 2020. The threat group targets Windows systems and the malware payload is generally spread via phishing campaigns.

However, on June 11, 2021, Avaddon had allegedly shut down its operation, likely due to the increased pressure by police agencies and US President Biden's plan to deliberate cyberattacks, along with Russian President Vladimir Putin. To support the shutdown claim, Avaddon published a total of 2,934 decryption keys to their victims. Additionally, Avaddon's TOR website became inaccessible, indicating that the threat group likely shut down operations.

While Avaddon has supposedly shut down, the operators behind the ransomware could return under a different name. In 2022, Avaddon could still be a threat if they were to return.

Latin America Constellation

F1 – Actioning 2022: Regional Themes and Trends

The section below provides key regional themes and trends observed throughout 2021. These insights provide valuable insights to organizations on what to expect from a geopolitical and cyberthreat perspective in 2022.

Brazil and Colombia to Face the Greatest Number of Cyberattacks

In 2021, Brazil faced 35.3% of the cyber incidents in the region, followed by Colombia (14.7%), Chile (8.8%), and Argentina (7.3%).

Brazil continues to be a hotspot for a wide variety of cyberattacks, from phishing and DDoS campaigns to ransomware. Cybersecurity investment in Brazil has not kept pace with average global spending, even considering the increasing numbers of users and cloud services in the country, making it more vulnerable to attacks. The huge-scale cyberattacks on the world's biggest meat producer and national treasury have created an alarming situation for Brazilian security experts. For Brazil to successfully restrict cybercrimes, a broader public discussion is required. Legislators, law enforcement agencies, businesses, civil society organizations, and private citizens all need to take cybersecurity much more seriously.

Colombia's economy experiences hundreds of millions of dollars of losses because of cybercrimes such as online information theft or phishing. The threat groups steal sensitive personal data and utilize it for financial gain. Colombia ranks among the worst countries in the world for phishing. Therefore, a clear and coordinated vision of the country's cybersecurity strategy, legal reforms, improved coordination and training, and improved cooperation between governments and public and private sectors is essential for securing Colombian cyberspace.

Public Sector and Retail Industries Are Likely to be Hit by Frequent Cyberattacks

The public sector (32.3%), retail industries (17.6%), financial services (13.2%), and telecommunication industries (11.7%) have been the primary targets for the threat groups in 2021.

The public sector has become a favored target for the threat groups. In the era of information and communication technology, governments are eager to digitize the public sector. The addition of cloud, mobile, and SaaS have enlarged a public organization's attack sphere. Unlike the private sector, the public sector is not necessarily profit-driven and, hence, can't justify the investments made to secure the digital space. This can manifest itself in the form of slow decision-making and inadequate training, as well as outdated IT infrastructure that's often deemed too expensive to update. The sector is at risk from illegal phishing, ransomware, cyber espionage, crypto mining, and software supply-chain attacks. The governments need to implement appropriate cyber response strategies and promote awareness and training to counter cyberthreats.

In the past few years, disruptive cyberattacks on retailers have become more common. The retail industry is more vulnerable to cyberattacks than other industries, due to its larger volume of online traffic and the design of e-commerce websites. Personal data theft and supply-chain disruption are the primary goals for threat actors targeting the retail industries. As retailers increasingly shift to a digital environment and as COVID-19 accelerates online purchasing, it is more important than ever for retailers to invest adequately in cybersecurity safeguards.

Threat Actors Are Likely to be Motivated by Financial Gain and Political Advantage

Latin American cyberspace is shaped by the region's socio-economic features and evolving technological adoptions. There has been a surge in financially motivated cyberattacks on critical infrastructures in the post-pandemic era. The ransomware attacks on Brazil's JBS meat producer and Chilean banks are a few of these. The threat groups have constantly targeted banks and financial institutions of Latin America. The vulnerabilities in infrastructure have been acting as a catalyst to these financially motivated cybercrimes.

Utilizing cyberattacks for gaining political advantage has been a trend among countries. Manipulating elections by conducting cyber campaigns is widely being observed. In addition to this, spreading misinformation campaigns, causing civil unrest, and running cyber-espionage campaigns against governments to fulfill political motives is very common. With the significant Brazilian General Elections and Colombian Parliamentary Elections and Presidential Elections approaching in 2022, learning from the past lessons, the respective governments have to be careful enough to tackle what's beneath the cyberthreats.

Ransomware Attacks and Phishing Campaigns Will be Most Prevalent

Latin America was slammed by numerous ransomware attacks in 2021. And for the last few years, Brazil and Colombia have been the two most affected countries. The escalating growth in ransomware attacks is a concern for the entire region. It has a significant economic impact due to the expense involved in restoring information systems, paying penalties, losing business, and paying the ransom. The presence of critical vulnerabilities in most devices, infrequent updates, and poor backup policies among Latin American organizations are the main reasons behind the surge in ransomware attacks. Not to mention that the threat actors consider it attractive. Therefore, unless the organizations continue to pay the ransom, the threat groups will continue to target them.

Recently, there has been an increase in phishing attacks accompanied by social engineering observed in the region. Brazil and Venezuela, the primary targets for phishing campaigns, are fighting an uphill battle against these cybercrimes. The utilization of advanced technologies and remote access Trojans (RATs) has made phishing a stealthier form of attack. For example, a remote access Trojan named BitRAT was used to carry out a large-scale phishing attack targeting Ecuador and Colombia's government, financial, healthcare, telecommunications, and energy sectors. Using solutions to detect account takeover attacks and practicing hygiene browsing rules can enable organizations to avoid phishing attacks.

F2 – Geopolitical Landscape

Here are some of the significant geopolitical developments observed in the Latin American constellation in 2021.

Cyberattack Response Network to Accelerate Brazilian Cybersecurity

Brazil has created a cyberattack response network to speed up response to cyberthreats and vulnerabilities through coordination between federal government bodies. It was created by Presidential order with the formal name of Federal Cyber Incident Management Network. This network will encompass the Institutional Security Office of the presidency and all bodies that fall under the federal government, including public companies, mixed capital companies, and their subsidiaries. The network will be led by the Information

Security Department of the Office of Institutional Security of the presidency through the government's Center for Prevention, Treatment, and Response to Cybersecurity Incidents. The network is expected to improve the articulation of SISP (Sistema de Administração dos Recursos de Tecnologia da Informação), a system for planning, coordinating, organizing, operating, controlling, and supervising the federal government's information technology resources across more than 200 bodies in terms of the prevention of incidents and actions required in a possible cyberattack. Possessing immediate knowledge about attacks and potential vulnerabilities being exploited will enable the government to alert other bodies to enforce the necessary measures to tackle the attacks. The network's primary goal will be to grow digital transformation without compromising the security underneath and promoting a culture of collaborative conflict within the government.

Brazil Might Drop EVMs for General Election 2022 with Possibility of Cyberthreat

The 2022 Brazilian General Election will be held on October 2, 2022. In August 2021, President Bolsonaro proposed returning to the paper ballot system instead of using Electronic Voting Machines (EVMs), due to the threat of cyberattacks. The counter-argument says that Brazilian voting machines have robust security measures and, as the devices are not connected to the internet, they are impossible to hack. However, looking at the history of cyber-campaigns conducted during past elections (e.g., United States Election-2016, German Election-2021, etc.) and concerns raised by the European Union regarding cyberthreats during the elections, it will be no surprise if a cyber-operation is launched to disrupt the Brazilian General Election-2022. Hence, the government and the election officials must be diligent in order to curtail the threats and ensure a free and fair conduct of the election.

Ecuador's Data Protection Law: A Resemblance of GDPR

On May 26, 2021, the government of Ecuador passed the Organic Law on the Protection of Personal Data unanimously. The draft law recognizes many familiar data protection principles, including transparency, purpose limitation, confidentiality, limited retention, accountability and data accuracy, and processor and controller obligations. Like the EU's GDPR, it has imposed obligations on the controller to implement appropriate technical and organizational security measures in the company. In addition, a data protection officer must be appointed and notify individuals before processing any personal data. This law possesses extraterritorial power. That is, the jurisdiction of the law extends to the controllers and processors providing services to the Ecuadorian residents, even if they are located outside the country. It establishes a national data protection authority; regulates cross-border data transfers; and provides Ecuadorians with the right to request access to, amend, and delete their data. Although the fines are lower than the GDPR, this law can play a vital role in managing the personal data of Ecuadorian citizens, similar to the GDPR.

Chile Fast-Tracking 5G Rollout, but with Tight Rules on Security

A new era of the digital economy will be unleashed upon the worldwide deployment of 5G, given its ability to support massive machine-to-machine (M2M) communications through greater bandwidth (such as between cellphones, sensors, "smart" machinery and appliances, and other IoT devices). The purported benefits of 5G include:

- Improved data speeds
- Decreased latency
- Cheaper rates
- More efficient energy usage
- A massive increase in device connectivity

Hence, in this world of competition over the 5G rollout, Chile surpassed its neighbors by becoming the first nation in South America to launch a spectrum auction on 5G technology in February 2021. While other significant countries in the region (such as Brazil and Colombia) are yet to start the bidding process, Chile completed the process in mid-2021. This allows Chile to accelerate their mobile 5G rollout plan across the country within the scope of two years, putting Chile way ahead of its neighbors. Furthermore, giving Huawei permission participate in the bidding process indicates that this small country has successfully maintained a balance between its two major trading partners, the United States and China, which are engaged in cybersecurity and data protection tensions. However, the government must be careful to employ strict security measures in its implementation of 5G.

Colombian elections prone to cyberthreats

The first half of 2022 will be marked by Colombian Parliamentary and Presidential elections. For years, threat groups have tried to disrupt elections in Colombia by attacking the computer system of electoral authorities. For example, during the Parliamentary Elections in 2018, Colombia faced thousands of cyberattacks on the country's voter registration systems, containing the identification data of more than 35 million voters. These were allegedly staged from Venezuela, which is suspected to be a proxy of Russia in the region. Similarly, there has been a history of fake news and misinformation campaigns conducted during Colombian elections to manipulate preferences. Therefore, the concerned authorities need to be vigilant about the cyber-operations and apply security standards to block any potential threats.

F3 – Cyberthreat Regional Landscape

Bandidos	
Industries Targeted	**Continents Targeted**
Finance, Services, Manufacturing, Healthcare, Retail, Construction	Venezuela
Bandidos is also known as: Colony, GrayBird	

Bandidos is a cyberespionage campaign targeting corporate networks in Latin America, especially Venezuela, to spy on victims and collect critical information. Bandidos used an updated version of Bandook malware in the cyberespionage campaign. Bandook malware was first observed in 2005 and, at that time, it was sold as a remote access Trojan. In 2015, the Dark Charcoal group allegedly circulated various Bandook malware variants. Bandidos threat actor group mainly targets construction, manufacturing, retail, and service sectors in the Latin American region.

The initial attack process starts with a phishing email containing a PDF attachment. Upon opening, it re-directs to one of the cloud storage platforms and then downloads a malicious DLL file that contains the malware payload. The malware creates a browser extension, which retrieves all the credentials stored in the browser storage. Bandidos activities are still being actively observed and the threat actors could continue to use Bandook malware in their campaigns.

ShinyHunter

Industries Targeted	Continents Targeted
Services, Finance, Manufacturing, HealthCare, Retail	Brazil

ShinyHunter is the threat actor behind several significant data breaches in the Latin American region. Its activities were first observed in April 2020. The group mainly targeted the healthcare, education, transportation, retail, and services sectors. The primary focus of the threat actors is to collect legitimate credentials, which can later be used to target databases to collect enterprise information and other critical data such as Pll, which will be sold on the Dark Web. Additionally, ShinyHunter's activities have shown that the group targets GitHub repositories to collect OAuth credentials, which can be used to access cloud infrastructures and scan victim organizations' GitHub source code vulnerabilities.

The ShinyHunter threat actors group isn't a direct comparison with the ransomware groups. However, their impact is significant, since the data they compromise could potentially be sold on the Dark Web forums. So, it's crucial to keep track of their activities and the tools being used.

Plotus Malware

Industries Targeted	Continents Targeted
Services, Finance, Manufacturing, HealthCare, Retail	Chile, Dominican Republic, Brazil

Ploutus is one of the most advanced ATM malware. It was first discovered in Mexico in 2013. Initially, the malware was installed using a CD boot disk. The threat actors break into the ATM and use physical ports to install the malware. A fifth iteration of the Ploutus malware, named Ploutus-I, was observed in 2021.

After consuming all information about the ATM software and its functionality, the malware is engineered in a very advanced way to establish connectivity with the ATM and perform a successful attack. The threat actors spoof the ATM's keypad connection as a webcam to evade detection in the OS logs. Then they use the keypad to execute several commands to activate specific codes to dispense money. Organizations should continuously share technical insights when such attacks take place so that other organizations can build their defense to avoid such attacks.

njRAT and AsyncRAT

Industries Targeted	Continents Targeted
Services	Brazil

njRAT is also known as: Colony, GrayBird

Recently observed cyber campaigns in 2021 targeting Latin America used ytwo of the most advanced and popular remote access Trojan's: njRAT and AsyncRAT. Threat actors gained initial access by utilizing macro-enabled Office documents. Once the threat actors gain access to the victim environment, they use PowerShell and VB scripts to disable anti-virus protection on the compromised asset to deploy the Trojan payloads. Additionally, the threat actors primarily use compromised websites to host the malicious payloads instead of public hosting services.

The websites used in the recent cyber campaigns targeting Latin America were reported registered in Brazil. Additionally, malicious documents observed in these attacks were named in Portuguese (documento.doc). Other file types observed are .XML and .xml.rels which, contained VBA macro code that downloaded the ultimate payload. However, the observed threat actors' activities did not reveal details about the targeted industries.

F4 – Industry Threat Landscape

Severity Score for Cyber Events Grouped by Industry
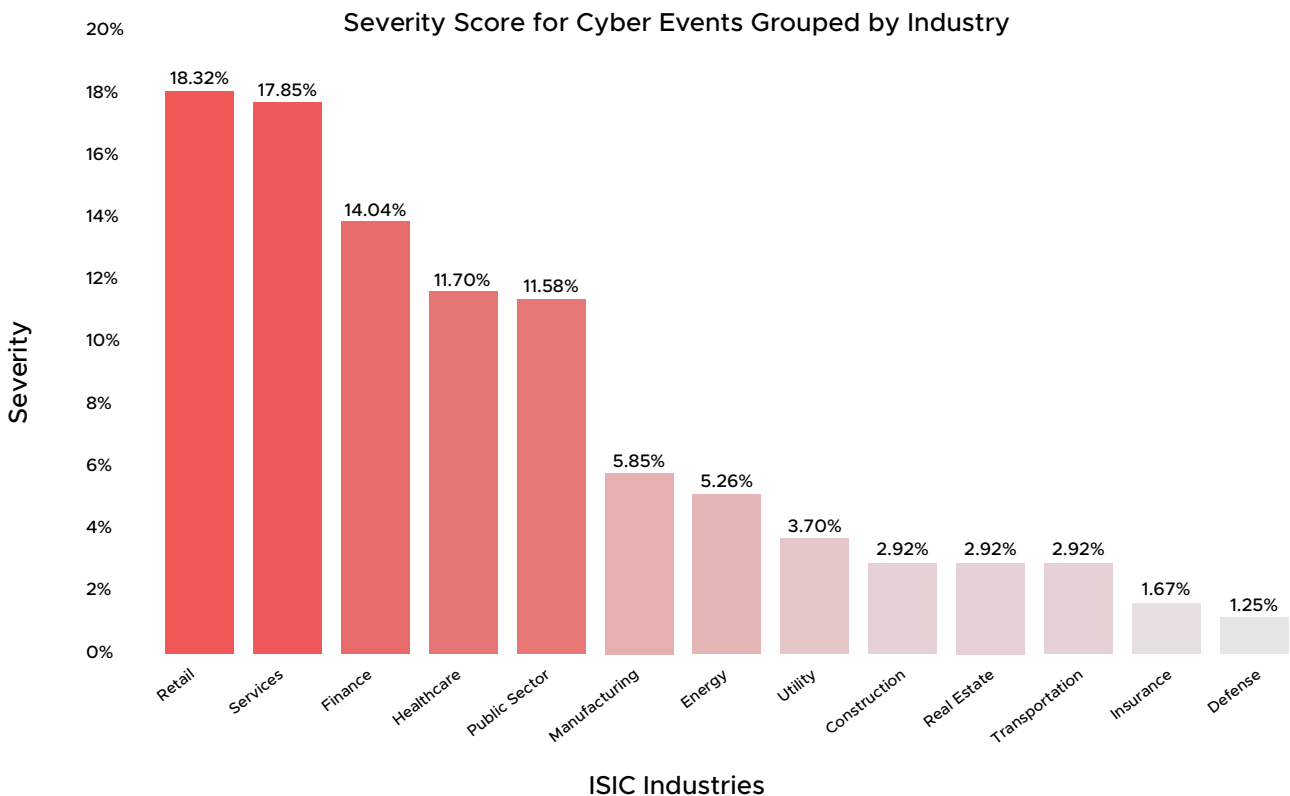
Figure 11 - Industry threat landscape in Latin America

Retail, Service, Finance, Healthcare, Public, and Manufacturing Are the Most Targeted Sectors in Latin American Regions

The retail sector is the most targeted sector in Latin America, accounting for 18.3% of the threat landscape in the region. This is followed by the service sector at 17.9%, the finance sector at 14%, the healthcare sector at 11.7%, and the manufacturing sector at 5.8%. The major motivation is financial gain. The cyberattacks are carried out by FIN7, FIN8, and FIN12, leading to cyber incidents, data breaches, and malware deployment.

The Service, Retail, Healthcare, Manufacturing, and Energy Sectors Were the Most Affected by Ransomware Attacks

The ransomware attacks primarily targeted the service sector, accounting for 34.7% of the total ransomware attacks. This is followed by the retail sector at 26.7%, the healthcare at 9.3%, and the manufacturing and energy sectors at 8% each. Brazil remains most affected by ransomware attacks, accounting for 45.6 % of all the ransomware attacks in the region. This is followed by Peru at 10.8%, Argentina at 9.8%, Chile at 7.6%, and Nicaragua at 6.5%. Lockbit ransomware was noted to be the most active, accounting for 28.3% of the region's total ransomware attacks. This is followed by Prometheus ransomware with a share of 13%. Avaddon, Conti, and Pysa ransomware also registered significant ransomware activity in the region, each with a share of 8.7% in ransomware attacks in the Latin America region.

Threat Actors Using Unique and Innovative Attack Vectors Motivated by a Successful Supply-chain Attack

Fin7 is a financially motivated threat actor using unique and innovative ideas to target technology companies in Panama. For example, injecting backdoor malware named lizard in pen-testing tools to later pivot to other companies and industries to gain network access. The threat actor group also masquerades as a legitimate security company and hires employees who are unaware that they are working for the threat actor group.

Brazil alone accounts for 37.2% of the total cyberattacks in the region. The region also noticed increased attacks from financially motivated threat actors using banking malware to target the financial sector. For example, a banking Trojan Vadokrist targets the financial sector in Brazil.

Banking trojan Janeleiro targets multiple corporate users from different sectors in Brazil, from government, healthcare, retail, and financial services.

Increase of Attacks Originating within the Region Significantly Impacts the Threat Landscape in the Latin American Region

Latin American industries and economies are experiencing rapid growth, in which digital transformation and technology play an essential role with the increase in cooperation among Latin American countries. The technology and service sectors observed a rise in cyberattacks targeting network access. To gain access to a company's internal network, threat actors attempt to compromise remote access services such as VPN, RDP, Citrix, and other related services. In addition, there is a significant increase in attacks on the financial sector, due to the lack of strong cyber laws. This includes a rise in crypto-jacking and banking malware attacks, as well as an increase in credit card and bank fraud via phishing, crimeware-as-a-service, and skimming.

F5 – Key Lessons from Most Impactful 2021 Attacks
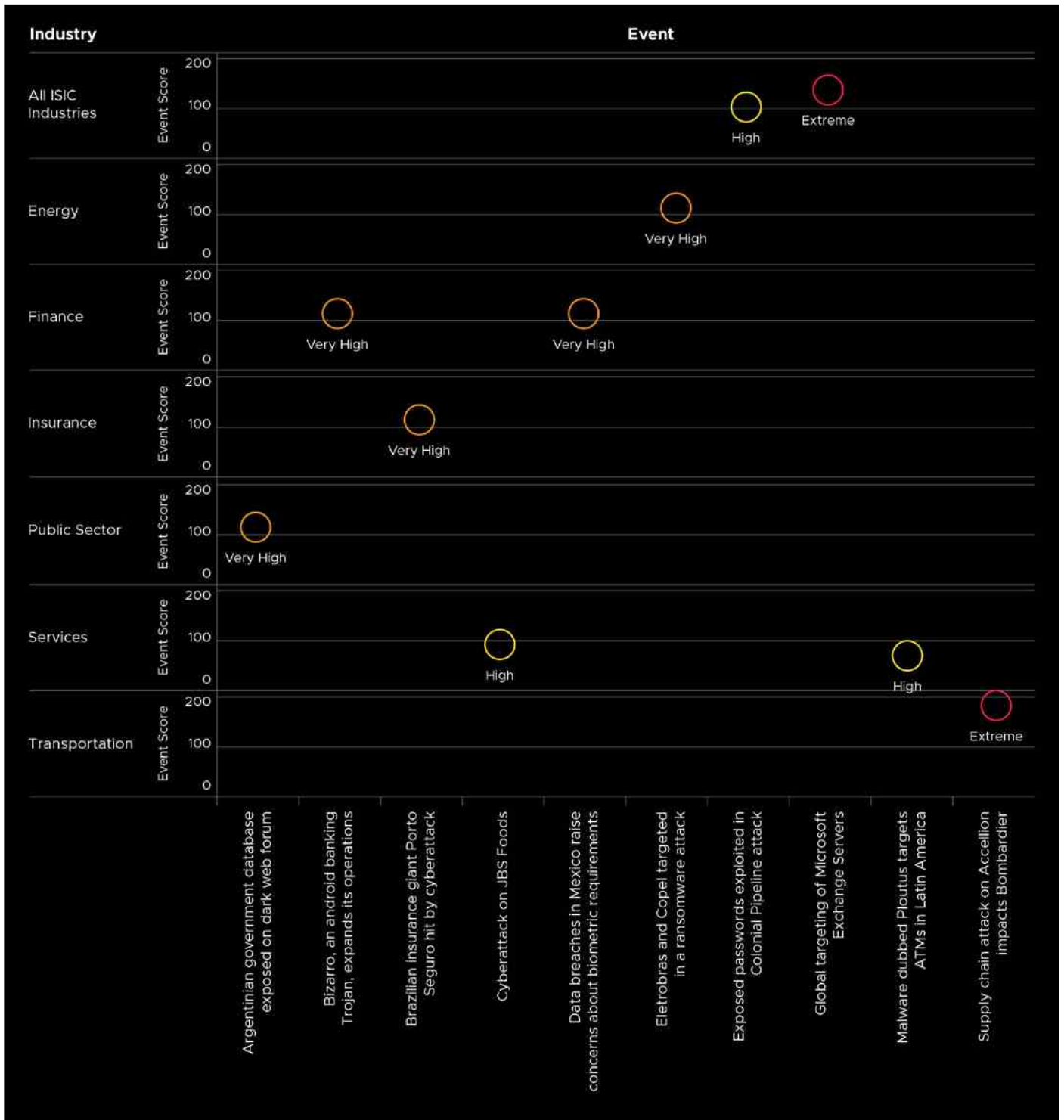
Figure 12 - Top events in Latin America

#1 Global targeting of Microsoft Exchange Servers

Severity: Extreme | **Industries Targeted:** All ISIC Industries

Quick Recap: On March 2, 2021, Microsoft published a detailed report addressing four previously unknown or zero-day vulnerabilities in Microsoft Exchange Server used in targeted attacks. Microsoft stated that a state-sponsored threat actor that allegedly operates from China, known as Hafnium, exploited Exchange email service, allowing them to gain access to internal systems. Additional threat actors have also been observed to exploit the vulnerabilities.

In March 2021, Chile's financial regulator, Comisión para el Mercado Financiero, disclosed that they were targeted in the campaign. Threat actors leveraged the ProxyLogon vulnerability to install web shells and attempted to exfiltrate credentials.

Impact: Hafnium is a threat actor group assessed to be state-sponsored and operating out of China, based on observed victimization, tactics, and procedures. In the attacks, the threat actor group exploited the vulnerabilities to access on-premises Exchange servers. The threat actor group appears to be politically motivated; however, due to the severity of the threat, all industries should be on alert. Additionally, ransomware groups taking advantage of compromised Exchange servers have posed a concern as cyberattack activities ramped up following Microsoft's patch release.

Future Considerations: Trending exploits such as Microsoft Exchange server's vulnerabilities tend to attract attention from ransomware operators and could be used to gain a foothold within an organization's network for malicious activities.

#2 Brazilian insurance giant Porto Seguro hit by a cyberattack

Severity: Very High | **Industries Targeted:** Insurance

Quick Recap: In October 2021, Porto Seguro, one of the largest insurance groups in Brazil, disclosed a cyberattack. The attack resulted in a disruption in their service channel operations and some of their internal systems. Following the cyberattack, the company stated that they had initiated security protocols and resumed operations. The company has shared no further details of the attack and no data exfiltration has been identified.

Impact: The organization suffered a disruption in its service channel operations and internal systems.

Future Considerations: The financial industry in Latin America is growing very rapidly. After COVID-19 hit, financial institutions accelerated their migration to digital services. This has increased the financial industry's attack surface and cyberattacks will likely grow.

#3 Argentinian Government database exposed on a Dark Web forum

Severity: Very High

Industries Targeted: Public Sector

Quick Recap: In October 2021, the Argentinian government suffered a significant data breach. The government database containing the national ID of citizens was for sale on the Dark Web. The database contains information such as the national ID of citizens used for employment and taxation, full name, residential address, and photo. The threat actor behind this breach posted personal information and national IDs of 44 Argentine celebrities as proof. The post further offered to look up citizens' personal information in exchange for a fee. However, the Argentinian government believes it was an insider operation, rather than an outsider intrusion.

Impact: The alleged breach exposed the personal information of Argentine citizens. In addition, national ID and other PII data of influential citizens were published. This could potentially expose the targeted citizens to phishing scams.

Future Considerations: Insiders are responsible for a significant percentage (30% in 2020) of data breaches. Organizations depend on third-party vendors and, in many cases, the absence of proper access control mechanisms could lead to difficulty in assessing insider threats. Additionally, organizations store a large amount of data, increasing the attack surface.

#4 Eletrobras and Copel, two major Brazilian electricity providers targeted in a ransomware attack

Severity: Very High

Industries Targeted: Energy

Quick Recap: In February 2021, Eletrobras and Copel, two major electricity providers in Brazil, suffered ransomware attacks. As a result, Electrobras had to disconnect two nuclear power plants. In addition, Copel was targeted in a ransomware attack believed to have been orchestrated by the DarkSide group. The threat actors claimed to have exfiltrated more than 1TB of sensitive documents such as infrastructure access information, personal details of top management and customers, network maps, backup schemes and schedules, domain zones of Copel's primary site, and the intranet domain belonging to the organization. The threat actors further claimed that they successfully exfiltrated plaintext passwords using high privilege access to the organization's CyberArk solution.

Impact: As a result of the ransomware attacks, both of the organizations experienced disruption, which forced them to shut down and disconnect some of the systems. Furthermore, threat actors exfiltrated sensitive information from Copel.

Future Considerations: Following the Colonial pipeline incident, the DarkSide group has discontinued its operation. However, ransomware attacks targeting the critical infrastructure remain a threat, as the attack surface is constantly growing. Furthermore, there is a high potential for destruction and there are minimal security features in OT. Hence, this trend is expected to grow.

#5 Bizarro, an Android banking Trojan expands its operations

Severity: Very High　　　　　　　　**Industries Targeted:** Finance

Quick Recap: In May 2021, a campaign was observed that leveraged a new banking Trojan dubbed Bizarro, originating from Brazil. The operation targeted Android users in Latin America, with the primary objective of acquiring online banking credentials and hijacking bitcoin wallets from Android users. The threat actors recruited money mules or other affiliates to aid their operations or help with transfers. They commonly use social engineering to install malicious applications on their smartphones to get potential victims. This group hosts their servers on Amazon's AWS, Microsoft's Azure, and compromised WordPress servers to stash their malware.

Impact: Bizarro is a Trojan malware detected targeting South American and European countries. The Trojan first operates by gathering data on the victim before taking control of the machine. This campaign is suspected of continuing to expand to other countries. This campaign predominantly poses a threat to banking credentials and user data.

Future Considerations: The number of newly introduced banking Trojans increased significantly in 2021. The attack surface is constantly growing as more users use their mobile devices for financial operations. The lack of security mechanisms available to regular users makes them the primary target of banking Trojan campaigns. Hence, it is very likely that this trend will continue to grow.

#6 Data breaches in Mexico raise concerns about biometric requirements

Severity: Very High　　　　　　　　**Industries Targeted:** Finance

Quick Recap: On January 23, 2021, the Mexican Network in Defense of Digital Rights (R3D) informed in a press release that databases of Mexican organizations and private banks were being put on sale on the Dark Web forums, following a data breach. The BBVA database (comprising one million records) contains sensitive information, including first name, last name, address, phone number, and Tax IDs. The Santander database (comprising three million records) contains the same information, as well as the account number of each user. In the case of the IMSS database (containing 42 million records), it also includes the information mentioned above, as well as the name and address of the employees and base salary, Clave Única de Registro de Población (CURP), and the affiliation number of the worker.

In addition to the databases mentioned, other databases of Mexican institutions were put on sale on January 25, 2021. Some of these databases are from companies such as Coppel, Movistar, Banamex, National Electoral Institute, Institute of the National Housing Fund for Workers, and Federal Electricity Commission.

Impact: R3D stressed that organizations must inform their users when they are victims of a breach in Mexico. However, at the time of this writing, neither BBVA nor Santander has announced the disclosure of these databases. The damage could be severe, with over 45 million records exposed. Impacted users could be targeted in future campaigns as well.

Future Considerations: A cyber incident should serve as a reminder of organizations' duty in protecting sensitive data. However, with the lack of cybersecurity that private and government organizations in Mexico have in managing their databases, such incidents could occur again in the future.

#7 Supply-chain attack on Accellion impacted Bombardier

Severity: Extreme

Industries Targeted: Transportation

Quick Recap: In December 2020, Accellion discovered several critical and zero-day vulnerabilities (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104) existing in the organization's File Transfer Appliance (FTA) product. FTA is a 20-year-old legacy software designed to allow organizations to transfer large files securely. The vulnerabilities were discovered as Accellion announced that April 30, 2021 would be the end-of-life date for the application. Based on publicly available reports, threat actors successfully exploited these vulnerabilities and implemented a newly discovered web shell dubbed DEWMODE on FTA. Starting in January 2021, some FTA users began receiving extortion emails from threat actors, threatening to exfiltrate data from their environments and publish it on the Dark Web leak site belonging to Clop ransomware operators. The number of targeted victims that reported a similar incident increased progressively through February 2021.

Bombardier reported a compromise due to Accellion's unpatched FTA application. The organization published an advisory on February 23, 2021, confirming that "personal and other confidential information relating to employees, customers and suppliers was compromised. Approximately 130 employees located in Costa Rica were impacted." Bombardier also contacted potentially impacted customers and stakeholders due to this incident.

Impact: Accellion provided software patches for all known vulnerabilities and worked closely with impacted organizations on mitigation efforts. However, around 130 employees in Costa Rica were reportedly affected by exposure of sensitive information due to the supply-chain attack.

Future Considerations: Critical vulnerabilities tend to attract attention from ransomware operators because these exploits could be used to gain a foothold within an organization's network for malicious activities. Additionally, Clop ransomware operators were actively involved in cyber incidents throughout 2021. As a result, the ransomware group is expected to continue targeting various industries worldwide in 2022.

#8 Cyberattack on JBS Foods forces shutdown of the world's largest meat processing company

Severity: High	**Industries Targeted:** Services

Quick Recap: On May 31, 2021, JBS Foods, the Brazilian-based organization, announced that it had been targeted in an organized malware attack on May 30, 2021. The company is the world's leading beef and poultry producer, operating across the United States, Canada, Australia, and the United Kingdom. The enterprise comprises 245,000 employees, serving a considerable portfolio of brands including Primo, Swiftm Seara, and more. The attack reportedly led to an internal system compromise, impacting one of the servers and forcing a shutdown of multiple production facilities. On June 2, 2021, the United States Federal Bureau of Investigation (FBI) published a press release regarding the cyberattack on the JBS Foods internal network stating, "We have attributed the JBS attack to REvil and Sodinokibi and are working diligently to bring the threat actors to justice."

Moreover, JBS Foods disclosed that the breach impacted over 47 facilities across Australia. The organization further stated that no evidence of the compromised data entailing customer, supplier, or employee information was detected. Additionally, JBS Foods noted that a detailed, ongoing forensic investigation into the incident did not uncover any evidence of compromising any financial information. To remediate the impact of the malicious attack, JBS Foods stated that external cybersecurity experts had been consulted to aid in the investigation and take the necessary actions. The JSB US spokesman then continued, "The company took immediate action, suspending all affected systems, notifying authorities, and activating the company's global network of IT professionals and third-party experts to resolve the situation." In Australia, the government worked closely with the organization to restore the facilities, distribution centers, and transportation hubs back online.

JBS Foods notified the federal government that the threat actors operating REvil ransomware had left a ransom note. They had not claimed JBS Foods as a victim on their leak site on the Dark Web at the time of writing this advisory. JBS Foods has stated that the attack did not impact the organization's backup servers, and the "vast majority" of the services were expected to be operational by June 2, 2021.

Impact: On June 2, 2021, the United States Federal Bureau of Investigation (FBI) published a press release attributing the JBS attack to REvil and Sodinokibi.

Future Considerations: On July 13, 2021, REvil's websites became inaccessible at approximately 1 AM EST. In the morning of July 13, 2021, the LockBit ransomware representative posted on a Russian hacking forum and claimed that REvil received a legal request from the government, forcing the ransomware group to close their server infrastructure. Security researchers claim that the evidence indicates REvil suffered a planned and concurrent shut down of their infrastructure.

However, on September 7, 2021, REvil returned, with both their TOR negotiation and data leak sites becoming accessible. All victims listed had their timers reset and their ransom demands were left as they were when the ransomware group supposedly shut down in July 2021. REvil is expected to continue targeting institutions in various industry sectors in 2022.

#9 Malware dubbed Ploutus targets ATMs in Latin America

Severity: High

Industries Targeted: Services

Quick Recap: ATMs in Latin American countries were constantly targeted by organized threat actors during 2021. Previous attempts involved breaking into the device's cabinet to access the physical ports and drives and installing a CD boot disk dubbed "Ploutus." Researchers recently uncovered the fifth variant of the malware, named Ploutus-I.

Most ATMs run a version of Microsoft Windows. However, Windows is not designed to run ATMs, so most run Extensions for Financial Services (XFS). This is a set of APIs designed to link the host Windows systems to the specific features of ATMs, such as displays and PIN pads. Additionally, most ATM vendors leverage a middleware layer, such as Aptra and Agilis, to interact with XFS. For example, all previous versions of Ploutus were observed to target middleware; however, Ploutus-I instead communicates directly with XFS to command the ATMs to disgorge money.

Impact: The operators were aware of the exact ATM version and its physical capabilities. After the malware is installed, the Ploutus gang employs a money mule to perform the cash-out. However, according to publicly available reports, it is not clear how the physical transfer of money occurs between the threat actors and money mules.

Future Considerations: The trend of targeting ATMs is not new in Latin America. Threat actors have persistently targeted ATMs since 2013, with criminals seeking to compromise the machines and collect their cash. Moreover, financial institutions across Latin America do not have a great track record of information sharing. Additionally, financial institutions heavily lack employing the best cybersecurity practices. Unless action is taken to counteract these incidents, threat actors are expected to continue targeting ATMs in the future.

#10 Colonial Pipeline attack, the exposed password for stale VPN account suspected as an initial infection vector

Severity: High

Industries Targeted: Services

Quick Recap: Researchers have identified that as part of the initial infection vector, the threat actors leveraged an abandoned account to establish a VPN (Virtual Private Network) connection and eventually connect into the internal network. Although it is unclear how the credentials were obtained initially, publicly available reports indicate that the account's password had been detected on Dark Web credential leaks of other third-party breaches. This finding suggests that the account holder might have used a similar password on other accounts as well.

On May 12, 2021, DarkSide claimed to have targeted three other companies, with their names posted on DarkSide's leak site. The data published on their site includes summaries of what was stolen, but not the actual data. One of the companies is located in the US state of Illinois and DarkSide claims to have stolen more than 600GB of critical data. The second attack was on a Brazilian company, where the threat actors exfiltrated over 400GB of sensitive information. Finally, a Scottish company also was targeted by DarkSide, where approximately 900GB of data was allegedly stolen. According to researchers, the criminals behind DarkSide ransomware brought in at least $60 million in their first seven months of operation, with approximately $46 million acquired during the first quarter of 2021.

Impact: The DarkSide operators have prior experience with other ransomware threat actor groups and are quite successful in this operation. They are also using their leak site to publish compromised data, which could lead to the disclosure of personally identifiable information (PII), intellectual property, and loss of reputation.

Future Considerations: On May 14, 2021, the DarkSide group allegedly closed its operations due to losing access to ransomware infrastructure servers. However, on July 31, 2021, the ransomware threat actors allegedly returned, rebranding themselves as BlackMatter ransomware. The encryption algorithm within the decryptor reveals the similarities between DarkSide and BlackMatter, indicating that the threat actors operating the ransomware are identical. Despite the rebranding, the group posted a message on their website on November 1, 2021, announcing that the entire operation would be shutting down within 48 hours, allegedly due to increased pressure from the authorities.

DarkSide has previously shut down and returned under a different name. It is likely that this could occur again soon.

Middle East and Africa Constellation

G1 – Actioning 2022: Regional Themes and Trends

The section below provides key regional themes and trends observed throughout 2021. These insights provide valuable insights to organizations on what to expect from a geopolitical and cyberthreat perspective in 2022.

Financial Gain and Political Advantage Will Continue to be Top Motivations for Attacks

In 2021, almost a third (31%) of the geopolitical and cybersecurity events in the region were motivated by financial gain and political advantage. This trend is likely to continue, given that other motivation factors were much less common over the past year, such as vandalism (11%), dominance (11%), and terrorist activities (10%).

Understanding the motivations behind cyberattacks contributes to better countermeasures. Financially motivated attacks are typically (but not always) conducted by threat actors through ransomware attacks. Organizations should assess the most common ransomware tactics and implement appropriate controls, including data breach liability insurance.

Data compromises not only impact business economics, but could also be used to mislead the public or cause political tensions. Therefore, organizations should be mindful of securing sensitive information tagged as critical assets and maintaining proper backups required for restoring any data that might be compromised.

Iran Likely to Continue Experiencing the Most Significant Geopolitical and Cybersecurity Activity in the Region

31.1% of the major geopolitical and cybersecurity events in the region are related to Iran, followed by Israel (18.1%), Saudi Arabia (10.3%), and Lebanon (5.8%).

Iran scores the top place with significant geopolitical and cybersecurity-related activities. This is due to the political differences with surrounding countries. The Islamic Revolutionary Guard Corps (IRGC) ultimately oversees Iran's offensive cyber activities without overlooking publicly elected officials in the country. The United States and a few other countries speculate that Iran receives technical assistance from Russia and North Korea. But, there has been no evidence to support those claims. However, Iran has acquired hardware for internet surveillance from Chinese telecommunication firms and maintains strong agreements with Russia on cybersecurity.

Israel and Saudi Arabia have always been at the forefront of advancements with cybersecurity-related tools. To control attacks from their opponents, they developed a solid infrastructure to prevent and contain those attacks. However, organizations not related to past attacks or incidents might still observe potential threats from the threat actors from other parts of the world.

Iran-based Threat Actors Will Continue to be the Most Active

The most active threat actors in the Middle East and Africa region are from Iran. 55.5% of the threat actors originated from Iran, followed by Israel (4.4%) and Lebanon (4.4%), while 15.5% were from threat actors with Unknown origin. Bax026 and Agrius, two Iran-based threat actors, are prominent threat actors, with a 5.4% share each.

Most of the time, Iran adopts an asymmetric warfare approach to accomplish its military, political, and cyberwarfare capabilities, which provides the means to attack stronger adversaries. Widely seen threat actor groups Include Siamesekitten, an Iranian APT group responsible for supply-chain attacks against IT and communication companies in Israel. Other threat actors include Charming Kitten, Agrius, OilRig's, MuddyWater, and Badblood.

Government and Public Sectors Are Prime Targets for Threat Actors

The top industries impacted by geopolitical and cyber events were government and public sector (49%), defense (4%), transportation (3%), energy (3%), and technology (3%).

The government and public sector is always a prime target for the threat actors. Most of the attacks are from organized crime groups, foreign countries, and political hacktivists. These attacks can cause a severe impact on operations and impede the ability to deliver necessary functions in a timely manner. This means that cybersecurity is a considerable growing concern for the government and public sectors. Increasingly, federal, state, local governments, and public entities are targets, as the threat actors attempt to steal or manipulate sensitive information or cause disruption to operations.

On the Lookout: Cyberattacks to Originate from both Inside and Outside the Region

Most cyber-related incidents were inbound attacks originating from a different place than the target location (52.6%), followed closely by outbound attacks originating from the Middle East and North Africa (47.3%).

Technology has become more accessible and affordable. Therefore, any individual with criminal intent can exploit the targets with ease. Also, ransomware or malware developers publicly sell the code or the software on Dark Web forums. So, organizations should actively gather threat intel to prevent the threat actors from exploiting their networks. Security controls must be kept updated with threat feeds. And maintaining asset inventory and actively patching all the assets is also critical.

Ransomware Will Continue to be the Top Method Used in Cyberattacks

Among the most significant cybersecurity events observed in 2021 in the region, the top three methods used by the threat actors were ransomware (17%), malware (10%), and spear phishing (8.7%).

The government and public sector is always a prime target for the threat actors. Most attacks are from organized crime groups, foreign countries, and political hacktivists. These attacks can cause a severe impact on operations and impeed the ability to deliver necessary functions when needed. This makes cybersecurity is a considerable growing concern for the government and public sectors. Increasingly, federal, state, local governments, and public entities are targets as threat actors attempt to steal or manipulate sensitive information or cause disruption to operations.

G2 – Geopolitical Overview

Here are some of the most significant geopolitical and regulatory developments observed in the region in 2021.

Israel, Iran Cyberwar Attacks on Civilian Targets

Israel and Iran have been engaged in a proxy war for a long time. Alhough the scope of the war has historically been between the respective governments and militaries, this has changed in the recent past. There have been multiple instances of civilian targets being considered under the scope of cyberattacks. One such example is the cyberattack on the Iranian fuel distribution system, making it impossible for Iranian drivers to buy gasoline. This attack paralyzed Iran's 4300 gas stations, which took almost 12 days to be fully restored. In retaliation, a cyberattack was launched by some Iranian actors targeting a major medical facility and a popular LGBTQ dating site, leading to the public disclosure of sensitive personal data of thousands of Israeli citizens. It is speculated that the respective governments have carried out these attacks to send an aggressive message to their counterparts. These cyberattacks on civilian targets between countries could create a new era of information and cyber warfare in the region, and be utilized widely to pressure the governments.

France Has Led Counterterrorism Operations in the Sahel Region of Africa

France has led counterterrorism operations in the Sahel region of Africa, where it has been focusing on the Islamic State in the Greater Sahara (ISGS) and, to a lesser extent, al-Qaeda affiliates in the region. France announced in July 2021 that it plans to withdraw over 2,000 of its current 5,400 troops by early 2022. The threat in the region will likely increase after this withdrawal. ISIS and al-Qaeda have repeatedly highlighted the importance of launching cyberattacks. However, despite their imposing rhetoric, the jihadists have yet to demonstrate any sophisticated cyber skills or conduct damaging cyber operations.

Lebanon Elections 2022

After two years of political paralysis and economic decline, the Lebanese state is falling apart. Service institutions and critical infrastructure are shutting down. Political elites appear unable to initiate overdue reforms that would compromise their hold on power. A cyber incident is expected to take place to manipulate the 2022 elections. Threat actors could exploit outdated versions of election software and databases or deploy ransomware against election vendors. Moreover, threat actors could target reporters by manipulating the results on election night.

UAE's Preparations to Address Cyber-Related Threats in the Coming Days

The United Arab Emirates (UAE)'s national budget will see a significant investment in cybersecurity standards for government agencies over the next five years . Cybersecurity is seen, primarily, as a sovereign priority for the nation. The UAE has developed several initiatives in the cybersecurity space, including forming a Cybersecurity Council, modernizing its cybersecurity strategy to respond to attacks and threats, and investing in digital transformation in a largely virtual world. The Gulf state is also looking into sharing more information efficiently between agencies, organizations, and sectors, both nationally and internationally. This significant investment in cybersecurity responds to pandemic-induced needs to invest in digital transformation and digital infrastructure. The UAE has been one of the most targeted countries in the region during the pandemic . However, just as important is that the UAE understands the critical need to firmly secure its cyber borders, given geopolitical developments in the Middle East.

Growing Cryptocurrency Trend in Middle East Is a Concern

Investments in cryptocurrency and blockchain technologies are a trend that continues to grow in the region. Dubai is particularly active in this space, having launched Bitcoin on the Dubai Nasdaq Exchange and supporting the creation of cryptocurrency-based businesses. Organizations should remain aware of emerging regulations in this space. For example, in October 2021, Dubai announced rules for investment tokens such as securities and derivatives. Saudi Arabia has generally refrained from supporting virtual currencies, given the links to cybercriminals and other illicit activities. Organizations investing in cryptocurrencies or who might be required to pay a ransom demand should proactively assess how these, and other developments, might affect their business.

Saudi Arabia Introduces Stringent Privacy Law Requirements

Saudi Arabia introduced its first privacy law on September 24, 2021 (to take effect March 23, 2022) and is likely to have significant financial and other impacts on organizations investing in compliance. The Personal Data Protection Law (PDPL) regulates data transfers and data protection of personal information undertaken by companies or public entities. The PDPL also provides new rights to Saudi residents, including access rights, rectification, erasure, and the right to claim damages for material and non-material loss, including cyber breaches. Penalties for non-compliance could include imprisonment for up to two years or a maximum fine of SAR 3,000,000 (~ USD 800,000).

G3 – Cyberthreat Regional Overview

MuddyWater

Industries Targeted	Continents Targeted
Services,Transportation, Public Sector, Safety, Energy	Azerbaijan, Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Saudi Arabia, Tajikistan, Turkey, UAE, Ukraine

MuddyWater is also known as: TEMP.Zagros, Static Kitten, Seedworm, MERCURY, COBALT ULSTER

During 2020-2021, several prominent Israeli organizations were targeted by ransomware attacks. Analysis of the attacks suggests connections to Iranian state actors dubbed MuddyWater (also known as Static Kitten, TEMP.Zagros, and Seedworm). It is speculated that the campaign was following a political agenda, due to the rising tensions between the two nations. Based on an analysis of past incidents, the threat actors might predominantly target government and educational institutions going forward. Since the motive is related to political interests, the threat actors may remain active and their activities can be widely observed.

Looking into technical details, the threat actors appear to employ two tactics in this campaign. The first tactic involves initiating an attack using phishing emails containing a malicious PDF or Excel file. Upon execution of the attachment, a secure connection using OpenSSL is created between the victim's machine and a Command and Control (C2) server, which is then used for downloading a payload. The second tactic consists of scanning public-facing infrastructure for unpatched Microsoft Exchange servers and attempting

to exploit CVE-2020-0688 to install a webshell and download a payload. The payload in both scenarios is a malware named PowGoop, a PowerShell-based module that acts as a loader.

Additionally, PowGoop utilizes a fake Google Update DLL file to execute on the victim's machine and prepares the infected environment to conduct the next attack phase, deploying Thanos ransomware. Thanos ransomware is a strain of malware first discovered in January 2020. It is primarily offered on Russian-speaking hacker forums as Ransomware-as-a-Service (RaaS). Researchers have, to date, analyzed more than 130 unique samples of Thanos. This malware boasts a highly modular architecture and is capable of containing various unique combinations of tools in each produced sample. Additionally, in the more recent versions, features such as rewriting the hard drive's Master Boot Record (MBR) were added to the available capabilities of Thanos.

Shamoon

Industries Targeted	Continents Targeted
Services, Defense, Energy, Finance, Public Sector, Manufacturing, Transportation	Saudi Arabia

Shamon is also known as: Disttrack

Shamoon malware was used in the data breach at one of the largest public petroleum and natural gas companies, Saudi Aramco. The compromised data includes employee information, including PII (Personal Identifiable Information) and other crucial documents such as pricing sheets, network topology diagrams, IP addresses, and client details. Threat actors released sample data to a data breach marketplace. The onion leak site had a countdown timer set to 662 hours and stated that after the countdown expired, the negotiations would begin; the price tagged was $5 million, which was negotiable. Based on the reports, Saudi Aramco and the threat actors have confirmed that this incident is unrelated to a ransomware attack. Technical details on this incident are not entirely known, but the initial access was obtained by exploiting a zero-day vulnerability.

APT34

Industries Targeted	Continents Targeted
Services, Manufacturing, Energy, Finance, Public Sector, Safety	Iraq, Israel, Jordan, Kuwait, Lebanon, South Africa, Turkey, United Arab Emirates

APT34 is also known as: Twisted Kitten, Cobalt Gypsy, Crambus, Helix Kitten, OilRig, APT 34, IRN2

Iranian threat group APT34 was observed targeting Lebanese companies using a backdoor named SideTwist. Since the first discovery of APT34, the group has been actively developing malware to evade detection. In addition, the threat actor group has also been observed using the widely used job opportunity luring technique to send malicious content over LinkedIn. Furthermore, the APT34 group has often used DNS tunneling for data exfiltration, making it easy for them to evade firewalls and other security controls. In the past, they have used an open-source utility called DNS Exfiltration. DNS Exfiltration uses DoH (DNS over HTTPS) as one of the ways it exfiltrates data from target systems. DoH is a protocol that encrypts DNS requests and is intended to be used for privacy purposes.

APT34 is also known as OilRig and Twisted Kitten. These groups frequently rely on social engineering and supply-chain attacks to breach victims. Activities of this group could increase in the coming days, considering the alleged involvement of the Nation-state. This is a forerunner of information published by Lab Dookhtegan on Telegram channels. The leaked information revealed APT34's hacking tools, infrastructure, victims, and the associated members.

Meteor

Industries Targeted	Continents Targeted
Public Sector, Transportation	Iran, Syria

A wiper dubbed Meteor, which was developed by a threat actor group named INDRA, was used to target Iranian railways and the impact was significant. The websites went down, causing significant disruptions to train services, and the threat actors displayed messages on the railway's digital boards stating that the delays were due to a cyberattack. A wiper is a malware that deletes files on the victim's system, after which it becomes unbootable.

The threat actors used RAR archives and later added the files to network shares. Additionally, the threat actors modified Windows group policies to launch the setup.bat file and then copied other files to the local devices and executed them. The process follows by evading all of the security detections and finally launching the wiper malware. It is possible that more advanced wiper malware could be developed in the future and become more accessible and affordable to the public for malicious usage. As most of the wiper malware developers intend not to generate revenue, their main goal is to create chaos for the victim organization or distract technical individuals while another attack is taking place.

Tracer Kitten

Industries Targeted	Continents Targeted
Services	Unknown

Tracer Kitten is also known as: Greenbug

Tracer kitten (a.k.a Greenbug) is an Iran-based threat actor motivated by espionage campaigns. First observed in 2016, the group predominantly targets telecommunications industries in the Middle East, North Africa, and South Asia. The group uses both custom and publicly available malware. For example, in a recent campaign, the Tracer Kitten group deployed DNSDAT and Plink to proxy the traffic from the victim to the threat actors. The victim includes an unknown technology and telecommunication company in both the Middle East and North Africa and a South Asian telecommunications provider.

G4 – Industry Threat Landscape

Within the Middle East and Africa, the Services Sector and the Public sector are examples of critical industries that have been targeted by cyberattacks throughout 2021. In addition, throughout several sectors, there has also been increased activity from Iranian Threat Actors (mainly targeting Israeli organizations) in the Middle East. The following graphic depicts the most substantially hit industries within the Middle East and Africa, based on Severity Score per event.
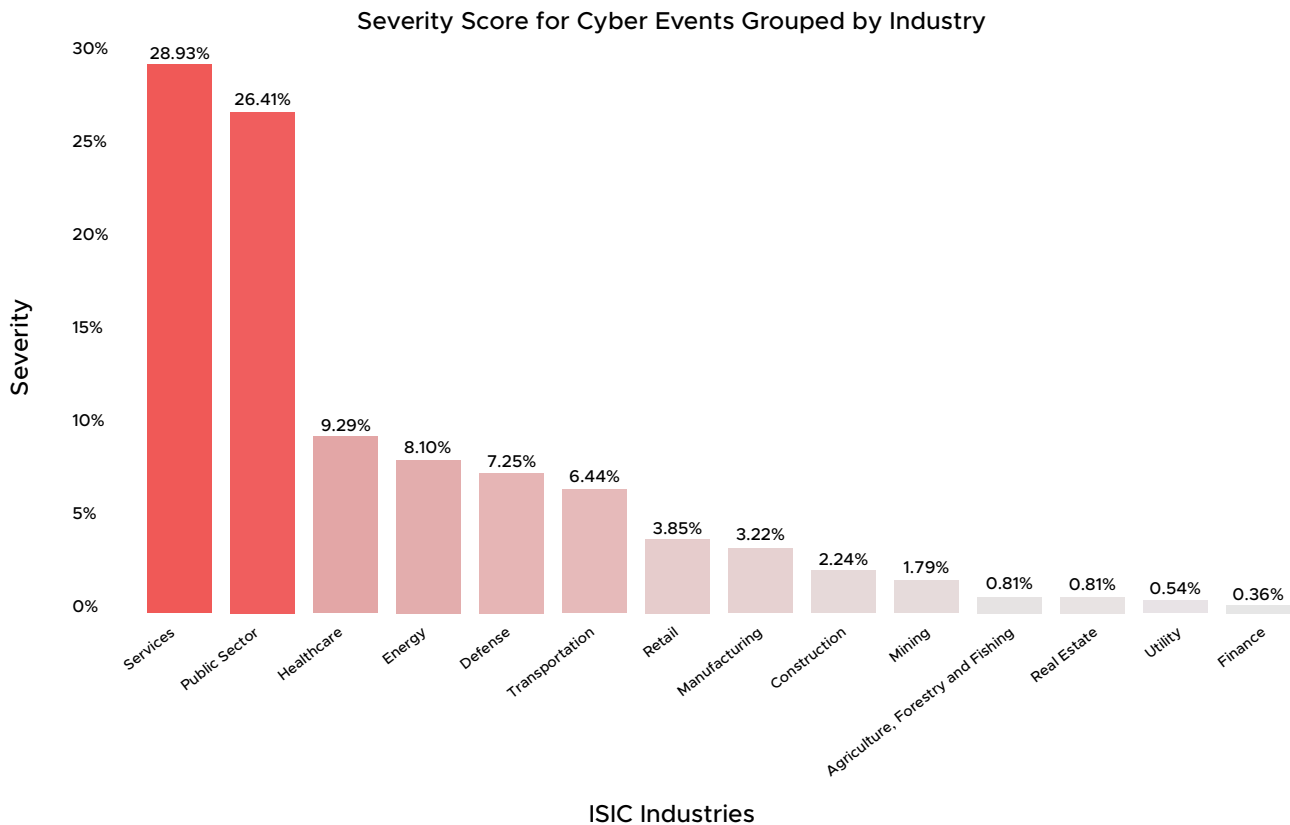
Figure 13 - Industry threat landscape in Middle East

Technology, Education, Hospitality, Press, and Media Services Are the Highly-Targeted Sectors in the Middle East and African Regions

The service sector is the most targeted, covering about 30% of the threat landscape in this region. The sub-sectors within the service sector are fragmented: technology at 41%, education at 22%, hospitality at 20%, and press and media services at 17%. Attacks performed by Lyceum, Deus, and coomingProject groups have resulted in data compromises, severe damages, and downtime to network infrastructures, including operational downtime in victim organizations.

Vulnerable devices, compromised accounts, and phishing emails are the primary vectors to gain initial access to victim networks. Financial gain seems to be the main motive behind most cyber incidents in 2021. TA453, Agrius, NSO group, and Hexane are among the threat actors to watch out for in the coming days. These threat actors might specifically target the service sector. There are some well-known methods that the threat actors utilize when performing an attack, including credential harvesting, spearphishing, HTTP Tunnelling, DDOS, and Waterholing. Due to continuous developments in technology and heavy investments coming into the Middle East and Africa, organizations in these regions should be prepared with all the defenses that could help prevent a breach.

APT Groups Are a Constant Threat to Government and Public Entities in This Region

The public sector sits in second place among the most targeted industries in this region, covering about 27.6% of the threat landscape. Government institutions were the most targeted by the threat actors within the public sector. APT34, Bax 026 of Iran, Lab Dookhtegan, Lyceum group, MuddyWater, Vanda TheGod, and charming kitten are the threat actors targeting the public sector and causing significant impact to network operations within the victim organizations. Financial gain and political advantage remain the top two motives for the threat actors to initiate the attack by utilizing spear phishing, vulnerability exploitation, and social engineering methods.

The threat actors prominently used PHP web shells, PowerShell, and remote desktop applications to perform a successful attack. Additionally, the Telegram application was used to establish communication between affiliates.

Ties between Nations Majorly Benefit to Defend Threat Actor Activities

In 2020, Israel and United Arab Emirates (UAE) signed a historic peace agreement in which UAE officially recognized Israel. These ties paved the way for a new alliance in the Middle East to counter the threat actors targeting critical infrastructure. Israel and the United Arab Emirates (UAE) have reportedly shared intelligence related to the Volatile Cedar threat actor group, which was responsible for compromising approximately 250 servers across Egypt, UAE, Saudi Arabia, Lebanon, Israel, and Palestine.

These two nations have also been working on significant technological developments in the Middle East region, with its niche in blockchain, cybersecurity, AI, and Quantum computing.

Significantly Increasing Threat Landscape in African Countries

Africa's cyberthreat landscape continues to increase, with more attacks targeting the public sector. As a result, most organizations have significantly focused on upscaling security controls due to the remote working setup and more assets being prone to attacks. As a result, cloud usage has proliferated, which explains why the use of cloud-based applications and platforms such as Microsoft Office 365, zoom, Google workspace, Microsoft Azure, and Amazon Web Services increased. In 2021, the biggest concern for cloud services entities was managing user access to information, data loss, and recovery.

Email attacks, web-based attacks, social engineering, deploying malware, and ransomware are the top techniques that the threat actor uses to conduct an attack. In some African countries, including South Africa, the threat landscape is low overall compared with North America and Europe in terms of cyberattacks. However, the threat actors are getting faster, more intelligent, and more automated. So, it is essential for organizations in the African region to follow the trends and upgrade their cyber posture regularly.

Hospitals and Healthcare Facilities in Iran, South Africa, and Israel Are Likely to be the Continuous Targets for Threat Actors

The healthcare sector sits in third place among the most targeted industries in this region, covering about 9% of the threat landscape. Major attacks on this sector include medical company Olympus; APT35 targeting Israeli genetic, neurology and oncology researchers; and Israeli hospitals. Additionally, BlackMatter and APT35 are the top threat actors targeting the healthcare sector in this region by utilizing the water-holing method and deploying malware. Financial gain and political advantage are the principal motivations, followed by hacktivism and cyber espionage.

These attacks caused disruptions to hospital operations resulting in the cancellation of new medical appointments. The main reasons behind these attacks are organizations utilizing outdated versions of email servers and virtual private networks (VPNs), which contained numerous vulnerabilities that could be exploited to access the victim's infrastructure.

Other Fragmentations in the Middle East and Africa Regions

Other sectors that complete the cyberthreat landscape in this region include healthcare at 9%, energy at 8%, defense at 7%, transportation at 6%, retail at 4%, manufacturing at 3%, construction at 2%, mining at 1%, agriculture at 0.8%, real estate at 0.8%, utility at 0.5%, and finance at 0.3.

Severity Score for Cyber Events Grouped by Industry

Government & Public Sector 1087	**Multiple Industries** 675	**Energy** 438
	Healthcare 295	**Retail** 258	**Transportation** 232
Technology 831	**Education** 288	**Defense** 189	**Financial Services & Insurance** 168	**Media** 108
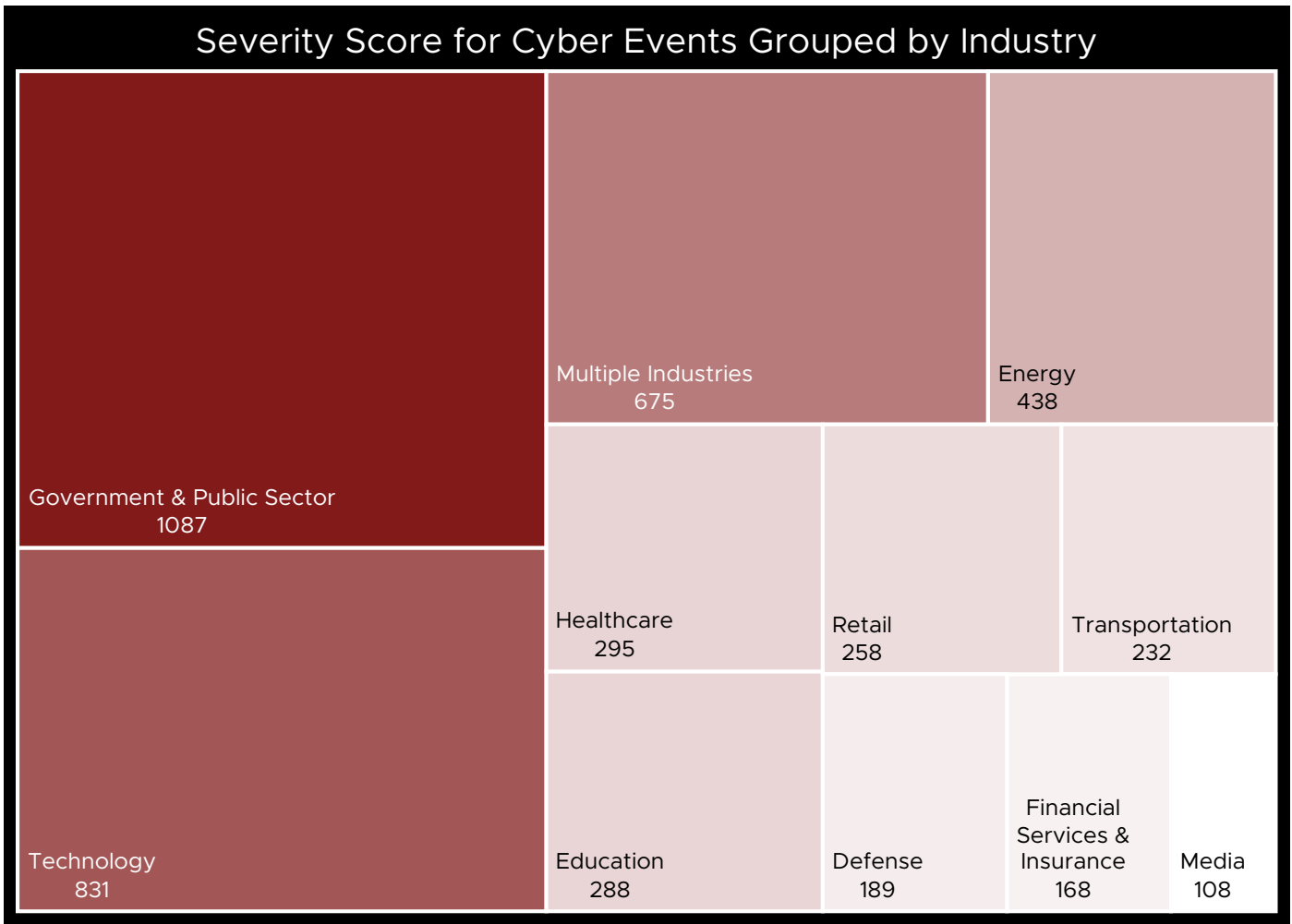
Figure 14 - Severity Score for Cyber Events Grouped by Industry

Government and Public Sectors Should Remain on High Alert

The Government and Public sectors in the Middle East and Africa were the most impacted in 2021. Given the importance of these sectors, especially to national security, we can anticipate that threat actors will continue to target them in 2022. For example, a significant event conducted by threat actor group "Indra" targeted Iran's transport ministry and national train system, disrupting train services and taking down their websites. There have also been links relating this attack group to the Wipers malware attacks that were previously carried out against Syrian organizations.

Ransomware and Data Theft Are a Constant Threat within the Technology Industry

The technology sector in the Middle East and Africa saw notable attacks throughout 2021. Campaigns orchestrated by threat actors such as BlackShadow, Deus, and Siamesekitten led to personal data theft/compromise and alarming disruptions in services for the victims. Additionally,There was noteworthy activity by Iranian threat actors in this space. These attacks are usually tied to financial gain through ransomware or similar attacks. Finally, elements of espionage were also observed., For example, Siamesekitten conducted impersonation attacks on technology companies to gain access to networks and conduct espionage.

Energy Sector Is Target of Threat Actors and Political Activists in 2021

The energy sector also observed several cyberattacks throughout 2021 within the Middle East and Africa. Activities ranged from ransomware and data theft to political activism. Prominent attacks against this industry include the data theft campaign targeting Saudi Aramco and the cyberattack on gas stations across Iran in the form of hacktivism.

APT Activity Continues within the Middle East

Activity from Middle East-based APT groups also continued during 2021. It was observed that APT 34 conducted a cyber-espionage campaign against Lebanon. At the same time, it was confirmed that APT 35 targeted several US-based and Israeli genetic, neurology, and oncology researchers in a phishing campaign to gather user credentials.

G5 – Key Lessons from Most Impactful 2021 Attacks

The Middle East and Africa region have seen their share of significant cybersecurity events that have significantly impacted organizations and entities across various sectors and countries. We've highlighted the top ten events of 2021 according to their severity level. The severity rating considers many factors, including the economic impact of the event, whether a ransom was demanded, which industry was affected, what type of information was breached and the quantity, level of disruption to operations, etc. The rating criteria are defined as low, medium, medium-high, high, critical, or extreme.
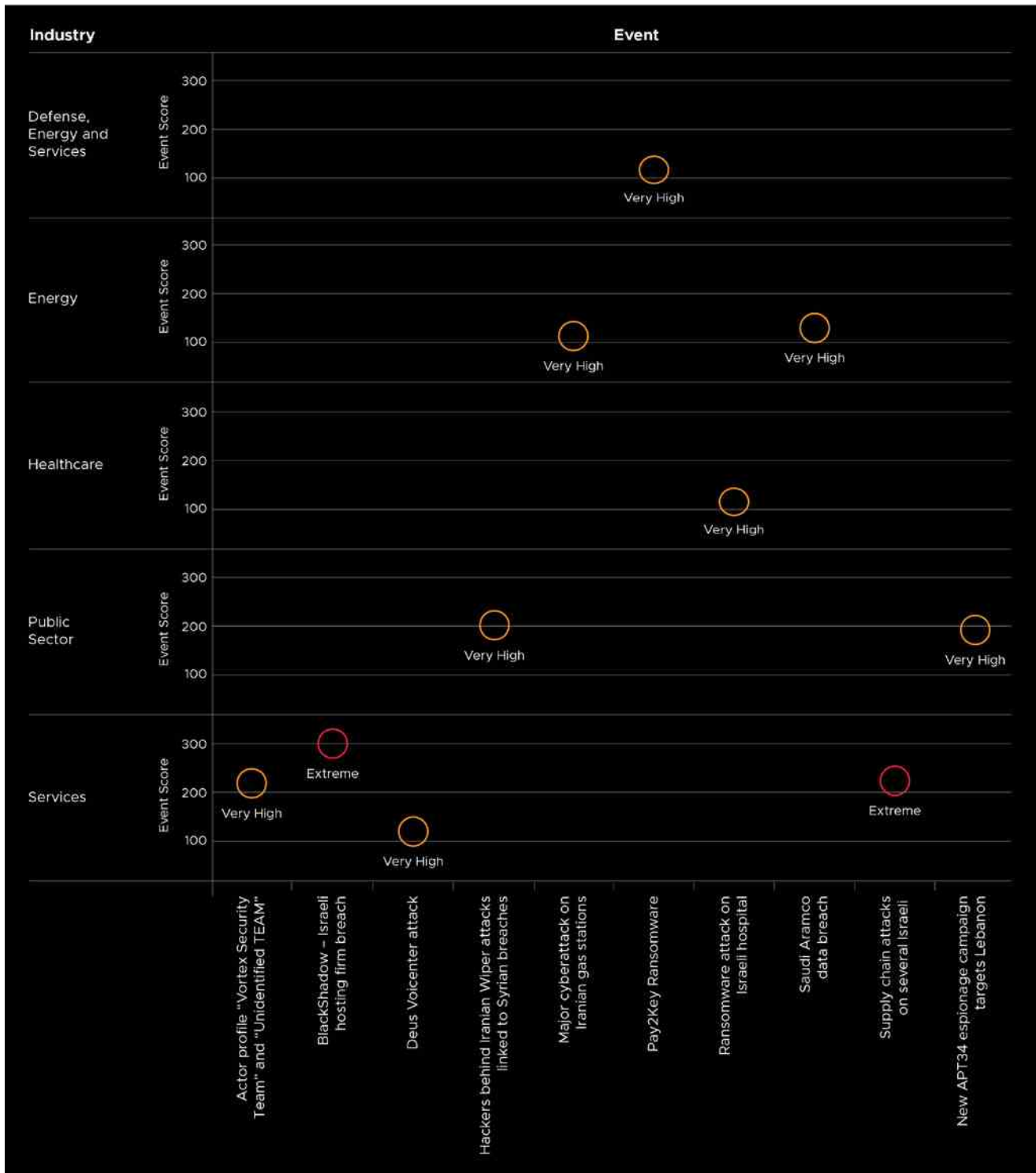
Figure 15 - Top 10 events in Middle East

The list of top ten cybersecurity events is addressed in more detail below. Provided are a brief description of each event, its impact on the affected organizations, and key considerations that all organizations should take away as they plan their cybersecurity strategy for 2022.

#1 BlackShadow hackers breach Israeli hosting firm and extort customers

Severity: Extreme

Industries Targeted: Services

Quick Recap: On November 1, 2021, the Israeli web development firm and hosting company Cyberserve (used by various organizations, including local radio stations, museums, and educational institutions) was attacked by the hacking group BlackShadow. Websites hosted at Cyberserve were made inaccessible due to the incident. BlackShadow claimed responsibility for the attack and demanded $1 million in cryptocurrency to not leak the stolen data. Although the deadline was set at 48 hours, BlackShadow immediately revealed a sample of 1,000 records to prove that they were in possession of the data. Included in the theft was a database containing the personal information of a large LGBT site named Atraf. This increased the impact and sensitivity of the theft because releasing this type of information in conservative societies puts individuals at significant risk. Cyberserve denied claims of negotiation by BlackShadow and has also emphasized that they do not intend to conduct negotiations with the hacking group.

Impact: BlackShadow leaked the entire database of sensitive personal information from Israel's Machon Mor medical institute, containing medical records for 290,000 patients. These records included medical treatments, appointments, test results, and vaccination records. BlackShadow also claimed to have uploaded the entire Atraf user database, as their demands were rejected.

Future Considerations: BlackShadow remains a threat for 2022. This is not the first time it has attacked Israel, attempting to disrupt Israeli interests. In 2020, BlackShadow conducted a similar attack on the Israeli insurance company Shirbit, also demanding a payment of $1 million in cryptocurrency while threatening to leak stolen data.

#2 Iranian hackers target several Israeli organizations with supply-chain attacks

Severity: Extreme

Industries Targeted: Services

What Happened: In May and July 2021, the Iranian hacking group Siamesekitten (aka Lyceum or Hexane) conducted several supply-chain attack campaigns on IT and communication companies in Israel. The hacking group conducted the attacks by impersonating the organization and its HR staff to target potential victims with fake job offers to penetrate their computers and access its client database. The job offers sent by the impersonated firms led the victims to a phishing website that contained files that unloaded a backdoor known as Milan. This would establish connections with a remote server and download a second-stage remote access Trojan named DanBot. The attack chain culminates in the installation of the C++-based Milan backdoor. In July 2021, the group replaced Milan with a new implant called Shark that is written in .NET.

Key Impact: IT companies such as ChipPc and Software AG have become subject to a targeted attack from Siamesekitten. Like others, they are still at risk of employees becoming victims of this impersonation attack.

Future Considerations: The Iranian group has been active since 2018 and, in the past, has mainly targeted oil, gas, and telecom companies. However, there have also been similar campaigns to this attack style conducted by Siamesekitten. Many attack groups use this technique, such as the North Korean Lazarus campaign in 2020 and the Iranian OilRig campaign that targeted Middle Eastern victims in the first quarter of 2021. It is believed that the group is attempting to conduct espionage and gain access to networks with the possibility of a future malware or ransomware attack. More generally, impersonation is a widely used attack vector and will likely be a threat throughout 2022.

#3 Tag Team: "Vortex Security Team" and "Unidentified T E A M"

Severity: Very High

Industries Targeted: Services

What Happened: Two Iran-based threat groups dubbed "Vortex Security Team" and "Unidentified T E A M" are often seen claiming responsibility for a cyber incident. However, because of the overlap, the two groups appear indistinguishable. For example, both groups claimed responsibility for several cyberattacks against Israeli businesses, one of which involved wiping server hard disks and infecting Industrial Control Systems (ICS) that belong to Israeli companies.

On January 6, 2021, the Unidentified T E A M claimed to have compromised the network of Four Point by Sheraton hotel in Perth, Australia. The group demonstrated their access by sharing a video of them gaining remote access to the Programmable Logic Control (PLC) panel that controlled the management system of the building, including Heating, Ventilation, and Air Conditioning (HVAC). Incidentally, on January 5, 2021, the Unidentified T E A M claimed to have gained access to a PLC panel controlling the US-based power plant dubbed "Wetwinds." The threat group provided evidence of their access by sharing a screenshot of the PLC panel showing an Iran-based Internet Protocol (IP) address falling under an autonomous system controlled by the Mobile Communication Company of Iran.
The two threat groups operate multiple Telegram channels to expand knowledge on Tactics, Techniques, and Procedures (TTPs) for cyber operations. Additionally, these channels are used to share information among threat actors.

Key Impact: The threat groups proved their capability to infiltrate into PLCs to control equipment used in the organization's system infrastructure and shared a video to demonstrate their successful compromise.

Future Considerations: These two threat groups have a history of targeting Israeli companies in 2020 and 2021, but have recently expanded their range of attacks against western businesses. With the further development of attacks, it is expected that these threat actors will appear again in future campaigns in 2022.

#4 Hackers behind Iranian wiper attacks linked to Syrian breaches

Severity: Very High

Industries Targeted: Public Sector

What Happened: A threat actor group dubbed Indra targeted Iran's transport ministry and national train system, disrupting train services and taking down their websites in August 2021. This threat group was previously engaged in a destructive attack against various Syrian organizations by deploying a malware called wipers. Wipers intentionally destroy data or brick-breached devices. Occasionally, threat actors leverage wipers as cover for other cyberattacks occurring simultaneously. For example, Indra's operators utilized the Meteor wiper against the compromised system. Additionally, the threat group would display messages on the railway's message board that the trains were delayed or canceled and prompted the passengers to contact the office of Supreme Leader Ali Khamenei for additional information.

In a report published in early August 2021, security researchers claimed that Indra managed to stay under the radar during the reconnaissance stage of their cyberattack despite showing a lack of skill. This indicates an uncoordinated division of responsibilities across teams. In addition, researchers stated that their methods are verbose and disorganized, unbecoming of advanced threat actors. Regardless, Indra identifies as a group of threat actors against the Iranian regime with alleged ties to cybercriminals that target entities affiliated with a branch of the Iranian Armed Forces named the Islamic Revolutionary Guard Corps (IRGC).

Key Impact: The threat group primarily leverages wipers to delete data on compromised systems completely. Furthermore, the group disrupted train operations after a successful compromise.

Future Considerations: Based on the threat group's social media activity since 2019, researchers found claims of four other cyber incidents occurring in 2019 and 2020. However, the group did not claim responsibility for an attack against Iranian Railways and the Ministry of Roads in July 2021, despite the similarities in the Tactics, Techniques, and Procedures (TTP) used.

#5 Saudi Aramco data breach sees 1 TB stolen data for sale

Severity: Very High

Industries Targeted: Energy

What Happened: On July 19, 2021, a threat actor dubbed ZeroX claimed to have stolen 1TB of data belonging to Saudi Aramco and offered it for $5 million on the darknet. Saudi Arabia's Saudi Aramco is one of the world's largest petroleum and natural gas organizations. The sample released in a forum by the threat actor group had Personally Identifiable Information (PII) redacted and was evaluated by the threat actor at $2,000 per 1GB sample, for a total of $5 million to be paid as Monero (XMR).

The threat actor claimed the stolen data was obtained by compromising Aramco's network and servers in 2020. The group utilized a "zero-day exploitation" to gain access to the company's internal system and then posted the stolen data on a data breach marketplace to generate traction among interested buyers and parties. A buyer requesting an exclusive, one-off sale is expected to pay a sum of $50 million per threat actor. The main objective of the "one-off sale" is to gain access to the full 1TB of Aramco's proprietary data and demand it to be wiped entirely from ZeroX's side. The threat actor claimed they had been negotiating with five other interested buyers.

Key Impact: The threat group leveraged a zero-day exploit to gain access to the internal system. ZeroX exfiltrated 1TB worth of data from Saudi Aramco, valued at $5 million by the threat group, and is selling it off using a data breach marketplace forum. The exfiltrated data contains complete information on 14,254 employees, including name, passport, email, phone number, residence permit, identification numbers, and more. This was not considered a ransomware attack incident, as the threat group did not encrypt data or demand a ransom.

Future Considerations: Limited information is available on ZeroX beyond the cyber incident involved. It is likely that Saudi Aramco was allegedly targeted by ZeroX, although the motives remain unknown. It does not appear to have been an opportunistic attack against a specific industry and there is no evidence at this time to suggest that this threat group poses a specific threat to the oil and gas industry.

#6 New APT34 cyber espionage campaign targets Lebanon

Severity: Very High

Industries Targeted: Public Sector

What Happened: On April 8, 2021, an advanced persistent threat (APT) tracked as APT34 (also known as Helix Kitten and Oil Rig) engaged in a new cyber espionage campaign targeting the Lebanese government. The threat group has since expanded its arsenal and is now leveraging a new backdoor in its attacks. The initial stage of this campaign involves a phishing campaign where a Microsoft Word document themed as a job posting for an IT consultancy firm based in Virginia is used as a lure. The Word document is embedded with malicious code that becomes activated once the user enables macros. The macro informs the threat actors of the infection via DNS tunneling. The macro script communicates with APT34's Command-and-Control (C2) server and downloads the backdoor dubbed SideTwist, which schedules a task on the victim's device to maintain persistence.

Key Impact: The threat group has carried out phishing campaigns targeting a wide range of organizations in the Middle East and has deployed a backdoor for C2 communications. Additionally, the group is known to exfiltrate account credentials by leveraging credential dumping tools and moving laterally onto other network systems.

Future Considerations: APT34 has reportedly been active since at least 2014. It carries out supply-chain attacks and targets organizations across various industries in the Middle East. The threat group mainly leverages phishing campaigns to compromise a system. The group is expected to continue its supply-chain attack into 2022 and organizations across different sectors in the Middle East are encouraged to be on alert.

#7 Pay2Key ransomware continues to be a threat to Israeli businesses

Severity: Very High

Industries Targeted: Defense, Energy, Services

What Happened: "Pay2Key" is an Iranian ransomware campaign that emerged in October 2020 and specifically targeted Israeli firms. The group is financially and ideologically motivated and posts compromised data on their online blog. The ransom demand usually ranges between seven and nine Bitcoin, with the demand being doubled if the ransom payment is late. Since the beginning of the "Pay2Key" campaign, the group has disclosed sensitive information from six Israeli organizations following their failure to pay the ransom. Additionally, on January 9, 2021, the group posted a warning message on its Twitter account, indicating that it would continue its ransomware operations. Given their previous targets, this message was likely directed to Israeli businesses.

Key Impact: Since the beginning of its activities, the "Pay2Key" campaign has claimed over 80 victims and has released sensitive information relating to six organizations for failing to pay the ransom demanded.
At the start of the Pay2Key ransomware campaign, it was believed that the actors attained initial access via brute-forcing or password-spraying public-facing servers with weak remote desktop protocol credentials. Pay2Key ransomware operators are likely to continue using this method to gain initial access. It was also reported that one victim's network was found to have been breached via a Fortinet server vulnerability (CVE-2018-13379).

Future Considerations: There have been multiple links between the Pay2Key ransomware campaign and the Iranian "Fox Kitten" campaign. Fox Kitten is believed to be sponsored by the Iranian government. The "Pay2Key" campaign has claimed well over 80 victims and the group has vowed to strike Israeli organizations again with their ransomware. Therefore, all organizations based in Israel should remain on high alert for 2022.

#8 Israeli hospital cancels non-urgent procedures following a ransomware attack

Severity: Very High

Industries Targeted: Healthcare

What Happened: The Hillel Yaffe Medical Center in Hadera, Israel, experienced a disruptive ransomware cyberattack on October 13, 2021, disabling its IT systems. Although some activities were able to continue using alternate IT systems and pen and paper, non-urgent procedures were canceled due to the attack. Health Ministry officials believe the hackers were likely motivated by financial gain rather than geopolitical goals. However, the Israel National Cyber Directorate (INCD) released several indicators of compromise to assist organizations and other hospitals in identifying intrusions. In addition, the INDC advised organizations to upgrade all corporate email and VPN servers to the latest versions, reset user passwords, and increase vigilance for exceptional events in corporate networks.

Key Impact: The Hillel Yaffe Medical Center had to cancel non-urgent procedures for the public while also resorting to using pen and paper to ensure continuity of services. IT systems were significantly impacted and disabled. The Health Ministry sent a letter to hospitals across Israel advising them to print patient medical files to ensure continuity in case of a further attack.

Future Considerations: Ransomware attacks are an ever-present threat and this trend will continue into 2022. Many attacks against Israel are attributed to Iranian-backed attackers, including a ransomware attack against call center service company Voicenter in September 2021.

#9 "Deus" (aka "D3u$") compromises 15 TB of data from Israeli virtual call center provider Voicenter

Severity: Very High

Industries Targeted: Services

What Happened: "Deus" (aka "D3u$"), allegedly an Iranian threat actor group, is a new ransomware group that emerged on September 19, 2021. It claimed responsibility for an attack against the large Israeli virtual call center provider Voicenter. The attack allegedly resulted in the theft of 15TB of data, including data belonging to over 8,000 Voicenter customers. The group's ransom tactics included setting the initial price of the ransom demand at 15 Bitcoin (~$700,000) and was set to increase 10 BTC every 12 hours until the ransom was paid. If not paid within 36 hours, the data would be destroyed and customer data would be disclosed.

The ransomware attack itself did not appear to have been highly sophisticated. However, a general lack of security at Voicenter (including the reuse of passwords), appears to have allowed the threat actors to pivot throughout the network, likely using compromised admin credentials for remote system administration. In one screenshot released from Deus, a victim's desktop and Google contacts list were shown. The date displayed on the desktop was June 26, 2021, indicating that the threat actors had been in Voicenter's computer systems for quite some time before initiating the ransomware attack in September 2021.

Key Impact: In addition to the customer data, the group also leaked information that demonstrated the extent to which Voicenter's network and customers had been compromised. This included access to Voicenter's call center management cPanel dashboards used by customers to manage calls, password managers, webmail and cloud storage accounts, WhatsApp accounts, pictures of official Israel-issued identification documents, and access to video surveillance cameras inside Voicenter facilities. Deus has also shared all 15TB of data that they claim to have from Voicenter and its customers on their leak site.

Future Considerations: Deus has not claimed responsibility for any other attacks outside the Voicenter breach. However, the ransom methods of incremental demands can provide organizations with an example during a ransomware tabletop exercise.

#10 Iran suffers a major cyberattack on gas stations nationwide

Severity: Very High

Industries Targeted: Energy

What Happened: On October 26, 2021, Iran's subsidized gas fuel card system was disabled due to a widespread cyberattack. As a result, the digital displays at gas pumps were modified to display the number "64411," a phone line connected to the office of Iranian Supreme Leader Ayatollah Ali Khamenei. Additionally, digital billboards overlooking major highways in the cities of Karaj and Isfahan were changed to display the message "Khamenei! Where is our gas?" The secretary of Iran's Supreme Council of Cyberspace, Abolhassan Firouzabadi, stated that he believed a nation-state conducted the attack, but declined to assign attribution until a full investigation was completed. Iranian President Ebrahim Raisi noted that the attack was meant to sow disorder and disruption in the country.

This act of hacktivism occurred near the second anniversary of massive protests that erupted throughout Iran beginning on November 15, 2019, in response to the government's increase in gas prices. The Iranian security forces cracked down on the protests violently, resulting in the death of approximately 180 to 450 people and thousands of arrests.

Key Impact: Although Iranians could still purchase gasoline outside of the subsidized system, the cyberattack led to extremely long lines at thousands of gas stations across the country. This resulted in many gas stations running out of fuel. As a result, gas prices skyrocketed from $0.36 per liter to $1.89 per liter.

Future Considerations: Hacktivism remains a significant threat throughout 2022 as political tensions continue in the Middle East and Africa. However, no group has claimed responsibility for this attack at this time.

Australia and New Zealand Constellation

H1 – Actioning 2022: Regional Themes and Trends

The section below provides key regional themes and trends observed throughout 2021. These insights provide valuable insights to organizations on what to expect from a geopolitical and cyberthreat perspective in 2022.

Telecommunication and Technology Sectors to Experience Maximum Cyberattacks

In 2021, 35.7% of the total cyberattacks were experienced by the telecommunication and technology sectors in the region, followed by financial services (18.5%) and the healthcare sector (11.4%).

Telecommunication infrastructure underpins almost all critical infrastructure and essential services, including energy, finance, healthcare, technology, defense, government, manufacturing, and retail. Promising technologies such as 5G, quantum science, and artificial intelligence assure transformative mobility by enabling the mass digitization of businesses and industries. However, with the rollout of 5G connectivity in Australia and New Zealand, the security concerns over telecommunication are also increasing rapidly in the region. Partnership with private players and international collaboration will shape, protect, and promote secure 5G solutions in the region.

Ransomware Deployment Will be the Most Frequently Used Method of Cyberattack

More than 57% of the cyberattacks conducted in the Oceania region were ransomware attacks, followed by data exfiltration (5.6%) and network access (5.6%).

Despite being a relatively new concept to the public, ransomware has evolved significantly over the past decade, causing the loss of billions of dollars. There has been a massive increase in ransomware attacks against Australian entities in the past year (2021). The ransomware business model has become so sophisticated that some threat groups specialize in developing and selling other groups' technology to mount attacks. As victim organizations are unquestioningly paying the ransom to the threat groups to save their breached data and reputation, this will give more confidence to the threat actors to conduct further attacks. Hence, organizations need to have a multi-layered security framework and well-managed secure backup policies to curtail these attacks.

Financial Gain Is Likely to be the Biggest Motivation for Threat Actors in the Future

Cybercriminal profiles can vary and the motivation behind an attack might not come down to just one motive. However, a common factor in most attacks is financial gain. The COVID-19 pandemic has pushed financial organizations to digitalize, focusing on cloud environments. Unfortunately, threat groups are taking advantage of these digital trends. It has been observed that many threat groups whose primary focus used to be cyber-espionage campaigns have conducted ransomware attacks for financial gain in the post-COVID era. In addition, various threat groups, such as APT38, have usually targeted banks and financial institutions. The frequent targeting of the critical national infrastructure and businesses of all sizes in the private and public sectors is alarming for the region's governments.

Russian Threat Groups to Pose a Significant Threat to the Region

For years, Russian threat groups have been preparing for the digital battlefield. They have been frequently alleged with most of the critical cyberattacks worldwide. Russian cyber operations represent a real and sophisticated threat to a wide range of sectors. In addition, alleged Russian state-backed cyber-espionage campaigns pose a significant threat to the region. Recently it has been observed that infamous Russian threat groups such as REvil, Avaddon, Darkside, etc., have been conducting cyberattacks in the region. Furthermore, the involvement of Russian threat groups in various elections across the world indicates that there might be a campaign to disrupt the Australian General Election in 2022. With the AUKUS deal being signed (a trilateral security deal signed between Australia, the United Kingdom, and the United States),the Oceania region is least likely to avoid state-sponsored cyberattacks in the future.

Oceania Region to Face a Surge of Attacks by LockBit Threat Actors

The LockBit operators were involved in more than 29% of the known cyberattacks in the region in 2021. The LockBit group operates as Ransomware-as-a-Service. This group rents its ransomware to other threat actors. Then those threat actors breach enterprise networks to steal data and deploy the ransomware payload to encrypt local copies. Recently, the group has been observed to launch attacks utilizing a newer version of ransomware called LockBit 2.0. LockBit 2.0 attains initial access by exploiting a vulnerability tracked as CVE-2018-13379 in the devices. The Australian Cyber Security Centre (ACSC) has alerted organizations to an increase in attacks from LockBit 2.0. Because the LockBit group is infamous for leaking organizational data in the dark web upon denial of payment, organizations and governments need to be vigilant regarding the attacks in the region.

H2 – Geopolitical Landscape

Here are some of the significant geopolitical developments observed in the Australian and New Zealand constellation in 2021.

AUKUS Deal: Fortifying Australian Cyberspace

AUKUS, a newly created trilateral strategic defense alliance comprising Australia, the United Kingdom, and the United States, is a full-fledged defense alliance that focuses on nuclear technology sharing, diplomatic coordination, artificial intelligence, and cybersecurity. Australia has been a constant victim of state-backed sophisticated cyberattacks in recent times. They need close alignment with major powers and advanced technologies to counter these threats. The mention of critical technology transfer in cybersecurity, artificial intelligence, machine learning, and cloud computing makes this much more than just a submarine deal. As China has already declared its intention to dominate the world in artificial intelligence by 2030, this deal can be considered a measure to counter the Chinese government in the Asia-Pacific region. This deal can also be a game-changer in Australia's civil nuclear electricity production, reducing their dependence on coal and accelerating their goal to reach net-zero. In that regard, this deal seems to be a significant milestone in Australian geopolitics.

New Zealand's Membership in Budapest Convention Likely to Counter Online Terror Campaigns

The government of New Zealand has confirmed joining the Budapest Convention (also known as the Council of Europe Convention on Cybercrime). The Budapest Convention on Cybercrime is an international treaty signed by 65 countries. It addresses the major cybercrimes that use technology or the internet (including

online sexual exploitation of children, computer-enabled fraudulent activities, violent extremist content corresponding to terrorism, and access to criminal evidence stored electronically). In addition, it creates a common framework for obtaining electronic evidence and strengthens cooperation between states on a wide range of criminal investigations. Tackling the expanding cybercrimes in New Zealand will be very difficult for the government without international cooperation. Moreover, the presence of large-scale online terror campaigns is a significant threat to its national security. Hence, their decision to join the Budapest Convention will be a wise step towards eradicating the online extremist campaigns run by terror outfits and cross-border evidence gathering, underpinned by international cooperation.

2022 Australian Federal Election to Experience Cyberthreats

The 2022 Australian Federal Election will be held on May 21, 2022. Although the deployment of stringent hybrid digital-analog mechanisms secures the voting processes in Australia, there is still the possibility of several small-scale cyberthreats that can indirectly target the integrity of the electoral system. The breac of Australia's parliamentary network, followed by gaining access to the emails of parliamentarians in 2019 is an example of this type of passive cyber operations, which leads to the spread of misinformation. Australia's Joint Cyber Committee on Electoral Matters considers the disinformation campaigns as serious threats to the country's democratic principles. These campaigns can manipulate election outcomes and cast doubt on democratic processes. In addition, the potential involvement of evil foreign powers in influencing public preferences can dilute the decision-making process. The Australian government's compulsory voting mandate can be beneficial in restricting foreign interference (i.e., polarization) in their elections. US-Australia Collaboration on Quantum Technology Likely to Pave the Way for a Quantum Revolution Quantum technology has tremendous potential in defense, cryptography, and computing. Australia has declared quantum technology one of the nine most critical technologies of immediate national interest. According to experts, there is a total of $4 billion initial business opportunity for Australia in quantum science soon. Australia has planned to invest $70 million in developing a Quantum Commercialization Hub. In addition to this, Australia has signed a landmark agreement to collaborate with the United States on quantum technology. This agreement allows both parties to exchange quantum knowledge and skills. The main focus will be on exploring new theoretical ideas on quantum technology and collaborating to turn the ideas into meaningful applications with mutual benefit of both nations. It will promote joint research and development backed by transparency, reciprocity, and accountability; build a global quantum marketplace, along with a secure supply-chain; and foster shared economic prosperity. It will also protect sensitive information related to both nations' national security by shared arrangements. Thus, quantum science will provide vast business and research opportunities for the Australian economy.

Online Safety Act Shaping a Framework
for Online Safety of Australians

Online safety regulations have been a major headache for most governments in the present era of information technology. Australia's Online Safety Act 2021 aims to create a modernized framework for online safety. According to the act, an eSafety Commissioner will be appointed to administer the complaints of cyberbullying against Australian children and adults, non-consensual sharing of intimate images, and online content schemes. The act introduces a set of basic online safety expectations (BOSE), including sufficient safety standards of the services, controlling the type of content available for services, controlling the type of content available for different demographics, implementing protection measures for the activity of minors in service, etc. The act also empowers the commision to issue removal notices against controversial services, applications, and links from the search engines. It also allows the commission to ask internet service providers to block specific domains names, URLs, and IPs promoting violent content or terrorist acts. This act introduces several significant obligations for the internet service providers, social media service providers,

and hosting service providers. They are required to practice the obligations, ensure that policies are updated according to the obligations, and ensure that requests are being taken down without delay to ensure the end user's safe online service.

H3 – Cyberthreat Regional Landscape

Naikon

Industries Targeted	Continents Targeted
Defense, Energy, Public Sector, Services	Australia

Naikon is also known as: PLA Unit 78020, APT30, Override Panda, Camerashy, APT.Naikon, Lotus Panda, Hellsing, BRONZE GENEVA.

Naikon is a China-based advanced persistent threat (APT) group backed by the Chinese government. This hacking group has been engaging in spying activities since 2010. It is believed that this group has a strong link with the People's Liberation Army. Naikon primarily targets the Chinese government's adversaries, including foreign affairs ministries, science and technology ministries, government-owned companies, and civil and military organizations.

This threat group's primary goal is to collect sensitive data through cyber-espionage campaigns. It extracts data from removable drives and harvests stolen data (including screenshots and key logs) for espionage activities. The method of attack is typically through an infected hoax email containing a Rich Text Format (RTF) file, allegedly from a trusted source. Then, the weaponized RTF starts exploiting systems on the network, spreading like a virus while analyzing file metadata mapping the chain of command. It has been observed that Naikon employs backdoors such as RainyDay and Nebulae to conduct its cyber-espionage operations. Before 2015, the group did not appear in the public domain. However, Kaspersky researchers first uncovered the group in 2015 while conducting attacks against top-level government agencies around the South China Sea. Naikon went silent after 2015 and, according to reports, spent the next five years conducting espionage activities and upskilling themselves. This indicates that Naikon operators have mastered new ways of avoiding detection by using advanced server infrastructure, ever-changing loader variants, and in-memory fileless loading. Alhough Naikon is less likely to attack ordinary individuals, anyone possessing sensitive classified information related to national security needs to be on alert.

TA505

Industries Targeted	Continents Targeted
Retail, Finance, Services, Manufacturing, Public Sector, Healthcare, Markets	Australia

TA505 has been an active Russia-linked threat actor since 2014. This financially motivated APT group uses Dridex Trojan, Locky, and Clop ransomware variants. They have attacked several industries, including finance and retail. Specifically, the attacks have used FlawedGrace and GraceWire malware for the financial sector. TA505 is known to be creative and tends to change the attack techniques to achieve their goals. For example, the threat actor group commonly uses phishing emails with malicious attachments, rather than relying on vulnerabilities to gain initial access.

TA505 has allegedly been attributed to a new cyber campaign named MirrorBlast, which was observed in April 2021. The MirrorBlast campaign shares many similarities related to landing pages, code, and domain-naming conventions. The attack chain starts with a malicious attachment that redirects to a fraudulent SharePoint or OneDrive site to evade detection. This is followed by an Excel file download containing a macro that executes and performs the other attack steps.

The threat actor remains active and demonstrates highly sophisticated capabilities to stay under the radar. TA505 has the capability to quickly advance and change its technical abilities on the go, which poses an increased threat to organizations across sectors in this region.

APT38

Industries Targeted	Continents Targeted
Finance, Public Sector, Services	Australia

APT38 is also known as: Operation DarkSeoul, Hidden Cobra, Hastati Group, Andariel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Subgroup: Group 77, Labyrinth Chollima, Operation Troy, Operation GhostSecret, Operation AppleJeus, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APT-C-26, NICKEL GLADSTONE, COVELLITE.

APT38 is a North Korea-based state-sponsored cyberthreat group actively operating since 2014. It has been conducting cyberattacks in at least 38 countries for the last seven years. Financial institutions, banks, casinos, ATMs, cryptocurrency exchanges, and SWIFT system endpoints are frequently targeted by this group. APT38 has been credited for bank heists across many countries, from Bangladesh to Chile and Vietnam to Mexico. It is believed that North Korea, being slammed by sanctions and frozen out of international trades, utilizes groups such as APT38 for financial gain to support its sinking economy. Recently, this group has been alleged by the FiveEye group to target several Australian banks and several banks situated in Southeast Asia.

Before beginning the heist, APT38 operators first gather information regarding the financial organizations' personnel and SWIFT transaction mechanisms. Then they gain initial access through watering holes and exploit the outdated version of Apache Struts2 to execute the malicious codes in the victim system. Next, they deploy and execute Dyepack malware to gather credentials to insert fraudulent SWIFT transactions and alter transaction history. The money is then transferred to bank accounts located in foreign countries that enable money-laundering. Finally, APT38 uses wiper malware to cover its tracks and destroy fraudulent transaction records.

Despite efforts to restrict the group, it remains a significant threat for financial institutions worldwide. By deep observation of the tactics and techniques of APT38, it isrecommended that organizations employ multi-layered security systems in their SWIFT transaction mechanisms. They should also keep their systems up to date with the latest security patches to curtail the activities of the group.

Silent Librarian

Industries Targeted	Continents Targeted
Services	Australia

Silent Librarian is also known as: COBALT DICKENS, Mabna Institute, TA407

Silent Librarian is a financially motivated Iran-linked state-sponsored threat group operating since 2013. Nine members of this group were indicted for hacking, wire fraud, and identity theft by the US Department of Justice in 2018. This group particularly targets higher education institutions and universities to steal and sell proprietary information.

Silent Librarian uses phishing campaigns and well-crafted social engineering techniques to conduct its activities. It employs malicious domains to host phishing web landing pages that redirect users to forged university library login pages. It uses Cloudflare for hostnames, which helps them hide the actual hosting origin. It also uses URL shorteners, linking, and abuse of legitimate services in its malicious campaigns. These threat actors have primarily targeted universities and other organizations' technology and medical departments. Additionally, the group leverages domain shadowing, in which they obtain compromised administrative credentials for a victim domain and then use those compromised credentials to conduct phishing attacks.

Organizations are recommended to take rigorous anti-phishing measures to minimize the threat posed by Silent Librarian. By putting the hosting domains under blacklist and setting up firewall rules for outbound traffic for the IP addresses, the threat posed by this group can be avoided.

Mazecart

Industries Targeted	Continents Targeted
Unavailable	Australia

Mazecart is an umbrella of threat actor groups operating under the name of Magecart. It is primarily motivated to steal card payment information through skimming and code injection attacks on e-commerce sites and other platforms. The group is known to target the retail and technology sector primarily, but the

malware could also be injected into other sites via supply-chain compromise. The group first appeared in 2014 when several e-commerce sites were observed running malicious JavaScript-based keyloggers, which the threat actors injected to harvest sensitive credentials and payment card information. More than 18 threat actors are known to operate with different tools and scripts targeting diverse geography and sectors and using different methods to obfuscate their activity.

Mazecart can also perform supply-chain attacks, which include injecting codes into sites and platforms that can execute code on various sites and platforms for advertising, analytics, or static content. For example, in a recent campaign seeking to retrieve payment card information, the threat actors used WebGL JavaScript API to evade detection. The script checked for the presence of swift shader, llvmpipe, and VirtualBox, which are used by sandboxes and VMs. This helped threat actors avoid detection by sandbox solutions and security researchers. The group can also hide their malware effectively in social media buttons and security scanners cannot find the malware using traditional techniques such as checking for valid syntax. The threat actor group is observed to hide the payload behind the image of five major social media sites: Facebook, Twitter, Instagram, Youtube, Pinterest, and Google buttons. All the techniques used by the threat actor group Mazecart are known by the name Magecart-style attack, which accounts for the unique techniques used by the group.

The widespread campaigns conducted by the threat group and its ability to perform supply-chain attacks on platforms can spread the malware to thousands of other sites using the infected platform. Additionally, using the site with a compromised platform puts individual site users at massive risk of banking fraud and sensitive information leaks. More attacks could be uncovered from the Mazecart group in the future.

H4 – Industry Threat Landscape

Severity Score for Cyber Events Grouped by Industry
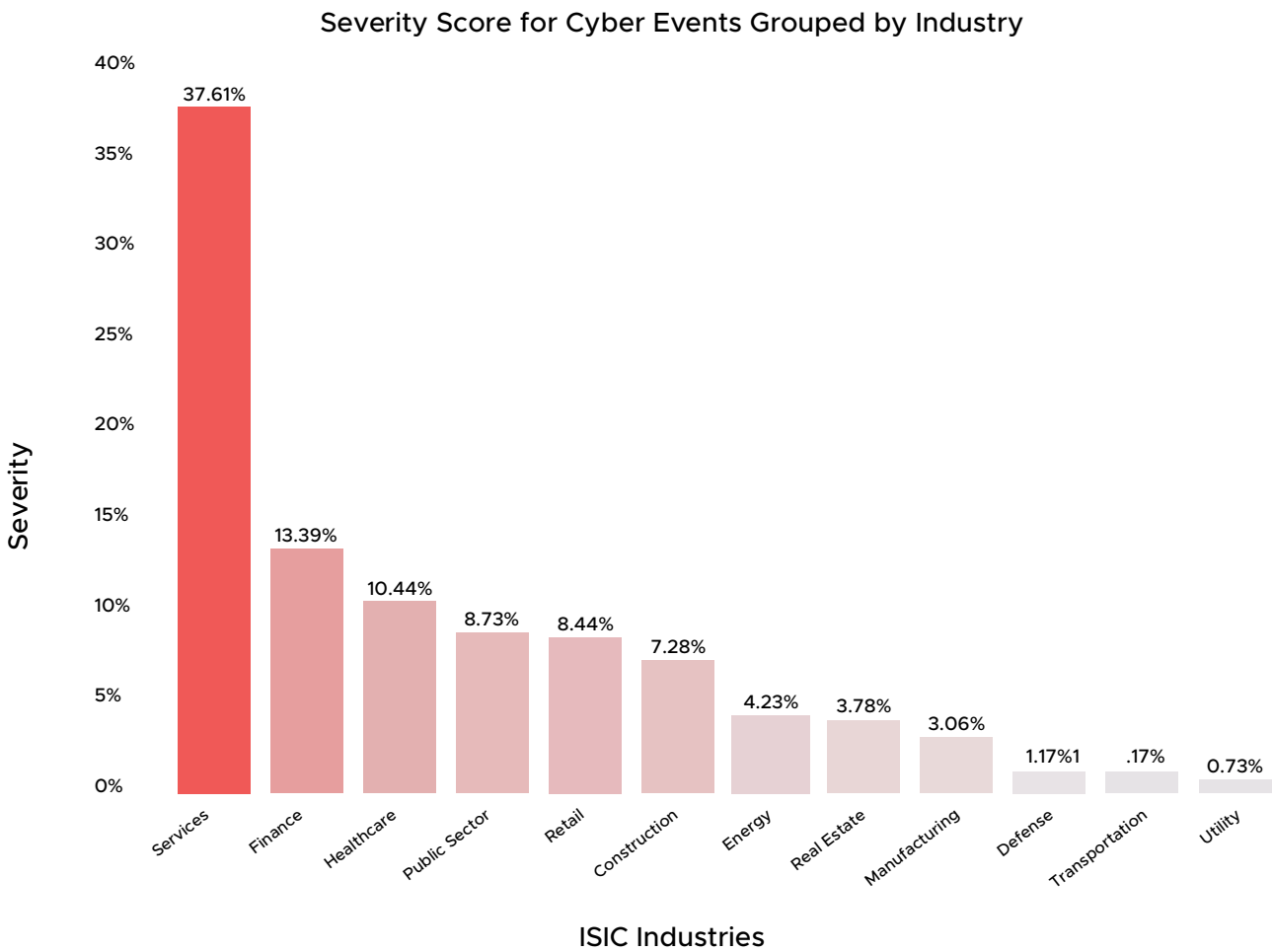
Figure 16 - Industry threat landscape in Oceania

Ransomware Is a Prominent Threat

Ransomware as a threat has grown significantly. Out of all the prominent cyber incidents occurring in Oceania, approximately 40% are constituted by ransomware attacks. Two of the most active ransomware groups in the region are LockBit 2.0 and Avaddon, who are behind about 27% and 17% of all ransomware attacks, respectively. The services sector was the most affected sector by ransomware attacks. The primary motivation behind the ransomware attacks is financial gain. The uptick in the ransomware attacks could be driven by several factors, including the rise in the Ransomware-as-a-Service model that allows sophisticated malware to be available for a greater number of operators. Another contributor to the increase in ransomware attacks is initial access brokers (IAB).

Critical Infrastructure and Essential Services under Constant Threat

Approximately 18% of all cyberattacks target critical infrastructure and essential services sectors. Ransomware attacks are behind around 84% of all attacks. Financial gain appears to be the primary motivation behind the attacks. Within the critical infrastructure and essential services sector, healthcare and construction industries are affected the most, constituting 46% and 30% of the cyberattacks, respectively.

Data Breaches Are on the Rise

As the number of cyberattacks is increasing, the organizations in the region are facing the threat of data breaches and the exfiltration of sensitive data. Approximately 10% of all cyberattacks lead to a data breach. Organizations in the financial services and technology sector are targeted by data breaches the most. Financial gain seems to be the primary motivation behind all data breach incidents.

Supply-Chain Attacks Are a Major Concern

Threat actors are constantly launching supply-chain attacks, which are apparently more cost-effective from their perspective. Although the SolarWinds supply-chain attack did not significantly affect organizations in the region, they were forced to take necessary mitigation steps to increase the operational overhead. Supply-chain attacks leveraging Accellion FTA and Kaseya VSA caused significant damage to organizations.

Growing nNumber of Zero-Day Vulnerabilities

The increasing number of zero-day vulnerabilities in widely used software and services is a cause for concern. In many cases, the proof of concepts (PoCs) and exploitation techniques are publicly available, significantly increasing the number of exploitation attempts. Furthermore, the increase in supply-chain attacks could directly be attributed to the growing number of zero-day vulnerabilities. In addition, vulnerabilities in third parties such as Log4j, Fortinet, Zoho ManageEngine, etc., have added significant operational overhead for the organizations in the region.

H5 – Key Lessons from Most Impactful 2021 Attacks
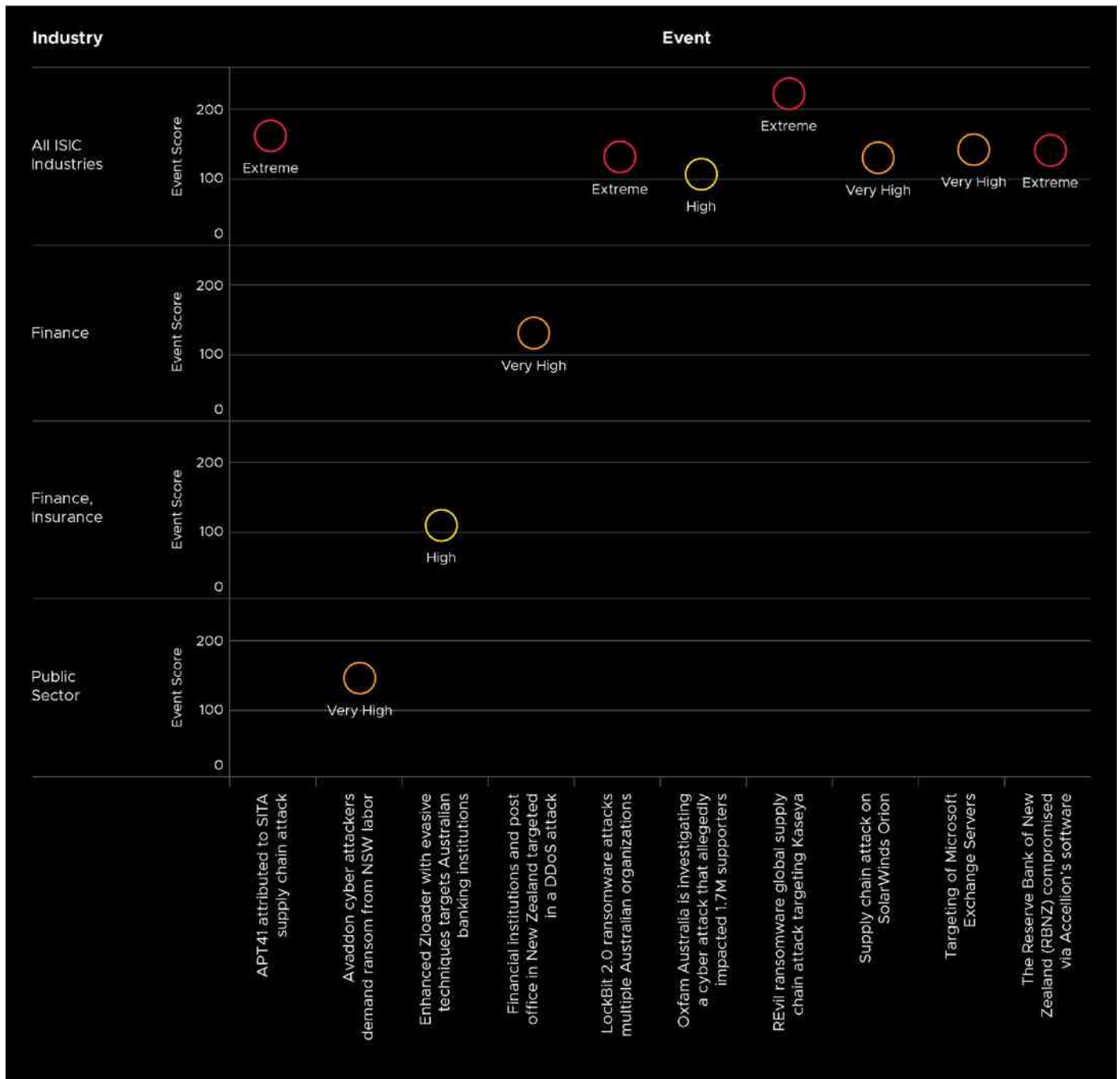
Figure 17 - Top 10 events in Oceania

#1 REvil ransomware global supply-chain attack targeting Kaseya

Severity: Extreme | **Industries Targeted:** All ISIC Industries

Quick Recap: On July 2, 2021, Kaseya, a prominent software solutions provider, announced that it was the victim of a cybersecurity incident. The incident has been attributed to the threat actors operating the REvil (also known as Sodinokibi or Sodin) ransomware group and alleged to be of Russian origin. The attack is believed to have compromised Kaseya's VSA remote IT monitoring and management solution. As a result, at least 1500 organizations were affected. In addition to the organizations affected worldwide, 11 schools in New Zealand had their files encrypted due to this attack.

Security researchers stated that Kaseya was initially breached due to a zero-day vulnerability tracked as 'CVE-2021-30116' in its systems, which was already reported to Kaseya. When it was breached, it was working on the patch, resulting in a compromise of its software updates. Additionally, victims of the supply-chain attack were compromised through a Kaseya software update, in which the REvil ransomware infected them.

Impact: REvil demanded $70 million in Bitcoin (BTC) to provide the decryptor for all systems locked during the Kaseya supply-chain attack. REvil ransomware has been associated with multiple high-profile breaches in the past. At least 200 organizations were affected, with some reports estimating that thousands of businesses might be potential victims.

Future Considerations: This attack was one of the most prominent supply-chain attacks of 2021. A supply-chain attack is more cost-effective for threat actors because compromising a single vendor could potentially lead to a security breach in multiple organizations. Furthermore, the increase in zero-day exploits could also aid the threat actors in future supply-chain attacks.

#2 APT41 attributed to SITA supply-chain attack

Severity: Extreme | **Industries Targeted:** All ISIC Industries

Quick Recap: On February 24, 2021, SITA, a global IT organization servicing 90% of the airline industry, confirmed that customer data was stolen in a breach of its Passenger Service System (PSS). The PSS contains information such as ticket transactions, boarding, and rewards/loyalty program members. Notably, frequent flyer programs have been used as an attack vector to spread quickly across many airlines. One of the notable frequent flyer membership programs affected was Star Alliance. Additionally, several prominent airlines notified the public of user data compromise.

Air New Zealand disclosed that the breach occurred via airline passenger processing system provider SITA. However, the organization assured that the threat actors had not acquired tier status, membership number information, contact information, passport numbers, or credit card information.

Impact: The SITA breach impacted several airlines and information surrounding frequent flyer programs. The threat actors leveraged Mimikatz and hashdump to obtain victims' credentials. Furthermore, they have used DNS tunneling to exfiltrate data. Air New Zealand claimed that sensitive customer information (including passport numbers, credit card information, and contact information) were not breached.

Future Considerations: The attack on SITA PSS ranks among the top five highly publicized supply-chain attacks, with global ramifications. A supply-chain attack is more cost-effective for threat actors because compromising a single vendor could lead to a breach in multiple organizations. Furthermore, the increase in the number of zero-day exploits could aid the threat actors in supply-chain attacks.

This attack has been attributed to the Chinese state-sponsored group APT41. The threat actors leveraged Mimikatz and hashdump to obtain victims' credentials. Cyberattacks are expected to either rise or fall in conjunction with political tensions between China and other nations in 2022.

#3 Lockbit 2.0 ransomware attacks multiple

Severity: Extreme

Industries Targeted: All ISIC Industries

Quick Recap: Since July 2021, there has been a consistent increase in LockBit 2.0 ransomware attacks worldwide. LockBit 2.0 is the enhanced version of LockBit ransomware malware, which was initially observed in June 2021. The latest version supplements a built-in information stealing function called 'StealBit,' as well as a feature that automatically encrypts devices across Windows domains by leveraging Active Directory group policies.

According to the Australian Cyber Security Centre, multiple organizations in Australia have been targeted by the LockBit group.

Impact: LockBit 2.0 is the successor to LockBit ransomware, with further enhanced capabilities to capture and automatically encrypt sensitive information. Monitoring outgoing traffic is crucial to identify insider threats, since the group is reported to be recruiting employees from the targeted organizations. Furthermore, traffic from 'LockBit 2.0' is routed through the TOR network, enabling greater anonymity for the threat actor to host illegitimately obtained sensitive information. Based on observed activities from the threat actors, ransomware attacks could potentially lead to significant loss of sensitive information, disruption in operations, and a negative impact on organizations' brand reputations.

Future Considerations: LockBit 2.0 is the successor to LockBit ransomware, with further enhanced capabilities to capture and automatically encrypt sensitive information. LockBit developers have updated the ransomware in multiple instances to upgrade and optimize some of its features. Previous reports show additional methods for anti-detection capabilities and the ability to circumvent Windows User Access Control (UAC). Additionally, threat actors behind LockBit adopted the double extortion technique, which refers to exfiltrating data before initiating the encryption process. his allows the attackers to have additional leverage to receive the ransom by threatening to publish the stolen information through data-leak sites. Based on the developments of the malware, Lockbit is expected to appear again soon.

#4 The Reserve Bank of New Zealand (RBNZ)

Severity: Extreme | **Industries Targeted:** All ISIC Industries

Quick Recap: On January 10, 2021, The Reserve Bank of New Zealand (RBNZ) released a statement that they were responding with urgency to a data breach of one of its data systems. According to the statement, a third-party file sharing service that RBNZ uses to share and store some sensitive information had been accessed illegally. Although sensitive commercial and personal information might have been exposed. RBNZ's core functions were not impacted by the incident and remained operational. However, affected systems were taken offline until RBNZ finished its initial investigation.

On January 11, 2021, RBNZ had revealed additional details of the cyberattack, stating that it was part of the Accellion supply-chain attack, which affected multiple organizations worldwide.

Impact: Accellion has provided software patches for all the known existing vulnerabilities and is working closely with impacted organizations on mitigation efforts. Additionally, Accellion stated that the cyberattack did not specifically target RBNZ, but didtarget users of the software 'FTA.' RBNZ did not indicate whether another government or a criminal organization might be behind the cyberattack.

Future Considerations: Along with Solarwinds, Kaseya, and Codecov: This attack was one of the most prominent supply- chain attacks of 2021. Threat actors are well aware that a supply-chain attack is more cost-effective, as compromising a single vendor could result in a breach of multiple organizations. Furthermore, the increase in the number of zero-day exploits could also aid the threat actors in future supply-chain attacks.

#5 Financial Institutions and Post Office in New Zealand targeted in a DDoS attack

Severity: Very High | **Industries Targeted:** Finance

Quick Recap: In early September 2021, multiple financial institutions and the New Zealand Post Office were targeted in a DDoS (distributed denial-of-service) attack. As a result of the attack, web portals of the affected organizations faced disruption and ultimately went offline. In addition, customers reported the outage on social media platforms. Some of the prominent organizations affected by this campaign were the KiwiBank, ANZ Bank New Zealand Ltd, and the New Zealand Post Office.

Impact: The incident resulted in disruption for financial organizations, which ultimately led to the affected organizations not being able to provide services to their customers. DDoS attacks could potentially lead to severe disruption and monetary loss for the affected organizations.

Future Considerations: With the development of numerous tools and botnets, it is becoming easier to perform a DDoS attack. Considering the potential impact, threat actors use DDoS attacks as a common attack vector to threaten organizations worldwide. Hence, this trend is expected to continue in the foreseeable future.

#6 Targeting of Microsoft Exchange Servers

Severity: Very High

Industries Targeted: All ISIC Industries

Quick Recap: On March 02, 2021, Microsoft published a detailed report addressing four previously unknown or zero-day vulnerabilities in Microsoft Exchange Server used in targeted attacks. Microsoft stated that a state-sponsored threat actor that allegedly operates from China, known as Hafnium, had exploited Exchange email service, allowing them to gain access to internal systems. Additional threat actors have also been observed to exploit the vulnerabilities. The four exploited vulnerabilities in these attacks are being tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065

On March 11, 2021, threat actors reportedly began to utilize the recently patched Microsoft Exchange Server vulnerabilities to deploy ransomware onto compromised servers. The ransomware family is tracked as DearCry, which uses the Microsoft Exchange vulnerabilities to target customers. Additionally, the ID-Ransomware website (a ransomware identification website) has reported an increase in submissions of files with the ".CRYPT" extension and the "DEARCRY!" marker, which are coming from the IPs of Exchange servers from Australia and the United States. The new ransomware notes and encrypted files that were submitted to the website began on March 9, 2021. For at least one of the reported victims, the ransomware group demanded $16,000 in ransom. However, there have been no reports on any weaknesses in the ransomware source code that would allow victims to recover the encrypted files for free at the time of writing this advisory.

Since at least March 18, 2021, it has been suspected that threat actors are targeting Microsoft Exchange Proxylogon vulnerabilities to deploy a second ransomware variant named BlackKingdom. This ransomware malware, written in Python, was first initially observed in June 2020 while targeting organizations by exploiting vulnerable Pulse VPN software for initial access. Submissions to the ID Ransomware website reveal more than 30 instances of BlackKingdome ransomware at the time of writing this advisory. Many of the reported submissions are directly from email servers. Targeted victims appear to be from countries such as Australia, the United States, Canada, Austria, Switzerland, Russia, France, Israel, the United Kingdom, Italy, Germany, Greece, and Croatia.

Impact: Threat actor groups are targeting an extensive range of countries leveraging the Microsoft Exchange vulnerabilities and deploying ransomware such as BlackKingdom and DearCry ransomware. In one instance, DearCry ransomware operators demanded $16,000 in ransomware to recover their exfiltrated data.

Future Considerations: The threat actor group appears to be politically motivated; however, the threat group did not engage in further cyber incidents during 2021. Nevertheless, trending exploits such as the Microsoft Exchange Server's vulnerabilities tend to attract attention from ransomware operators, as these vulnerabilities could be used to gain a foothold within an organization's network for malicious activities.

#7 Avaddon Cyberattackers demand ransom from NSW Labor

Severity: Very High

Industries Targeted: Public Sector

Quick Recap: Threat actors operating Avaddon ransomware recently targeted the NSW Labor Party in Australia. The allegedly Russian-based threat actors provided up to 10 days to pay a ransom after the group had successfully compromised the internal computer network in a cyberattack. Threat actors further threatened to publish the exfiltrated data in case of a futile negotiation process. Exfiltrated data is believed to contain personal and sensitive information such as passports, driver's licenses, employment contracts, as well as company details. Threat actors have also threatened the organization to conduct Distributed Denial-of-Service (DDoS) attacks.

Threat actors promoted their configurability and set of features, including file encryption via AES256 and RSA2048, full offline support, encryption of all local and remote drives, and much more. Encrypted files were renamed with an extension of randomly generated letters unique for each victim. As of April 1, 2021, more than 60 companies were li

Impact: Avaddon encrypts files and renames them with a unique added extension consisting of randomly generated letters and uses a TOR site for the ransom payment. The exfiltrated data could contain sensitive information, including passports, driver's licenses, employment contracts, and company details. Avaddon operators provided the NSW Labor Party ten days to pay the ransom. Failure to comply would result in publicly publishing the exfiltrated data.

Future Considerations: Avaddon is a ransomware operating in a Ransomware-as-a-Service model and was initially discovered in June 2020. The threat group targets Windows systems and is generally spread via phishing campaigns.

However, on June 11, 2021, Avaddon had allegedly shut down its operation, likely due to the increased pressure by police agencies and the United States President Biden's plan to deliberate cyberattacks along with Russian President Vladimir Putin. To support the shutdown claim, Avaddon published a total of 2,934 decryption keys to their victims. Additionally, Avaddon's TOR website is currently inaccessible, further indicating that the threat group likely shut down operations.

While Avaddon supposedly shut down, the operators behind the ransomware could possibly return under a different name. In 2022, Avaddon could still be a threat if they were to return.

#8 Supply-chain attack on SolarWinds Orion

Severity: Very High

Industries Targeted: All ISIC Industries

Quick Recap: On December 13, 2020, cybersecurity firm FireEye published a report on details of a sophisticated and widespread supply-chain attack targeting SolarWinds Orion software. FireEye is tracking this threat actor as UNC2452—also known as Nobelium Nobelium and Dark Halo. Orion is a scalable infrastructure monitoring and management platform used by various industries. This cyber-espionage campaign was commenced by implementing a Trojan malware in the SolarWinds Orion software update, which distributed a malware named SUNBURST.

On March 18, 2021, a new report from Prodaft—a Swiss cybersecurity firm—disclosed another highly technical and sophisticated advanced persistent threat (APT) group dubbed SilverFish. This threat group is suspected of having conducted three waves of attacks. Based on the report, SilverFish has commenced more than 4,720 attacks on prominent private and public organizations while primarily focused on European countries and the United States. Reportedly, the threat actor had targeted a wide range of industries such as the government and public sector, defense, manufacturing, and professional services, while maintaining specific interest in critical infrastructure organizations.

Impact: The SolarWinds campaign appears to be primarily focused on espionage and, therefore, the victims should expect malicious activities in their environment—including, but not limited to, sensitive data exfiltration, file execution, and forensic and anti-virus services termination. Additionally, the threat actors have been observed to compromise email exchange servers. The current list of alleged victims related to this campaign includes victims from government, consulting, technology, telecom, and extractive entities in Europe, North America, Asia, and the Middle East. It is anticipated that there are additional victims in other countries.

Future Considerations: The SolarWinds supply-chain attack has gained significant attention as a number of press reports have focused on identifying the threat actors involved. Additionally, the United States Government and cyber community provided detailed information on how the campaign was potentially carried out, along with the malware used. With the aid of MITRE's ATT&CK team, the tactics, techniques, and procedures were mapped to UNC2452.

While not as significant as the SolarWind's cyber incident, the threat actor group actively targets the technology sector. UNC2452 is expected to make a presence in 2022, possibly leveraging vulnerabilities in the outdated software application to gain unauthorized access.

#9 Oxfam Australia is investigating a cyberattack that allegedly impacted 1.7 million supporters

Severity: High

Industries Targeted: All ISIC Industries

Quick Recap: Oxfam Australia is investigating a cyber incident that impacted the data of 1.7 million supporters following a threat actor claiming to be selling their database on a hacker forum. Oxfam Australia is an independent, not-for-profit, community-based aid organization focused on alleviating poverty within the indigenous Australian people and people from Asia, Africa, and the Middle East. The hacker forum displays a post containing samples of the supposed database, with information including full names, addresses, email addresses, phone numbers, and amounts donated. Researchers identified at least one of the records containing legitimate information for a donor from the sample posted by the threat actor.

Oxfam Australia reported to the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC). Additionally, the company hired forensic specialists to aid in identifying the damage, whether data have been accessed, and the impact on the supporters.

Impact: TAn unidentified threat actor allegedly accessed the data of 1.7 million supporters and claimed to be selling their database on an online hacker forum. One record posted on the forum was confirmed to be legitimate. Oxfam Australia reported it to the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC).

Future Considerations: While the threat actor was not identified and the means of the breach was not disclosed, users are advised to constantly change their passwords. Additionally, if registered members use the same password on other sites, they are advised to change it there as well. With the alleged data breached, all members should be on the lookout for phishing attacks atimed towards them following this incident.

#10 Enhanced Zloader with evasive techniques targets Australian banking institutions

Severity: High

Industries Targeted: Finance, Insurance

Quick Recap: In September 2021, researchers observed an active campaign involving Zloader malware utilizing a new infection chain to disable Microsoft Defender Antivirus on compromised machines to avoid detection. Additionally, researchers stated that the complexity of the cyberattack had been enhanced to be stealthier.

Zloader was a banking Trojan first observed in August 2015, targeting customers of several British financial institutions. The malware is believed to be based on the Zeus v2 Trojan's source code that was leaked on a public forum in late 2010. More recently, the Trojan has been targeting financial institutions worldwide, primarily Australian banking organizations.

The Trojan is further known to be capable of delivering ransomware payloads, including Egregor and Ryuk. Additionally, Zloader contains remote access capabilities and can operate as a malware loader to drop additional payloads on compromised systems.

Impact: The Trojan is capable of deploying various kinds of payloads, including ransomware such as Egregor and Ryuk. As a result, organizations impacted by the Trojan would risk data breach. And in the case of a ransomware payload, double extortion methods could apply; however, that has not been previously observed.

Future Considerations: Zloader was a banking Trojan first observed in August 2015 targeting customers of several British financial institutions. It is a banking Trojan similar to Zeus Panda and Floki bot, due to significant similarities in their source code with the Zeus v2 Trojan source code that leaked nearly a decade ago. Zloader has gone through multiple enhancements over time. For example, the delivery of the first stage dropper has changed from phishing emails embedded with a malicious document to a signed MSI payload hosted on external servers. While there is no shortage of banking Trojans coming into 2022, Zloader is expected to return with more enhancements targeting financial services organizations.

SECTION I

Industry Cyberthreat Landscape

I1 – Industry Impact: Construction

CONSTRUCTION THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. PHANTOM PANDA
B. Energetic Bear
C. Berserk Bear
D. Winnti Group
E. Andariel group
F. Babuk Ransomware
G. DoppelPaymer
H. Bandidos
I. Conti
J. Hive

SUB-INDUSTRIES

A. Building construction
B. Heavy construction
C. Special trade construction

COUNTRIES

A. Austria
B. Canada
C. Malaysia
D. India
E. United States
F. Germany
G. Europe
H. Taiwan
I. Israel

TACTICS, TECHNIQUES, AND PROCEDURES

A. Process Discovery
B. Rootkit
C. Subvert Trust Controls: Code Signing
D. Command and Scripting Interpreter: Windows Command Shell
E. Data Encrypted for Impact
F. Deobfuscate/Decode Files or Information
G. File and Directory Discovery
H. Inhibit System Recovery
I. Native API
J. Network Share Discovery
K. Obfuscated Files or Information
L. Process Discovery
M. Process Injection: Dynamic-Link Library Injection
N. Remote Services: SMB/Windows Admin Shares
O. Remote System Discovery
P. Service Stop
Q. System Network Configuration Discovery
R. System Network Connections Discovery
S. Taint Shared Content

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 18 - Construction Threat Landscape

The construction sector has been less prone to cyberattacks, but this has recently changed. The increased cyber activity in the construction industry can be explained in part by the increase in using emerging technologies and trends such as robotics, automation, and machine learning (ML). In 2021, the countries and regions most impacted in this sector were Austria, Canada, Malaysia, India, United States, Germany, Europe, Taiwan, and Israel. The main threat actors responsible were ALTDOS, Phantom Panda, Energetic Bear, Berserk Bear, Winnti group, Andariel group, Babuk Ransomware, Doppelpaymer, Bandidos, Conti, and Hive. These threat actors used various MITRE techniques, including application programming interface (API) calls during execution, using stolen certificates to sign its malware, using a rootkit to modify typical server functionality, and discovering files on the local system.

Key Insights

Currently, the threat actors view the construction sector as an easy target, due to the immature employment of cyber defense strategies. Hence, the amount of cost and effort required for the threat actors to launch a successful cyberattack is significantly reduced. Additionally, the adoption of digitization programs and state-of-the-art technologies by various construction companies has made this industry a lucrative choice for many cybercriminals, due to the substantial financial rewards. An increase in the digital footprint has resulted in various types of malicious cyber activities, such as ransomware attacks, business email compromise (BEC) attacks, intellectual property theft, spear-phishing campaigns, etc. Although financial gain has been the biggest motivation for threat actors targeting the construction industry, disrupting business operations and intellectual property theft have also triggered several cyberattacks on this sector. Ransomware attacks constituted more than 68% of the total cyberattacks on construction companies in 2021. For example, towards the end of December 2020, Amey, the UK infrastructure management company, was hit by a Mount Locker ransomware attack. In another case, construction company Houle experienced a data breach after

being hit with a Conti ransomware attack. In August 2021, a Singapore-based construction firm faced a massive data breach by a threat actor dubbed ALTDOS. Therefore, construction companies need to employ a multi-layered security architecture in their IT infrastructure. They need to identify the cybersecurity risks that are unique to their operational environment and activities, perform proper risk assessment, and adopt a comprehensive cybersecurity strategy in order to counter the growing cyberthreats.

I2 – Industry Impact: Defense

DEFENSE THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. APT33
B. Fox Kitten
C. DEV-0343
D. TortoiseShell
E. Lazarus
F. PortDoor
G. CetaRAT
H. Naikon
I. LockBit2.0
J. CoomingProject

SUB-INDUSTRIES

A. Multi-nation defence
B. Air defence
C. Naval defence
D. Ground defence
E. Space defence

COUNTRIES

A. United States
B. United Kingdom
C. Venezuela
D. Mexico
E. Australia
F. Israel
G. Iran
H. Lebanon
I. Morocco
J. New Zealand
K. Cuba

TACTICS, TECHNIQUES AND PROCEDURES

A. Inhabit System Recovery
B. Credentials
C. Archive Collected Data
D. Boot or Logon Autostart Execution: Shortcut Modification
E. Data Destruction
F. System Time Discovery
G. External Remote Services
H. Brute Force
I. Network Service Scanning
J. Query Registry
K. Remote Services: Remote Desktop Protocol
L. Web Protocols
M. Compromise Accounts: Email Accounts
N. Archive via Custom Method
O. Create or Modify System Process: Windows Service

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 19 - Defense Threat Landscape

With a large, integrated network of legacy cyber technologies, the defense sector provides substantial and diverse scope for cyber-enabled attacks to disrupt military operations. Disabling key systems and communications links, manipulating industrial control systems to cause physical damage, and exfiltrating sensitive data are some of the major impacts faced by the defense sector due to cyberattacks. There have been multiple allegations of governments employing advanced persistent threat (APT) groups (e.g., APT33, DEV-0343, Naikon) to target the defense sectors of their adversaries. Iran, the United States, the United Kingdom, Israel, Venezuela, Mexico, and Australia are among the most at risk of cybercrimes in their defense sectors. Among the top threat actors targeting this sector are Cooming Project, Pay2Key, TortoiseShell, Lazarus, PortDoor, CetaRAT, etc. Methods such as vulnerability exploitation, spear-phishing, and social engineering are utilized to obtain the initial access for the attacks. Some of the frequently used MITRE attack techniques include brute force, password spraying, standard encoding, symmetric cryptography, ingress tool transfer, network sniffing, and obfuscated files or information.

Key Insights

The defense sector is aimed at ensuring the security of the nation, citizens, enterprises, infrastructures, and organizations. Hence, the threat actors are identifying the critical defense technologies and exploiting the vulnerabilities in the defense solutions in order to disrupt the battle capabilities of the adversary. The aerospace industry has experienced similar cyberattacks. The Pay2Key group, which evolved during October 2020, has been observed to perform ransomware attacks on Israeli defense manufacturers. This group disclosed very sensitive employee data of six Israeli firms after they denied paying the ransom amount. In June 2021, the REvil ransomware attacked Sol Oriens, a small US nuclear weapon contractor and subcontractor for the US Department of Energy. The exfiltrated data included a large amount of the company's payroll and exposed sensitive personal information of employees, including quarterly pay, full names, and social security numbers. In July 2021, threat groups allegedly originating from Iran targeted more than 250 Office 365 accounts, most of which belong to defense companies in Israel and the United States. The targeted entities are known for providing military-grade radars, satellite systems, and military drones to the US, Israel, and the European Union. In November 2021, Iran's Mahan Air was hit by cyberattacks that took down the company's websites. In addition to these, there have been instances in the Asia-Pacific where defense entities were targeted by the threat groups. For example, in April 2021, the Chinese-speaking Naikon threat group was found to be targeting the defense sectors in Southeast Asia using Nebulae backdoor. This allowed the threat actors to harvest system information, manipulate files and folders, download files from the command-and-control server, and manipulate processes on the target system with the goal of data exfiltration and cyber-espionage.

From these events, it can be concluded that the Middle East and the North American regions have been deeply affected by cyberattacks targeting the defense industry. Iran tops the list of highly impacted countries, due to attacks against its defense entities, with 41.6% of the total attacks, followed by the US (33.3%) and Israel (16.7%). Most of these attacks have been motivated by financial gain (58.3%). Also, political advantage and regional dominance have triggered more than a quarter of the total events. Ransomware deployment has been the favorite method adopted by threat groups. More than 25% of the attacks conducted against the defense sector are basically ransomware, while 16.7% of the total attacks are data exfiltration and cyber-espionage campaigns.

Because the defense and aviation industries are extremely critical for national security, they are heavily regulated, dominated by multinational giants, and always under close supervision of the government. The growth of the arms race and defense trade has been attracting nations to employ APT groups to steal intellectual properties, conduct cyber-espionage campaigns, and disrupt military activities as a measure to counter their rivals.

I3 – Industry Impact: Energy

ENERGY THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. Energetic Bear
B. APT28
C. nei
D. APT10
E. Lazarus Group
F. APT34
G. Maze
H. Fin7
I. FIN8
J. zerox296
K. zanko
L. barf
M. MuddyWater
N. bl33d
O. Kimsuky
P. ChamelGang

SUB-INDUSTRIES

A. Oil and Gas
B. Nuclear
C. Pipeline
D. Natural Gas

COUNTRIES

A. United States
B. Russia
C. Qatar
D. Indonesia
E. Saudi Arabia
F. South Korea
G. Pakistan
H. Australia
I. Netherlands
J. Iran
K. India

TACTICS, TECHNIQUES, AND PROCEDURES

A. Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
B. Command and Scripting Interpreter: Windows Command Shell
C. Trusted Relationship
D. Scheduled Task/Job: Scheduled Task
E. Obfuscated Files or Information
F. Phishing: Spearphishing Attachment
G. Remote Services: Remote Desktop Protocol
H. System Information Discovery
I. Ingress Tool Transfer
J. Command and Scripting Interpreter: PowerShell
K. User Execution: Malicious File
L. Indicator Removal on Host: File Deletion
M. Application Layer Protocol: Web Protocols
N. Masquerading: Match Legitimate Name or Location
O. Data from Local System

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 20 - Energy Threat Landscape

Given the energy sector's vital role in critical infrastructure, any successful cyberattacks in this space could have significant consequences on geopolitics, economies, and social stability. A cyberattack in this space might cause a single point of failure, which could include attacks against PLCs (Programmable Logic Controllers), ICS (Industrial Control Systems), and OTs (Operational technologies). Many of these systems and technologies are equipped by aiming at remote operations. The majority of these systems are implemented on legacy hardware with built-in features, as most of these systems are designed to be low maintenance. These factors create a long and complicated updating and patching process of the vulnerabilities, giving attackers and threat actors an upper hand.

Attacks on the energy sector in 2021 mostly targeted the United States, Russia, Qatar, Indonesia, Saudi Arabia, South Korea, Pakistan, Australia, Netherlands, Iran, and India. The most impacted sub-sectors were oil and gas, nuclear, pipeline, and natural gas. Most attacks were performed by Energetic Bear, APT28, APT10, Lazarus group, APT34, Maze, Fin7, FIN8, and MuddyWater threat actor groups.

Key Insights

Financially motivated threat actors remain the primary source of threat to the energy sector. Ransomware attacks and network access-related attacks were observed to be the prominent attacks. Spear-phishing, phishing campaigns, compromised credentials, and weak or misconfigured applications were exploited by threat actors to gain initial network access to the private network. The use of malicious links and attachments with obfuscated payloads to execute malicious executables to gain system access was prominently observed across the energy sector. Threat actors also exploited trusted relationships between businesses to leverage lateral movement among vendors, which resulted in ransomware and malware deployment extorting the victims and providing network access to other trusted partners.

The energy sector is a crucial part of CNI (Critical National Infrastructure), making it an attractive target for nation-state-sponsored APT groups. US-based Colonial Pipeline suffered a high-profile attack, which led to country-wide disruptions. Saudi Arabia-based Aramco suffered a data breach that resulted in threat actors leaking confidential key documents on hacking forums. A South Korean nuclear research facility also reported a data breach when threat actors successfully exploited a vulnerability to gain VPN access in an attempt to gain sensitive information; this attack was later attributed to the Kimsuky APT group. Iran's nuclear and oil facility suffered a major cyberattack targeting Natanz nuclear facility. In another campaign, several Iranian gas stations and refineries were targeted.

APT groups were reported to use Trojans and espionage campaigns to gather and exfiltrate sensitive information about supervisory control and data acquisition (SCADA) systems and other critical infrastructure such as nuclear research facilities. Given the importance of the energy sector in critical infrastructure, nation-state-linked threat actors pose high threats motivated by sensitive data theft, which later can be leveraged to cause disruption at an increased scale.

Cyberattacks on the transportation sector have significantly increased, compared with previous years. Based on the latest cyber intelligence, organizations within the energy sector should prepare for 2022 by assessing the following:

- The energy sector should be on alert, as nation-state-linked threat actors are always lured by disruptions and intelligence theft. In addition, the complexity of interconnected Industrial Control Systems (ICS) could be more susceptible to attacks. This is due to the fact that the threat landscape and attacks are evolving against ICS and Operational technologies (OT) and might have unknown risks associated with it. Insurance companies should ensure that appropriate measures and procedures to evaluate cyber risks are in place. They should also perform due diligence with vendors to protect against espionage and disruption attacks.
- Insecure and proprietary protocols and high availability are challenges to Industrial Control Systems (ICS), which also have a huge risk of lateral movement from IT networks. However, this risk could be mitigated by following the best practices for ICS systems, such as monitoring for access, securing remote access, and network segmentation.
- Threat actors use compromised systems for lateral movement to other infrastructure, as well as several IAB (initial access broker) target IT systems to sell network access to organizations. These risks can be largely mitigated by following the principle of least privilege and segmenting high-risk devices and applications. Proper authentication mechanisms should also be in place.

I4 – Industry Impact: Finance

FINANCE THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. Cuba
B. Evil Corp
C. Conti
D. LockBit
E. Hidden Cobra
F. Rakuda
G. TA544
H. Ionel Roman
I. FIN7
J. Bizarro
K. Sprite Spider
L. APT38
M. TA413
N. TA428
O. Carbanak

SUB-INDUSTRIES

A. Central banking
B. Investment funds
C. Private banking
D. Fund management
E. Savings

COUNTRIES

A. United States
B. Australia
C. New Zealand
D. Germany
E. Malaysia
F. Bangladesh
G. Brazil
H. South Korea
I. Japan
J. Italy
K. Ukraine
L. Canada
M. Singapore
N. United Kingdom
O. China

TACTICS, TECHNIQUES, AND PROCEDURES

A. Spearphishing Attachments
B. Spearphishing Link
C. User Execution
D. Command and Scripting Interpreter
E. Shared Modules
F. Boot or Autologon Execution
G. Remote Desktop Protocol
H. Data from Network Share Drives
I. Account Discovery
J. System Information Discovery
K. Exfiltration Over Web Service: Exfiltration to Cloud Storage
L. DNS Communication
M. Create or Modify System Process: Windows Service
N. Event Triggered Execution: Application Shimming
O. Encrypted Channel

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 21 - Finance Threat Landscape

Financial institutions possess a significant amount of sensitive data, including the personal information of their customers. As they continue to embrace digital transformation through increased digitization, person-to-person (P2P) payments, cloud computing, and blockchain technology, the finance sector attracts numerous threat actors.

Countries that were highly targeted by threat actors in 2021 include the United States, Australia, New Zealand, Germany, Malaysia, Bangladesh, Brazil, South Korea, and Japan. The various threat groups involved in targeting the financial sector are Cuba, APT38, Hades (Ransomware), Conti, LockFile, Clop, Hidden Cobra, APT28 (Fancy Bear), Rakuda, Ursnif, Ionel Roman, Prometheus, FIN7, Bizarro, Zaneleiro, Sprite Spider, Vadokrist, Darkside, DanaBot, Carbanak, etc. In order to gain initial access, these threat actors employ several methods, such as spear-phishing campaigns, social engineering, password spraying, vulnerability exploitation, etc. Other MITRE techniques that they employ include user execution, command and scripting interpreter, account discovery, application shimming, exfiltration over web service, exfiltration to cloud storage, etc.

Key Insights

In first week of February 2021, the Automatic Funds Transfer Services (AFTS) (which is frequently used by many cities and agencies in the US as a payment processor and address verification service) was targeted by a Cuba ransomware attack. It significantly disrupted business operations and made the AFTS website unavailable. Cuba operators typically breach a network, steal network credentials, spread slowly through servers, and deploy the ransomware to encrypt devices. In a huge-scale attack, the North Korea-based APT38 group is alleged to have stolen more than $1 million from various banks worldwide. The Reserve Bank of New Zealand suffered a data breach after actors illegally accessed its information through one of the bank's third-party file sharing services. The Bank of Australia has already warned of inevitable large-scale cyberattacks on the banking and financial sector.

In 2021 there was a 200% growth in cyberattacks targeting the financial sector. Almost 32% of the attacks were performed against the United States. Australia was second the list, at 13.4%. More than 90% of the attacks against the finance sector are motivated by financial gain. And because financial institutions contain very sensitive data regarding their customers, some attacks are meant for cyber-espionage as well. Also, ATM jackpotting activities have been rising recently. However, more than 28% of the attacks on the financial sector are ransomware attacks. The PowerShell script has been observed to be widely used by the threat actors to gain initial access.

I5 – Industry Impact: Healthcare

HEALTHCARE THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. APT37
B. APT28
C. ShinyHunters
D. APT40
E. Evil Corp
F. Winnti Group
G. Lazarus Group
H. Pinchy Spider
I. FIN11
J. Hive Ransomware
K. WIZARD SPIDER
L. PIONEER KITTEN
M. APT35
N. TA505
O. APT10
P. DOPPEL SPIDER
Q. Bandidos

SUB-INDUSTRIES

A. Patient diagnostics
B. Telemedicine
C. Patient monitoring

COUNTRIES

A. United States
B. Canada
C. Mexico
D. Ireland
E. New Zealand
F. United Kingdom
G. Germany
H. France
I. Spain
J. Israel
K. Singapore
L. Costa Rica
M. Australia

TACTICS, TECHNIQUES, AND PROCEDURES

A. System Information Discovery
B. Process Injection
C. Windows Command Shell
D. Abuse Elevation Control Mechanism: Bypass User Account Control
E. Phishing: Spearphishing Attachment
F. User Execution: Malicious File
G. Active Scanning: Vulnerability Scanning
H. Password Spraying
I. Command and Scripting Interpreter: PowerShell
J. Exploit Public-Facing Application
K. Exploitation of Remote Services
L. Remote Services: SMB/Windows Admin Shares
M. User Execution: Malicious Link
N. Exfiltration Over C2 Channel
O. Impair Defenses: Disable or Modify Tools
P. Process Injection: Dynamic-Link Library Injection

Impact: • Informational, • Caution, • High Risk, • Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 22 - Healthcare Threat Landscape

Across the globe, we have observed several attacks on healthcare systems. The most impacted countries were the United States, Canada, Mexico, Ireland, New Zealand, United Kingdom, Germany, France, Spain, Israel, Singapore, Costa Rica, and Australia. Looking a little in depth, highly impacted and prone to malfunction are patient monitoring systems, remote diagnosis technology (Telemedicine), and patient diagnostics systems. Threat actors that have highly affected this sector and caused significant disruption across the globe are Hive, FIN11, Winnti group, Lazarus group, and ShinyHunters. These threat actors heavily use phishing emails, vulnerability exploitations, and password spraying attacks to gain initial access to the IT systems. Other MITRE techniques used throughout the attack are Bypass User Account Control, Process Injection, Exploit Cloud Accounts, Disable or Modify Tools, Dynamic-link Library Injection, and Exfiltration Over C2 Channels.

Cybercrime revved up during the pandemic as the threat actors took advantage of the situation and caused significant disruption to organizations across all sectors. Hospitals and healthcare facilities were among the most impacted, covering about 8.9% of the attack surface. As a result, healthcare facilities are focusing on hardening their systems and cyber defenses, which increases ongoing operations expenses. The associated costs and the recovery time of sensitive data create a financial burden and disable hospitals' ability to provide proper health care, ultimately impacting human life.

Key Insights

Among the most impacted organizations in this sector in 2021 were the Irish Health Service Executive (HSE), Oloron-Sainte-Marie and Dax hospitals in southern France, Hillel Yaffe Hospital in Israel, the Eye & Retina Surgeons (ERS) in Singapore, Eastern Health in Australia, New Zealand's Waikato DHB, UF Health in central Florida, US Medical Laboratory, Memorial Health Systems in the United States, and Newfoundland and Labrador Healthcare and Humber River Hospital in Canada. In all of these attacks, IT systems infrastructure took the first hit, leading to disruptions in day-to-day operations.

Many of these attacks had a key motive in common: compromising systems that hold sensitive data. This not only creates a significant risk to organizations (regulatory, financially and reputationally), but also to impacted individuals. Personally identifiable information (PII), patient history, and health history can be used by the threat actors for identity fraud, selling of PII on the Dark Web, and other nefarious actions.

Cyberattacks on healthcare facilities across the globe doubled in 2021, compared with the previous year. Based on the latest cyber intelligence, organizations within the healthcare sector should prepare for 2022 by assessing the following:

■ Key healthcare organizations that should be on alert: Applications providing healthcare-related services such as online consultation and remote diagnostics are more susceptible to threats and exploitations because the threat actors could more easily access and exploit the applications on the web. Also, healthcare facilities rely on third-party vendors for medical services and instruments. Healthcare organizations should ensure that appropriate measures are in place and perform due diligence with vendors to protect highly sensitive information, such as clinical or R&D data and patient data.

■ A key observation from all these attacks is that employee accounts or service accounts are widely exploited due to a lack of password protection and cross-platform password reuse. Enabling multi-factor authentication (MFA) on critical systems and all employee accounts could be crucial.

■ Other critical areas to focus on are securing remote access channels, providing appropriate training to all employees (including the medical staff), building an incident response plan by engaging cybersecurity experts, and emphasizing internal and external communication and transparency.

I6 – Industry Impact: Insurance

INSURANCE THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. FIN8
B. 7h0rf1nn
C. FIN7
D. APT34
E. MuddyWater
F. Maze
G. Marketo

SUB-INDUSTRIES

A. Life Insurance
B. Non-life insurance

COUNTRIES

A. France
B. Israel
C. Mexico
D. Italy
E. United States
F. Canada
G. United Kingdom
H. Germany
I. Puerto Rico

TACTICS, TECHNIQUES, AND PROCEDURES

A. Windows Management Instrumentation
B. Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
C. Command and Scripting Interpreter: Windows Command Shell
D. Trusted Relationship
E. Scheduled Task/Job: Scheduled Task
F. Obfuscated Files or Information
G. Phishing: Spearphishing Attachment
H. System Information Discovery
I. Data from Local System
J. Ingress Tool Transfer
K. Deobfuscate/Decode Files or Information
L. Command and Scripting Interpreter: PowerShell
M. User Execution: Malicious File
N. Masquerading: Masquerade Task or Service
O. Indicator Removal on Host: File Deletion
P. User Execution: Malicious Link
Q. Phishing: Spearphishing Link

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 23 - Insurance Threat Landscape

Digitalization is the key formula to a successful business. Many industries, including the insurance industry, have adopted several technologies that proved to be a game-changer in the way organizations look at business and everyday operations. The global pandemic has propelled the insurance industry towards accelerated digitalization, with positive results, but this also comes with increased exposure. These changes have also lured threat actors to the insurance sector, particularly towards personally identifiable information (PII), owing to the fact that insurance companies hold a significant amount of PII data on their clients. Data relating to clients is necessary for business operations, such as managing claims. The data can include sensitive information such as medical or other proprietary records, as per the business needs of the industry. They can also include government-issued identity cards or other documents such as business and strategic plans, legal documents, and financial statements. With the increasing need to access the data remotely and quickly, it is now stored digitally. This includes copies of agreements, IDs, and other sensitive information that isn't limited to medical history and disease records. Most of this change is driven by migrating to cloud infrastructures in order to collaborate with multiple channels such as banks and hospitals. With the insurance sector experiencing a wider scope of growth, terms such as business insurance, risk insurance, and cyber insurance are gaining popularity. At the same time, the threat actors are becoming increasingly sophisticated. Instead of operatiang on their own, they prefer to collaborate with each other for increased revenue and impact. It is becoming more and more common for threat actors to collaborate with teams and individuals that specialize in their own attack techniques and have unique capabilities.

Threat actors targeted multiple geographies across the Insurance sector in 2021, with major impact in France, Israel, Mexico, Italy, the United States, Canada, United Kingdom, Germany, and Puerto Rico. Additionally, these attacks impacted both Life Insurance and Non-Life Insurance sub-sectors. Primary threat actors who affected business operations and caused significant disruptions across the sector are FIN8, 7h0rf1nn, FIN7, APT34, MuddyWater, and Maze. These threat actors primarily exploited trusted relationships

among different organizations. However, cases of phishing and spear-phishing campaigns were also observed in some of the disruptions. The loader and executables used in these attacks are highly obfuscated and sometimes novel; they are also capable enough to evade defense mechanisms such as anti-malware solutions.

Key Insights

Most of the attacks are successful in the insurance sector because the majority of small- and medium-scale insurance companies outsource their technical resources from other companies and third-party organizations. Threat actors are also aware of the time-sensitive nature of the sector, which requires individuals to be proactively engaged in important conversations. For example, a TrickBot campaign that targeted insurance firms in North America lured employees by sending phishing traffic violation emails. The Marketo threat actor group targeted insurance software providers with cyber extortion attacks that involved leaking sensitive stolen files and data on the Dark Web for auctioning the data. Fancy Lazarus was observed to perform DDoS attacks on victims and perform extortion by demanding ransom via emails. European-based insurance company AXA was targeted in a ransomware attack by the Avaddon gang after it announced major changes to its insurance policy. AXA states that the company will stop reimbursing their clients affected by ransomware attacks. This attack caused business disruption in Asia, including Thailand and Hongkong, allowing the threat actor group to exfiltrate 3TB of sensitive data from the company. Other major insurance companies that suffered cyberattacks include France-based Mutuelle Nationale des Hospitaliers (MNH), US insurance giant CNA (victim of new Phoenix CryptoLocker ransomware), UK-based One Call (hit by Darkside ransomware), Florida-based Cloudstar, and Tokio Marine Holdings in Singapore. Most of these attacks were financially motivated, including the share of ransomware attacks and IABs (Initial Access Brokers) selling network access to the organizations.

Cyberattacks on the insurance sector have significantly increased, compared with previous years. These attacks can lead to loss of confidential data, damage to reputation, and disruption in business operations. Based on the latest cyber intelligence, organizations within the insurance sector should prepare for 2022 by doing the following:

■ Providing employees with necessary phishing and security awareness training and exercises to reduce human errors that lead to attacks (which, based on analysis, is the cause of the majority of attacks).

■ Implementing role-based access controls to ensure that sensitive information is only available to individuals that require access for business needs. In addition, monitoring and logging of central databases and other systems containing PII (personally identifiable information) can only be ensured through proper alerting.

■ Employing in-house security and access management teams with the key responsibility to protect proprietary data and implementing a proper incident response plan with proper gap and risk assessments can help significantly lower the attack impact.

I7 – Industry Impact: Manufacturing

MANUFACTURING THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. WIZARD SPIDER
B. PIONEER KITTEN
C. APT 34
D. APT 35
E. PHANTOM PANDA
F. Energetic Bear
G. Berserk Bear
H. FIN11
I. Sandworm Team
J. TA505
K. DOPPEL SPIDER
L. SPRITE SPIDER
M. MALLARD SPIDER
N. Lazarus APT group
O. APT10
P. Winnti Group

SUB-INDUSTRIES

A. Food and Drink
B. Textile
C. Furniture
D. Chemicals
E. Petroleum
F. Automotive
G. Medical Equipment
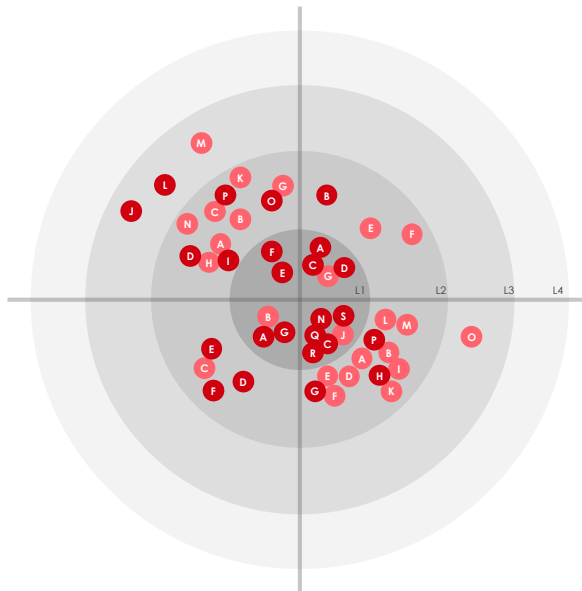
COUNTRIES

A. United States
B. Australia
C. Canada
D. Europe
E. Mexico
F. New Zealand
G. UK

TACTICS, TECHNIQUES, AND PROCEDURES

A. Account Discovery: Domain Account
B. Account Discovery: Email Account
C. Account Manipulation
D. Acquire Infrastructure: Domains
E. Acquire Infrastructure: Server
F. Account Discovery: Email Account
G. Application Layer Protocol: Web Protocols
H. Command and Scripting Interpreter: PowerShell
I. Command and Scripting Interpreter: Windows Command Shell
J. Command and Scripting Interpreter: Visual Basic
K. Command and Scripting Interpreter: JavaScript
L. Credentials from Password Stores: Credentials from Web Browsers
M. Data Encrypted for Impact
N. Dynamic Resolution: Fast Flux DNS
O. Ingress Tool Transfer
P. Inter-Process Communication: Dynamic Data Exchange
Q. Phishing: Spearphishing Attachment
R. Phishing: Spearphishing Link

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 24 - Manufacturing Threat Landscape

There has been a drastic rise in the number of cyberattacks on the manufacturing industry, which is attributed to an increase in automation and connectivity across many major industries. Many manufacturing machines were made at a time when there were fewer security concerns. This makes them much more vulnerable to present-day attacks. The industry includes sub-industries such as food and drink, textiles, furniture, chemicals, and medical equipment.

The major regions impacted by attacks on the manufacturing industry include the United States, Australia, Canada, Europe, Mexico, New Zealand and the UK. The main threat actors involved in these cyberattacks were Revil, Wizard Spider, APT 34, APT 35, FIN11, Sandworm Team, TA505, APT10, and Winnti group.

Key Insights

The rapid surge in ransomware attacks has seriously impacted the manufacturing sector. For example, JBS Foods, (the largest meat producer globally) was hit by ransomware attacks towards the end of May 2021. REvil group was reported to be behind this huge-scale attack. JBS was demanded to pay $11 million in ransom, with cryptocurrency as the mode of transaction. Frequent supply-chain attacks have also been observed, significantly affecting the manufacturing industry. The supply-chain attacks on SolarWinds affected around 40 defense manufacturers across the world. Similarly, the Canadian plane manufacturer Bombardier was severely impacted by the Accellion supply-chain attack. Security breaches and data exfiltration have been another concern for security personnel in the manufacturing sector. Towards the end of December 2020, Japan's Kawasaki Heavy Industries (which is active in heavy equipment, rolling stock, automotive, aerospace, and defense equipment) announced a security breach and potential data leak after unauthorized access to a Japanese company server from multiple overseas offices. Similarly, in June 2021, automobile manufacturers Audi and Volkswagen experienced a data breach that was reported to affect 3.3 million customers. Some of the extremely sensitive customer information held by manufacturers is also exposed to the outside, due to data breach incidents.

More than 1.6% of the total cyber events in 2021 targeted the manufacturing industry. More than 64% of the total cyberattacks in the manufacturing sector are ransomware attacks. It has been observed that most of these attacks are financially motivated. The technological developments (including the convergence of IT/OT systems), the sensitivity of the industries towards downtime, and the lack of segmentation have attributed to the surge in industrial cyberthreats. Being the most important artifact of the global economy, any attack on this sector paves the way for the active disruption of the global supply-chain, affecting all other industries in a chain reaction. Implementation of enterprise-level risk management, the introduction of real-time network visibility to track adversaries, compact segregation of IT and OT systems, and implementation of strong patching policies could be very effective in defending against these cyberthreats.

I8 – Industry Impact: Public Sector

PUBLIC SECTOR THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. MAK (Movement for the self-determination of Kabylie)
B. TrickBot
C. Sodin, REvil
D. Pysa
E. NOBELIUM APT group
F. Drumrlu
G. APT10
H. RedFoxtrot
I. TA406
J. Persian Security Group, H4shur
K. Lab Dookhtegan
L. "Bax 026 of Iran" (aka "Bax026," "Iranian Cyber Army")
M. APT34, Helix Kitten, Oil Rig
N. Seedworm
O. TAG-28
P. SharpPanda
Q. SideCopy
R. Lyceum Group
S. APT36

SUB-INDUSTRIES

A. International Affairs
B. National Security
C. Federal Government
D. Provincial Government

COUNTRIES

A. South Korea
B. United States
C. Iran
D. Australia
E. Israel
F. China
G. Israel
H. Saudi Arabia
I. Canada
J. Lebanon
K. Germany
L. Fiji
M. Russia
N. Syria
O. Japan
P. United Kingdom
Q. Algeria
R. Egypt
S. Sudan

TACTICS, TECHNIQUES, AND PROCEDURES

A. Data from Local System
B. System Information Discovery
C. Phishing: Spearphishing Link
D. Active Scanning: Vulnerability Scanning
E. Brute Force: Password Spraying
F. Acquire Infrastructure: Domains
G. Phishing for Information
H. Query Registry
I. Command and Scripting Interpreter
J. Exfiltration Over C2 Channel
K. Account Discovery
L. External Remote Services
M. User Execution: Malicious File
N. Data Encrypted for Impact
O. Modify Registry

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 25 - Public Sector Threat Landscape

The public sector was observed to be one of the most targeted sectors worldwide, with impacted nations including Canada, the United States, Australia, Russia, Germany, North Korea, the United Kingdom, Germany, Pakistan, Turkey, Saudi Arabia, the United Arab Emirates, Iran, Israel, Iraq, Egypt, Qatar, Libya, Kuwait, Morocco, and many more. Moreover, some of the governmental sectors prone to attacks are international affairs, national Security, and federal government. A portion of the known threat actors responsible for the cyber incidents are REvil, TrickBot, LockBit 2.0, Charming Kitten, Balikbayan Foxes, Goblin Panda, Kimsuky, LuminousMoth, Lyceum Group, RedFoxtrot, Pysa, APT36, APT34, APT31, APT29, APT10, and more. These threat actors leveraged phishing emails, vulnerability exploitations, and password spraying attacks to gain initial access to the IT systems. Other predominant MITRE TTPs observed include Exfiltration Over C2 Channel, Account Discovery, External Remote Services, User Execution: Malicious File, Data Encrypted for Impact, and Modify Registry.

Cyber incidents escalated during the pandemic as the threat actors targeted government agencies. The public sector is a prime target for cyberattacks where agencies hold on to large, diverse data about

their citizens, including social care data and passport information. The public sector is among the most targeted industries worldwide, covering about 29.5% of cyberattacks. However, in 2021, public sector IT teams indicated that the right security technologies have been identified and are in the process of being implemented. In addition, new government policies such as the Presidential Cybersecurity Executive Order in the United States are paving the way for cybersecurity improvements and addressing agency cyber risks.

Key Insights

Many of the cyberattacks targeting the public sector are successful due to the fact that many government agencies rely on the data security of outdated computer systems. Hence, threat actors view government agencies as easy targets to compromise. In addition, with the vulnerable security controls in place, public sector groups realize too late that they have been infected or targeted in a cyberattack.

Most publicly owned companies are under-resourced, especially in matters involving cybersecurity. Globally, the public sector is one of the most targeted industries for threat actors, with more cyber incidents in 2021 than the year before. In combination with outdated security systems, poor funding, and lack of security training, publicly owned organizations are more vulnerable to cyber espionage or financially motivated attacks. Many of these attacks have a common motive in compromising systems that hold sensitive data. This creates a significant risk to organizations and impacted individuals. The threat actors can use personally identifiable information (PII) and an individual's history for purposes of identity fraud, selling of PII on the Dark Web, and other heinous actions.

Based on the latest cyber intelligence, organizations within the public sector should prepare for 2022 by assessing the following:

- In the public sector, cybersecurity awareness needs more attention. Educating employees on methods such as social engineering and phishing could be vital to preventing the threat actors from gaining initial access into target networks. Most of the time, the threat actors deliver malicious payloads using emails, so providing required training to employees on identifying suspicious activity is essential. For example, inattentive users could easily download a malicious document and compromise a network. With proper cyber education, employees could identify instances of social engineering tactics being applied and avoid potential compromise.

- Public organizations are one of the most targeted sectors, while also holding critical information about their users. Therefore, public sector groups need to invest in building or upgrading a threat intelligence program to support their needs. A comprehensive and strategic threat intelligence program can detect emerging threats, increase situational awareness, and provide actionable intelligence to mitigate potential threats.

- Many public sector companies rely on the data security of an outdated computer system and utilize obsolete software. Applications not updated to the latest patch are subject to being exploited via vulnerabilities. Applications should be constantly patched and updated with the latest security updates released by the vendor. Additionally, organizations need to closely monitor applications approaching the end-of-life period. With such applications, vendors typically discontinue support, which could create security vulnerabilities for threat actors to leverage.

I9 – Industry Impact: Retail

RETAIL THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

- A. Nei
- B. inthematrix1
- C. ShinyHunters
- D. Winnti Group
- E. APT10
- F. Lazarus Group
- G. Carbanak
- H. TA505
- I. Maze
- J. Magecart
- K. Evil Corp
- L. FIN8
- M. FIN7
- N. HAFNIUM
- O. APT37
- P. OceanLotus
- Q. Astro Locker Team
- R. barf
- S. Stari4ok
- T. denis2363
- U. DataBox

SUB-INDUSTRIES

- A. Food stores
- B. Retail
- C. Food services
- D. Automotive dealers

COUNTRIES

- A. United States
- B. India
- C. Russia
- D. Germany
- E. France
- F. United Kingdom
- G. Brazil
- H. Australia
- I. Canada
- J. Spain
- K. Italy
- L. Japan
- M. China
- N. Sweden
- O. Mexico
- P. Argentina
- Q. Czech Republic
- R. Thailand
- S. Saudi Arabia

TACTICS, TECHNIQUES, AND PROCEDURES

- A. Trusted Relationship
- B. Ingress Tool Transfer
- C. Application Layer Protocol: Web Protocols
- D. Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
- E. Deobfuscate/Decode Files or Information
- F. Scheduled Task/Job: Scheduled Task
- G. System Information Discovery
- H. Active Scanning
- I. Command and Scripting Interpreter: PowerShell
- J. Command and Scripting Interpreter: Windows Command Shell
- K. Drive-by Compromise
- L. Network Service Scanning
- M. Obfuscated Files or Information
- N. Phishing: Spearphishing Attachment
- O. Process Discovery

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely
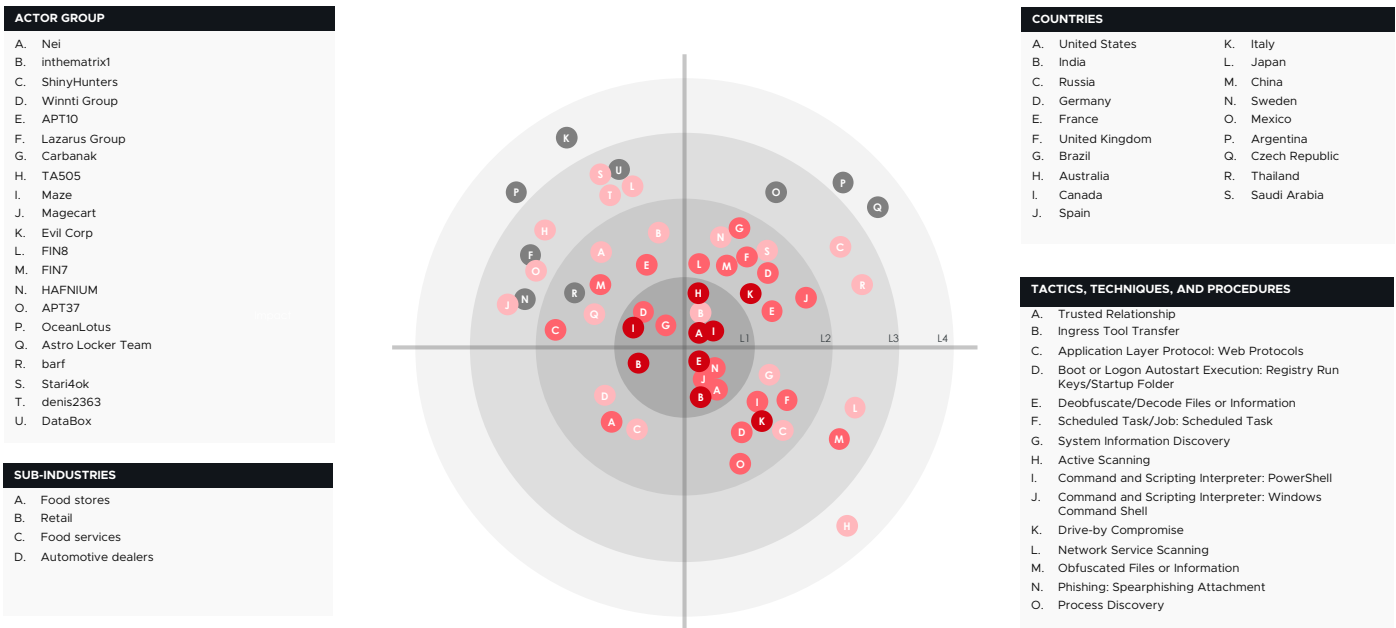
Figure 26 - Retail Threat Landscape

The retail sector is a significant contributor to any country's economy and acts as a key factor in keeping supplies and the demand for goods in check, both nationally and internationally. As part of the global supply-chain network, the retail sector owns a considerable share of the global economy; and with it comes a huge surge of network traffic and data. With the COVID-19 pandemic and lockdown globally, the retail sector registered a slowdown in sales in both offline retailing and retail stores. The pandemic has transformed the way industries look at business. As a result, the retail market has observed an enormous increase in online marketing and retailing. With this change, the attitude towards online shopping has increased positively, due to the added convenience and benefits. Together, these factors have compelled the offline small and big retailers, businesses, and retail stores to shift their focus to online retailing in order to survive. Small businesses have moved their products online and rented gateways to enable online payments by cards and other modes, with other prominent businesses focusing on machine learning and data optimization to gain profits. These shifts require storing user data on the retailer website and the payment and credit card information with other PII (Personally Identifiable Information), such as email addresses, mobile numbers, names, and residential addresses. The threat actors are harnessing this opportunity to gain both financial information and PII. They know that the retail sector has a lucrative amount of monetary funds involved, which might lure not only threat actors, but also insider threats.

Common threats such as ransomware, phishing, cryptojacking, and attacks specific to retail industries affect the retail threat landscape. These include attacks on POS (point of sale) systems, EMV and digital skimming, waterhole attacks, and authentication bypass attacks—making the retail sector's threat landscape very vulnerable. Many threat actors and APT groups are also observed to conduct waterhole campaigns on a massive scale. These attacks embed keylogging scripts that record the user's activity on the website. These malicious scripts can also collect sensitive information such as credit card numbers and other data

when users enter the website's information, which is then sold on carding and hacking forums. In a recent campaign, a threat actor was observed to embed malicious scripts behind the social media icons, making it impossible for anti-malware systems to detect and stop keylogging. Threat actors are also observed to perform web attacks such as traffic redirection and session token hijacking. These attacks redirect the victim to some other malicious website or steal the tokens, which can later be used to impersonate the user for malicious purposes (selling the account access for carding, etc.). Threat actors leverage third-party vendors and plugins to perform supply-chain attacks. The attacker compromises a third-party vendor and then pivots to different servers (including the POS systems) to harvest credentials and payment details stored on the system.

Threat actors targeted multiple geographies and various businesses across the retail sector, having a major impact in the United States, India, Russia, Germany, France, United Kingdom, Brazil, Australia, Canada, Spain, Italy, Japan, Italy, China, Sweden, Mexico, Argentina, Czech Republic, Thailand, and Saudi Arabia. These attacks also impacted sub-sectors in the retail industry, including food stores, retail, food services, and automotive dealers. The primary threat actors who highly affected the industry with their cyber operations and campaigns are Nei, inthematrix1, ShinyHunter, Winnti group, APT10, Lazarus group, Carbanak, TA505, Maze, Magecart, Evil Corp, FIN8, FIN7, HAFNIUM, APT37, OceanLotus, and Astro Locker Team. These threat actors prominently exploited trusted relationships among different organizations, while others leveraged drive-by compromise, spear phishing and phishing, malicious attachments, Remote Desktop Protocol, user execution, supply-chain attacks, and brute-force attacks as initial access vectors. The threat actors also leveraged pivoting by exploiting Active Directory, WMI, and PowerShell to execute commands remotely on victim systems.

Key Insights

Due to high attack surface area and engagement with different people (including customers, employees, and staff required in various stages of the supply and demand chain), the retail sector is vulnerable to attacks. As a result, financially motivated threat actors remain the top retail sector threat, followed by APT groups motivated by espionage activities. SparklingGoblin, an APT group under the umbrella of the Winnti group, was observed to conduct an espionage campaign targeting organizations with spear-phishing emails, aiming to deliver a backdoor to victim's systems. This campaign severely affected organizations from the United States and South Korea. MageCart group was reported to inject a new skimmer malware capable of operating without detection on May 17, 2021. Dairy Farm, an Asia-based company, was targeted by a ransomware attack by Revil Ransomware, demanding $30 million in ransom; FatFace, a clothing retailer, paid $2 million to Conti ransomware; Home Hardware, one of Canada's largest hardware retailers, reported a ransomware attack from DarkSide ransomware. Furniture Village, a UK-based furniture retailer, also suffered a ransomware attack; Guess, an America-based fashion brand, fell victim to a DarkSide ransomware attack, causing the breach of 200GB of customer data; Famous Smoke Shop, a Pennsylvania-based retailer, was forced to shut down its website and lounges after falling victim to a ransomware attack. Ermenegildo Zegna, an Italy-based luxury fashion house, fell victim to RansomEXX, resulting in a breach of 20.74GB of data. Media Market, a Germany-based retail giant, suffered a ransomware attack by the Hive gang, leading to a demand of $240 million ransom and causing disruption of services. Several IABs (initial access brokers) were also observed to advertise the network access to retail companies throughout the globe on underground hacking forums.

Cyberattacks on the retail sector have significantly increased, compared with previous years. These attacks can lead to loss of confidential data, damage to reputation, disruption in business operations, and exfiltration of payment data from POS systems. Based on the latest cyber intelligence, organizations within the retail sector should prepare for 2022 by assessing the following:

- The systems storing critical data (such as point-of-sale systems and other databases) should be identified and isolated on different secure networks, so these systems are out of reach from undesirable network traffic. Vulnerability assessment of applications accessing these databases should be performed, testing and remediating any known vulnerabilities.
- Because the retail sector is always at a risk of insider and outsider threats, proper access control should be enforced on sensitive information and the systems hosting or storing proprietary information. In addition, the concept of least privilege should be followed, to prevent employees' use of sensitive information and data.

I10 – Industry Impact: Services

SERVICES THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP

A. ShinyHunters
B. TeamTNT
C. Conti
D. Avaddon
E. Sprite Spider
F. TrickBot
G. REvil
H. Cozy Bear
I. Ragnar
J. LockBit2.0
K. Agrius
L. TA453
M. Deus
N. BlackShadow
O. Evil Eye

SUB-INDUSTRIES

A. Telecommunication and Technology
B. Media and Entertainment
C. Education
D. Consulting
E. Travel & Leisure
F. Legal Services
G. Professional Services
H. Hospitality
I. Social Media

COUNTRIES

A. United States
B. Australia
C. New Zealand
D. Germany
E. Malaysia
F. Bangladesh
G. Brazil
H. South Korea
I. Japan
J. Italy
K. Ukraine
L. Canada
M. Singapore
N. United Kingdom
O. China

TACTICS, TECHNIQUES, AND PROCEDURES

A. Spearphishing Attachments
B. Spearphishing Link
C. User Execution
D. Command and Scripting Interpreter
E. Shared Modules
F. Boot or Autologon Execution
G. Remote Desktop Protocol
H. Data from Network Share Drives
I. Account Discovery
J. System Information Discovery
K. Exfiltration Over Web Service: Exfiltration to Cloud Storage
L. DNS Communication
M. Create or Modify System Process: Windows Service
N. Event Triggered Execution: Application Shimming
O. Encrypted Channel

Impact: ● Informational, ● Caution, ● High Risk, ● Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely
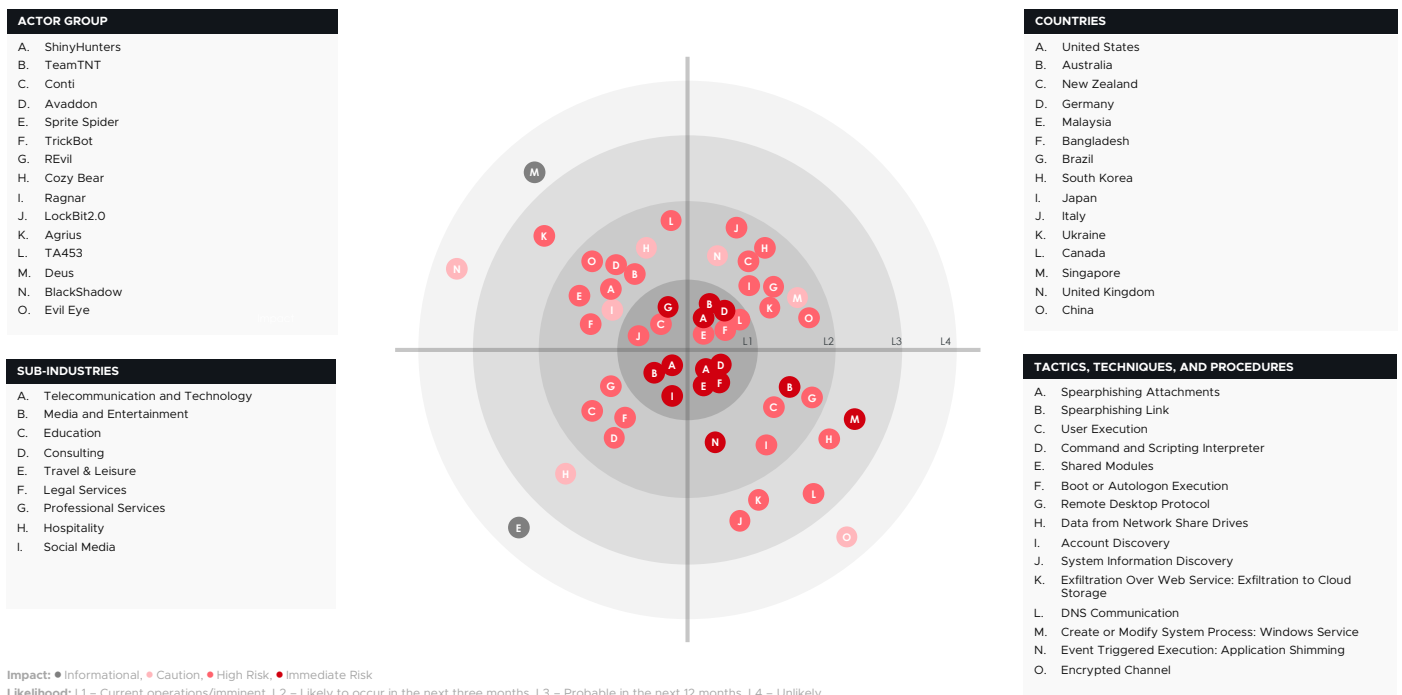
Figure 27 - Services Threat Landscape

The service sector is the most diversified industry. It includes various sub-industries such as education, telecommunication and technology, consulting, media and entertainment, hospitality, professional services, legal services, travel and leisure, social media, accounting services, etc. Hence, the service sector has been the most frequently targeted industry by the threat groups. The countries whose service sector has been under constant threat of cyberattacks include the United States, Australia, Canada, the United Kingdom, Brazil, India, China, Germany, Japan, Israel, Iran, etc. Due to the diverse nature of the services, the threat groups are employing different methods to perform their malicious activities against each sub-industry. For example, unauthorized network access and ransomware attacks against the telecommunication and technology industries; data breach and intellectual property theft against the education sector; cyber-espionage and data breach campaigns against media and entertainment; and ransomware attacks against the travel and leisure industry. In addition, spear-phishing and social engineering techniques are used against the consulting and social media sectors to target individual sub-industries. Various threat groups targeting the service sector are ShinyHunters, Sprite Spiders, Conti, LockBit, Avaddon, DeadRinger, TA453, Revil,

Ragnar, etc. The MITRE attack techniques utilized frequently by these threat actors include OS credential dumping, acquiring web services infrastructure, spear-phishing via services, malicious link execution, compromised software supply chain, inhabit system recovery, archive collected data, etc.

Key Insights

25.6% of the total cyberattacks conducted in 2021 targeted the services sector. Because this sector includes a lot of critical infrastructure, it has been rapidly attracting the threat groups. Almost 62.5% of the cyberattacks targeting the services sector were directed against the telecommunication and technology sub-sector. In June 2021, SAC Wireless, an independently operating subsidiary of the Nokia company, was hit with a Conti ransomware attack. It is suspected that more than 250GB of sensitive data of current and former employees (including details on their health plans' dependents or beneficiaries) was exfiltrated in this attack. Kaseya, an IT solution provider, was attacked by the Russian-based REvil group in July 2021 in a supply-chain attack affecting more than 1500 organizations all over Europe. In August 2021, T-mobile was slammed with a huge-scale data breach by a 21-year-old threat actor. The personal data of 40 million current, former, and prospective customers was compromised in this attack in which the threat actor performed brute-force attacks and gained entry into IT servers that contained customer data.

Apart from the telecommunication and technology sector, the media and entertainment sector (10.8%), education sector (6.9%), and consulting sector (4.9%) are among the most impacted industries in the services sector. In March 2021, a threat group suspected to be from China was found targeting the journalists and activists working for the rights of the Uyghur community. These threat actors leveraged social media platforms by creating fake accounts and sending phishing links to their targets. In another such instance, an APT group named as InkySquid (with alleged origin in North Korea) targeted South Korea media outlets by deploying a malware called Bluelight through browser exploitation. In September 2021, some pro-Russian threat groups targeted 32 prestigious western media outlets in over 16 countries in a misinformation campaign.

Attacks on the education sector were more prominent in 2021. For example, in May, a European biomolecular institute was hit by Ryuk ransomware attacks. It turned out to be a student who was the unwitting conduit of this infection during his hunt for a free version of expensive data visualization software. In July 2021, an Iranian-based threat group termed TA453 (aka APT35, Charming Kitten, and Phosphorous), in an operation named "Operation SpoofedScholars," targeted professors and writers in the UK by posing as British scholars. This group launched phishing campaigns, followed by social engineering to offer legitimacy to their operations. In September 2021, some Israeli universities were targeted by a Middle East-based threat group called Agrius using a new version of Apostle ransomware. There were also multiple attacks on consulting and professional services. Various massive supply-chain attacks (such as the SolarWinds attack and the Accellion breaches) put consulting firms all over the world at great risk of data breaches and operational disruption. Consulting firms such as Morgan Stanley, Bombardier, and Singtel experienced massive losses due to the Accellion FTA supply-chain attacks. And in October 2021, giant IT solution provider and management consulting firm Accenture confirmed being attacked by LockBit ransomware. The threat actors had successfully obtained network access and then gained access to the organization's corporate data.

From these events, it can be concluded that the United States experienced almost 36% of the total attacks targeting the services sector, followed by Australia with 16.25%. Attacks on this sector also highly impacted European countries, South East Asian nations, and some Middle East countries such as Iran and Israel. Almost 83% of the attacks were motivated by financial gain. Vulnerabilities in infrastructure and in well-known applications triggered around 26.6% of the total attacks. 2021 saw a surge in ransomware attacks against the services sector: 32.5% of the total attacks were ransomware, followed by data exfiltration (19.2%), network access (8.9%), and spear-phishing (5%). Telecommunication and technology firms need

to secure their infrastructures by keeping up to date with the latest patches in order to avoid vulnerability exploitation. Educational institutions should train their students and faculty on cybersecurity risks. Users should be acknowledged for using genuine version of applications and avoiding insecure bootleg versions, in order to counter threats. Strong international cooperation and technological advancements are essential for tackling these cyberattacks on civilian targets.

I11 – Industry Impact: Transportation

TRANSPORTATION THREAT LANDSCAPE
GALAXY 2022 OUTLOOK

ACTOR GROUP
A. WIZARD SPIDER
B. PIONEER KITTEN
C. APT28
D. APT35
E. DOPPEL SPIDER
F. SPRITE SPIDER
G. MALLARD SPIDER
H. Muddy Water
I. SPECTRAL KITTEN
J. CHRONO KITTEN
K. APT41

SUB-INDUSTRIES
A. Water transportation
B. Local and suburban transit
C. Railroad

COUNTRIES
A. Canada
B. India
C. United States
D. Malaysia
E. Iran

TACTICS, TECHNIQUES, AND PROCEDURES
A. Brute Force: Password Cracking
B. Modify Registry
C. Network Share Discovery
D. Process Injection
E. Data Encrypted for Impact
F. Data from Local System
G. Domain Generation Algorithms
H. Execution Guardrails: Environmental Keying
I. External Remote Services
J. Exploit Public-Facing Application
K. DLL Search Order Hijacking
L. Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
M. Clear Windows Event Logs
N. Ingress Tool Transfer
O. Spearphishing Attachment
P. SMB/Windows Admin Shares
Q. Obfuscated Files or Information
R. Software Discovery: Security Software Discovery
S. Windows Management Instrumentation

Impact: Informational, Caution, High Risk, Immediate Risk
Likelihood: L1 – Current operations/imminent, L2 – Likely to occur in the next three months, L3 – Probable in the next 12 months, L4 – Unlikely

Figure 28 - Transportation Threat Landscape

Digitization has spread widely across the transportation sector, creating significant efficiencies in developing revenue streams for the companies. However, it has also made them more vulnerable to cyberattacks. In 2021, these attacks caused a heavy impact on transportation sectors in the United States, Canada, India, Malaysia, and Iran. Threat actors who were observed actively performing these attacks include: Wizard Spider, Pioneer Kitten, APT41, APT35, Muddy Water, Spectral kitten, and Doppel Spider.

Victims associated with these attacks belong to the railroad, local and suburban transit, and water transportation industries. The threat actors mainly used vulnerability exploitations, phishing, and brute force attacks to obtain initial access to the systems. MITRE techniques used during the attack process include: Archive via Utility, Modify Registry, Network Share Discovery, Process Injection, Data from Local System, Execution Guardrails, Environmental Keying, DLL Search Order Hijacking, Exfiltration Over Unencrypted/ Obfuscated Non-C2 Protocol, Clear Windows Event Logs, SMB/Windows Admin Shares, Compiled HTML File, Obfuscated Files or Information, Steal or Forge Kerberos Tickets. Kerberoasting and Windows Management Instrumentation.

There were not many recorded cyberattacks on the transportation sector in the past because most of the systems were wire-based networks. However, with digitization, the systems used in vehicles that travel on water, roads, and the air started communicating with mobile networks and wireless networks, which significantly increased the possibility for more compromises.

Key Insights

There are several reasons why the transportation sector is targeted so heavily. For example, threat actors might want to target a particular commodity or affect trade. And because the sector is interdependent on various infrastructures, railways and roads could be targeted to prevent containers from reaching shipping ports, thereby hindering essential exports. In addition, airports could be targeted to disrupt tourism or military deployments.

Among the most impacted organizations in the transportation sector in 2021 were Toronto Transit System, New York Transit Agency, Metropolitan Transportation Authority (MTA), Air India, Malaysia Airlines, Iran's transport ministry and rail network, Swire Pacific, one of Canada's post suppliers, and ATC Transportation and Steamship Authority. Since the transportation industry is still in its early phase of cybersecurity, threat actors are more aggressively targeting companies belonging to this industry. Financial gain seems to be the primary motive behind all these attacks.

Cyberattacks on the transportation sector have significantly increased compared with previous years. Based on the latest cyber intelligence, organizations within transportation sector should prepare for 2022 by assessing the following:

- Specifically, in the transportation industry, cybersecurity awareness is critical. Educating employees on methods such as social engineering and phishing could be vital to preventing the threat actors from gaining initial access into target networks. Often, the threat actors deliver malicious payloads using emails, so providing required training to employees on identifying suspicious activity is essential.
- The transportation sector is adapting more and more IoT solutions, primarily for connectivity between vehicles. This increased connectivity could introduce new vulnerabilities. Moreover, not all IoT solutions have sufficient built-in security, which enables the threat actors to easily leverage them. Insufficient cybersecurity standards invites cybercrime and can increase the likelihood of a successful attack, so companies should be mindful when choosing their vendors and using their IoT solutions.

I12 – Other Industries

Real Estate

With buildings getting smarter through technology designed to make them more efficient, local governments, real estate owners, and developers investing in and implementing the latest building automation systems (BAS) are faced with increased and unique cybersecurity risks. With huge fund transfers happening on a daily basis in real estate, the sector has always been a lucrative target and there has been an increase in ransomware attacks against real estate entities. In September 2021, a Canadian real estate management company, Ronmor Holdings, was the victim of a ransomware attack. The REvil ransomware group took responsibility and claimed that it had downloaded 755GB of private and confidential data from Ronmor's servers. IoT networks embedded in the real estate sector are becoming increasingly vulnerable, due to increased online connectivity, weak security design, and the spread of targeted malware.

Mining

In today's market for manufactured products, there is an increased dependency on the natural resources that are needed for economic development. This has made industries such as mining a target for many cyber groups and attacks. This industry has seen a rise in cyberattacks, due to an increase in their use of

modern technologies such as machine learning, Internet of Things (IoT), and robotics. Although this helps to boost revenue for mining companies, it also adds a new level of complexity to their systems and makes them more vulnerable to cyberattacks. According to a survey, 74% of companies that added operational technology to their systems suffered a breach in the following 12 months. These attacks led to loss of revenue, system downtime, and theft of confidential information. The mining industry's position in global supply chains and the need for countries to use their mineral deposits puts it at risk of cyber espionage. Another threat is 'Hacktivism,' a cyber campaign carried out by environmentally conscious hackers who want to disrupt the activities of any companies that are potential threats to the environment. The demand and rise of prices related to the mining industry are influenced by countries that have a higher amount of natural resources, such as Australia, the United States, China, India, Canada, and Russia. Therefore, they face a larger impact, compared to countries that depend on other countries for natural resources.

In 2021, there were many cyberattacks on the mining industry in various regions, including Russia, Australia, South Africa, the United States, Canada, Europe, and India. The main threat actors involved in these attacks were Wizard Spider and Conti. Among other MITRE techniques, they employed TTPs (tactics, techniques, procedures) such as using stolen credentials to access administrative accounts within the domain, using stolen certificates to sign its malware, using a rootkit to change typical server functionality, gaining unauthorized access to systems, ransomware attacks, phishing, and spear-phishing techniques. .

An example of an attack on the mining industry was when Scottish multinational engineering firm Weir Group (a major supply company in mining and technology) suffered a cyberattack that resulted in shutting down IT systems such as enterprise resource planning (ERP) and engineering applications. The cyberattack caused a disruption in manufacturing, shipment, and engineering, which led to a drop in their revenue of close to 50 million euros.

Utility

As power and water facilities start to move towards more integrated industrial automation, the risks associated with cyberattacks significantly increase. Successful cyberattacks on organizations operating in this space can have dire consequences on a massive scale. For example, should threat actors gain access to operations technology (OT) at a hydro plant and manipulate its operations, this could cause the utility to poison the local water supply and put human lives at risk.

Exploiting remote applications and employee credentials are two of the main attack vectors utilized by the threat actors to obtain initial access to utility networks. Threat actor motives in this sector range from seeking financial gain, to stealing sensitive information (such as machinery details and proprietary documents) to cause destruction. This sector needs to be particularly efficient and effective in prioritizing and understanding the cyber risks associated with their infrastructure. It is important to segregate networks and enable more protection of critical systems.

Agriculture, Forestry, and Fishing

Prior to the widespread use of modern technology in the agriculture, forestry, and fishing sector, they were relatively immune to threat groups because there were no cyber operations to disrupt. However, with the introduction of internet-based industrial control and automation systems, they are now prone to cyber threats and threat actors are taking an interest. Agricultural businesses rely on autonomous tractors, soil sensors, GPS mapping, and drones, as well as other IoT devices. This increase in connectivity with IoT devices introduces new vulnerabilities, since not all IoT solutions have sufficient built-in security, which enables the threat actors to easily leverage and exploit them. Insufficient cybersecurity standards invites cyberthreats, putting many organizations at risk. An FBI report highlighted that a successful ransomware attack might lead to substantial remediation fees, productivity declines, and financial loss. Organizations in this sector could also become victims of intellectual property theft, personally identifiable information (PII) data loss, and incur reputational harm.

Safety

The safety industry comprises several sectors that have a deep impact on public safety, including police services and the judiciary, etc. Cyberattacks in this sector can have adverse impacts on government, citizens, and public safety. Ransomware gangs are increasingly targeting law-enforcing agencies. In April 2021, the Metropolitan Police Department of Washington, DC was targeted by a ransomware group named Babuk. They gained access to very sensitive data related to more than two dozen officers, including social security numbers and psychological assessments. The group stole more than 250GB of data and threatened to leak confidential information unless a ransom was paid. Other ransomware attacks were observed against police departments, which involved taking down 911 systems, blocking officers from checking suspects' criminal histories during traffic stops, and impeding investigations by blocking access to investigative files or videos.

Threat groups haven't spared the judiciary services either. Near the end of 2020, the information technology office that provides IT support to the Texas judicial service was hit by a huge-scale ransomware attack. It forced all of the websites of Texas courts, including the Texas Supreme Court, to remain offline. In May 2021, cyberattacks forced the online server of the Alaska Court System (ACS) to disconnect temporarily. This attack, conducted by malware deployment, resulted in disruption in virtual hearings, online payment of bail, and submitting juror questionnaires, etc. In another incident, various courthouses in Jefferson Parish, Louisiana were slammed by cyberattacks in the wake of Hurricane Ida. As the hurricane knocked out power and internet to most of the courtrooms' computers, the threat actors tried to exploit the vulnerabilities and gain access to the networks. The judiciary department needs to prepare for forthcoming information warfare. It is the responsibility of the judiciary to uphold and protect the significantly sensitive data they possess.

Trade

Cyberattacks on trade can have critical impacts on many other sectors that depend on the global supply chain. This was apparent on several occasions throughout 2021. The global shipping giant Maersk Line (which handles more than 16% of the world's seaborne trade and 25% of the Asia-Europe trade) was hit by ransomware attacks leveraged by a virus called NotPetya. This breach affected the servers of Maersk's parent companies, impacting all of its business units— including container shipping, port and tug-boat operations, oil and gas production, drilling services, and oil tankers. It is estimated that Maersk Line experienced a loss of more than $300 million due to this attack. In May 2021, the world's largest meat producer, JBS SA, was hit by a cyberattack that forced it to shut down all of its beef plants in the United States, wiping out one-fourth of the supply. This generated a chain reaction as trade was blocked, causing the takedown of several subsidiary meat plants of JBS worldwide (mainly in Canada, Australia, and Brazil). This trade disruption caused retailers to increase meat prices, significantly affecting consumers.

Markets

Markets are considered the backbone of the modern-day business economy and serve as a source for investing in economies of business. With the emergence of cryptocurrency, crypto markets are a source of enormous debate. But evolving blockchain technology terms such as blockchain applications and NFTs (non-fungible tokens) have spurred the popularity of cryptocurrencies. Although blockchain is secure in itself, the other third-party applications might still be vulnerable to some attacks, out of which a large portion of the cyberthreat landscape is still unknown. Nevertheless, several crypto markets and exchanges came into the picture in 2021, paving the way for the general public to invest in cryptocurrency. The market sector has observed some attacks in the past, which include exchange hacking and crypto wallet key stealing. These attacks aim to steal data for financial gain and involve transferring a large sum of money to attackers' wallets, making it difficult to trace and recover the money. A majority of these attacks targeted individuals in order to steal keys to access the wallets associated with the account. This is usually done by executing malware to steal and keylogger the user activity to gather passwords and other information needed to access the account. In addition, threat actors were also observed to use malware that replaced the sender's wallet address in the clipboard with the threat actor's address, which ultimately resulted in cryptocurrency being transferred to attackers' addresses. In August 2020, New Zealand's Stock Exchange website was hit with DDoS attacks. This resulted in the market being inactive for at least four days. Then, upon market restoration, the threat actors targeted the individual companies. The prevalence of this type of attack and the resulting market disruption, along with the interconnected nature of the markets, paves the way for significant widespread impact on the markets and the consumers.

CyberResGalaxy.com

About CyberRes

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by building both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

We are a part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today, keep the lights on, and transform to grow and take advantage of tomorrow's opportunities.

To learn more about our solutions, visit us at CyberRes.com

If you have questions or comments about this report, or if you would like to obtain permission to quote or reuse this report, please contact us by emailing:

cyberres.galaxy@microfocus.com