BlackBerry | Cybersecurity

GLOBAL THREAT INTELLIGENCE REPORT

ACTIONABLE AND CONTEXTUALIZED INTELLIGENCE TO INCREASE YOUR CYBER RESILIENCE

2023 AUGUST EDITION

Reporting Period: March 1 - May 31, 2023

CONTENTS

INTRODUCTION

Since the publication of our first quarterly issue in January 2023, the *BlackBerry Global Threat Intelligence Report* has quickly become a key reference guide in the cybersecurity industry. This report is used by cybersecurity professionals worldwide, including CISOs, security managers, and other decision makers, to stay informed of the latest cybersecurity threats and challenges affecting their industries and platforms.

In this new issue, our global BlackBerry Threat Research and Intelligence team examines the challenges to governments and public entities, vulnerabilities in the healthcare sector, risks to financial institutions, and the criticality of safeguarding vital infrastructure. We also include a new geopolitical analysis and comments section that provides additional context and gives a strategic perspective to the data presented. The report covers March 2023 to May 2023.

Here are some of the highlights:

- **90 days by the numbers**. From March 2023 to May 2023, BlackBerry® Cybersecurity solutions stopped over **1.5 million attacks**. On average, threat actors deployed approximately **11.5 attacks per minute**. These threats included roughly **1.7 novel malware samples per minute**. This represents a **13 percent increase** from the previous reporting period's average of 1.5 new samples per minute, demonstrating that attackers are diversifying their tooling in an attempt to bypass defensive controls, especially those legacy solutions based on signatures and hashes.
- **Most targeted industries.** The healthcare and financial services industries were among the most targeted sectors. In healthcare, the combination of valuable data and critical services presents a lucrative target for cyber criminals, resulting in ransomware gangs directly targeting healthcare

THIS REPORT IS USED BY CYBERSECURITY PROFESSIONALS

WORLDWIDE

INCLUDING CISOs, SECURITY MANAGERS, AND OTHER DECISION MAKERS.

organizations and in the proliferation of information-stealing malware, or infostealers. This report highlights the importance of securing patient data and safeguarding the uninterrupted delivery of essential medical services.

- **Remote access increases cyber risk.** Financial institutions face persistent threats due to their economic significance and wealth of sensitive data. This report delves into the finance sector's challenges, including the growing availability of commodity malware, ransomware attacks, and the rise of mobile banking malware targeting digital and mobile banking services.
- **Country-specific cyberattacks.** In the second quarter of 2023, the APT28 and the Lazarus Group—state-sponsored threat actors linked to Russia and North Korea respectively—were very active. These threat actors have a significant history of specifically targeting the United States, Europe, and South Korea. Their focus extends across government agencies, military organizations, businesses, and financial institutions, posing a serious threat to national security and economic stability. These threat groups continually adapt their techniques, making it challenging to defend against their attacks.
- **Wrapping up and looking ahead**. Finally, we present our conclusions and cyberthreat forecast for the coming months of 2023.

To provide actionable and contextual cyber threat intelligence, the Common MITRE Techniques and Applied Countermeasures and Remediation sections summarize the top 20 techniques used by threat groups and compare the trends to the last quarterly report. For example, we confirmed that the five most frequently used tactics are in the categories of discovery and defense evasion. The techniques reported as part of those tactics can be incorporated into purple team exercises and used to prioritize tactics, techniques, and procedures (TTPs) as part of practical threat-modeling exercises.

In addition, the BlackBerry Threat Research and Intelligence team used MITRE D3FEND™ to develop a complete list of countermeasures for all the techniques used during this period. MITRE D3FEND is available in our public GitHub repository. This report lists the most effective Sigma rules to detect the malicious behaviors exhibited by the 224,851 unique samples that BlackBerry Cybersecurity solutions powered by Cylance® AI stopped in this reporting period. Our goal is to enable readers to translate our findings into their own practical threat hunting and detection capabilities.

Finally, I'd like to thank our elite team of global researchers on the BlackBerry Threat Research and Intelligence team for continuing to produce world-class, first-to-market research that informs and educates our readership while continuously improving BlackBerry data- and Cylance AI-driven products and services. We hope you will find value in the detailed and actionable data presented in our latest edition.

Ismael Valenzuela
Vice President, Threat Research and Intelligence at BlackBerry
@aboutsecurity

ATTACKS BY COUNTRY AND INDUSTRY

CYBERATTACKS BY COUNTRY

Top Five Countries That Experience the Most Cyberattacks

Figure 1 shows the five countries where BlackBerry Cybersecurity solutions prevented the most cyberattacks and where unique malicious samples were used. As in the previous reporting period, BlackBerry prevented the greatest number of attacks in the United States. We've since seen growth in the Asia-Pacific (APAC) region, with South Korea and Japan entering our top three. Both New Zealand and Hong Kong broke into the top 10. Even though the United States remains on top, we've noted a far greater diversification of the countries where these novel samples were observed.

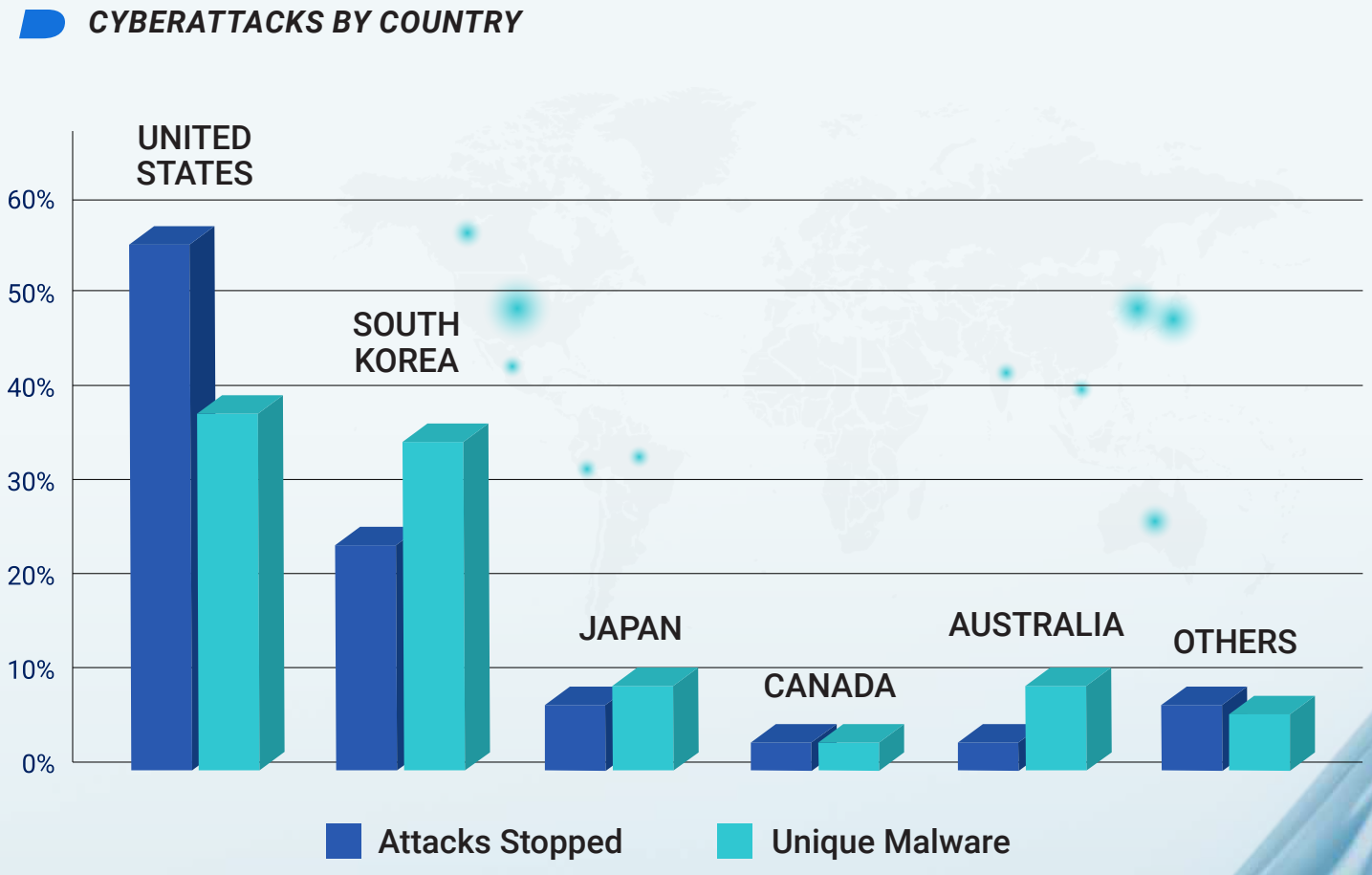


Figure 1: Top 5 countries where BlackBerry clients were targeted by cyberattacks and where unique malicious samples were used in these attacks against BlackBerry-protected devices.

ATTACKS BY INDUSTRY

According to BlackBerry telemetry, below are the top industries with the highest distribution of cyberattacks that BlackBerry Cybersecurity solutions protected during this reporting period:

- Financial institutions
- Healthcare services and equipment including hospitals, clinics, and medical devices
- Government/Public entities
- Critical infrastructure

During this reporting period, the industries attacked were a more diverse group than in the last report. Figure 2 shows the distribution of cyberattacks among the top 3 industries. It also shows that there's an inverse relationship on how the industries rank from 1 to 3 in attacks stopped vs. unique hashes stopped:

CYBERATTACKS STOPPED BY INDUSTRY

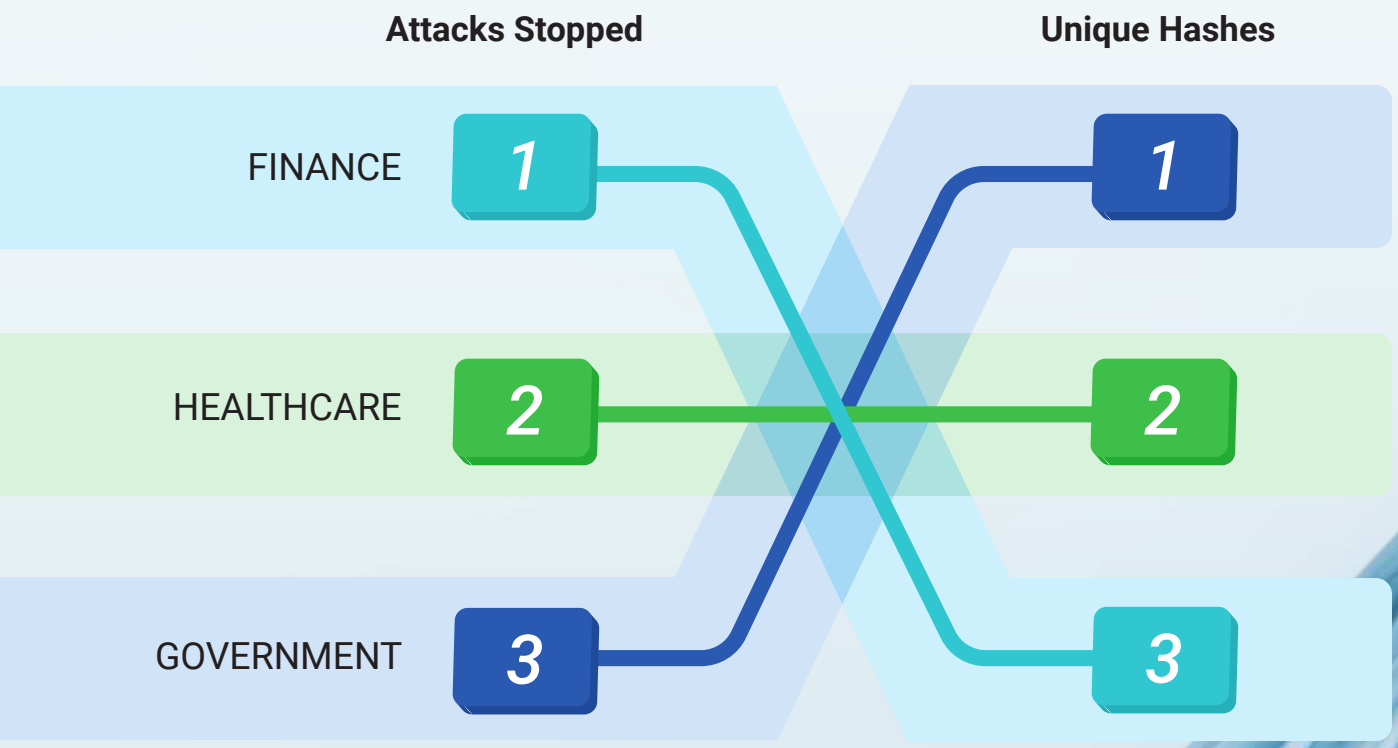


Figure 2: The three industries with the highest distribution of stopped cyberattacks and of stopped unique/different samples during this period.

Government/Public Entities

Government organizations are attractive targets for threat actors whose motivations may be geopolitical, financial, or disruption. Because threat actors may include private individuals, small groups, or state-sponsored APT groups (which use APT tactics), government organizations must defend against a wide range of threats.

During this reporting period, BlackBerry Cybersecurity solutions stopped more than 55,000 individual attacks against the government and public services sector, up nearly 40% from the previous reporting period.

BlackBerry Cybersecurity solutions stopped the greatest number of attacks against government entities in North America and the APAC region, where Australia, South Korea, and Japan were the most heavily targeted countries in the region.

Top Government Threats

In the previous reporting period, the BlackBerry Threat Research and Intelligence team documented multiple inexpensive and easily accessible commodity malware families targeting government entities, including RedLine, Emotet, and RaccoonStealer (RecordBreaker). Commodity malware loaders PrivateLoader and SmokeLoader also targeted the government sector.

DCRat, also known as Dark Crystal RAT, was documented in this reporting period. DCRat has been commonly observed since 2019 and enables threat actors to take control of a victim's device, which then serves as a convenient access point into the compromised environment.

Examining the Wider Government Threat Landscape

This reporting period was heavily dominated by news of ransomware groups targeting and breaching city and state government systems in North America.

In March, the ransomware group LockBit targeted the city of Oakland,[1] California. The group operates a ransomware-as-a-service (RaaS) and typically employs multiple tactics and techniques to infiltrate networks, identify critical and confidential information, and exfiltrate data to be used as collateral in double-extortion ploys to pressure victims into paying larger ransom demands. Also, this reporting period, the threat group BlackByte claimed credit for Royal ransomware attacks against the cities of Dallas, Texas and Augusta, Georgia.

The Clop ransomware group (also referred to as Cl0P or CLOP) is a similar RaaS that was observed abusing

BLACKBERRY CYBERSECURITY SOLUTIONS

STOPPED

THE GREATEST NUMBER OF ATTACKS AGAINST GOVERNMENT ENTITIES IN NORTH AMERICA AND THE APAC REGION, WHERE AUSTRALIA, SOUTH KOREA, AND JAPAN WERE THE MOST HEAVILY TARGETED COUNTRIES IN THE REGION.

the since-patched CVE-2023-0669[2] vulnerability in the managed file transfer (MFT) application GoAnywhere. After this vulnerability was exposed, Clop claimed responsibility for several other attacks this reporting period, including an attack on the city of Toronto,[3] Canada, where the group claims to have encrypted devices and exfiltrated metadata of over 35,000 citizens.

Poland was also a target for attack. According to Reuters,[4] the Polish Tax Service was knocked offline in March by a suspected Russian cyberattack. According to Poland's commissioner for information security,[5] the Russia-aligned group NoName instigated the attacks, which he described as "simple" by today's standards.

In May, the hacktivist group Mysterious Team targeted government and finance ministry sites in Senegal[6] in a distributed denial-of-service (DDoS) attack.

Healthcare

The healthcare sector is one of the most consistently targeted industries by threat actors. Because they deliver critical services, healthcare systems and infrastructure cannot be offline for long periods of time. This makes them enticing targets for ransomware gangs who pressure victims to pay quickly so the healthcare provider can return to service. According to a recent FBI Internet Crime Complaint Center (IC3) report, healthcare and public health were the most targeted critical infrastructure sector by ransomware gangs in the U.S. in 2022, with 210 officially reported attacks.[7]

The healthcare sector is also targeted because of the value of the confidential data within its systems, including personal identifiable information (PII) for individuals including names, addresses, birthdates, social security numbers, and often sensitive health records. PII can be further weaponized for crimes such as identity theft,[8] sold on dark web market forums, or used for blackmail and ransom.

According to the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal,[9] there were 146 "hacking/IT incident" events against U.S. healthcare providers during this reporting period.

Top Healthcare Threats

During the reporting period, BlackBerry Cybersecurity solutions detected and stopped 13,433 unique malware binaries and prevented over 109,922 disparate attacks across the wider healthcare sector.

The most prominent attacks were made using commodity malware, particularly infostealers such as RedLine. Another prevalent threat was Amadey (a bot linked to a botnet of the same name), which can perform reconnaissance on an infected host, steal data, and deliver additional payloads.

Threat actors also used malware families such as Emotet, IcedID, and SmokeLoader to target the healthcare sector. A commonality in these attacks on healthcare providers is that they employ infostealing malware that can also deliver additional malicious payloads.

BLACKBERRY CYBERSECURITY SOLUTIONS

DETECTED

AND STOPPED 13,433 UNIQUE MALWARE BINARIES AND PREVENTED OVER 109,922 DISPARATE ATTACKS ACROSS THE WIDER HEALTHCARE SECTOR.

Examining the Wider Healthcare Threat Landscape

This reporting period included several large-scale and notable cyberattacks across the wider healthcare threat landscape. In early March, the Spanish hospital Clínic de Barcelona was the victim[10] of a ransomware attack thought to have been perpetrated[11] by the RansomHouse cybercrime organization. The attack targeted virtual machines within the hospital's infrastructure and severely disrupted scheduled medical services. A little more than a week later, Alliance Healthcare—one of Spain's leading pharmaceutical suppliers—was targeted in an attack resulting in the complete shutdown[12] of the company's website, billing systems, and order processing.

Also in March, Mumbai-based pharmaceutical manufacturer Sun Pharmaceuticals—the largest of its kind in India and the fourth largest in the world—was attacked[13] by the ALPHV/BlackCat ransomware operator, who added the company's stolen data to their leak site shortly afterwards. In roughly the same period, the group also attacked Pennsylvania-based Lehigh Valley Health Network, after which they threatened to publish photos of female breast cancer patients,[14] a move that was universally condemned as a new low for the cybercrime industry.

State-sponsored threat actors are also suspected to have targeted the healthcare industry during this period. In May, South Korean law enforcement disclosed that North Korean-based hackers had breached the Seoul National University Hospital and stolen confidential medical data. The breach occurred in mid-2021, followed by a two-year investigation. Media sources alleged that the Kimsuky APT group perpetrated this attack.[15]

These varied attacks demonstrate that the healthcare industry is an attractive target for all types of threat actors. Because healthcare organizations typically hold sensitive data and provide critical services, the number of attacks against this industry is likely to rise.

BECAUSE HEALTHCARE ORGANIZATIONS TYPICALLY HOLD SENSITIVE DATA AND PROVIDE CRITICAL SERVICES, THE NUMBER OF ATTACKS AGAINST THIS INDUSTRY IS LIKELY TO RISE.

Finance

The financial industry is a frequent target of cyber criminals seeking large payouts, destructive impact (including possible government fines, legal fees, threat mitigation costs, and damage to the target's reputation), and sensitive financial data that can be sold on dark web forums. This data is often purchased by secondary threat actors who weaponize it to achieve other malicious goals.

During this reporting period, BlackBerry Cybersecurity solutions stopped over 17,000 attacks targeting financial institutions, with close to 15,000 of those attacks against U.S. organizations. The remaining attacks on the financial sector were detected and stopped in countries located in South America and Asia.

BLACKBERRY CYBERSECURITY SOLUTIONS STOPPED OVER

17,000

ATTACKS TARGETING FINANCIAL INSTITUTIONS.

Top Threats to the Financial Industry

During this reporting period, BlackBerry telemetry observed a continuous trend in the use of commodity malware such as RedLine, which can harvest information including saved credentials, credit card information, and (in a more recent version) cryptocurrency. BlackBerry also observed attacks using the backdoor malware SmokeLoader and the open-source framework MimiKatz.

Amadey, a botnet sold on Russian-speaking hacking forums, was detected threatening the financial industry. Amadey sends the targeted victim's information back to its command and control (C2) while waiting for commands by the attacker. Amadey's main function is loading malicious payloads onto compromised machines.

Examining the Wider Finance Threat Landscape

The financial industry—particularly banks—experienced numerous attacks this reporting period. Another common threat to financial institutions was the Clop ransomware, a variant of the CryptoMix ransomware family. The group behind this malware also abused a new vulnerability found within the GoAnywhere MFT software, which suffered from a pre-authentication command injection vulnerability tracked as CVE-2023-0669[16] in the recent banking platform Hatch Bank[17] breach.

Early in this reporting period, the RaaS group behind Lockbit 3.0 targeted Fullerton India,[18] a non-banking financial company in India. The group behind the attack claimed to have stolen over 600GB of data that they shared on their dark web leak site.

In Australia, the loan giant Latitude Financial Services[19] and the Indonesian unit of Commonwealth Bank of Australia[20] were both targeted by cyberattacks earlier in 2023.

The financial sector was also targeted by new Android malware. The Android Trojan known as "Chameleon"[21] mimics an electronic banking service application from the PKO Bank Polski to deceive victims. The Xenomorph Android malware group released updated versions and reportedly stole credentials from more than 400 banks[22] around the world.

Critical Infrastructure

Because reliable critical infrastructure is necessary for delivering essential services that entire populations depend on, infrastructure is a high-value target for hostile nation-states and other groups planning attacks. As noted in our previous report, Ukraine's energy sector has been physically and digitally targeted by suspected Russian-backed groups. Given the growing focus on the security vulnerabilities in operational technology (OT) by malefactors, governments, and critical infrastructure, entities must prioritize the security of their infrastructure.

During this reporting period, BlackBerry telemetry recorded the most attacks against U.S. infrastructure, followed by India, Japan, and Ecuador. Overall, BlackBerry Cybersecurity solutions stopped over 25,000 attacks against critical infrastructure during this reporting period.

Top Critical Infrastructure Targets

Critical infrastructure is often isolated from other systems in an effort to mitigate external threats. However, increasing digitization and integration with the Internet of Things (IoT) in both IT and OT ecosystems can present unforeseen risks. As new technologies are adopted, sophisticated cyberthreats will no doubt follow. In addition to damaging infrastructure, cyber criminals also seek access to data and systems.

Commodity malware is also a growing threat to infrastructure. For example, BlackBerry detected the Vidar infostealer, a commodity malware.

Examining the Wider Critical Infrastructure Threat Landscape

Several highly publicized attacks on critical infrastructure occurred during the reporting period, most notably an attack against the United States by an alleged Chinese state-sponsored threat actor Volt Typhoon. According to Microsoft research,[23] Volt Typhoon is primarily involved in espionage. The group leverages living off the land (LotL)[24] techniques and compromises network equipment to funnel network traffic while remaining undetected.

In April, a suspected North Korean-based group thought to be behind the X_Trader supply chain attack[25] was linked to the compromise of critical infrastructure in the United States and Europe. The rising geopolitical tensions have raised public awareness of the elevated threat to Western-based critical infrastructure. The UK National Cyber Security Center (NCSC), for instance, issued an alert[26] calling for vigilance because of increased activity by state-aligned threat actors sympathetic to Russia's invasion of Ukraine.

BLACKBERRY CYBERSECURITY SOLUTIONS STOPPED OVER 25,000 ATTACKS AGAINST CRITICAL INFRASTRUCTURE.

GEOPOLITICAL ANALYSIS

AND COMMENTS

We live in an age of digital geopolitics. Malicious cyber activity has emerged as a frequently employed tactic for some nation-states to project power, disrupt adversaries, and achieve their geopolitical goals. As the Canadian Centre for Cyber Security described in its National Cyber Threat Assessment for 2023-24,[27] cyberthreat activity "has become an important tool for states to influence events without reaching the threshold of conflict." Motivations behind cyberattacks can range from intellectual property theft to cyber-espionage, disrupting critical infrastructure, and powering digital influence campaigns to undermine public confidence in government (see U.S. National Cybersecurity Strategy).[28] As more and more IT and OT infrastructure comes online, it is likely that cyber activity will continue to be used as a tool to achieve economic, social, geopolitical, and military ends.

During this reporting period, BlackBerry documented a nearly 40 percent increase in the number of cyberattacks against public sector entities that were stopped by BlackBerry Cybersecurity solutions. Critical infrastructure sectors have become strategic targets for state-sponsored cyber actors because downtime in the government's delivery of essential services can be particularly harmful, undermining public trust. For this reason, Five Eyes governments, an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom, and the United States, have consistently assessed that state-sponsored cyber actors are "almost certainly conducting reconnaissance activity against critical infrastructure" with the goal of "pre-positioning on industrial OT networks" and to "send intimidating messages about [their] power and capability [to] threaten a population's health and safety." (The Cyber Threat to Canada's Oil and Gas Sector,[29] Canadian Center for Cyber Security, 2023; also see CISA Cybersecurity Alerts & Advisories).[30]

In the face of escalating cyberattacks, governments are stepping up collaboration to help investigate, respond to, and recover from incidents. Examples include rapid mobilizations from the United States and other allied partner nations to help Costa Rica,[31] Albania,[32] and Montenegro[33] in 2022 as each of their governments faced cyberattacks against critical infrastructure. More recently in Vancouver, Canada, some 30-plus governments reaffirmed the need for broad international co-operation to counter cyberthreats and uphold responsible state behavior in cyber space (see "Nations urged to be responsible in cyber space after meeting in Vancouver").[34]

As hostilities in Ukraine continue, the link between geopolitics and cyberattacks has become increasingly clear. Australia, Canada, New Zealand, the UK, and the U.S. have issued multiple joint cyber advisories[35] warning of potential cyber activity targeting critical infrastructure by both "Russian state-sponsored" and "Russian-aligned", non-state criminal-hacktivist groups in support of the Russian invasion of Ukraine. During this reporting period, BlackBerry documented attacks by suspected Russian-affiliated threat actors targeting EU diplomatic missions and U.S. healthcare entities providing medical support to Ukrainian refugees. We anticipate that this trend will continue as this geopolitical crisis escalates.

TOTAL NUMBER OF THREATS STOPPED

From March to May 2023, BlackBerry Cybersecurity solutions stopped 1,528,488 cyberattacks. During that time, threat actors deployed an average of 16,614 malware samples per day against BlackBerry customers. That's an average of 11.5 malware samples per minute.

These samples included 224,851 new and unique malware samples. On average, this equals 2,444 novel samples per day or 1.7 new samples per minute. This represents a 13 percent increase from the previous reporting period's average of 1.5 unique samples per minute.

The following graph shows the dynamics of cyberattacks that BlackBerry Cybersecurity solutions powered by Cylance AI prevented during this period.

DYNAMICS OF PREVENTED ATTACKS

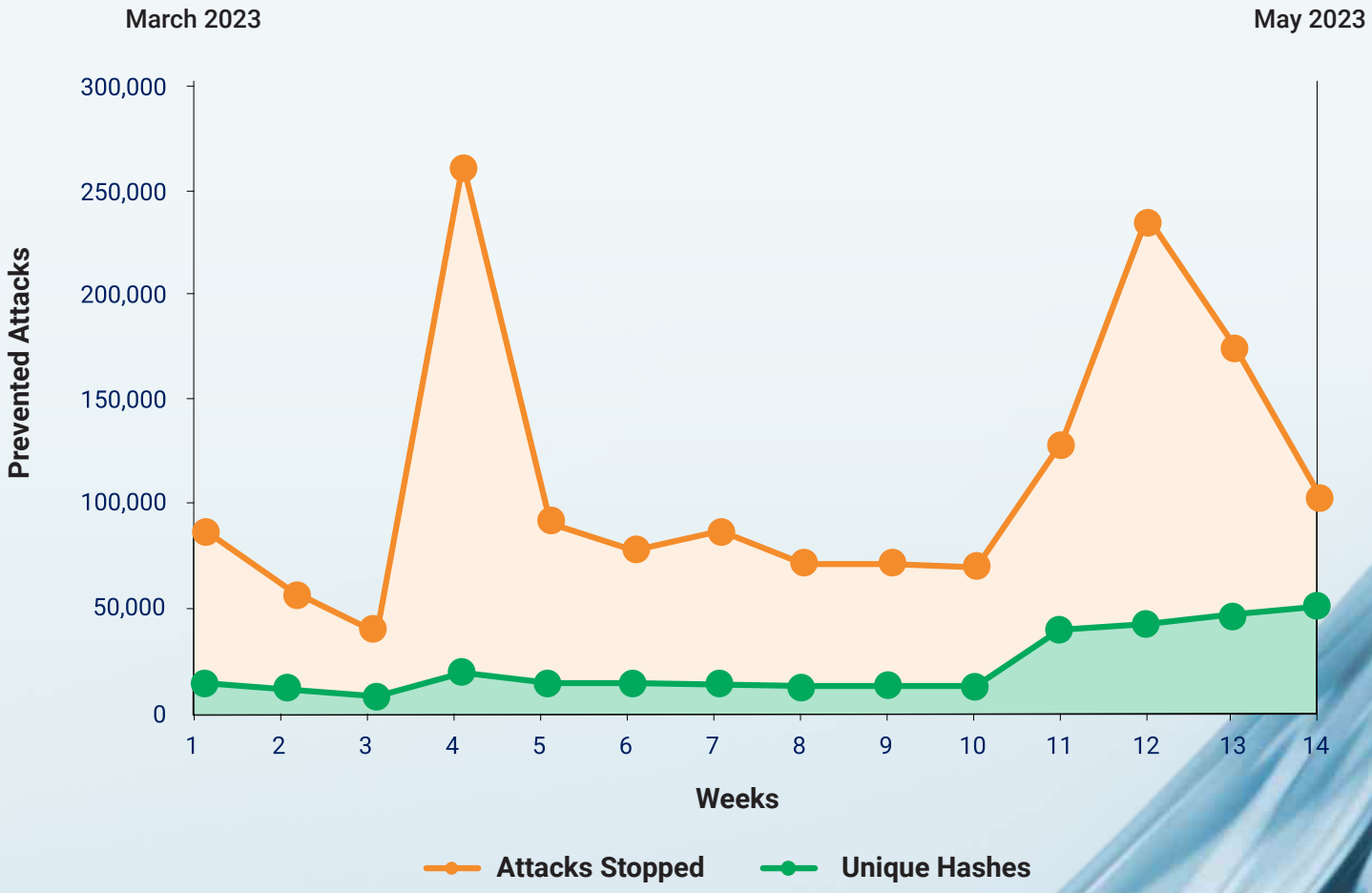


Figure 3: Dynamics of BlackBerry-prevented attacks during this reporting period.

THREAT ACTORS AND TOOLS

During this reporting period, BlackBerry Cybersecurity solutions driven by Cylance AI, defended customers against these advanced threat actors and tools.

THREAT ACTORS

APT28

APT28, also known as Sofacy/Fancy Bear, is a highly skilled and well-resourced cyber espionage group widely assumed[36] to operate on behalf of the Russian government and focused on Western countries and their allies. Active since at least 2007, the group targets a wide range of sectors that includes government, military, defense contractors, and energy companies. The group has been suspected of being involved in advanced persistent threat (APT) campaigns including Operation Pawn Storm and Operation Sofacy.

In November 2015, the group began using a weapon called Zebrocy that has three main components: a downloader and dropper that can discover running processes and download the malicious file onto systems, and a backdoor that establishes persistence in the system and exfiltrates data.

Lazarus Group

The Lazarus Group[37] also known as Labyrinth Chollima, Hidden Cobra, Guardians of Peace, Zinc, and Nickel Academy, is believed to be a North Korean state-sponsored cyberthreat group attributed to North Korea's Reconnaissance General Bureau intelligence agency. The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster.[38]

This group used a custom remote-access Trojan (RAT) called Manuscrypt[39] that collects system information, executes commands, and downloads additional payloads.

TOOLS

AdFind

AdFind is an open-source command-line tool that gathers information from Active Directory (AD). AdFind is used during discovery stages to gather victims' AD data.

Mimikatz

Mimikatz is an open-source penetration testing (pen-testing) framework and tool that offers multiple features for testing network security and hardening systems. Mimikatz can extract confidential information such as passwords and credentials and offers many other features to help security professionals identify vulnerabilities, including privilege escalation on Windows®-based computers. Because of its powerful capabilities, threat actors often abuse Mimikatz to achieve their malicious goals.

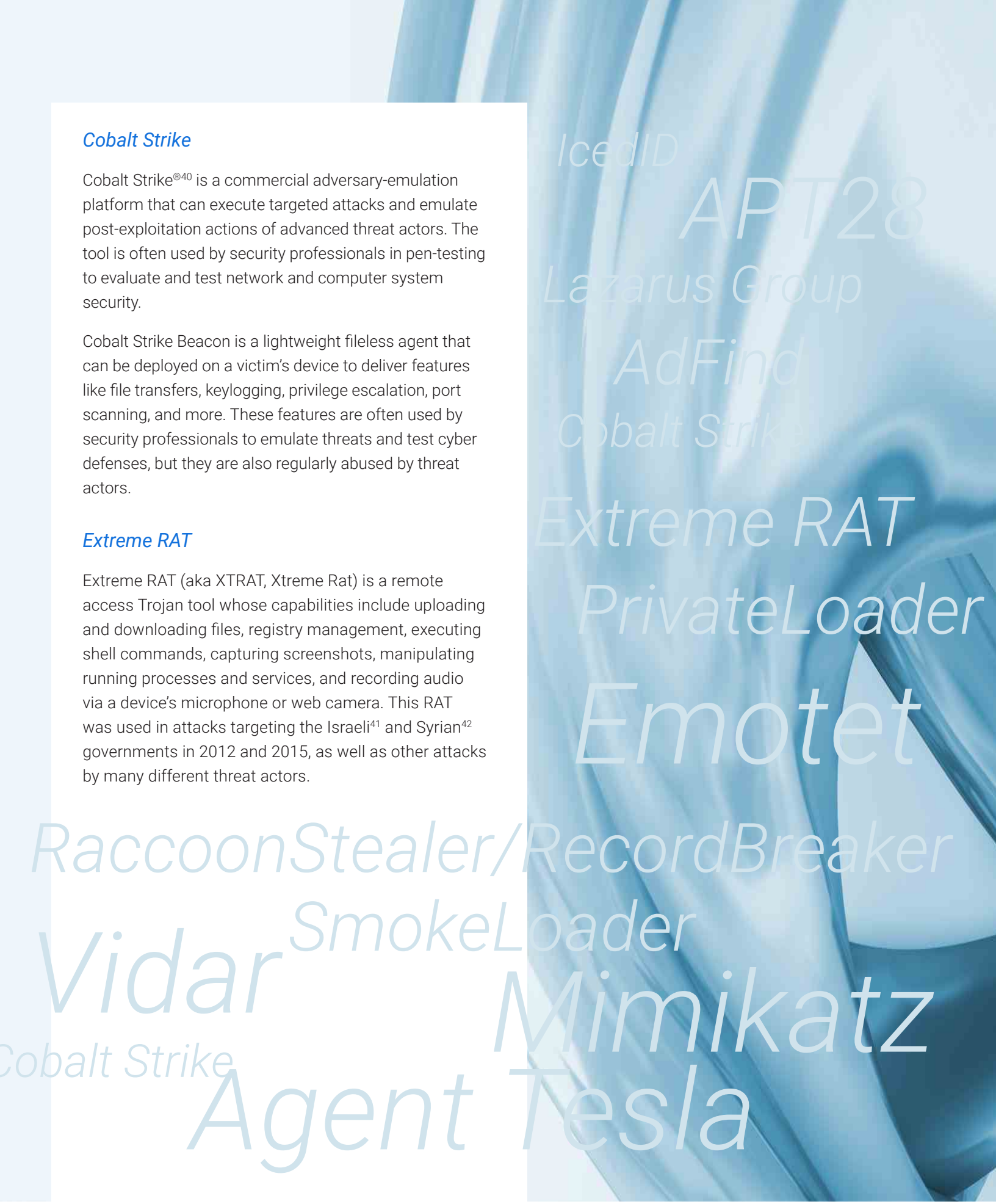
Cobalt Strike

Cobalt Strike®[40] is a commercial adversary-emulation platform that can execute targeted attacks and emulate post-exploitation actions of advanced threat actors. The tool is often used by security professionals in pen-testing to evaluate and test network and computer system security.

Cobalt Strike Beacon is a lightweight fileless agent that can be deployed on a victim's device to deliver features like file transfers, keylogging, privilege escalation, port scanning, and more. These features are often used by security professionals to emulate threats and test cyber defenses, but they are also regularly abused by threat actors.

Extreme RAT

Extreme RAT (aka XTRAT, Xtreme Rat) is a remote access Trojan tool whose capabilities include uploading and downloading files, registry management, executing shell commands, capturing screenshots, manipulating running processes and services, and recording audio via a device's microphone or web camera. This RAT was used in attacks targeting the Israeli[41] and Syrian[42] governments in 2012 and 2015, as well as other attacks by many different threat actors.



MOST PREVALENT MALWARE FAMILIES

WINDOWS

Droppers/Downloaders

Emotet

Over the past decade, Emotet has evolved from its original inception as a standalone banking Trojan to become malware-as-a-service (MaaS) operated behind a trio of botnets dubbed Epoch1, Epoch2, and Epoch3. The botnets serve as a delivery mechanism for various other commodity malware such as TrickBot, IcedID, Bumblebee Loader, and have also been known to deploy malicious Cobalt Strike Beacons.

In the past, the infamous Ryuk ransomware gang used Emotet in conjunction with TrickBot to facilitate access to victim environments. Emotet uses spam emails and infected Microsoft® Office documents as its primary infection vector. After surviving a law enforcement takedown effort and more than one self-imposed sabbatical, Emotet remains present in today's threat landscape.

PrivateLoader

PrivateLoader first appeared on the threat landscape in 2022 and was connected to a pay-per-install service. Using Trojanized versions of "cracked" (or modified) software as its primary infection vector, PrivateLoader has been used in numerous campaigns to deliver a variety of commodity malware including RedLine, Remcos, njRAT, SmokeLoader, and others. The BlackBerry telemetry indicates that PrivateLoader will likely become a regular, albeit unwelcome, visitor in the future.

SmokeLoader

SmokeLoader is a regular feature on the threat landscape and has continuously evolved since its appearance in 2011. Until 2014, it was primarily used by Russian-based threat actors and has been used to load an array of malware, including ransomware, infostealers, cryptominers, and banking Trojans. SmokeLoader is often distributed via spam

AdFind
Extreme RAT
PrivateLoade
Emotet
Mimika
Agent Tesla
Cobalt Strike

BLACKBERRY TELEMETRY INDICATES THAT

PRIVATELOADER

WILL LIKELY BECOME A REGULAR, ALBEIT UNWELCOME, VISITOR IN THE FUTURE.

emails, weaponized documents, and spearphishing attacks. Once installed on a victim's host, SmokeLoader can create a persistence mechanism to survive after reboot, perform DLL injection to attempt to hide within legitimate processes, perform host enumeration, and download/load additional files or malware. SmokeLoader also contains anti-sandbox and anti-analysis techniques such as code obfuscation.

During the previous reporting period, SmokeLoader was used twice to target Ukrainian entities in execution chains that included archives, decoy documents, JavaScript loaders, and the use of PowerShell to deliver a SmokeLoader payload.

Infostealers

RedLine

RedLine is a well-known .NET-based infostealer that targets Windows systems. According to BlackBerry telemetry, RedLine was one of the most widely observed malware families during this period. This widespread malware family was also discussed in the Global Threat Intelligence Report – April 2023.

RedLine is a relatively inexpensive infostealer that attempts to exfiltrate personal information from an infected system, such as passwords, social security numbers, and credit card information saved in browsers. Additionally, RedLine can gather and send lists of applications (including security software) installed on a victim's device to the attacker, which helps attackers plot secondary attacks. RedLine can also execute commands and is often one component of a multi-stage execution chain.

RedLine is widely distributed on underground forums and is sold as a standalone product or as part of a MaaS subscription package. At the time of writing, it can be purchased for approximately $100 to $150 USD.

RedLine's popularity and ability to inflict damage are a result of its versatility. The malware can be delivered in several different ways and is often deployed as a secondary or tertiary payload of other malware to increase the damage to a victim's system. In recent months, RedLine was distributed via Trojanized Microsoft® OneNote attachments to phishing emails.

RaccoonStealer/RecordBreaker

RaccoonStealer is an infostealer that obtains browser cookies, passwords, auto-fill web browser data, and cryptocurrency wallet data. The malware has been reportedly sold as MaaS across dark web forums and similar platforms.

In mid-2022, after a hiatus and temporary suspension of operations, the group behind the malware announced a new version of RaccoonStealer dubbed RaccoonStealer 2.0 or RecordBreaker. This updated malware is currently distributed as MaaS across dark markets. The group claims that they rebuilt it from scratch with an updated infrastructure and improved infostealing capabilities.

Vidar

Vidar is another frequently used commodity malware that is openly distributed in underground forums. Reportedly a fork of the Arkei infostealer, Vidar harvests banking information, browser credentials, and cryptocurrency wallets, as well as standard files. On execution, the malware gathers critical system information as well as data about hardware, running processes, and software and sends it back to the threat actor.

Since its initial release in 2018, multiple iterations of Vidar have bolstered its capabilities, capacity for evasion, and overall complexity, which has increased its popularity with threat actors. Other malware families have been observed dropping Vidar as a secondary payload.

IcedID

Often referred to as BokBot, this banking Trojan was first uncovered in 2017. Since then, IcedID has reinvented itself multiple times to become consistently prevalent across the threat landscape. IcedID is modular by nature, and its core functionality is that of a sophisticated banking Trojan.

Because IcedID is frequently updated to be more evasive and damaging, it remains a prominent threat in 2023. In addition, IcedID often serves as a dropper of additional payloads for secondary-stage malware, including ransomware and Cobalt Strike compromises.

Remote Access Trojans

Agent Tesla

Agent Tesla is a .NET-compiled RAT and infostealer that has been prevalent on the threat landscape since at least 2014. It is a full-fledged RAT that can steal and exfiltrate a wide range of data (including keystrokes, screenshots, and credentials from many commonly used applications).

Agent Tesla has used multiple infection vectors, including spam emails and weaponized Microsoft® Word documents. It has also spread through the exploitation of Microsoft® Office vulnerabilities and through compiled HTML files. During the previous reporting period, Agent Tesla became one of the most active RATs in the global threat landscape.

Ransomware

BlackCat/ALPHV

Initially appearing in the wild in 2021, BlackCat or ALPHV/Noberus is a ransomware family written in the Rust programming language. The malware is sold as RaaS and can target both Windows- and Linux-based operating systems.

ANDROID'S POPULARITY MAKES IT AN ENTICING

TARGET

FOR THREAT ACTORS, SO THE ANDROID THREAT LANDSCAPE HAS NEVER BEEN LIVELIER.

ALPHV is a prolific ransomware that has been used to target high-profile victims. After infecting the host, ALPHV ransomware becomes evasive and attempts to block recovery and reporting functions before detonating the final ransomware payload.

ALPHV has gained further notoriety for exfiltrating sensitive data and using a double extortion method to pressure victims into paying larger ransoms to restore access to their encrypted files and keep them from being released to the public.

According to an FBI Advisory,[43] BlackCat/ALPHV is potentially linked to the older groups DarkSide and BlackMatter.

MOBILE

Android

Since its first release in 2008, Android™ has become the mobile platform of choice for over three billion[44] active handheld device users, encompassing nearly 71 percent of the worldwide market.[45] Unfortunately, Android's popularity also makes it an enticing target for threat actors, so the Android threat landscape has never been livelier. Here are some of the most prevalent Android threats we encountered during the this reporting period.

SpyNote

SpyNote[46] (also known as SpyMax) is a family of malware used for spying on victims. SpyNote extracts sensitive information like credentials and credit card details from mobile devices. SpyNote can also monitor user location, access a device's camera, intercept SMS text messages (which helps threat actors bypass two-factor authentication), monitor and record phone calls, and control a device remotely.

SpyNote continues to evolve. The latest iteration, dubbed SpyNote.C, is the first variant to be delivered by fake apps that masquerade as legitimate apps from prominent financial organizations, as well as other

commonly used mobile applications. Following a source code leak in October 2022, samples of SpyNote have increased significantly on the mobile threat landscape.[47]

SpinOk

SpinOk, which was first documented in late May 2023, is a malicious software component with spyware capabilities that appears to be a software development kit (SDK) for a marketing app. In the previous reporting period, SpinOK was unintentionally embedded into dozens[48] of applications in an SDK supply chain attack.[49]

Once embedded, SpinOK displays ads that appear to be mini games to encourage users to keep the app open. SpinOk enables threat actors to identify the device's contents and exfiltrate data to remote servers. It can also impede threat analysis efforts.[50]

SMSThief

SMSThief can intercept, forward, or copy a victim's SMS text messages while running in the device's background. Variants of SMSThief have been in use for at least the past decade. SMSThief can also enroll victims into premium number scams[51] by sending text messages from the user's device to a premium number that incurs excessive charges.

LINUX

Linux® is primarily used on enterprise servers (both on-premises and cloud-based) and IoT devices, instead of user systems. The most popular infection vectors are via brute-forcing passwords to gain Secure Shell (SSH) access or by exploiting vulnerabilities in public-facing services. This reporting period's attacks remain consistent with the previous period, including DDoS attacks, cryptominers, and ransomware specifically targeting VMWare ESXi servers.

Because Linux is an active target for threat actors, organizations must act to lessen their risk. Applying security patches should be a priority. Patching can help protect Linux environments from remote exploits as well as from local privilege escalation (LPE) vulnerabilities, which are commonly used in sophisticated attacks. These remote exploits include advanced malware such as backdoors. Because many threats to Linux environments rely on brute-forcing weak passwords to gain access, we recommend requiring strong credentials as well as an effective vulnerability management program.

Distributed Denial of Service

Malware-based DDoS attacks were the most common threat to Linux systems during this reporting period. The most-deployed malware variant was Mirai, which has been active since at least 2016. Mirai's source code is published in underground forums, making it difficult to attribute attacks to specific groups. Mirai mostly targets IoT devices without current security updates.

Gafygt,[52] which has been active since 2014, is a Linux-based botnet that uses a code base similar to Mirai and generally targets devices like IoT routers. In the previous reporting period, XorDDos[53] was the most advanced malware used in DDoS attacks, although it was also the least common. XorDDoS spreads mostly by brute-forcing access to SSH and can include a rootkit that hides its presence from system administrators.

Cryptominers

The second most common threat to Linux servers during this reporting period was cryptominers—threat actors using a victim's system resources to mine cryptocurrency (mainly Monero). While the open-source cross-platform software XMRig is the most common cryptominer, this reporting period revealed a spike in usage for the Prometei botnet,[54] which has been active since at least 2020 and is also available as a Windows version. Prometei's advanced features include using domain-generated algorithms to make it difficult to stop the botnet. Prometei targeted victims around the globe—but not Russian hosts. Originally, Prometei was allegedly designed to not target the CIS nations of Russia, Ukraine, Belarus, and Kazakhstan. However, later editions of the malware suggest that this is no longer the case. The

malware appears to be designed to infect everything but Russian-based devices. Given this, it appears as though pro-Russian hactivists are looking for ways to attack nations that have supported Ukraine against the Russian invasion.

Ransomware

While most ransomware attacks target Windows, most prominent threat groups create a Linux version of their malware, often targeting VMWare ESXi. This included activity from multiple prominent groups including Lockbit, Black Basta, BlackCat/ALPHV, Babuk, Royal, and Hive. Trigona[55] and Money Message[56] are new ransomware strains that include a Linux version.

In the future, we expect new ransomware groups to develop a Linux variant at the launch of their operations, increasing the probability for ransomware attacks against Linux systems.

macOS

While considered to be safer than Windows, macOS has nonetheless been targeted by advanced threat actors for a long time. For detailed information, watch macOS: Tracking High Profile Targeted Attacks, Threat Actors & TTPs,[57] BlackBerry's presentation at RSA 2023.

While typical macOS malware displays adware or hijacks web browser searches, a growing number of threat actors during this reporting period used cross-platform programming languages to develop malware targeting macOS itself. For example, we observed a new strain called Atomic macOS (AMOS), an infostealer based on the cross-platform programming language GoLang (aka Go).

Adware and Browser Hijacking

While many people consider adware to be no more than an unwanted application, adware can download and install harmful components like backdoors. In this reporting period, our telemetry shows that AdLoad and Pirrit remain the most widely deployed adware. We also observed the recurrence of Genieo, an older threat that redirects search bar results to point the user towards potentially malicious adware. Adware can be programmed to point people searching the web to malicious websites that download malware on the victim's device. These malicious sites may be cloned to look identical to legitimate sites. For example, the threat group RomCom recently cloned sites hosting legitimate enterprise applications and used typosquatting to create URLs that are similar to the ones used on the real website. Visitors to the fake sites unknowingly downloaded Trojanized versions of popular software that gave threat actors a backdoor to their machine to exfiltrate information.

Atomic macOS (AMOS) Stealer

Atomic macOS (AMOS) is a new strain of infostealer targeting macOS that emerged this reporting period[58] and has been seen deployed in the wild. AMOS is advertised on the popular cloud-based messaging app Telegram. The malware can collect user credentials from keychains, browsers, and crypto wallets and exfiltrate files from specific user directories such as Desktop and Documents. On the Windows platform, initial access brokers (IABs) use the stolen credentials to compromise networks and deploy ransomware. While this behavior hasn't been observed in AMOS, it may conceivably occur in the future.

IN THE FUTURE, WE EXPECT NEW RANSOMWARE GROUPS TO DEVELOP A LINUX VARIANT AT THE LAUNCH OF THEIR OPERATIONS, INCREASING THE PROBABILITY FOR RANSOMWARE ATTACKS AGAINST LINUX SYSTEMS.

MOST INTERESTING STORIES

SIDEWINDER USES SERVER-SIDE POLYMORPHISM TO ATTACK PAKISTAN GOVERNMENT OFFICIALS—AND IS NOW TARGETING TURKEY

In early May, the BlackBerry Threat Research and Intelligence team published findings uncovering a campaign by the APT group SideWinder,[59] which is believed to originate in India. The campaign focused on Pakistani government targets and was delivered by a complex execution chain that relied on phishing emails and weaponized documents that exploit the CVE-2017-0199[60] vulnerability to perform remote template injection. The group used unique server-side[61] polymorphism to bypass signature-based detection mechanisms. If successful, the exploit would then deliver a next-stage payload.

The campaign first occurred in December 2022. In March 2023, the BlackBerry Threat Research and Intelligence team uncovered evidence of an additional SideWinder campaign targeting Turkey. This campaign's timing overlapped with geopolitical events in the region, notably Turkey's public support of Pakistan in its dispute with India over Kashmir.[62]

INITIAL IMPLANTS AND NETWORK ANALYSIS SUGGEST THE 3CX SUPPLY CHAIN OPERATION GOES BACK TO FALL 2022

At the end of March 2023, the business communication supplier 3CX announced[63] a major security breach that resulted in the worldwide distribution of Trojanized versions of their VOIP software, 3CXDesktopApp.

3CXDesktopApp is a voice and video conferencing product widely used for calls, video, and live chat. The company website states that 3CX has approximately 600,000 customer companies, with over 12 million daily users in 190 countries.[64]

3CX announced[65] the breach the day after the attack. In a later update about the incident,[66] 3CX stated that North Korea-affiliated threat actor UNC4736 was behind the attack, which deployed Taxhaul (aka TxRLoader) malware in conjunction with the Coldcat downloader.

The malware was initially delivered by a malicious installer that appeared as a compromised dependency file that enabled the Trojanized files to be signed and appear as legitimate files from the vendor.

BlackBerry telemetry and analysis of the initial samples and the corresponding network infrastructure indicate that the operation began between summer and the beginning of fall 2022. The attack affected the healthcare, pharmaceutical, IT, and financial industries across Australia, the United States, and the United Kingdom.

NOBELIUM USES POLAND'S AMBASSADOR'S VISIT TO THE U.S. TO TARGET EU GOVERNMENTS ASSISTING UKRAINE

In early March, BlackBerry researchers observed campaigns targeting European entities by the Russian state-sponsored threat actor known as NOBELIUM (APT29), which is publicly linked to the Russian foreign intelligence service SVR.

The group created custom lures targeting people interested in Polish Ambassador Marek Magierowksi's trip to Washington, D.C. to discuss the ongoing war in Ukraine. Another lure was designed to abuse the legitimate systems LegisWrite and eTrustEx, which EU nations use for information exchange and secure data transfer.

The lures were designed to coax a victim to download a malicious HTML file named EnvyScout.[67] The tool uses an HTML smuggling technique to deliver further malicious components (often as an ISO or IMG file) to the victim's machine, which then steals sensitive information. The overlap between the Polish Ambassador's visit to the U.S. with the lure used in the attacks provides evidence that NOBELIUM uses geopolitical events to lure victims and increase the likelihood of a successful infection.

FROM GOOGLE ADS ABUSE TO A MASSIVE SPEARPHISHING CAMPAIGN IMPERSONATING SPAIN'S TAX AGENCY

In early April 2023, the BlackBerry Threat Research and Intelligence team published findings from several months of tracking two malicious campaigns that leveraged typosquatting[68] for different goals and purposes.

The first—a malvertising[69] campaign abusing the Google Ads platform—had been in operation for at least several months. Fake and Trojanized versions of common software such as Libre Office, AnyDesk, TeamViewer, and Brave delivered commodity infostealers including Vidar and IcedID. To fool unsuspecting victims, the threat actor cloned legitimate websites and assigned domain names that used typosquatting to mimic the URLs of the real websites.

The second campaign was a large-scale targeted spearphishing campaign that mimicked the Spanish national tax agency. The campaign attempted to steal email credentials from victims in key industries such as technology, construction, energy, agriculture, consulting, government, automotive, healthcare, and finance.

PAPERCUT RCE VULNERABILITY HEAVILY EXPLOITED BY THREAT ACTORS

In March 2023, a remote code execution (RCE) flaw in PaperCut NG/MF versions 8.0 and higher was publicly disclosed.[70] PaperCut is a print management software developer whose products are used worldwide. The vulnerability (tracked as CVE-2023-27350)[71] has since been patched, but because it's available as a public proof of concept (POC) and difficult to detect, the RCE flaw is an ideal infection vector for threat actors to breach systems running unpatched versions of the vulnerable software.

The Bl00dy ransomware operators have been leveraging this flaw to target[72] entities in the education sector. The Clop and LockBit gangs have also been seen targeting vulnerable servers,[73] and in early May, Microsoft disclosed[74] that they observed multiple Iranian state-sponsored APT groups including Mango Sandstorm and Mint Sandstorm actively exploiting the vulnerability.

RUSSIAN ESPIONAGE MALWARE OPERATION DISMANTLED BY LAW ENFORCEMENT

In a massive blow to Russian cyber espionage capabilities, the U.S. Department of Justice announced[75] in early May that the infrastructure used by notorious threat actor Turla had been dismantled. The group, which has been linked to the Federal Security Service of the Russian Federation (FSB), used a sophisticated infostealer called Snake to obtain confidential documents from states in the North Atlantic Treaty Organization (NATO) and the United Nations. The Snake infrastructure included a botnet found on infected systems across at least 50 countries, including members of NATO, and was allegedly abused for over 20 years.

In response to the discovery, the FBI developed a utility aptly named Perseus (a Greek hero and slayer of monsters). Perseus disables Snake malware without damaging infected systems.

NEW THREAT GROUP "RHYSIDA" ATTACKS CHILE'S ARMY

In late May 2023, a ransomware attack against Chile's army (Ejercito de Chile) by a new threat group called Rhysida was made public.[76] The details of the attack have not been fully disclosed, but an Army corporal has been arrested [77] for alleged involvement in the ransomware attack.

The BlackBerry Threat Research and Intelligence team found indicators of compromise (IoCs) indicating that Rhysida is in the initial stages of development. Sample analysis indicates that the group executed a .exe file through PowerShell. This portable executable (PE) file tries to modify the user's desktop wallpaper via registry keys; encrypts files using an XOR and AES algorithm; and adds the Rhysida extension to encrypted files (to avoid encrypting OS folders that would interrupt the functioning of the system). Process injection to Explorer has also been observed.

After that, a ransom note named "CriticalBreachDetected.pdf" is placed that contains information about how to contact the group through a TOR portal. The group requests a ransom to be paid in Bitcoin (BTC). If the victim agrees to pay, they must provide an ID and fill in an additional form to be contacted by the group.

IN RESPONSE TO THE DISCOVERY,

THE FBI

DEVELOPED A UTILITY APTLY NAMED PERSEUS, WHICH DISABLES SNAKE MALWARE WITHOUT DAMAGING INFECTED SYSTEMS.

COMMON MITRE TECHNIQUES

Understanding threat groups' high-level techniques can aid in deciding which detection techniques should be prioritized. BlackBerry observed the following top 20 techniques being used by threat actors.

An upward arrow in the last column indicates that usage of the technique has increased since our last report. A downward arrow indicates that usage has decreased since our last report. An equals (=) symbol means that the technique remains in the same position as in our last report.

The full list of MITRE techniques is available in the Threat Research and Intelligence public GitHub.

Technique Name	Technique ID	Tactic	Last Report	Change
1-System Information Discovery	T1082	Discovery	1	=
2-Virtualization/Sandbox Evasion	T1497	Defense Evasion	3	↑
3-Security Software Discovery	T1518.001	Discovery	4	↑
4-Process Injection	T1055	Defense Evasion	2	↓
5-Masquerading	T1036	Defense Evasion	5	=
6-Remote System Discovery	T1018	Discovery	6	=
7-Application Layer Protocol	T1071	Command-and-Control	7	=
8-File and Directory Discovery	T1083	Discovery	8	=
9-Non-Application Layer Protocol	T1095	Command-and-Control	9	=
10-Process Discovery	T1057	Discovery	10	=
11-Input Capture	T1056	Collection	13	↑
12-DLL Side-Loading	T1574.002	Persistence	12	↓
13-Software Packing	T1027.002	Defense Evasion	14	↑
14-Command and Scripting Interpreter	T1059	Execution	12	↓
15-Registry Run Keys/Startup Folder	T1547.001	Persistence	19	↑
16-Encrypted Channel	T1573	Command-and-Control	17	↑
17-Disable or Modify Tools	T1562.001	Defense Evasion	15	↓
18-Rundll32	T1218.011	Defense Evasion	16	↓
19-Obfuscated Files or Information	T1027	Defense Evasion	18	↓
20-Application Window Discovery	T1010	Discovery	20	=

The top five techniques remain the same as the last reporting period, although their order in the list has changed. Virtualization/Sandbox Evasion moved from the third spot to the second, and Security Software Discovery moved from fourth to third. At the same time, Process Injection techniques dropped two places compared to the last report.

Using MITRE D3FEND, the BlackBerry Threat Research and Intelligence team developed a complete list of countermeasures for the techniques observed during this reporting period, which is available in our public GitHub.

APPLIED COUNTERMEASURES AND REMEDIATION

DETECTION TECHNIQUES

The BlackBerry Threat Research and Intelligence team identified 386 public Sigma rules that detected threat-related behaviors in the 224,851 unique samples stopped by BlackBerry Cybersecurity solutions in this reporting period. Figure 4 shows the top 10 Sigma rules that detected the most malicious behaviors.

TOP 10 SIGMA RULES THAT DETECTED MALICIOUS BEHAVIORS

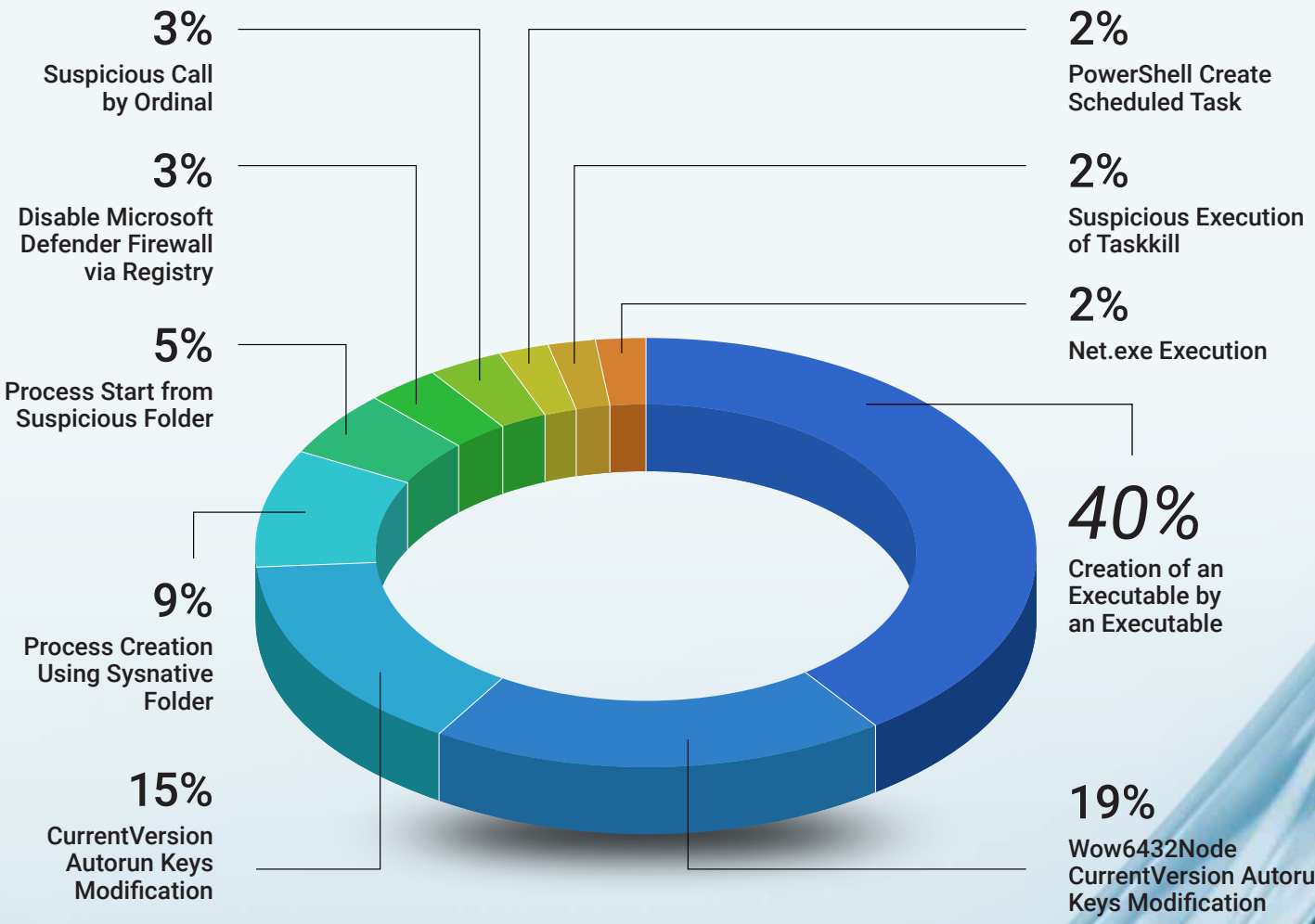


Figure 4: Top 10 Sigma rules detecting suspicious behaviors during this reporting period.

Sigma Rule	Description	MITRE ATT&CK Technique	MITRE ATT&CK Tactic	Last Report	Change
1-Creation of an Executable by an Executable	Detects the creation of an executable by another executable	Develop Capabilities: Malware - T1587.001	Resource Development	1	=
2-Wow6432Node CurrentVersion Autorun Keys Modification	Detects modification of autostart extensibility point (ASEP) in registry	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001	Persistence	2	=
3-CurrentVersion Autorun Keys Modification	Detects modification of autostart extensibility point (ASEP) in registry	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001	Persistence	6	↑
4-Process Creation Using Sysnative Folder	Detects process creation events that use the Sysnative folder (common for Cobalt Strike spawns)	Process Injection - T1055	Defense Evasion	3	↓
5-Process Start from Suspicious Folder	Detects process start from rare or uncommon folders, like temporary folder or folders	User Execution - T1204	Execution	5	=
6-Disable Microsoft Defender Firewall via Registry	Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage	Impair Defenses: Disable or Modify System Firewall - T1562.004	Defense Evasion	7	↑
7-Suspicious Call by Ordinal	Detects suspicious calls of DLLs in rundll32.dll exports by ordinal	System Binary Proxy Execution: Rundll32 - T1218.011	Defense Evasion	9	↑
8-PowerShell Create Scheduled Task	Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code	Scheduled Task/ Job: Scheduled Task - T1053.005	Persistence	8	=
9-Suspicious Execution of Taskkill	Adversaries may stop services or processes in order to conduct Data Destruction or Data Encrypted for Impact on the data stores of services like Exchange and SQL Server.	Service Stop - T1489	Impact	NA	↑
10-Net.exe Execution	Detects execution of Net. exe Windows utility, whether suspicious or benign	Multiple techniques: Permission Groups Discovery – T1069 Account Discovery – T1087 System Service Discovery – T1007	Discovery	NA	↑

Sigma Rule: Net.exe Execution

Related to Sysmon Event ID 1 Process Creation. This Sigma rule identifies executions with specific command lines. Interesting behaviors that we have observed include the following:

Parent Process from \AppData\Local\ executing

> C:\\Windows\\system32\\net.exe view

Parent Process from \AppData\Local\ executing

> net stop "TeamViewer"

Parent Process C:\Windows\SysWOW64\cmd.exe executing

> net user

Parent Process from \AppData\Local\ executing

> net group "Domain Admins" /domain

Sigma Rule: Suspicious Execution of Taskkill

Also related to Sysmon Event ID 1 Process Creation, this Sigma rule's goal is to identify behaviors related to "kill" processes in the system.

> taskkill /F /IM chrome.exe /T

> taskkill /f /t /im <FILENAME>.exe

> taskkill /im google* /f /t

Most of the observed behaviors included the /F flag, which means that the process will be forced to finish. The /T flag means that any child process will be terminated as well. Finally, the parameter /IM specifies the image name of the process to be terminated, and wildcards (*) are allowed.

Sigma Rule: Process Start from Suspicious Folder

This Sigma rule indicates processes that are started from uncommon folders in the OS. The following is an example of common folders:

> C:\Users\<USER>\AppData\Local\Temp

> C:\Windows\Temp

Uncommon folders that match this Sigma rule include:

> C:\Users\Public\Libraries (Used by RomCom and other threat actors)

> C:\Users\Public

> C:\Users\<USER>\AppData\Local\Temp\~[a-zA-Z]+\.tmp\ (Regular Expression ~[a-zA-Z]+\.tmp)

SIGMA TO MITRE

Sigma is a text-based, open signature format that can describe log events and log patterns. Sigma rules typically are mapped to MITRE techniques, and multiple MITRE techniques can be mapped to an individual Sigma rule. During this reporting period, 386 Sigma rules detected malicious behavior in more than 220,000 new and unique malware samples.

Mapping these back to MITRE techniques, we do not see a direct correlation with this reporting period's "Common MITRE Techniques".

The top five MITRE techniques observed in the Sigma rules are listed below.

Technique	Number of Sigma Rules
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001	14
Impair Defenses: Disable or Modify Tools - T1562.001	11
Command and Scripting Interpreter: PowerShell – T1059.001	10
Command and Scripting Interpreter - T1059	9
Scheduled Task/Job: Scheduled Task – T1053.005	9

Reviewing the MITRE tactics associated with the 386 Sigma rules that detected malicious behavior reveals the location of detection targets during intrusions. Indeed, defense evasion is one of the most commonly used tactics that can be seen in the Common MITRE Techniques section.

TACTICS OBSERVED IN THE SIGMA RULES

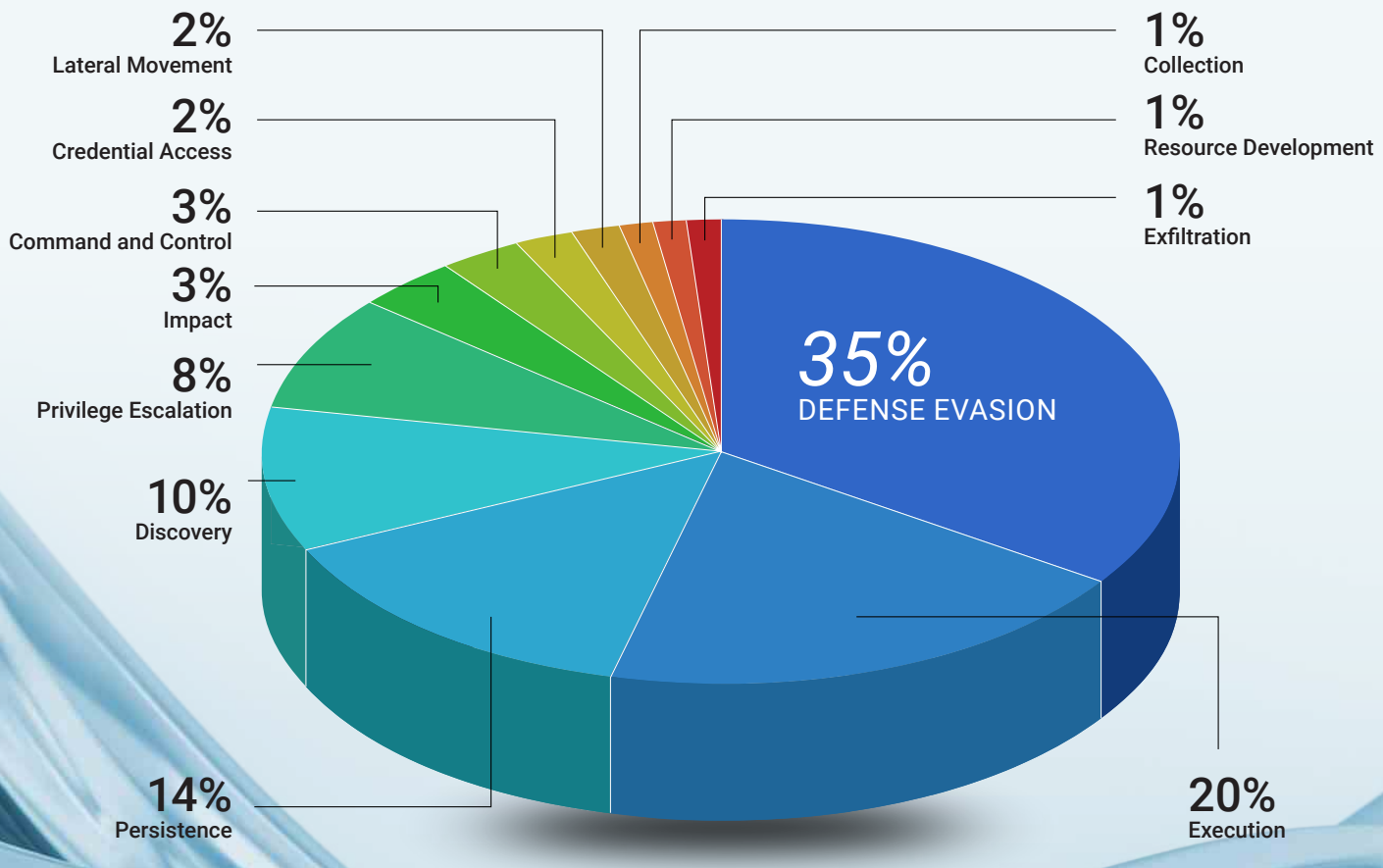


Figure 5: MITRE tactics observed in Sigma rules this reporting period.

CONCLUSION

The 13 percent increase in unique malicious samples targeting our customers demonstrates efforts by threat actors to diversify tooling in compilation. This process produces different hashes for similar samples that could be used to bypass simple feeds and filters used by traditional security operations centers (SOCs).

APT28 and the Lazarus Group were two of the most active threat actors targeting our customers during this reporting period. They are both thought to be state sponsored, with APT28 linked to Russia and Lazarus linked to North Korea. These two groups have a long history of targeting the West with a specific focus on the United States, Europe, and South Korea. Their targets include government agencies, military organizations, businesses, and financial institutions. Both groups pose a serious threat to national security and economic prosperity. Because these groups are constantly evolving their techniques to make defense more difficult, organizations must be aware of these threat actors' latest TTPs and include them in purple team exercises to boost defensive strategies and apply countermeasures.

Healthcare and financial institutions were the most targeted industries during this reporting period. Infostealers that steal and trade stolen credentials were the most common exploits against both finance and healthcare. However, we have also seen high-profile attacks on hospital and financial organizations connected to relief efforts in Ukraine. For example, cyberthreat groups such as RomCom targeted medical entities based in the U.S. providing humanitarian aid to refugees from Ukraine.

Ransomware remains an ongoing threat to both financial and healthcare institutions. Based on our telemetry from this and the previous reporting period, these two industries are likely to remain heavily targeted.

While working with the samples from this reporting period, we confirmed that the most frequently used tactics are discovery and defense evasion. Prioritizing the detection of these tactics in a network is critical. By learning these TTPs and threat actor profiles, a cybersecurity team may significantly reduce the impact of attacks, as well as aid threat hunting, incident response, and recovery efforts.

FORECASTS

- In late May, software corporation Progress Software informed customers about a vulnerability in their MOVEit Transfer[78] product. The vulnerability (CVE-2023-34362[79]) can be exploited via SQL injection and could lead to escalation of privileges and a system breach. The vulnerability has been heavily exploited on unpatched systems in the wild, most notably by the Clop ransomware gang, which leveraged it to allegedly[80] breach hundreds of organizations. We anticipate that threat actors will continue to attempt to exploit this vulnerability until all vulnerable systems are patched.[81]

- Recent research[82] indicates that the value of the global mobile banking market is estimated to reach $1.82 billion in 2026, and trends like the rise of neobanks[83] indicate that digital and mobile banking service usage is likely to continue to rise over the next decade. Unfortunately, this growth will likely be accompanied by an increase in mobile banking malware. Several alarming[84] events occurred in the past few months, including a new Android botnet that targeted approximately 450 financial applications.[85] Smartphone-centric malware will likely increase as threat actors attempt to exploit consumers who are heavy users of online banking.

- Phishing campaigns are growing more sophisticated in their efforts to avoid detection. In recent months, increasing numbers of new web domains were registered that act as proxies before delivering malicious content. The use of proxies and geofencing to target victims in a specific country or region makes it difficult to detect fraudulent websites early. These types of phishing campaigns will increase, providing phishers more operational time to obtain information from their victims before they are detected.

- Generative AI like ChatGPT presents organizations with a potential cybersecurity issue. ChatGPT has already been used to generate new malware—for example, researchers from HYAS Labs created BlackMamba,[86] a proof-of-concept polymorphic keylogger that automatically changes its code on the fly to evade detection, exploiting a large language model (LLM)—the technology on which ChatGPT is based. Threat actors are also exploiting global interest in ChatGPT to lure the public into installing malware. For example, around 2,000 people a day installed a malicious browser extension called Quick access to ChatGPT [87] that harvested information from Facebook Business accounts. We predict that ChatGPT will continue to present innovative threats at an increasing rate as 2023 progresses.

To learn more about how BlackBerry can secure your organization, visit https://www.blackberry.com/.

LEGAL DISCLAIMER

The information contained in the *2023 BlackBerry Global Threat intelligence Report* is intended for educational purposes only. BlackBerry does not guarantee or take responsibility for the accuracy, completeness and reliability of any third-party statements or research referenced herein. The analysis expressed in this report reflects the current understanding of available information by our research analysts and may be subject to change as additional information is made known to us. Readers are responsible for exercising their own due diligence when applying this information to their private and professional lives. BlackBerry does not condone any malicious use or misuse of information presented in this report.

ACKNOWLEDGEMENTS

The 2023 BlackBerry Global Threat Intelligence Report represents the collaborative efforts of our talented teams and individuals. In particular, we would like to recognize:

Dmitry Bestuzhev

Geoff O'Rourke

Dean Given

Maristela Ames

Natalia Ciapponi

Jacob Faires

Jose Luis Sanchez

Pedro Drimel

Patryk Matysik

ENDNOTES

1 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-now-also-claims-city-of-oakland-breach/
2 https://nvd.nist.gov/vuln/detail/CVE-2023-0669
3 https://www.cybersecurity-insiders.com/details-of-a-failed-clop-ransomware-attack-on-city-of-toronto-canada/
4 https://www.reuters.com/world/europe/poland-says-russian-hackers-attacked-tax-website-2023-03-01/
5 https://www.thefirstnews.com/article/cyber-attacks-have-become-commonplace-says-govt-official-36902
6 https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/
7 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
8 https://www.fraudsmart.ie/personal/fraud-scams/phone-fraud/identity-theft/
9 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
10 https://www.clinicbarcelona.org/en/news/computer-attack-on-the-frcb-idibaps
11 https://www.bleepingcomputer.com/news/security/hospital-cl-nic-de-barcelona-severely-impacted-by-ransomware-attack/
12 https://www.scmagazine.com/news/incident-response/cyberattack-hits-spanish-pharmaceutical-company-alliance-healthcare
13 https://www.cpomagazine.com/cyber-security/fourth-largest-generic-drugs-manufacturer-sun-pharmaceuticals-hit-by-ransomware-attack/
14 https://twitter.com/vxunderground/status/1632464810863390721
15 https://www.bleepingcomputer.com/news/security/north-korean-hackers-breached-major-hospital-in-seoul-to-steal-data/
16 https://nvd.nist.gov/vuln/detail/CVE-2023-0669
17 https://www.bleepingcomputer.com/news/security/hatch-bank-discloses-data-breach-after-goanywhere-mft-hack/
18 https://www.timesnownews.com/technology-science/lockbit-3-0-ransomware-targets-fullerton-india-demand-a-staggering-2400-crores-ransom-in-just-5-days-article-99721253
19 https://www.bleepingcomputer.com/news/security/latitude-financial-data-breach-now-impacts-14-million-customers/
20 https://www.reuters.com/technology/commonwealth-bank-australias-indonesian-arm-hit-by-cyber-attack-2023-03-08/
21 https://www.bleepingcomputer.com/news/security/new-chameleon-android-malware-mimics-bank-govt-and-crypto-apps/
22 https://www.bleepingcomputer.com/news/security/xenomorph-android-malware-now-steals-data-from-400-banks/
23 https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
24 https://darktrace.com/blog/living-off-the-land-how-hackers-blend-into-your-environment
25 https://techcrunch.com/2023/04/20/3cx-supply-chain-xtrader-mandiant/
26 https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups
27 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024
28 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
29 https://www.cyber.gc.ca/sites/default/files/cyber-threat-oil-gas-e.pdf
30 https://www.cisa.gov/news-events/cybersecurity-advisories?page=0
31 https://www.reuters.com/world/americas/costa-ricas-alvarado-says-cyberattacks-seek-destabilize-country-government-2022-04-21/
32 https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a#:~:text=In%20September%202022%2C%20Iranian%20cyber,ties%20between%20Albania%20and%20Iran.
33 https://apnews.com/article/russia-ukraine-nato-technology-hacking-religion-5c2bd851027b56a77eaf9385b7d5d741
34 https://www.itworldcanada.com/article/nations-urged-to-be-responsible-in-cyberspace-after-meeting-in-vancouver/541968
35 https://www.cyber.gc.ca/en/alerts-advisories/understanding-ransomware-threat-actors-lockbit-joint-cybersecurity-advisory
36 https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed
37 https://attack.mitre.org/groups/G0032/
38 https://www.usna.edu/CyberCenter/_files/documents/Operation-Blockbuster-Report.pdf
39 https://www.cisa.gov/news-events/analysis-reports/ar20-133a
40 https://attack.mitre.org/software/S0154/
41 https://cyware.com/news/xtreme-rat-a-deep-insight-into-the-remote-access-trojans-high-profile-attacks-14dea04b
42 https://archive.f-secure.com/weblog/archives/00002356.html
43 https://www.cisa.gov/news-events/alerts/2022/04/22/fbi-releases-iocs-associated-blackcatalphv-ransomware
44 https://www.theverge.com/2021/5/18/22440813/android-devices-active-number-smartphones-google-2021
45 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/
46 https://cyware.com/news/spynote-infections-on-the-rise-after-source-code-leak-c5d36dce
47 https://www.threatfabric.com/blogs/spynote-rat-targeting-financial-institutions
48 https://github.com/DoctorWebLtd/malware-iocs/blob/master/Android.Spy.SpinOk/README.adoc
49 https://www.cloudsek.com/threatintelligence/supply-chain-attack-infiltrates-android-apps-with-malicious-sdk
50 https://news.drweb.com/show/?i=14705&lng=en
51 https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/mobile-premium-services
52 https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/
53 https://www.bleepingcomputer.com/news/security/microsoft-detects-massive-surge-in-linux-xord-dos-malware-activity/
54 https://blog.talosintelligence.com/prometei-botnet-improves/
55 https://unit42.paloaltonetworks.com/trigona-ransomware-update/
56 https://blog.cyble.com/2023/04/06/demystifying-money-message-ransomware/
57 https://www.rsaconference.com/library/presentation/usa/2023/macOS
58 https://blog.cyble.com/2023/04/26/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/
59 https://attack.mitre.org/groups/G0121/
60 https://nvd.nist.gov/vuln/detail/cve-2017-0199
61 https://nakedsecurity.sophos.com/2012/07/31/server-side-polymorphism-malware/
62 https://moderndiplomacy.eu/2023/03/26/breaking-diplomatic-norms-indian-response-to-oic-turkish-support-for-kashmir-issue/
63 https://www.3cx.com/blog/news/desktopapp-security-alert/
64 https://www.3cx.com/
65 https://www.3cx.com/blog/news/desktopapp-security-alert/
66 https://www.3cx.com/blog/news/mandiant-initial-results/
67 https://attack.mitre.org/software/S0634/
68 https://support.microsoft.com/en-us/topic/what-is-typosquatting-54a18872-8459-4d47-b3e3-d84d9a362eb0
69 https://www.cisecurity.org/insights/blog/malvertising
70 https://www.papercut.com/blog/news/rce-security-exploit-in-papercut-servers/
71 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27350
72 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a
73 https://www.bleepingcomputer.com/news/security/microsoft-clop-and-lockbit-ransomware-behind-papercut-server-hacks/
74 https://twitter.com/MsftSecIntel/status/1654610012457648129
75 https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled
76 https://www.cronup.com/ejercito-de-chile-es-atacado-por-la-nueva-banda-de-ransomware-rhysida/
77 https://izoologic.com/2023/06/19/rhysida-ransomware-exposes-stolen-data-from-the-chilean-army/
78 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
79 https://nvd.nist.gov/vuln/detail/CVE-2023-34362
80 https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/
81 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
82 https://www.alliedmarketresearch.com/mobile-banking-market
83 https://www.bankrate.com/banking/what-is-a-neo-bank/
84 https://blog.cyble.com/2022/12/20/godfather-malware-returns-targeting-banking-users/
85 https://www.cleafy.com/cleafy-labs/nexus-a-new-android-botnet#3
86 https://www.darkreading.com/endpoint/ai-black-mamba-keylogging-edr-security
87 https://www.darkreading.com/application-security/chatgpt-browser-extension-hijacks-facebook-business-accounts

BlackBerry | Cybersecurity

About BlackBerry: BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 235M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*