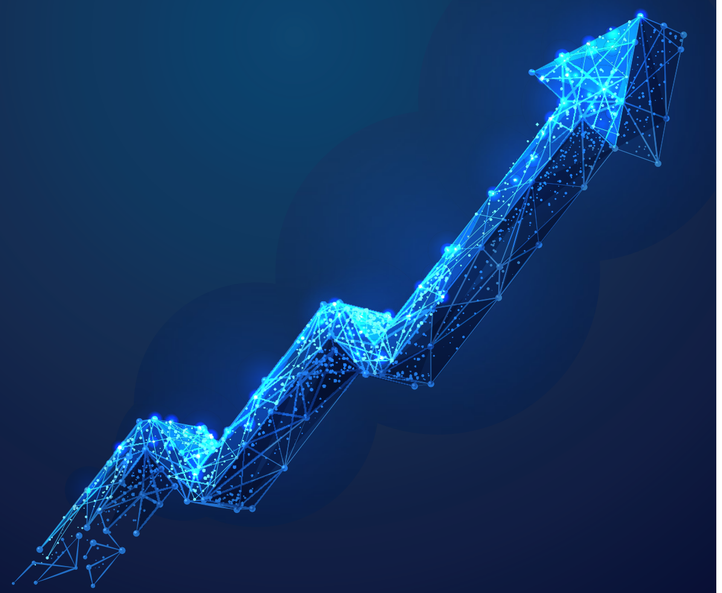

FOX IT
part of nccgroup
nccgroup
NCC Group
Annual Threat Monitor
2021
www.nccgroup.com

Table of Contents

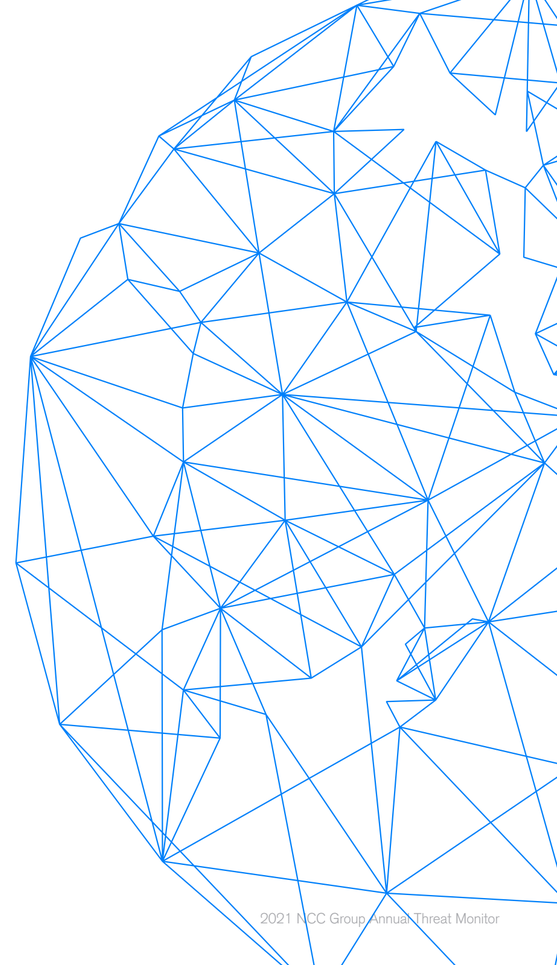


Report context

This report presents the insights of NCC Group's Threat Intelligence team, discussing the events of 2021 and their impact on the cyber threat landscape.

The scope of this report is to provide an overview of incidents across all sectors and highlight trends we have identified from incidents identified by our global managed detection and response service (MDR) and our global cyber incident response team (CIRT).

The aim is to provide strategic level insight into the threat landscape to support decision making and enable organisations to adjust defensive posture against increasingly sophisticated threat actors.



2021 in review

Well, what a year that was! 2021 truly was one of the most intriguing years in information security…

Ransomware

The Ransomware threat landscape has been very dynamic over the last twelve months, and has also been somewhat turbulent for ransomware operators who have to some extent been the victims of their own success.

We have seen new players come to the table, but with incidents including the Colonial Pipeline attack and the Kaseya supply chain attack, the issue of ransomware has been brought to the forefront of international law enforcement and governments, forcing some ransomware operators to hang up their boots.

The overall business model used by groups has also changed during the course of the year. Ransomware operators have moved away from purely extorting victims by making them pay for the decryption key to unlock files on their networks.

The vast majority of groups now employ the 'double extortion' business model, following in the footsteps of the Maze Group, who were doing this as early as 2019.

In these cases, if the victim refuses to pay the initial ransom (to decrypt their files), ransomware operators are now also leaking data that was stolen from the victim on dedicated leak sites.

The aim being to force the victim to pay the demands to have this data removed from being publicly accessible.

NCC Group also observed a small selection of criminal groups skipping the deployment of ransomware altogether and going straight to the leaking of sensitive corporate data.

More recently, we have also observed certain ransomware operators offering for sale 'access' to their victims' environments as well as access to leaked data.

Supply chain

Without too much of a surprise, and hot off the heels of the Solarwinds incident at the end of 2020, once again threat actors showed us that the threat of third party compromises was real, and here to stay.

Once in the cross hairs of sophisticated APT groups, managed service providers and 'aaS' (as a service) vendors, are now just as susceptible to targeting by crime groups seeking to maximise their financial gain from their endeavours.

In July 2021, the IT Management Company Kaseya was breached and a prolific strain of ransomware was deployed across their networks. The attack was ultimately attributed to the REvil crime group.

This event had a wide and far reaching impact on several hundred Managed Services Providers and clients of Kaseya.

Quick to weaponise

There have been several highly critical vulnerabilities disclosed in 2021 in relation to a number of widely used platforms, including Pulse VPN, F5 BigIP, Citrix's Application Delivery Control, NetLogon, and Log4j.

What has been apparent is that threat actors, particularly those affiliated with Nation States and Foreign Intelligence Services, have sought to weaponise these vulnerabilities at pace.

We have confirmed that industry research aligns with what we are seeing in practice – time to exploitation of a vulnerability in the wild after a patch has been released has dropped from several weeks as of a few years ago, to only a few days now.

This presents a challenge for defensive teams as this requires a seriously retooled approach to vulnerability management.

Furthermore, it puts tremendous pressure to patch on key intermediaries in the software supply chain – many of whom are open-source maintainers.

Critical Events Monitor 2021

The timeline highlights major incidents that shaped the global threat landscape during 2021

5 January
Attribution

U.S. accuses Russia of Solarwinds attacks

U.S. intelligence agencies accused Russia of being behind the earlier discovered SolarWinds hack that compromised much of the federal government. The Solarwinds hack can be regarded as on of the most successful publicly known cyber espionage cases.

12 February
Law Enforcement

Egregor Ransomware affiliates arrested

Three members of the Egregor ransomware cartel were apprehended in Ukraine in a crackdown conducted by the French and Ukrainian authorities.

27 January
Law Enforcement

Law enforcement hijacks Emotet botnet

In an international police operation dubbed 'LadyBird' authorities successfully took action against the Emotet botnet by hijacking its core C2 servers. However successful the operation was, the malware became active again at the end of the year.

14 February
Ransomware

CL0P gang using Accellion FTA 0-days

TA505, also known as the CL0P ransomware operation were observed using a chain of zero-day exploits to compromise Accellion FTA appliances and exfiltrate data without spreading ransomware. The victims were extorted by threatening to leak the data on the dark web.

2 March
Vulnerability

Critical Microsoft Exchange Server RCE bug reported

After Microsoft released four critical patches for on-premise Exchange servers widespread exploitation by threat actors was observed. Microsoft also reported that a Chinese State affiliated actor dubbed 'Hafnium' had been exploiting the vulnerability since January.

18 March
APT

SilverFish campaign exposed

The offensive intelligence company Prodaft revealed a Russian actor dubbed 'SilverFish'. According to the report the actor has breached more than 4500 organizations in an espionage campaign. However, the report draws some conclusions about collaboration between different criminal groups and the Russian State that are not verifiable and somewhat dubious.

29 April
Ransomware

BABUK ransomware gang retires after DC Police attack

The BABUK ransomware group called quits and released free decryption keys to its victims. The announcement came shortly after the group had tried to extort the DC Metropolitan Police with ransomware and data theft.

7 May
Ransomware

Colonial pipeline ransomware attack by Darkside group

The Colonial Pipeline hack by affiliates of the DarkSide extortion service resulted in shutdown of oil supplies and fuel shortages in the US. The incident, together with the Kasaya attack can be seen as the biggest escalation in the ransomware threat this year. The attack sparked a response at the highest policy circles and it could be argued that this attack, together with the Kasaya incident sparked the much more offensive stance governments are taking against ransomware actors today.

14 May
Ransomware

CONTI targets Irish hospitals

In a crippling CONTI ransomware attack aimed at the Irish Health Service Executive (HSE), 90 percent of the county's hospitals were shut out of patient records, scheduling systems and emails. The attackers also exfiltrated 700GB of sensitive (patient) data. The negotiation path took an unexpected turn when the extorters released a free decryptor for the ransomware but continued to demand 20 million USD to stop them for publishing the data.

2 July
Ransomware

Kaseya VSA ransomware attack

Leveraging a not public vulnerability in Kasaya VSA REvil ransomware operators were able to encrypt somewhere between 1000 and 1500 organizations in one go. The group demanded 70 million USD for a universal decryptor but went offline after a week into the crisis. Three weeks later the FBI provided a decryptor to Kasaya as it had apparently been inside the REvil infrastructure already for some time.

15 August
Data Leak

T-Mobile hack leads to massive data breach

After a successful hack the personal details of 50 million T-Mobile customers were stolen. A 21 old year man later claimed responsibility for the attack and said that he carried out the hack for attention and to show the poor security at T-Mobile.

29 September
Nation State

Russia arrests Group-IB CEO on suspicion of treason

Ilya Sachkov, a co-founder of the prominent Russian cybersecurity company, was arrested by Russian officials on the suspicion of treason. According to reports the arrests could have a link to Group-IB's increased efforts to expand to western countries and the possibility of the organization cooperating with western government organizations.

30 October
Nation State

Iran hit by sweeping cyber-attack taking down gas stations across country

In what is believed to be a continuation of the lasting Israeli – Iranian conflict, a cyber attack was carried out against the Irian petrol supply. Leaving gas stations inoperable. Whilst the crisis went on matrix boards on highways said: Khamenei! Where is our gas?

9 December
Vulnerability

Critical 'Log4Shell' vulnerability published

Apache released a patch for a critical bug that allowed RCE by sending a specific string to an application running Log4j, a Java-based logging library. The vulnerability was quickly designated as one of the worst vulnerabilities ever published as millions of applications use the library and administrators often don't even know. Mass scanning and widespread exploitation attempts were quickly observed because of the triviality of the exploit. However, the vulnerability did not (yet) lead to the 'internet meltdown that was expected.

5 August
Ransomware

Conti gang's technical manuals

After a supposed disagreement about payment a disgruntled Conti 'pentester' leaked internal training materials used by the Conti operation on a forum on the dark web. The detailed walkthroughs described how the Conti operators are taught to compromise enterprise networks without much in-depth technical skill.

13 September
Hack-for-Hire

Apple patches an NSO zero-day flaw affecting all devices

After a report by Citizen Lab Apple patched an iMessage zero day that was used by NSO group for the proliferation of their infamous Pegasus spyware. Over the year the organization faced a lot of backlash and legal action because of their spyware being discovered to have infected numerous journalist, politicians and human rights activists.

21 October
Ransomware

REvil ransomware operation disrupted

A disruptive operation spearheaded by numerous US Agencies including Cyber Command led to what seems to be the definite takedown of the REvil Ransomware operation. A REvil spokesperson posted on a forum: "The server was compromised, and they were looking for me. Good luck, everyone; I'm off."

15 November
Malware

Emotet comes back to life

After a nearly yearlong absence after a takedown in January the Emotet initial access malware came back to life. The malware was observed being dropped by TrickBot but was later also observed in separate malspam campaigns.

11 December
Nation State

Russia blocks Tor service

Russia has increased censorship efforts in the country by fully blocking access to the Tor web network, coinciding with the ban of six virtual private network (VPN) operators, as the government continues its efforts to control the internet and crack down on attempts to circumvent locally imposed web restrictions.

Incidents of note in 2021

Ransomware: Colonial Pipeline

On May 7 2021, DarkSide ransomware affiliates successfully targeted Colonial Pipeline's digital infrastructure, resulting in the disruption of operations and fuel shortages. Responsible for roughly 45% of the fuel delivered to the US East Coast, this event marked the largest, publicly disclosed attack against US critical infrastructure, and evoked the real-world consequences of a successful cyberattack.

The exfiltration of 100 gigabytes of data prior to infecting the IT network with ransomware and demanding a payment of 75 bitcoins, roughly $4.4M in ransom fees, prompted the shutdown of company infrastructure.

Colonial Pipeline paid the fee for the decryption key to resume operations, however, collaboration with law enforcement saw the successful trace of the payment and identification of the digital wallet used, allowing for the recovery of 64 bitcoins.

Critically, the threat actor's use of double extortion tactics to cripple the company's IT network is highly characteristic of the current threat landscape and indicative of a growing trend in multi-level extortion schemes of which we must remain vigilant. Additionally, the DarkSide Ransomware-as-a-service (RaaS) model underscores the threats posed by an increasing accessibility to ransomware by diverse threat actors.

As such, this opens the door to a plethora of victimisation opportunities, even recognised by DarkSide themselves where announcing the need to 'vet' the targets of their affiliates following the Colonial Pipelines attack, thus emphasising the risk.

Finally, this highly public targeting of critical infrastructure raises concerns as to whether this will serve as a precursor to potential future attacks pursuing vital industries, and thus one to watch.

NSO Group exploit Apple zero-day

First identified in August, a significant zero-day vulnerability (CVE-2021-30860) exploiting a flaw in Apples iMessage silently hacked devices, dodging Apple's 'BlastDoor' protections whose purpose is to filter malicious code.

Dubbed FORCEDENTRY for its intrusive manner, this mode of access was attributed to the Israeli NSO GROUP to push their Pegasus spyware, providing government customers with unauthorised access to the devices of human rights activists. The breach proved highly significant for its capacity to circumvent both BlastDoor's capabilities.

In September, Citizen's Lab revealed new artefacts pertaining to the recently discovered CVE-2021-30860.

Specifically, the analysis of a Saudi activist's iPhone suspected to have been hacked by Pegasus software, showed the exploit to also abuse a weakness in how Apple devices render images on the display. 27 copies of an identical file with the '.gif' extension in reality concerned a 748-byte Adobe PSD file that caused an IMTranscoderAgent crash on the device, and loaded four PDFs containing a JBIG2-encoded stream.

Citizens Lab has attributed the exploit to the NSO Group with high confidence.

Whilst Apple has released several security updates to patch the NSO zero-day flaw to further address the features of the FORCEDENTRY exploit chain, the targeting of Apple devices has illustrated the potential for vulnerabilities in even the latest iOS software.

With Pegasus providing near-complete access to a targets personal data, photos, messages and location, its continued use as a tool for future surveillance, certainly by authoritarian states, is likely.

The ability to facilitate unsolicited nation-state surveillance raises major concerns for human and digital rights, emphasising the need for robust security measures and a continued awareness of such threats to ensure a secure-by-design approach in software development.

Incidents of note in 2021 continued

Vulnerability: Log4shell

We could write an entire report about what came to light on December 9 2021, when a new zero-day vulnerability in the Apache Log4j Java-based logging library captivated the information security ecosystem.

This popular open-source tool used globally in enterprise and cloud-software makes it potentially the most severe computer vulnerability in years, critically impacting any software that incorporates Java.

Specifically, it is the Java Naming and Directory Interface (JNDI) which has the ability to 'look up' resources allows for malicious string input, performing a request to the attacker-controlled site.

First tracked as CVE-2021-44228, with a CVSS score of 10, its exploitation has opened the door to a myriad of threats, including sensitive data exfiltration, ransomware attacks and cryptomining. Since its discovery, threat actors have actively scanned the Internet for vulnerable instances of Log4jShell, leveraging the vulnerability to install malware such as, Cobalt Strike, botnets and backdoors.

The Russian-based Conti ransomware group weaponised Log4j2 with a full attack chain, while APT Aquatic Panda sought to steal intelligence and military secrets from academic institutions. Crucially, the attack vector presents ample potential for novel vulnerabilities to surface and widespread exploitation by cybercriminals and nation states alike, and here in lies the danger.

As it's more recent vulnerabilities have shown use (CVE 2021-45046 and CVE-2021-44832) there is a constant push by Apache to release further updates, and as such, the possibility for future exploits leveraging Log4j remains a very real threat.

> "It was on the evening of Log4J being released to the world and started with a Monero miner being downloaded to a server of the customer. Almost an hour later one of our ML rules triggered on a suspicious file download from a rare host resolving to an IP in Russia. The file in question was a script to install a backdoor and disable the system firewall (ufw)"
>
> **SOC Analyst**

Takedowns and Arrests in Ransomware

2021 was also a year of widespread global collaboration and cross-industry effort to mitigate the ransomware threat. In February, French and Ukrainian authorities headed a joint investigation culminating in the arrest of three Egregor affiliates, the seizure of their infrastructure and assets.

While the prominence of those arrested and thus the potential for long-lasting disruption to this RaaS model was questioned, the observed inactivity of the extortion site and C2 infrastructure thus far appears to support its success. Yet, like any group, absence may reflect a hiatus; there is always the possibility of a re-emergence under a new identity.

Additionally, a multi-government operation spearheaded by the U.S disrupted REvil, removing online infrastructure and arresting several members.

Judicial efforts to prosecute the RaaS group responsible for paralysing numerous global systems accelerated following Kaseya, placing it 'top of the list'. One internal response to the crackdown read, 'the server was compromised, and they were looking for me. Good luck, everyone; I'm off', hinting perhaps to its more permanent removal and persistent crackdown by law enforcement to come, as exemplified by further arrests in January 2022.

Likewise, counter-measures were echoed in government, with policy seeking to adopt a more proactive stance. Malicious campaigns of the likes of Kaseya and Colonial Pipeline catalysed government efforts to strengthen cyber security measures and assign state-responsibility, with the Biden-Administration's Executive Order as a core example.

The ransomware threat landscape will continue to demand a collaborative effort, invoking the expertise and know-how of diverse sectors. It is therefore important to recognise this year's co-operative efforts in their continued clampdown and reinvigorated bid to quash ransomware. However, all the more important to continue to push for anticipated zero-trust architectures and a whole-of-society approach to remain on the heels of the threat.

NCC Group Security Operations Centre (SOC) Findings

This section of the report focuses on the data gathered from our SOCs based in Europe and Asia-Pacific regions.

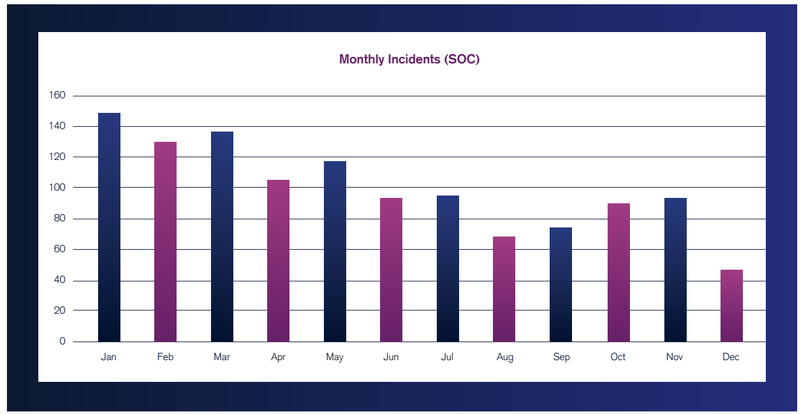
Monthly Incidents

We collected data from over a thousand incidents detected by our global network of SOCs this year.

Incident distribution across the 12-month period reveals a gradual decline within the year in attacks targeting NCC Group customers, however no dramatic developments are noted in the data.

The periods of June, July, August and December present the lowest number of incidents and may be the result of seasonal fluctuations in cybercrime activity, i.e criminals and targets on holiday.

Equally however, this is not definitive and other confounding variables are likely to influence pattern change and should be taken into consideration.



Sectors

When analysing incidents targeting our client base according to sector, the data suggests that the top sector to be targeted was academic & educational services (21.56%).

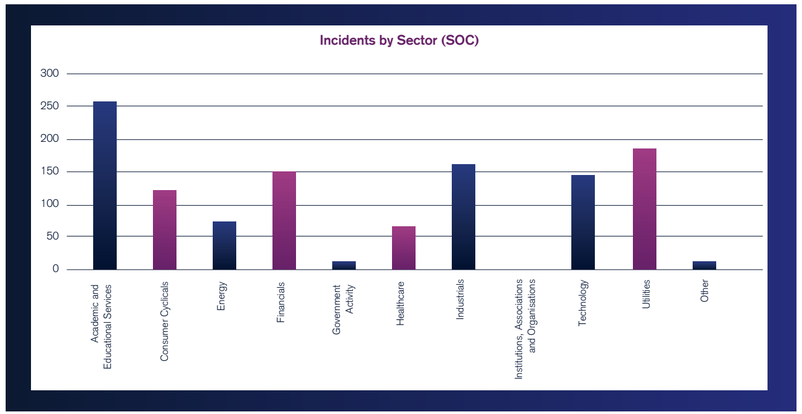
In total, 252 incidents were reported across schools, colleges & universities, with over half targeting universities (66.26%).

This significant number of incidents is in line with the general growth of malicious activity we have seen, following a shift by educational organisations to digitalise their offerings, and the drive in 2021 for such institutions to research COVID-19. These factors have made organisations in this sector particularly valuable targets.

This is most likely a trend we will continue to see as the world battles the pandemic and cybercriminals seek to exploit it.

Further comparisons revealed some interesting patterns. Notably, attacks in the academic sector saw spikes in May and November, contrasting their usual uptake in the September- October period.

These observations help us to understand when attacks may occur within these specific sectors, and help to support prevention efforts by increasing awareness around attack periods.



Within the SOC, and outside of it, it seems that universities and other educational institutions are being targeted more often.

This can be noticed in the SOC with a few FIR/CIRT cases that have developed out of successful exploitation at such institutions.

NCC Group Incident Response Findings

NCC Group's global Cyber Incident Response Teams (CIRTs) responded to the largest number of incidents in the public (19.35%) and industrial sectors (19.35%) in 2021, followed by consumer cyclicals (16.13%).

Within the public sector, the government and education industries were notably targeted. The former experienced several ransomware attacks, although not unusual as our ransomware leak data has identified that ransomware has represented a particular threat to the industry, with a prominent spike towards the end of the year (November).

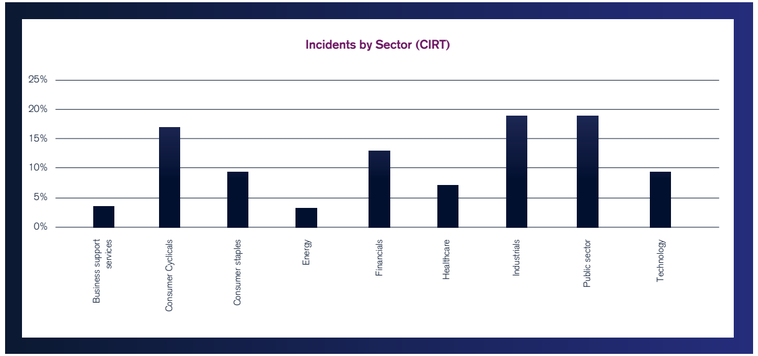
Additionally, attacks in the education industry echo the SOC findings with respect to their being high-value targets. Their prevalence across the incidents recorded underscores the importance for heightened prevention efforts within.

The types of industries within consumer cyclicals were varied and mirrored by diverse attacks types, including ransomware, DDoS and data breaches.

Finally, machinery, construction and engineering were most targeted in the industrial sector.

The sector's critical role in supporting the functioning of vital products and services signifies that any breach or hiatus in production could result in a damaging domino effect. Organisations that are susceptible to down-time will always be firmly in the crosshairs of financially motivated threat groups.

Among the attack types, ransomware prevails, accounting for 65.38% of incidents dealt with by our CIRT teams in 2021. These incidents included some of the more prolific ransomware variants, including Conti, REvil and PYSA.



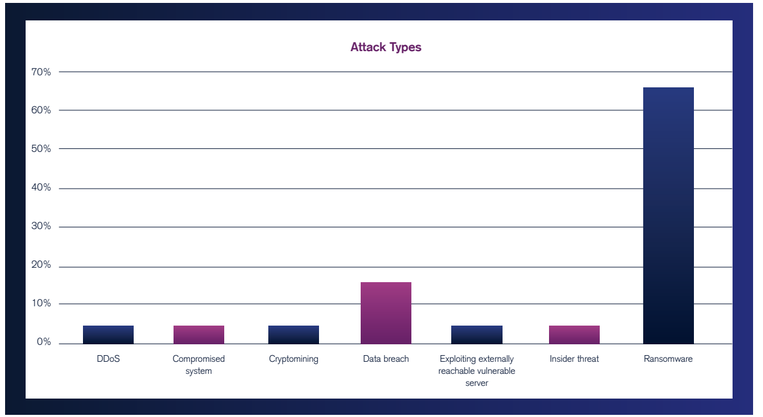
Additionally, a cross analysis of crime types and sectors, identified ransomware to be most prominent in the industrials, public, technology, and consumer cyclicals sectors.

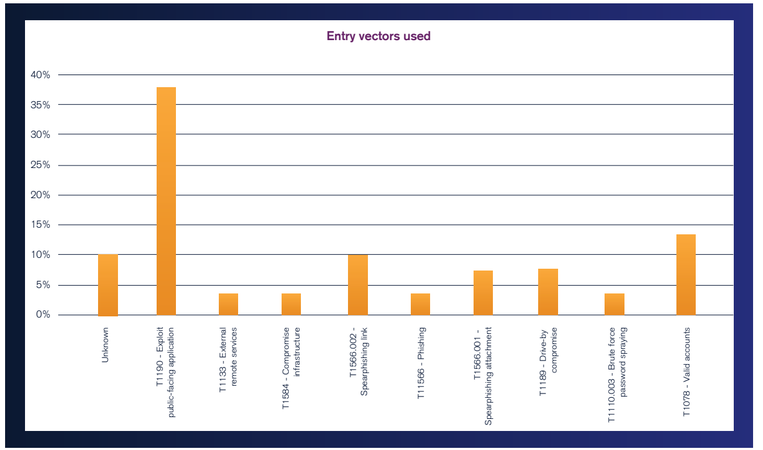
The highest number of targets were identified in the industrials sector and echoes a pattern identified in our analysis of ransomware leak data throughout the year, in which this sector has remained the most targeted.

Finally, the data showed that exploiting a public facing application provided the most popular entry vector for cybercriminals (37.93%).

Notably, the data suggests that a higher number of off-the-shelf tools were used to target public facing applications, and therefore supports the wider trend that an increasing number of hackers are 'living off the land', rather than creating their own toolsets.

This offers important consideration for prevention, such as secure-by-design opportunities to prevent malicious use, certainly as further analysis reveals that off-the-shelf tools were most employed when conducting ransomware attacks, the most prominent attack type in the data.





Threat Landscape: Ransomware

We are continuing to track ransomware groups operating the hack and leak double extortion tactic, this is achieved by actively monitoring the leak sites used by each ransomware group and scraping victim details as they are released.

For this annual report we have collated all the data that we have gathered across the whole year to provide some insights into ransomware trends across 2021 and have, where possible, contrasted it with data from 2020.

When we cross-reference the data from 2020 and 2021, we can see a general upward trend throughout both years, although 2020's increase was much more significant between January and September.

From June – July in 2020 and 2021, we saw a decrease in the number of victims. Again, the drop in 2020 was more significant at 63%, with a 31% drop over the same period in 2021.

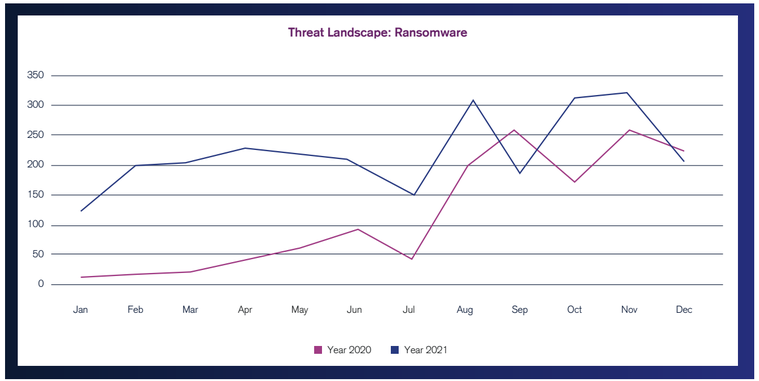


Figure 1: Number of Ransomware Victims by Month – 2020 & 2021

It will be interesting to see whether a similar drop will be seen in 2022, and whether this is in fact a seasonal trend which could be attributed to the fact that organisations will have a period of inactivity due to summer holidays, or that the crime groups themselves have some down-time in the summer.

Following this minor dip in activity, the data suggests a further concerted effort by ransomware operators in the run up to December. From July to August the victims increased by 167 in 2020, and 155 in 2021, again showing the mirrored pattern between the two.

Additionally, these were the largest percentage surges in activity from a month-to-month basis (a massive 477.2% for 2020 and a 103.3% increase for 2021).

Further adding validity to the observation that these fluctuations were caused by holidays.

From here there is less consistency between the two years, though they do both exhibit a drop-off in the winter holiday period.

Based on the assumption that 2022 will follow the same patterns seen in 2020 and 2021, we can make educated predictions, primarily that there will be a steady volume of victims who have data leaked until July where they will drop off, and then surge back in August with many threat actors once again postponing their activity for the Christmas period.

With the lowest quantity of reported ransomware attacks being in January 2020 (two months before WHO declared the Covid-19 virus outbreak to be a pandemic) with just 9 recorded ransomware victims and the most being in November of 2021 with 318 victims. Interestingly, as the cases of national lockdowns rose, the increasing frequency of hack and leak ransomware attacks coincided. This highlights the reinvigorated motivation that threat actors exhibited following national lockdowns; more remote workers, weaker security and likely more money to be made.

Approximately half of the world's population was in lockdown by May 2020. In our data we can see that from May to June of 2020 there was an 86.3% increase in ransomware victims, suggesting that ransomware groups began reacting accordingly to this influx of remote workers and this trend continued to progress through to end of 2021. We propose that the coronavirus pandemic may have caused a permanent shift in the quantity of ransomware cases that we will see in the future, as displayed by the telling 93% increase in ransomware attacks when comparing 2020 and 2021. We will continue to look out for the development of this trend in 2022.

In our monthly threat pulses, we provide detailed insights into these ransomware stats; most prevalent threat actors, most targeted sectors and industries, as well as the most targeted regions and countries.

As we developed and formalised our process in July 2021, we don't have all these stats for comparison but can still extrapolate threat actor trends from the data.

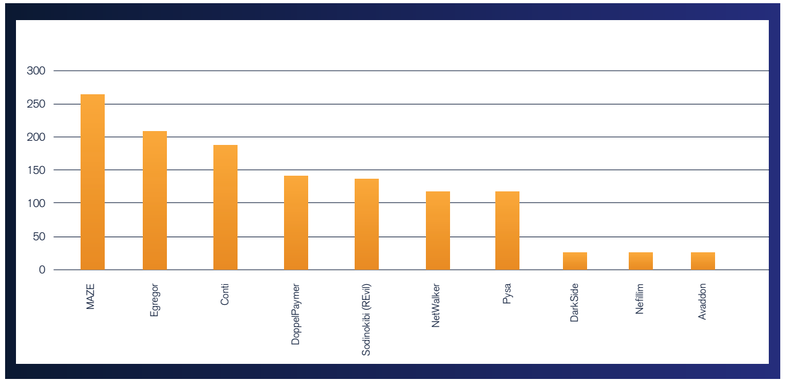


Figure 2 - No of hack & leak ransomware victims by ransomware group 2020

Figure 3 - No of hack & leak ransomware victims by ransomware group 2021

Ransomware operators

Conti has continued to be one of the most prevalent threat actors throughout both 2020 and 2021, representing 18% of all attacks in the two years. Interestingly, after Lockbit's brief hiatus and metamorphosis into Lockbit 2.0 in June 2021, we can see that they went from being absent from our 2020 top 10, to being one of the biggest contributors to double extortion ransomware in 2021 in which they accounted for 16.3% of the entire year's ransomware cases.

We can see that, following their dominant presence and eventual announced discontinuation at the end of 2020, MAZE ransomware was not present at all in our 2021 data showing that they stayed true to their word. There have been no reports of them re-establishing their crime operations under a different alias as of yet, but due to the constant influx of new players in the ransomware threat landscape it is impossible to say for sure.

Another once rampant but now absent ransomware gang is Egregor, that has also been reported to have gone underground, with our last sighting of them being on the 30th of December 2020.

We have seen significant dips in DoppelPaymer cases year on year of almost 46%. This decrease is likely caused by their rebranding into Grief ransomware which, as we can see, has now surpassed DoppelPaymers figure for 2021. Our last sighting of them was on the 6 May 2021, which was quickly followed by Grief's first appearance on the 31 May, of which we have seen constant activity through to December. Due to this pattern, links to DoppelPaymer's ransom portal in ransom notes, and coding similarities between the two, we can deduce that DoppelPaymer has not disappeared but has in fact evolved. Although Grief has been maintaining a low (albeit constant) profile throughout 2021, 2022 will likely bring an increased quantity of victims from them as they will have the whole year to tally up successful compromises.

Although REvil's victim volume has remained largely consistent from 2020-2021 (3.6% increase), our last sighting of them was on the 14 October 2021 and we haven't seen anything since, which interestingly aligns with a multi-country takedown operation wherein REvil's servers were brought offline (following intensified efforts catalysed by the Kaseya VSA supply chain attack).

After this supply chain compromise, NCC Group reported to our clients that Kaseya had eventually managed to decrypt all of the affected victims, to which we suggested that Kaseya may have paid the ransom. However, it has come to light in a Reuters article on the 21 October that the FBI infiltrated some of REvil's servers and obtained a universal decryption key for all the Kaseya VSA victims. However, before awarding the key to the affected victims, they withheld it for weeks in an effort to further track REvil staff movements, which resulted in the eventual takedown of their systems.

How have ransomware TTP's changed this year?

"Encryption of ESXI servers which includes encryption of the virtual disks/hypervisor level.

Deployment of legitimate remote access tools which they fall back on when other access is cut."

Incident Responder

The remaining ransomware groups contributed significantly to the increase in victims this year with PYSA, DarkSide and Avaddon increasing their recorded attacks by 90%, 216% and 619% respectively. PYSA's notable but comparatively smaller increase in activity can be attributed to a rise in the aggressiveness of their campaigns.

Darkside and Avaddon however, first arrived later on in the year of 2020 (August and June respectively) which has likely contributed to their explosive increase in numbers in 2021.

Due to 2020 only accounting for a fraction of their operational uptime, we can expect their 2022 to yield similar volumes of attacks to that of 2021, if not more.

Targeted regions

As we currently only have granular statistics for July onwards, the following sections will be analyses of data from the last two quarters of 2021. Remaining consistent with our monthly threat pulses, the most targeted regions during 2021 were North America and Europe, accounting for 50% and 30% of all attacks respectively.

These regions are densely populated with wealthy organisations which provides an incentive to threat actors that employ a big-game-hunting methodology, resulting in concentrated ransomware activity in these areas. This trend will likely continue throughout 2022 and beyond.

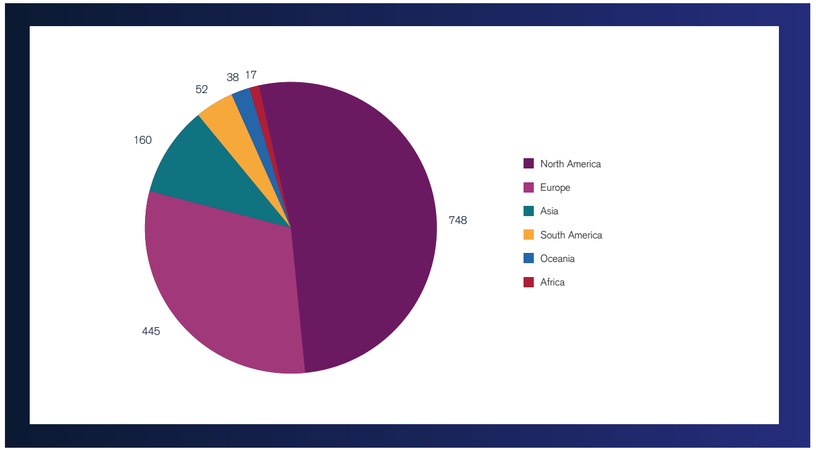


Figure 4 - No. of Victims by Region

Targeted sectors and industries

Following previously documented trends, in 2021 Industrials, Consumer Cyclicals and Technology were the most targeted sectors. Industrials greatly surpasses any other sector in terms of the total attacks that occurred within the sector, representing a titanic 35.5% of our hack & leak data.

As professional & commercial services fall under the industrials sector, it is no surprise that this is the most targeted industry also.This sizeable industry encompasses organisations such as law firms, outsourcing and staffing services, and various consultancies, meaning that it contains wealthy and thus enticing targets for ransomware gangs.

NCC Group has seen numerous instances of law firms being targeted in this sector, likely due to the sensitive data and PII that they store, making them ideal targets for GDPR-centric extortion.

The most targeted industry in consumer cyclicals was Food & Tobacco with 73 victims, which includes corporations involved in fishing, farming and food processing.

Finally, Software & IT Services is the most targeted industry in Technology with 86 total victims. There has been an accelerating trend that NCC Group has observed gaining traction throughout the latter half of 2021 that can be extremely damaging to the victim and profitable to the attacker.

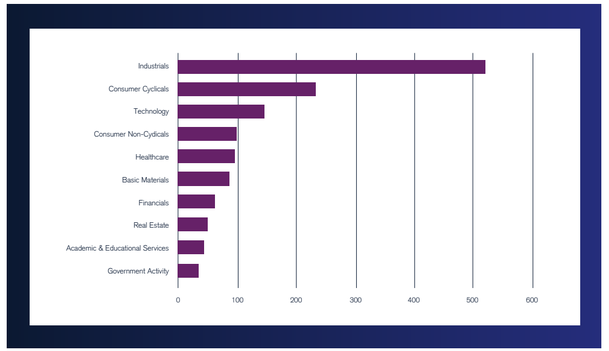


Figure 5 - Number of victims by Sector

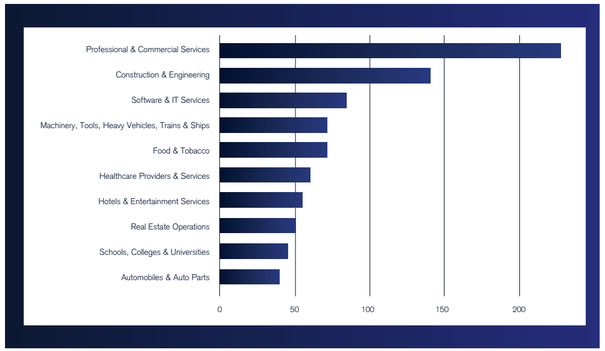


Figure 6 - Number of victims by Industry

Supply chain compromises

With widely publicised examples such as the Microsoft Exchange exploits, Kaseya VSA and Accellion, evidently ransomware gangs have discovered the money to be made from this mode of operation. We expect this trend to continue through to 2022 and, though it may appear that we have reached a plateau in the frequency of these attacks, this may continue to increase throughout 2022 as the quantity of threat actors seeking out these opportunities increase also.

Law enforcement interventions

2021 saw some of the most coordinated activities by governments and law enforcement entities to date. Here, we look at some of the key operations that focused on disrupting the activities, infrastructure, tooling, and monetisation channels of various threat groups over the year.

International cooperation

This year transnational cooperation remained pivotal to prevention efforts. 2021 kick-started with the shutdown of the notorious EMOTET botnet, the result of successful collaboration between international law enforcement and judicial authorities. EUROPOL announced that 'Operation Ladybird' was a joint effort between EU countries and the US. The hijacking of several hundred global servers allowed for the control of the infrastructure and depletion from its epicentre. Whilst its emergence in late December illustrates the ever-present challenge that is defeating threat actors, collective international pressure demonstrates an all-important coherent response prevention demands.

Heat on REvil

It is worth further exploring the prominence of the REvil arrests mentioned above. This major operation was particularly representative of US pressure against Ransomware given its continued targeting by REvil. Not only for the attack on Kaseya, but Apple suppliers, the major meat processor JBS, Travelex and Acer. The US Treasury's Financial Crimes Enforcement Network went as far as to label them the biggest ransomware group in terms of reported payouts.

This operation challenged Russia's ability to crackdown on ransomware on its own soil, and as such, remains a political provocation in the height of US-Russian tensions from which we can continue to geopolitical ramifications.

Netwalker Arrests

In January of 2021, the U.S Department of Justice arrested a member of the NetWalker ransomware gang (Sebastien Vachon-Desjardins), seized almost half a million dollars in cryptocurrency and disabled the dark web resource that NetWalker used to communicate with ransomware victims. This incident, alongside the other law enforcement interventions in 2021, illustrates the collective efforts of governments and law enforcement globally to approach cyber-crime proactively as opposed to reactively. This increased frequency of cyber-crime related arrests in 2021 could potentially lead to another year of ransomware crackdowns in 2022 with greater intensity.

Vulnerability landscape

Exploiting vulnerabilities are a proven point of entry for threat actors. In this section we highlight critical vulnerabilities that have been published during 2021, and enable readers to gain insights into the dynamics of the vulnerability landscape.

The shift to hybrid and fully remote-working business structures has continued into 2021, with increasing numbers of employers offering this mode of working (48% of employees work from home now compared to 30% before the pandemic). This new way of working has caused an increased dependence upon cloud services for day-to-day tasks and data storage, and with this change in direction, critical vulnerability exploitations for cloud appliances have been rising in frequency throughout 2021. We expect to see this trend continue into 2022, as threat actors actively search for critical zero-days in cloud appliances to target service providers, and thus infiltrate a myriad of organisations with one attack vector in a form of supply chain compromise.

In fact, one of the farthest-reaching ransomware attacks, in terms of victim volume, was the Kaseya VSA supply chain compromise in which a critical vulnerability present in cloud software was leveraged to facilitate the attack. This instance, which will be analysed in further detail below, highlights the devastating threat that cloud vulnerabilities present.

As a result of this, it has become essential for organisations to employ a zero-trust mindset and practice scrutiny when employing third parties, especially those that offer cloud services.

During 2021, around 20,138 vulnerabilities have been identified and assigned CVE numbers by various vendors and researchers.

Overall, this is an increase of approximately 10% compared to 2020. The number of vulnerabilities in various versions of Windows operating systems increased by 30% - from 580 to 748.

Similarly to 2020, the proportion of vulnerabilities rated as critical is an average of 14% as shown below.

Figure 7 – Percentage critical CVE's disclosed per quarter

Supply chain vulnerabilities

Kaseya

Analysis of vulnerabilities in 2021 points to an intelligent selection of specific software by attackers as they sought to exploit the supply chain attack vector, providing them with a foothold into a plethora of organisations.

The Kaseya supply chain compromise by REvil specifically targeted its VSA product, a program used by Managed Service Providers (MSPs) to remotely monitor and administer IT services to its customers. The ransomware gang exploited the zero-day vulnerability CVE-2021-30116 to deliver the payload, a trojanised VSA update masquerading as legitimate software. Specifically, its successful deployment and execution permitted hackers root access and administrator rights within the systems of the MSPs, and subsequently their customers.

Perhaps what is most impressive with regards to this attack is that whilst MSPs saw their on-premises VSA servers targeted, the management of client environments from these servers led to thousands of organisations becoming victims of REvil ransomware.

Critically, this demonstrates how an attack on a single company's software can instigate a destructive ripple effect across multiple organisations, serving as an initial access into numerous victim networks.

Microsoft Exchange

In a similar vein, this year's attack on Microsoft Exchange Servers provided an entry vector into numerous organisations. As one of the most severe cyberattacks to occur this year, it saw the exploitation of multiple zero-day vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) by nation-state actors and cybercriminals alike.

In essence, the vulnerabilities formed a detrimental attack chain to facilitate remote code execution (RCE), opening the door to diverse threats such as, data theft, backdoors and further malware distribution. Collectively referred to as ProxyLogon, the vulnerabilities specifically impacted on-premises Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019, whose functions provide organisations access to every-day resources; email, calendar and collaboration solutions.

Over 30,000 organisations in the US alone were impacted, increasing to almost double this number by the end of the year, emphasising the wide-spread and highly invasive nature of the attacks.

Notably, responsibility was assigned to Chinese state-sponsored group Hafnium by the United States and several allies, underscoring the threat of espionage and re-enforcing the need for international pressure where denouncing and countering nation-state activity.

Crucially however, the targeting of unpatched systems was widespread amongst malicious actors, stressing the speed with which the attacker community exploit novel vulnerabilities and consequently, organisations are victimised.

Once again, vulnerabilities in major software used by, and vital to, countless organisations, continue to prove a highly effective entry vector. This allows attackers to target initial victims and set themselves up for the higher value targets.

Ultimately, if we are to remain one step ahead of the threat actors, this will demand a joint effort; rigorous analysis of security systems by third-party services and organisations alike.

Chaining vulnerabilities

As touched upon earlier in this report, the Log4J bug alone has generated ripples throughout the cyber security community and has now been used in conjunction with a SolarWinds Serv-U vulnerability to facilitate attempted Log4J attacks on LDAP servers.

As the Serv-U vulnerability allowed unchecked inputs to traverse the network to LDAP servers, threat actors leveraged this in an attempt to propagate the Log4Shell exploit to them but, as Windows Domain Controllers aren't vulnerable to the Log4J exploits, the attacks failed.

Irrespective of this failed attempt, this example highlights the adaptability of threat actors to combine the exploitation of multiple vulnerabilities to compromise and take over victim systems.

This further demonstrates the fact that threat actors will often pursue vulnerabilities in the supply chain to have access to a greater population of victim systems. Although LDAP servers are not vulnerable to log4j, this same attack vector has been used previously in the deployment of Conti ransomware and, as a result, the vulnerability has been patched by SolarWinds.

Going forward we can expect to see additional implementations of the log4j bug, combined with new vulnerabilities in the supply chain in attempts to expand the attack surface.

Threat Searchlight: Chronicle of Lazarus

Over the past 12 months, NCC Group's RIFT (Research & Intelligence Fusion Team) team have tracked and responded to multiple attacks that have been attributed to the North Korean adversary known as the Lazarus Group.

These campaigns were spread over multiple sectors, and all had different goals and motivations.

Military & Aerospace

In 2021, NCC Group's Incident Response team responded to an incident that consisted of a limited compromise targeting a government contractor.

During this campaign, they were able to observe the Lazarus group's signature move: *Fake job vacancies through LinkedIn social engineering.*

By engaging in a conversation with the employee and gaining its trust by sharing non-malicious documents, the Lazarus group was able to infect the unsuspecting employee.

During this incident, NCC Group's RIFT was able to identify & monitor multiple attacker managed domains and servers that were used during this campaign; abusing organisation names such as BAE Systems, Airbus, General Motors and Rheinmetall.

Even though the Lazarus group was able to infect and compromise the employee's laptop, the incident was quite limited. The targeted organisation was able to limit the adversary's ability of lateral moving through by implementing network segmentation. Besides the network segmentation, the targeted organisation also used different workstations to separate confidential and non-confidential information & activities.

Pharmaceuticals & Cybersecurity Researchers

In the last month of 2020 and the first quarter of 2021, a subunit of Lazarus group showed their interest in pharmaceuticals. During these campaigns, the Lazarus group used a backdoor that is known as ThreatNeedle or Klackring.

This backdoor has been actively distributed throughout 2020 but made its debut in 2021 in the attack against cybersecurity researchers.

By using backdoored version of IDA Pro, security blogposts rigged with a 0-day or social engineering through Twitter, Lazarus tried to infected systems of researchers.

While researching these campaigns, NCC Group's RIFT was able to observe multiple successful infections and a unique insight into the Lazarus group's infrastructure management.

Although it is commonly known that attackers use proxies to hide their command-and-control server to control the infections, the Lazarus group used an extensive list of compromised websites and self-managed servers.

These servers were actively reused for multiple different campaigns up until November 2021.

Investments, Stock trading, Blockchain and NFT's

Throughout the year of 2021, NCC Group CIRT and RIFT also observed the Lazarus group targeting financial organisations with a backdoor that showed identical features with a backdoor used in the attack against Sony.

While tracking this campaign, NCC Group's RIFT was able to identify multiple victims in Australia, China, India, Netherlands, Russia, the United Kingdom and the United States of America. Most of these victims were operational in stock/fast trading, capital investments, blockchain auditing and Non-Fungible Tokens (NFT's).

By using a diverse set of tooling, targeting both Windows, Linux and OSx operating systems, the Lazarus group's main goal seems to be to gain long and persistent access. This persistent access is paired with different backdoors, keyloggers, credential dumpers and log wipers.

Report guidance and points to note

The data and charts contained within this report represent NCC Group's own dataset collected from across our Security Operations Centres and our Global Cyber Incident Response Team's findings.

The data should be considered a sample, including factors potentially skewing the analysis: we do not analyse every malware sample on the threat landscape, merely those assessed to represent a cross-section from a variety of sources.

Our sources may be skewed towards certain types, families or regions which can introduce further bias. The report documents the dataset over a fixed period of time allowing for comparative analysis, whereas when referring to previous datasets a discrepancy with previous reports may seemingly occur due to inclusion of the updated dataset that may contain recent data impacting the statistical outcome.

Furthermore, the lists of data we use to identify targets for attacks can also be biased because they will naturally contain more data pertaining to NCC Group customers than organizations not part of the MDR community.

Although we augment customer supplied data (such as URLs for online banking and BINs) with autonomously collected data, the customer supplied data will always be more detailed and extensive. In short, these charts provide indications, and should be incorporated by interested parties as such. Customers are advised to incorporate and correlate multiple feeds with internal network telemetry.

Copyright © 2022 NCC Group

All rights reserved. No part of this document shall be reproduced, stored in a retrieval system or transmitted by any means without written permission from NCC Group.