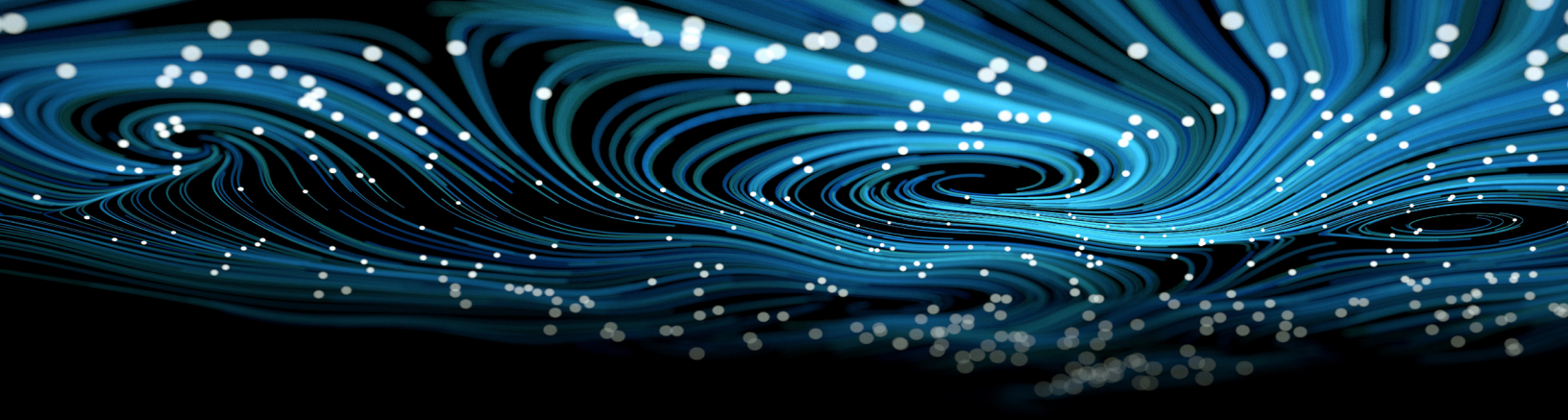
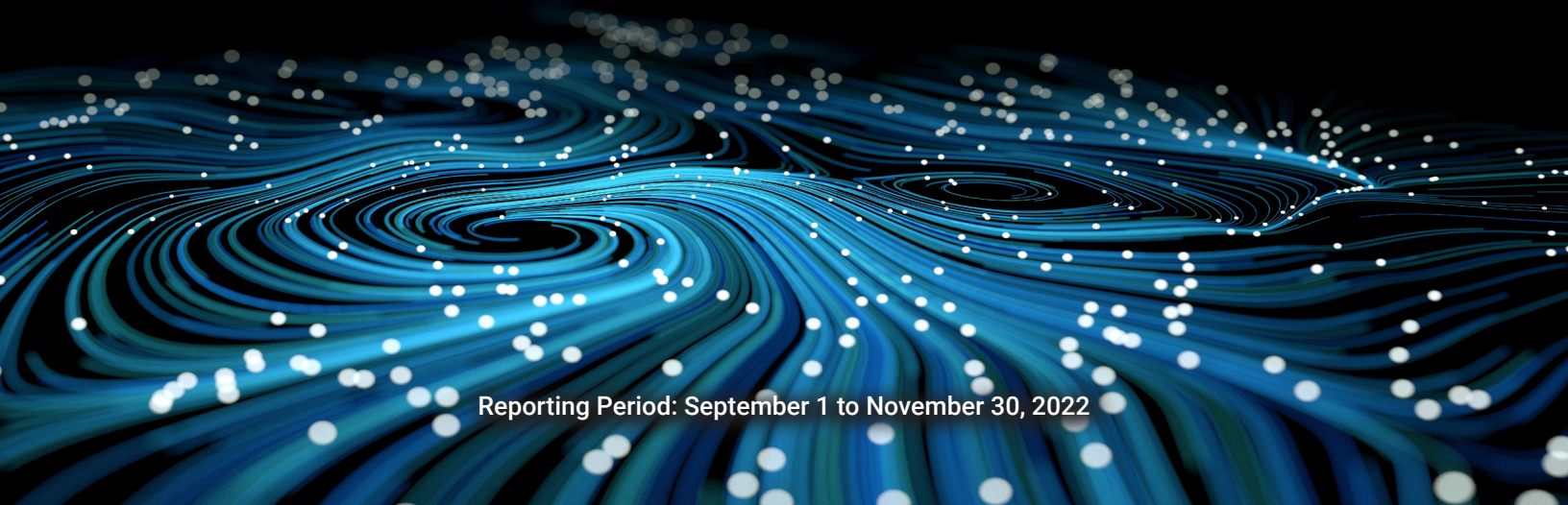


BlackBerry | Cybersecurity

GLOBAL THREAT INTELLIGENCE REPORT

DELIVERING ACTIONABLE AND
CONTEXTUALIZED INTELLIGENCE
TO INCREASE CYBER RESILIENCE



Reporting Period: September 1 to November 30, 2022

CONTENTS

INTRODUCTION

*THREAT INTELLIGENCE CAN BE CONSIDERED **"THE ART OF TAKING THE ADVERSARY BY SURPRISE."** ANTICIPATING, MITIGATING, AND PREVENTING SURPRISES IN THE FORM OF CYBERATTACKS IS THE PRIMARY MISSION OF A PRACTICAL THREAT INTELLIGENCE PROGRAM.*

Achieving that goal requires a proactive approach that answers critical questions like the following: Which threat actors are most likely to cause an impact in my organization? What are their motivations, goals, and capabilities? How do they behave, and what cyber-weapons do they use to achieve those goals? And most importantly, what actionable countermeasures can I deploy to improve my organization's cyber defense capabilities?

Our team is proud to release our first **BlackBerry Cybersecurity Global Threat Intelligence Report.** The mission of this report is to provide actionable intelligence on targeted attacks, cybercrime-motivated threat actors, and campaigns targeting organizations like yours so that you can make well-informed decisions and take prompt effective actions.

In this first edition, you'll find reports from some of the top threat researchers and intelligence analysts on the BlackBerry Threat Research and Intelligence team, world-class experts who understand not only technical threats but also local and global geopolitical developments and their impact on organizational threat models in each region. To produce this report (covering the 90 days between September 1 and November 30, 2022), the team leveraged data and telemetry obtained from our own artificial intelligence (AI)-driven products and analytical capabilities, complemented by other public and private intelligence sources.

Some of the research highlights in this report include:

- **90 days by the numbers.** An overview of the 90-day reporting period in statistics, including the number of unique malware samples that BlackBerry prevented from impacting our customers and the geographical distribution of those attacks. Here's a preview: our technology stopped an average of 62 new malicious samples per hour, or approximately one new sample per minute.
- **Most common weapons.** Information about the most common weapons used in cyberattacks, including the resurgence of malicious loaders like Emotet, Qakbot's extensive presence on the cyberthreat landscape, and the increase in downloaders like GuLoader.

- **Remote access increases infostealers.** With the post-pandemic rise of remote and hybrid work, the need to access internal networks from the outside has become widespread. Attackers are taking advantage of new remote access possibilities by using information stealers (infostealers) to steal corporate credentials to sell them on the black market. Our report discusses some of the most prevalent and widespread infostealers we saw deployed during this time period.
- **No platform is 'safe.'** Threat actors have multiple strategies for targeting different server, desktop and mobile platforms. For example, despite prevailing opinion, macOS is not a "safer" platform: macOS malware and vulnerabilities abound. Other topics covered include trends such as the increasing number of attacks against Linux platforms; the way that less mainstream programming languages like GoLang are being used to develop cross-platform malware; and an in-depth analysis of threats affecting mobile devices running Android and iOS.
- **Unique industry perspective.** Due to our strong presence in both the cybersecurity and Internet of Things (IoT) industries, BlackBerry is uniquely positioned to uncover threats to industries such as automotive that aren't often discussed in other threat reports. This edition includes information about cybersecurity trends we observed that will impact the automotive industry as well as the healthcare and financial industries.
- **Top threat actors and countermeasures.** Our telemetry also revealed the activities of many different threat actors. The report includes information about some of their most common tactics, techniques, and procedures (TTPs) as well as links to public lists of applied countermeasures mapped to MITRE ATT&CK and MITRE D3FEND. Our goal is to make it easier to update your organizational defenses and threat models based on this actionable information.
- **Wrapping up and looking ahead.** Finally, we present our conclusions and cyberthreat forecast for 2023.

I want to thank our **elite global researchers on the BlackBerry Threat Research and Intelligence team** who made this report possible and continue to produce numerous "first-to-market" research reports while continuously improving 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

Pedro Drimel

Jacob Faires

Dean Given

Eoin Healy

Geoff O'Rourke

Jose Luis Sanchez

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 NUMBER OF ATTACKS

In the 90 days between September 1 and November 30, 2022, Cylance® Endpoint Security solutions by BlackBerry stopped 1,757,248 malware-based cyberattacks. On average, threat actors deployed approximately 19,524 malicious samples per day against customers protected by our technologies. These threats included 133,695 unique malware samples, which translates to an average of 1,485 novel malware samples per day and 62 samples per hour: in other words, an average of roughly one new sample per minute.

The following graph shows the dynamics of potential cyberattacks that Cylance Endpoint Security solutions prevented between September 1 and November 30, 2022. The spikes during week 4 (September 29 to October 5) and week 7 (October 20 to October 26) were a result of threat actors reusing malware samples.

DYNAMICS OF PREVENTED ATTACKS

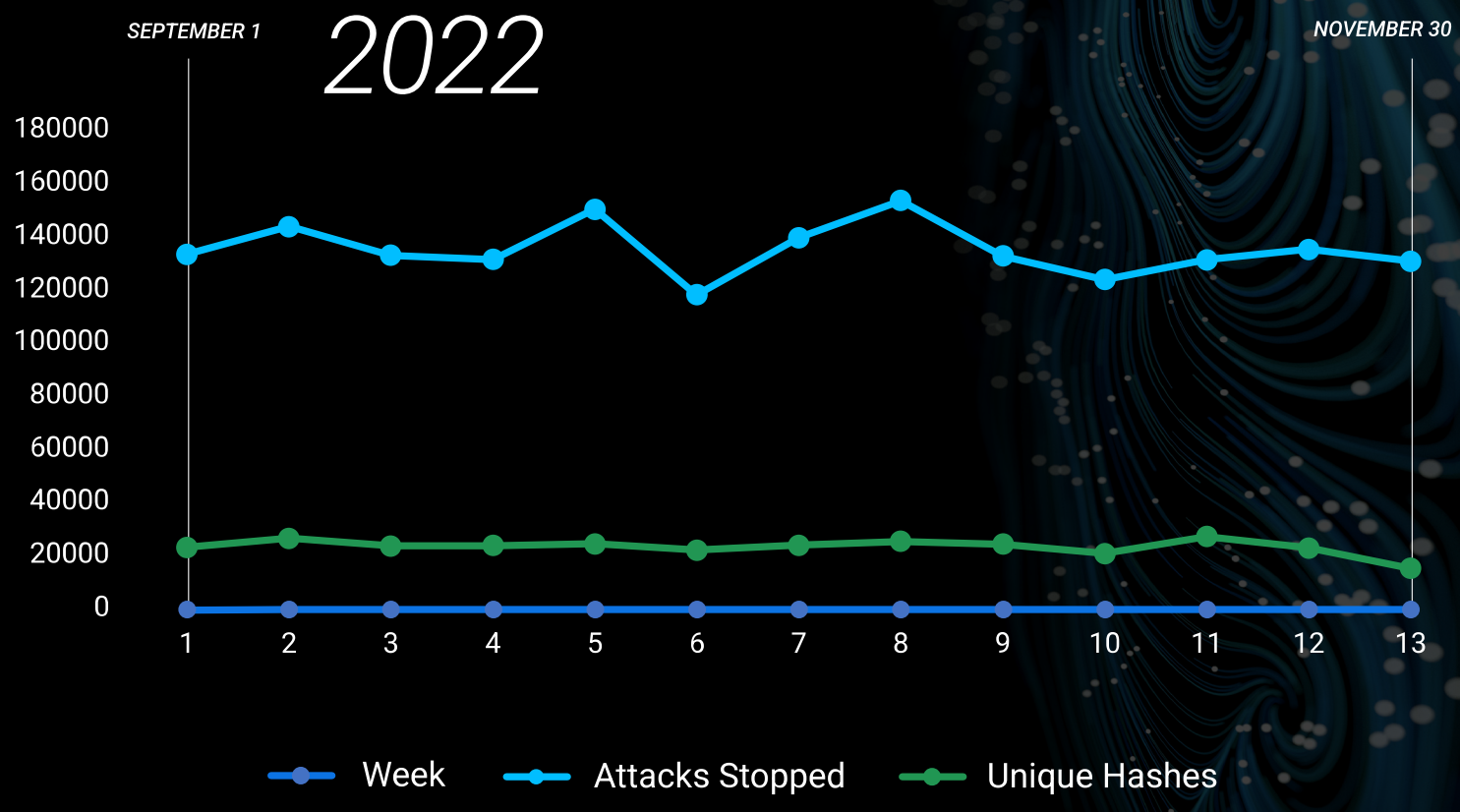
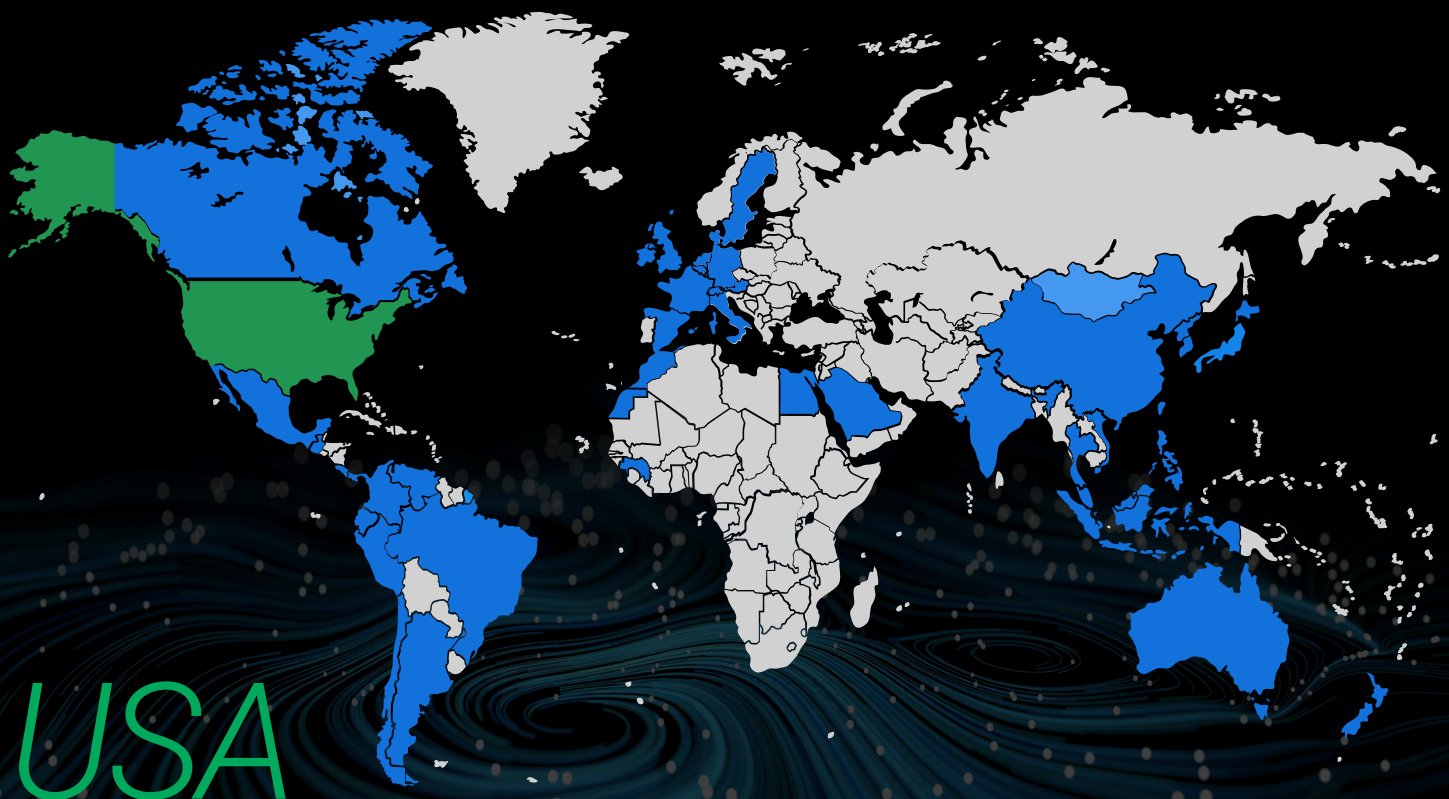


Figure 1: Cyberattacks prevented by BlackBerry per week from September 1 to November 30, 2022

GEOGRAPHY OF ATTACKS PREVENTED BY CYLANCE ENDPOINT SECURITY SOLUTIONS

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

COUNTRIES WHERE BLACKBERRY PROTECTED CUSTOMERS FROM CYBERATTACKS



USA

WAS THE MOST PROTECTED COUNTRY WITH ALMOST ONE MILLION ATTACKS STOPPED.

Figure 2: Countries where BlackBerry protected clients from cyberattacks. Darker blue represents more cyberattacks. Countries without blue shading do not currently contain a statistically significant number of BlackBerry clients.

FIGURE 3 SHOWS THE TEN COUNTRIES WHERE CYLANCE ENDPOINT SECURITY SOLUTIONS PREVENTED THE GREATEST NUMBER OF CYBERATTACKS.

TOP 10 COUNTRIES EXPERIENCING CYBERATTACKS IN Q4

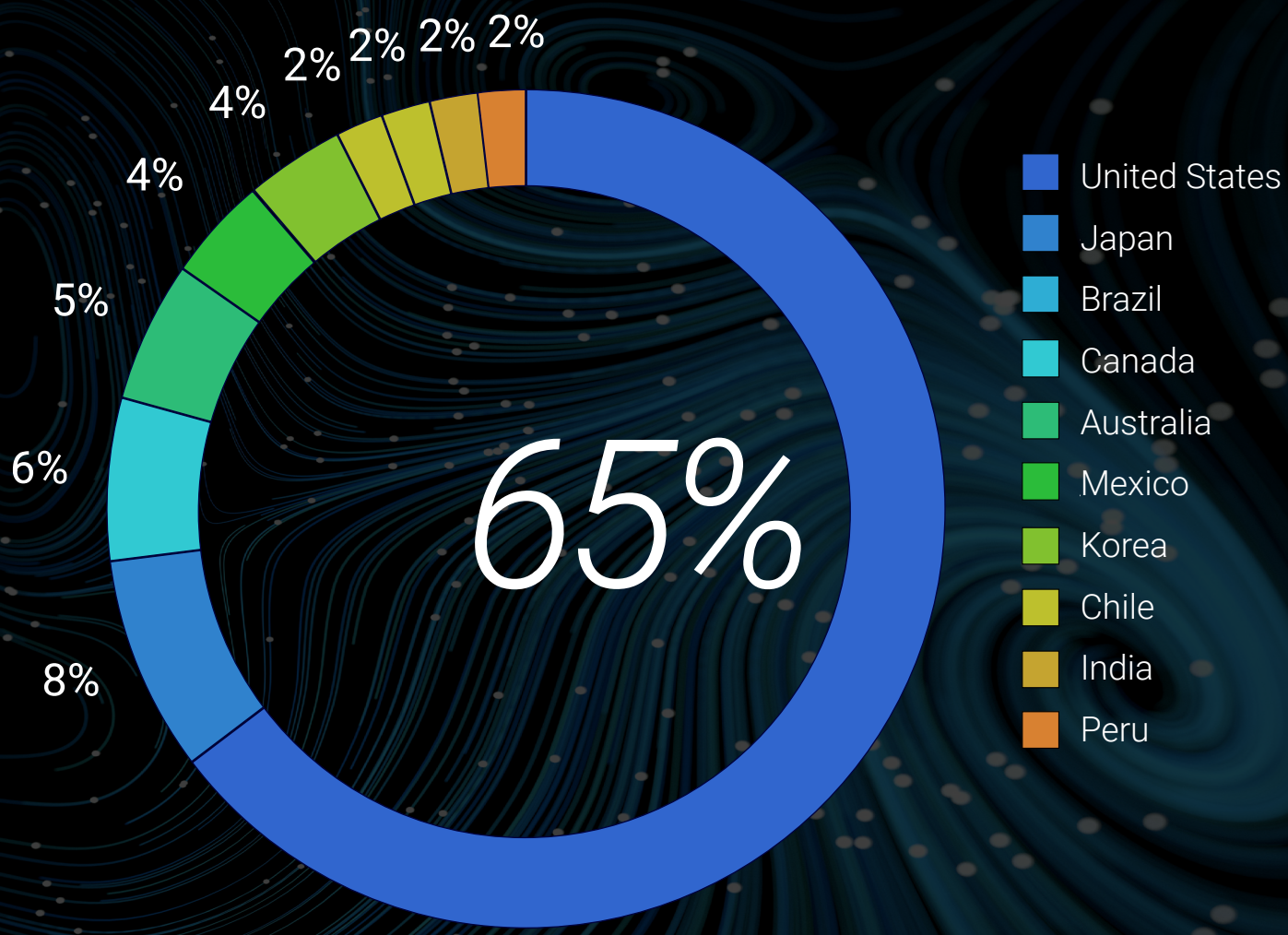


Figure 3: Top 10 countries where BlackBerry clients were targeted by cyberattacks

*FIGURE 4 SHOWS THE COUNTRIES WHERE BLACKBERRY CLIENTS WERE **MOST** FREQUENTLY ATTACKED WITH UNIQUE MALICIOUS SAMPLES.*

TOP 10 COUNTRIES WHERE UNIQUE MALWARE SAMPLES WERE USED

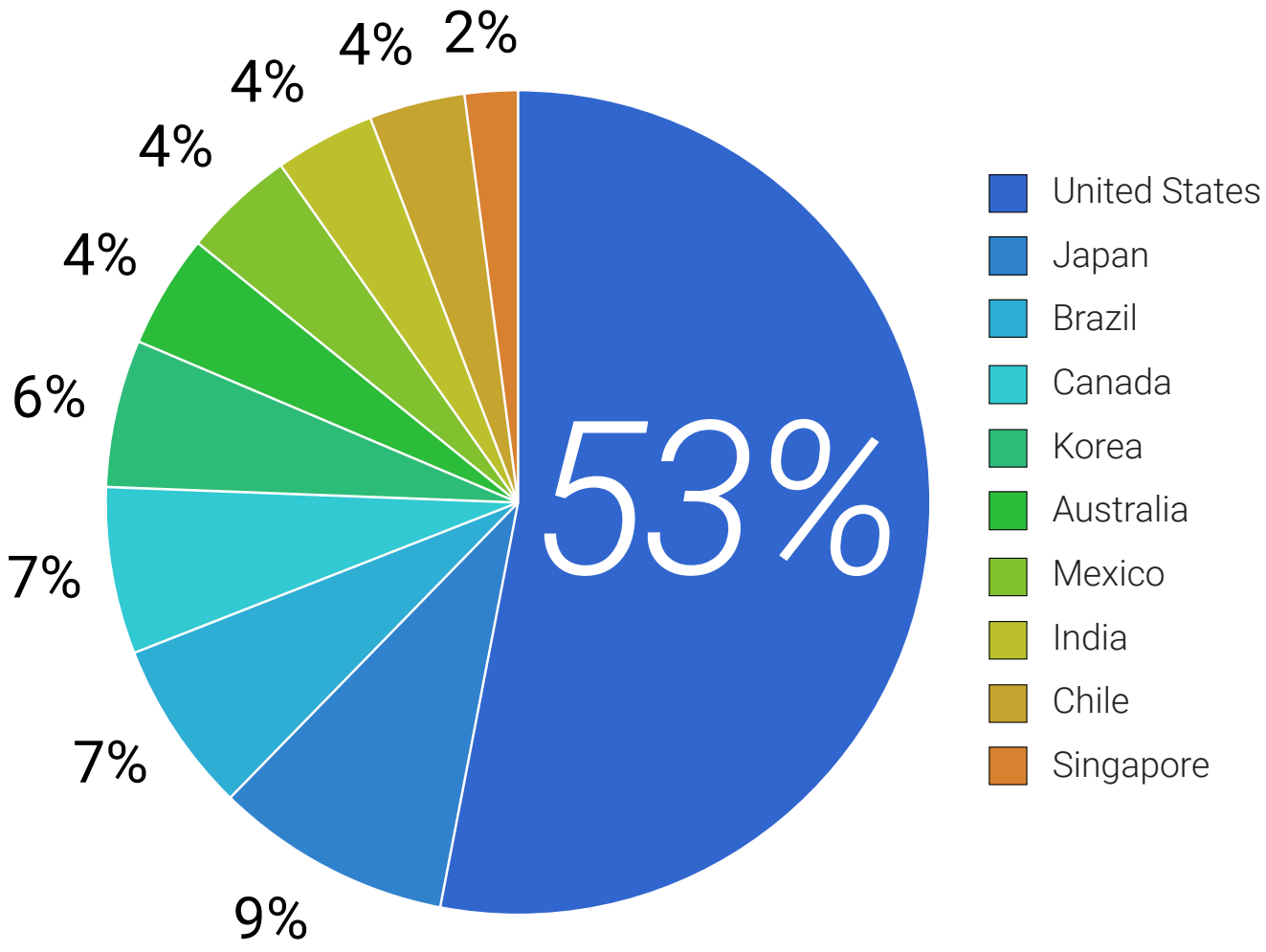


Figure 4: Top 10 countries where unique malicious samples were used in cyberattacks against BlackBerry clients

TYPES OF MALWARE

USED DURING ATTACKS IN THIS REPORTING PERIOD

Between September 1 and November 30, 2022, threat actors used a wide variety of malware to achieve their financial, geopolitical, military and tactical goals. The most widespread and interesting malware families identified are organized by operating system (OS) below.

It's important to note that while Windows® is still the most attacked OS, its users may be somewhat better prepared to face a malware attack than other OS users, who may still believe they are 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

While malware can run on any OS, Microsoft® Windows® remains the most commonly attacked. Reasons include the popularity of the OS, the wide range of documentation for developers, and the many years of cumulative experience in the cybercriminal community, where tips and tricks are frequently shared in forums.

Downloaders

Downloaders lure victims to open files that download malware. The files frequently pose as legitimate digital documents or executables. Common downloaders include the following:

- Emotet is one of the most prolific threats in current use. It first surfaced in 2014 and survived an April 2021 law-enforcement takedown, resurrecting at the end of 2021. This past quarter, Emotet resurged after a four-month hiatus, using previously seen techniques including a phishing campaign that distributed malicious Microsoft® Office documents. These documents attempt to persuade the victim to copy them into an official Microsoft directory, where macros are automatically executed without asking for the user's permission. Emotet has long been known for dropping the banking Trojan IcedID, which has strong connections with multiple ransomware groups.
- Qakbot is usually delivered through phishing techniques, using a lure email. The lure typically contains a LNK hyperlink that redirects to a malicious webpage containing a password-protected ZIP file that contains an ISO file. The LNK file executes a JavaScript file, which in turn executes a Qakbot malicious DLL with a .DAT extension. An interesting Qakbot feature is its use of existing email threads as a means of propagation. Its ability to "reply to" recipients can make intended victims believe that the link or attachment in the existing email thread is being sent from a trusted source. Qakbot is frequently used by many ransomware groups, and was associated this quarter with Black Basta, a possible Conti rebrand that targeted a rash of U.S.-based companies in 2022.

- GuLoader downloads and implements an executable from a remote location, and is frequently used to download and execute infostealers such as RedLine and Raccoon. GuLoader commonly abuses cloud-based services such as Google Cloud™ and OneDrive® to host its payloads; however, we have also detected it using Telegram bots.

Ransomware

LockBit remained the most active and successful ransomware-as-a-service (RaaS) used in 2022, and the 90 days covered in this report showed no signs that the threat group is slowing down. LockBit has now evolved to version 3.0, which uses several anti-debugging techniques that make it harder to analyze and string encryption and other techniques borrowed from the now-retired BlackMatter ransomware.

Infostealers

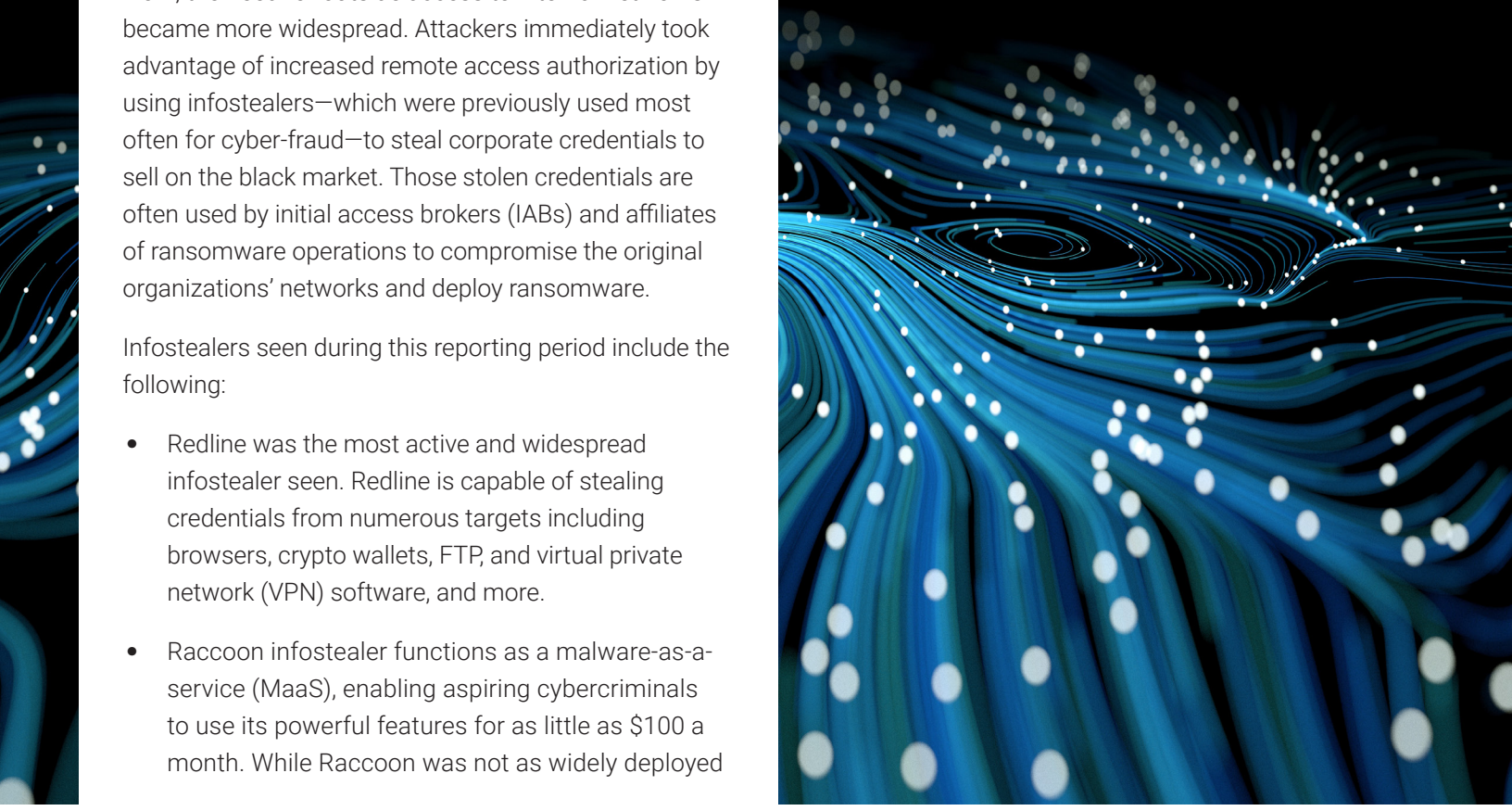
With the post-pandemic rise of remote and hybrid work, the need for outside access to internal networks became more widespread. Attackers immediately took advantage of increased remote access authorization by using infostealers—which were previously used most often for cyber-fraud—to steal corporate credentials to sell on the black market. Those stolen credentials are often used by initial access brokers (IABs) and affiliates of ransomware operations to compromise the original organizations' networks and deploy ransomware.

Infostealers seen during this reporting period include the following:

- Redline was the most active and widespread infostealer seen. Redline is capable of stealing credentials from numerous targets including browsers, crypto wallets, FTP, and virtual private network (VPN) software, and more.
- Raccoon infostealer functions as a malware-as-a-service (MaaS), enabling aspiring cybercriminals to use its powerful features for as little as $100 a month. While Raccoon was not as widely deployed

REDLINE

IS CAPABLE OF STEALING CREDENTIALS FROM NUMEROUS TARGETS INCLUDING BROWSERS, CRYPTO WALLETS, FTP, AND VIRTUAL PRIVATE NETWORK (VPN) SOFTWARE, AND MORE.



as Redline, it is still considered a potent threat. BlackBerry even detected cases where Raccoon was dropped by an initial Redline infection. Raccoon can steal credentials from crypto wallets, browser extensions, Discord, and Telegram; take screenshots; and act as a loader to launch additional payloads.

In September 2022, threat actors attempted to compromise Uber[1]. The attack was publicly attributed to affiliates of the Lapsus$ group. No ransomware was deployed in the Uber incident due to the company's swift actions to shut down the attack.

File Infectors

File infectors work by infecting other executable files and can spread through network shares or removable devices. The file infector Neshta was first identified in 2003 and is still observed decades later. Neshta has previously been associated with BlackPOS, a point-of-sale (POS) malware used to scrape credit card data from POS systems, which was highly prevalent in attacks against the consumer goods, energy, finance, and manufacturing industries in 2018. We published an in-depth report on Neshta in 2019 and have continued to observe similar traffic every year since then.

BLACKBERRY RESEARCHERS NOTED THAT A WHOPPING

34%

OF CLIENT ORGANIZATIONS USING MACOS HAD DOCK2MASTER ON THEIR NETWORK, WHERE IT WAS FOUND ON 26% OF THEIR DEVICES.

Remote Access Trojans

Remote access Trojans (RATs) can log keystrokes, access the user's webcam, steal browser credentials, and provide attackers a remote shell command-line program that can execute shell commands on the infected device as well as on other computers in the network. RATs observed during this reporting period include the following:

- njRAT was initially seen in 2015 and is still one of the most popular RATs in use today. It has been deployed by financially motivated threat actors as well as in more targeted attacks. njRAT's builder is widely available, making it easy for threat actors to adapt it to any desired attack model. It is commonly used by threat actors in the Middle East, and our proprietary telemetry identified an instance of njRAT with a command-and-control server (C2) hosted in Jordan.
- FlawedAmmyy, which appeared in 2018, is based on leaked source code of the valid remote access tool Ammyy Admin, which is used by both businesses and consumers to handle remote control and diagnostics on Microsoft Windows machines. While FlawedAmmyy was primarily attributed to cybercrime group TA505 (known for performing ransomware operations through its Cl0p ransomware), it is commonly used by multiple cybercrime threat actors.

MACOS/OSX

While macOS is not the most widespread corporate platform, it is being installed on a growing number of enterprise systems[2]. Although macOS has a reputation as a "safer" platform than Windows, macOS malware and vulnerabilities exist.

Adware/Spyware

Adware and spyware are by far the most widely seen threats that impact macOS. These applications masquerade as legitimate software, with the underlying intent to take advantage of the user. Unlike threats that are placed on computers by a targeted infection

campaign, users often install adware and spyware themselves because they believe them to be legitimate applications and they are unaware of the (often free) software's dangers. During the 90-day reporting period, the malicious application Dock2Master was the most-seen threat on macOS: BlackBerry researchers noted that a whopping 34 percent of client organizations using macOS had Dock2Master on their network, where it was found on 26 percent of their devices. Officially designated as a potentially unwanted application (PUA), Dock2Master surreptitiously injects ads directly into web pages that users visit and collects user and system data to sell on the underground market.

Browser Hijackers

Browser hijackers, which change a browser's search engine and manipulate other browser settings, aren't as prevalent as they were in the early 2000s, but they are still plentiful. While the most noticeable effect of a browser hijack is the user's default search engine changing without their consent, browser hijackers also may monetize the installation by stealing user identity information stored in browsers and injecting ads into displayed web pages. This quarter, active browser hijackers included OriginalModule and SearchInstaller, which uses InstallCore to target multiple platforms.

Proxy Malware and Agents

Proxy malware is a type of Trojan that turns an infected system into a proxy server that allows an attacker to execute actions on your behalf. Proxy agents are proxy malware that also add RAT-like capabilities, such as running local commands on infected machines. Proxy malware typically tends to support fewer functions than other malware types, allowing it to target a larger range of victims because fewer libraries are required. The GoLang programming language is used heavily in this class of malware because its support for proxy libraries like Proxit make development easy for novice cybercriminals.

BlackBerry has noticed the increasing use of GoLang to target macOS systems as part of a wider cross-platform attack against multiple platforms for opportunistic attacks like malicious spam (malspam). To operate effectively on multiple platforms, these attacks rely on simple functions that exist across all platforms. Most proxy malware samples observed are proxy agents that attack browsers that are available on multiple platforms.

LINUX

The Linux operating system is powerful, flexible, largely open-source, and ubiquitous: up to 90 percent of public cloud services run on Linux[3]. As a result, Linux is an appealing target for cybercriminals who rapidly weaponize and exploit weaknesses and vulnerabilities disclosed by vendors or other industry players.

Bots and Botnets

A bot is an autonomous program that executes commands without human intervention, and a botnet is a group of bots controlled by a single threat actor. Botnets are typically formed by taking advantage of a misconfiguration or unpatched vulnerability that allows installation of malicious code that adds the victim's computer to the botnet. Since the emergence of the now-infamous Mirai bot-network that conducted large-scale distributed denial-of-service (DDoS) attacks in 2016, more Linux botnets have emerged.

Noted Internet Relay Chat (IRC) botnets like ShellBot still lingered at the end of 2022, using brute-force tactics to enter systems via misconfigured or default credentials[4]. In addition, we've seen the Sysrv botnet abusing remote-code execution (RCE) flaws[5] via CVE-2022-22947[6] to compromise systems and grow their botnet at scale.

Malware and Tooling

BlackBerry observed and identified other malware and malicious tooling during this reporting period. SSH tooling (based on the secure shell protocol that enables remote access) is often dropped in tandem with malicious code to brute-force credentials and/or scan networks for propagation opportunities. During the

90-day reporting period, use of the tool Faster than Lite (FTL) increased. The tool is often abused by threat group OutLaw[7] and was noted to be bundled with ShellBot.

Our telemetry revealed similar campaigns deploying the GoLang-based SSH brute-force tool Spirit, which is also abused as a propagation tool. Spirit is typically dropped alongside the Pwnrig and Tsunami IRC bots, which we can attribute with reasonably high confidence to the hacking group 8220 Gang.

The now-infamous Log4j vulnerability was regularly abused by various malware families and threat actors during the reporting period. For example, the Kinsing Trojan abused the Java Log4j package vulnerability[8] CVE-2021-44228[9] for RCE on Linux platforms, and has been seen more recently abusing Oracle WebLogic Server vulnerability[10] CVE-2020-14882[11]. This Trojan attempts to disable a device's security and cloud service agents and kill any rival malware and cryptocurrency miners (crypto miners) on the victim system before deploying its own crypto miner.

Crypto Miners and Cryptojacking

Cryptojacking is a widespread scheme in which a threat actor installs malicious crypto mining software on a victim's device to mine cryptocurrency coins without the user's consent. Crypto miners have been a persistent plague on the cyberthreat landscape for the past decade. Crypto miners affect all major computing systems and can linger a long time before discovery.

Even though cryptocurrency in general lost value during the reporting period, deploying crypto miners at scale can generate tangible financial benefits for threat actors. Overall, despite the market changes, crypto is still king for many of these Linux-based threat actors.

This quarter, crypto miners made up a significant portion of the threats targeting Linux devices. The act of crypto mining has become more resource-intensive and therefore more costly. As a result, attackers have begun compromising the environments of multiple victims to deploy miners and misappropriate needed computing

THIS QUARTER, CRYPTO MINERS MADE UP A SIGNIFICANT PORTION OF THE

THREATS

TARGETING LINUX DEVICES.

resources. Both the previously mentioned ShellBot and the Sysrv bot infiltrate systems, deploy crypto miners, and hijack system resources.

Typically, crypto miners make their way onto a victim's environment post-compromise through a dropped payload or by exploiting a vulnerability such as CVE-2022-26134[12] (Atlassian Confluence) or CVE-2019-2725[13] (WebLogic), as frequently seen[14] with the PwnRig crypto miner. Crypto miners attempt to blend in with standard background resources such as cron jobs (which schedule routine tasks to repeat at specific times in the future) and remain undetected for as long as possible.

The quarter also revealed detections related to CryptoNight, a mining algorithm used to secure networks and validate transactions in some cryptocurrency such as Monero and Webchain, including a spike in the use of the Webchain miner as well as several XMRig-based miners. XMRig is a popular open-source utility commonly used to mine cryptocurrencies including Bitcoin and Monero, and is one of the most abused coin miners by threat actors today.

MOBILE DEVICES

Mobile devices continue to replace laptops and desktop computers for many functions, including electronic banking, mobile payments, messaging apps, and social networks. In fact, 59.54 percent of all Internet traffic in 2022 was generated by mobile devices[15].

Android

In 2022, nearly 71 percent of mobile devices worldwide used the Android™ operating system. Threats during the reporting period include the following:

- Lotoor is a tool that can be used for both benign and malicious purposes. Android owners can use Lotoor to root or unlock additional capabilities on their devices, but the tool can also be used to bypass Google's embedded security features and implant persistent malware.
- AdvLibrary infects devices to monetize Internet traffic by showing unsolicited ads and generating outgoing traffic on paid ads. Victims typically do not experience a direct financial loss, but they may incur additional expenses for increased data traffic. Cybercriminals generate income with AdvLibrary through clicks on ads and traffic to maliciously advertised sites.

iOS

iOS® is generally considered to be a more secure mobile OS than others. While zero-day iOS exploits are expensive and rarely used in uncontrolled attacks, iOS is not immune to exploits that "jailbreak" or unlock iPhone® devices, a potentially hazardous activity that removes original Apple® security features and provides complete access to the device. While some owners intentionally jailbreak their iPhones for purposes like removing unwanted default apps, jailbroken phones are vulnerable to attacks.

Many levels of threat actors rely on iPhone jailbreaks to deploy implants onto victims' devices. For example, Vortex is a potentially malicious malware family that targets iOS users. Like Lotoor for Android, Vortex is a rooter that can jailbreak iPhones that cybercriminals can use to install malware. This technique is most common among mid-level threat actors without the technical capability to launch zero-day threats. In the past quarter, BlackBerry saw at least two different versions of Vortex intended to jailbreak iOS devices.

INDUSTRY-SPECIFIC ATTACKS

While every industry is susceptible to cyberattacks, the automotive, healthcare, and financial industries present unique opportunities for cybercriminals.

AUTOMOTIVE

The century-old automotive industry is in the midst of a major technological revolution. Breakthrough technology advances are enabling the development of new types of vehicles, systems, and services. This digital transformation offers many benefits but has also introduced new cybersecurity challenges.

As vehicles become more connected and autonomous, they become potentially more vulnerable to cyberthreats and threat actors. In addition, the increasingly complex manufacturing systems that produce vehicles are also at risk of cyberattacks.

In previous years, the automotive industry was relatively unaffected by large-scale and highly publicized threats. However, malicious entities have begun targeting not only automobile manufacturers but the industry as a whole through efforts to disrupt operations, steal sensitive data, and compromise supply chains. In 2022, we observed an increase in both the number of malicious entities targeting the auto industry and the amount of disruption that they cause.

To protect against these threats, companies in the automotive industry must recognize the potential risks inherent in a more connected automotive future and implement strong cybersecurity measures to protect vehicles and drivers.

Recent Threat Trends

Because of its global scale, the automotive industry presents an immense number of endpoints to monitor and protect. It includes every organization in the value chain, from companies that source raw building materials all the way up to automotive dealerships and automobile owners. The vast digital attack surface of this complex supply chain must be secured to keep this important global business operational.

Attacks between September 1 and November 30, 2022 ranged from sophisticated spearphishing to commodity malspam, indicating that the automotive industry is constantly under attack from both advanced and novice cyber adversaries.

Downloaders

Malware downloaders are prevalent in almost every type of cyberattack, and can vary in appearance, file type, and relative sophistication of the techniques they use to enter systems. Deceptive threat actors coax unwitting victims to install the downloader as the first part of a cyberattack. Once the code is executed, downloaders install additional malicious code and payloads to carry out more wide-reaching cyberattacks.

GuLoader is a prime example of a downloader that targeted the automotive industry during this reporting period. The malware was first identified in 2019 and continues to evolve. GuLoader often poses as legitimate digital documents or executables before downloading other commodity malware.

Infostealers

The automotive industry's valuable and often proprietary data makes the industry a prime target for cyber thieves. This data is a commodity that can often be more valuable than the vehicles themselves.

Malware infostealers are a type of malicious code that seeks out and illicitly exfiltrates data from a victim's system that can then be used to support financial and/or tactical goals. Infostealers can be used in conjunction with RATs like Remcos as commodity malware that is often sold as a service for other threat actors to gain malicious access and control of victim systems.

Ransomware

Ransomware is every security team's nightmare, and threat actors know that ransomware targeting industry supply chains can be devastating. In the automotive industry, a ransomware attack at any stage of the supply chain could cease production or distribution, causing loss of revenue and reputation throughout the industry's ecosystems.

BlackCat ransomware was observed in some of the more notorious ransomware attacks throughout 2022. Often preying on small- to medium-sized business, the cybercrime groups who use this particular RaaS appear to be largely financially motivated and have largely targeted manufacturing. BlackCat ransomware infiltrates an environment, exfiltrates valuable data, and then encrypts connected systems.

ALPVH (the threat group behind BlackCat ransomware) frequently uses double-extortion ploys, often publicizing compromised victims' data via their leak site (a website that hosts stolen private and potentially sensitive documents). Their goal is to pressure the targeted organization to pay the ransom, capitalizing on the fear that more valuable data will be published or sold to competitors[16].

Dual-Use Tools

Dual-use applications are typically legitimate tools and software that offer features or functions that threat actors can potentially misuse or abuse. The term "living off the land" (LotL) describes the actions of threat actors who abuse legitimate tooling to bypass security systems and avoid detection.

Threat actors increasingly rely on dual-use tools instead of malicious code to propagate within an environment, exfiltrate valuable data or even deploy malware as an "allowed" tool. System administrators should remove all dual-use tools for which there are no valid use cases or business justification.

Wider Automotive Threat Landscape

Because of the proliferation of "smart" and Internet-connected features in modern cars and the advent of software-defined vehicles (SDVs) that receive and manage new features through software updates, vehicles present an increasingly enticing attack surface for threat actors. In fact, estimates show that that there will be as many as 775 million connected cars on the road by 2023[17]. The number of attempted cyberattacks is likely to increase because adversaries know that disruptions of any kind cannot be tolerated during production, manufacturing, shipping, and sales.

Various types of direct attacks on vehicles have occurred in the last few years, and keyless-entry-enabled vehicles have been shown to be particularly vulnerable.

48%

OF CAR THEFTS WERE VEHICLES EQUIPPED WITH KEYLESS TECHNOLOGY.

In fact, data from U.K.-based insurance company LV= General Insurance shows that 48 percent of car thefts were vehicles equipped with keyless technology[18]. Europol announced in October 2022 that it dismantled a European car theft ring that targeted keyless-entry and keyless-start vehicles, using fraudulent software to steal vehicles without a physical key fob[19]. (The disclosure occurred after the exploit was reported and patched.)

Overall, the automotive industry has suffered a near-continuous string of cyberattacks over the last five years, including data breaches, ransomware, and attacks by advanced persistent threat (APT) groups. The number of threats spiked in 2022 and is likely to continue because of the proliferation of embedded technology in new vehicles.

For example, in 2017, an automobile manufacturer fell victim to WannaCry ransomware[20], which forced them to briefly halt production. In 2019, the group APT32 (also known as OceanLotus) emerged[21], which some sources link with providing support to Vietnam's automotive sector[22]. The same group also targeted and compromised other automotive manufacturers' networks[23]. From 2020 to 2022, the number of attacks (predominantly ransomware) increased. In 2022, notable ransomware attacks affected one of Europe's biggest car dealerships[24], a Dutch specialist vehicle manufacturer[25], and an American tire manufacturer[26].

The figure below shows a timeline of a sample of larger attacks reported within the auto industry in 2022.

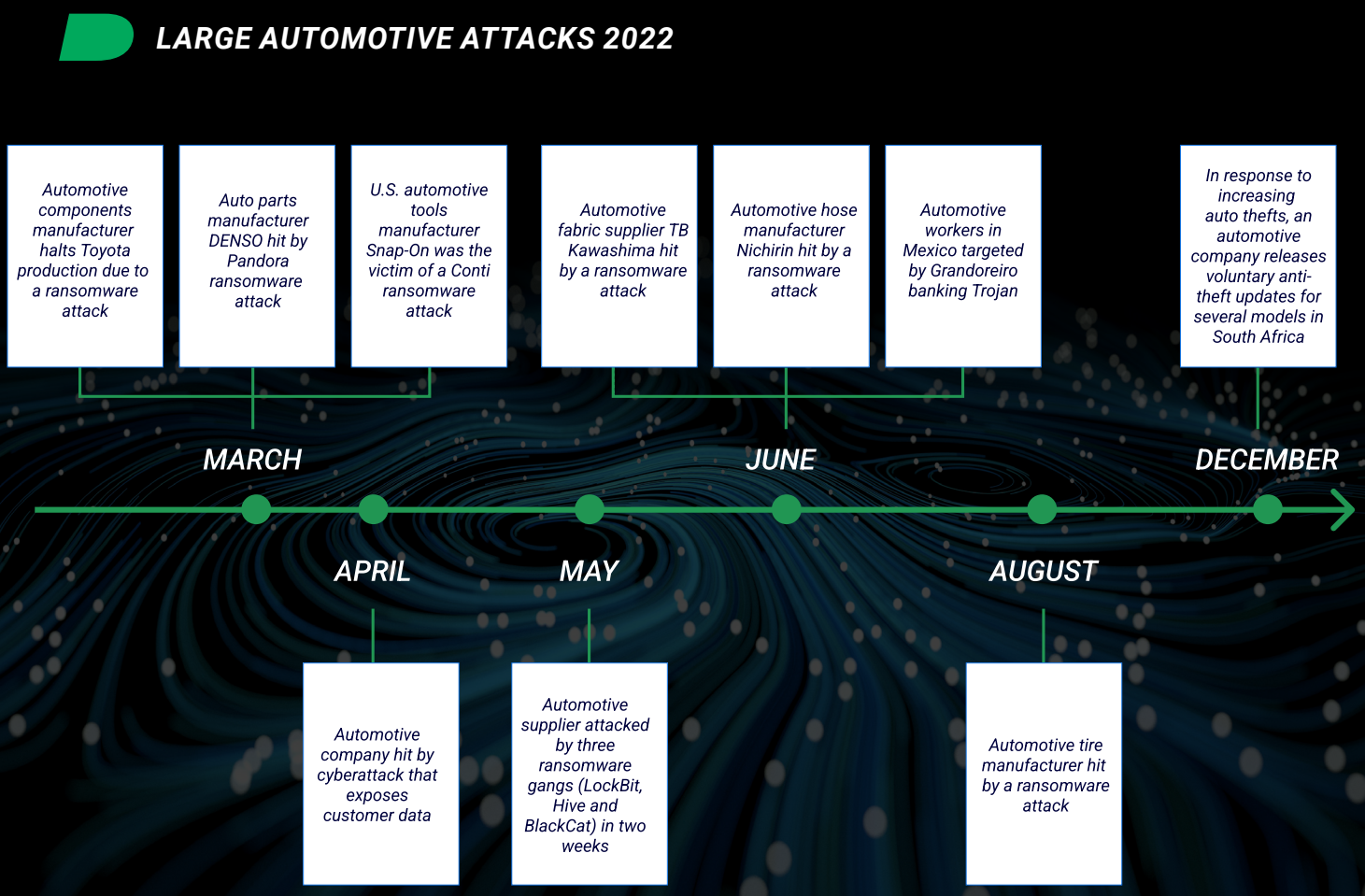


Figure 5: Timeline of larger automotive attacks in 2022.

Supply-Chain Attacks

Both the pandemic and the Russian invasion of Ukraine have revealed that supply chains are fragile. The automotive industry is not immune to the delays, shortages, and disruptions that other industries face.

Given the complexities of the industry, many businesses rely on a just-in-time (JIT) supply-chain strategy to maintain their vast ecosystems of vendors, parts, and manufacturers, creating an extremely large attack surface that can potentially be exploited by threat actors. The hallmark of JIT strategy is that products are not manufactured until they are needed. As a result, manufacturing may be slowed or stopped if needed components and materials are not immediately available. As a result, a cyberattack within the supply chain can effectively halt automobile production.

Instead of directly targeting auto manufacturers, which may be heavily fortified against intrusions, malicious adversaries may instead attack its various vendors, especially those with less cybersecurity. For example, in March 2022, compromised file systems at plastic and electronic supplier resulted in production delays for an estimated 13,000 vehicles at a Japanese automotive company. According to a spokesperson quoted by Automotive News Europe, the automotive company's supply chain includes 60,000 companies across four tiers[27]. Cyberattacks anywhere in a supply chain of that size can potentially impact the ability of other companies to receive necessary parts and materials.

Trends for the Future

As discussed above, the automotive industry's sprawling supply chains and business ecosystems present attractive targets for cyberattacks. However, the industry is taking steps to build greater security and resilience. In 2022, the Swedish state-backed research institute RISE announced the launch of the RISE Cyber Test Lab for Automotive Cyber Security, which is designed to be Europe's most advanced hub for automotive cybersecurity. It plans to start advanced testing in 2023.

In addition, NHTSA's Cybersecurity Best Practices for the Safety of Modern Vehicles, updated in 2022, strongly recommends vehicle manufacturers and suppliers to protect, detect, and respond to cyber risks across the whole vehicle lifecycle[28]. This guidance is supported by the global automotive cybersecurity engineering standard ISO/SAE 21434.

HEALTHCARE

The healthcare industry is facing an increasing number of cyberthreats as threat actors target healthcare organizations for their highly confidential data and valuable information. This is a significant issue for healthcare providers, as a successful cyberattack can have serious consequences including the loss or publication of sensitive patient data, financial losses, and even direct physical harm to patients. Healthcare is particularly vulnerable to these threats due to a combination of factors including the widespread use of medical technology with a long service life, the complex and often interconnected nature of healthcare systems and the vast amounts of sensitive data that are routinely collected and stored. It is imperative that healthcare providers understand the dangers of the current cyberthreat landscape and proactively protect themselves and their patients from potential harm.

Overall, ransomware still poses the biggest threat to the healthcare industry, and threat groups that rely on ransomware are still very actively targeting it, as we can see by the ransomware attack on CommonSpirit Health in October, where data belonging to more than 600,000 patients was compromised[29]. In the past, some RaaS groups like Maze indicated they would not attack hospitals, but such promises cannot be guaranteed. With the diversity of multiple RaaS groups and the proliferation of affiliate models, the group that executes an attack may not be the same group that developed the malware, which makes tracing and attribution a concern.

According to our telemetry, Cylance Endpoint Security solutions stopped 7,748 unique malware samples targeting the healthcare industry during this reporting

600,000

PATIENTS' DATA WAS COMPROMISED IN THE RANSOMWARE ATTACK ON COMMONSPIRIT HEALTH IN OCTOBER.

period, accounting for an average of more than 80 unique malware samples per day. The most popular Trojan was Qakbot, which has been used by cybercriminals since at least 2012 and poses a high risk to the healthcare industry. In 2022, Qakbot was mostly used by affiliates deploying Black Basta ransomware. Because Emotet did not operate many campaigns after its recent four-month shutdown and TrickBot seems more focused on improving its Bumblebee malware, we believe that Qakbot continues to be the most active Trojan facilitating healthcare network access for RaaS affiliates and IABs.

Meterpreter (a Metasploit payload that provides an interactive shell for the attacker) and BloodHound were also active during this timeframe. We detected an attack that used Meterpreter alongside the execution of SharpHound, a collector for BloodHound that is commonly used for lateral movement inside a network after an attack takes place. The Cybersecurity and Infrastructure Security Agency (CISA) recommends that network and system administrators intentionally execute BloodHound themselves to understand possible attack paths on their environments[30].

We also observed TinyNuke dropping the Netwire RAT. Originally a banking Trojan with similar functions as ZeuS, TinyNuke is a fully featured Trojan that includes the VNC server device controller and reverse SOCKS functionality. TinyNuke has also been used by Kimsuky Group[31] and attributed to the Democratic People's Republic of Korea (DPRK). While examining this attack, we found TinyNuke downloading and executing Netwire RAT and connecting to a domain hosted on DuckDNS, which is commonly used by RATs.

BlackBerry researchers also found an instance where an unknown threat actor deployed the PlugX RAT, which is commonly used by multiple nation-state threat actors including Mustang Panda (learn more in our public report), indicating that both cybercriminals and nation-state actors are interested in attacking the healthcare industry. And, while we haven't seen infostealers like Redline and Raccoon specifically targeting healthcare, we did encounter an instance of GuLoader, a downloader commonly used by cybercriminals to deploy infostealers.

THE FINANCIAL INDUSTRY

The financial industry has historically been targeted by cybercriminals as well as nation-state threat actors who reside in areas affected by financial sanctions. During this 90-day reporting period, Cylance Endpoint Security solutions stopped 9,721 unique malware samples launched against targets in the financial industry, with an average of about 108 unique malicious samples identified per day.

Different threat actors, including nation-state actors, have relied on commercial penetration testing (pen testing) tools like Cobalt Strike and others to blur the attribution line between cybercriminals and legitimate testing activities. This confusion gives cybercriminals more time

to operate within a network after they gain access. In 2022, we witnessed several incidents where commercial adversary-simulating software including Cobalt Strike and pen testing software Metasploit, Mimikatz, and Brute Ratel were used inside financial institutions. Brute Ratel is an adversarial attack simulation tool, and attackers and security professionals both commonly use Mimikatz to extract confidential information such as passwords and credentials from a system's memory. At this time, it is not known whether the presence of Mimikatz and Brute Ratel were part of legitimate pen testing activities or real attacks.

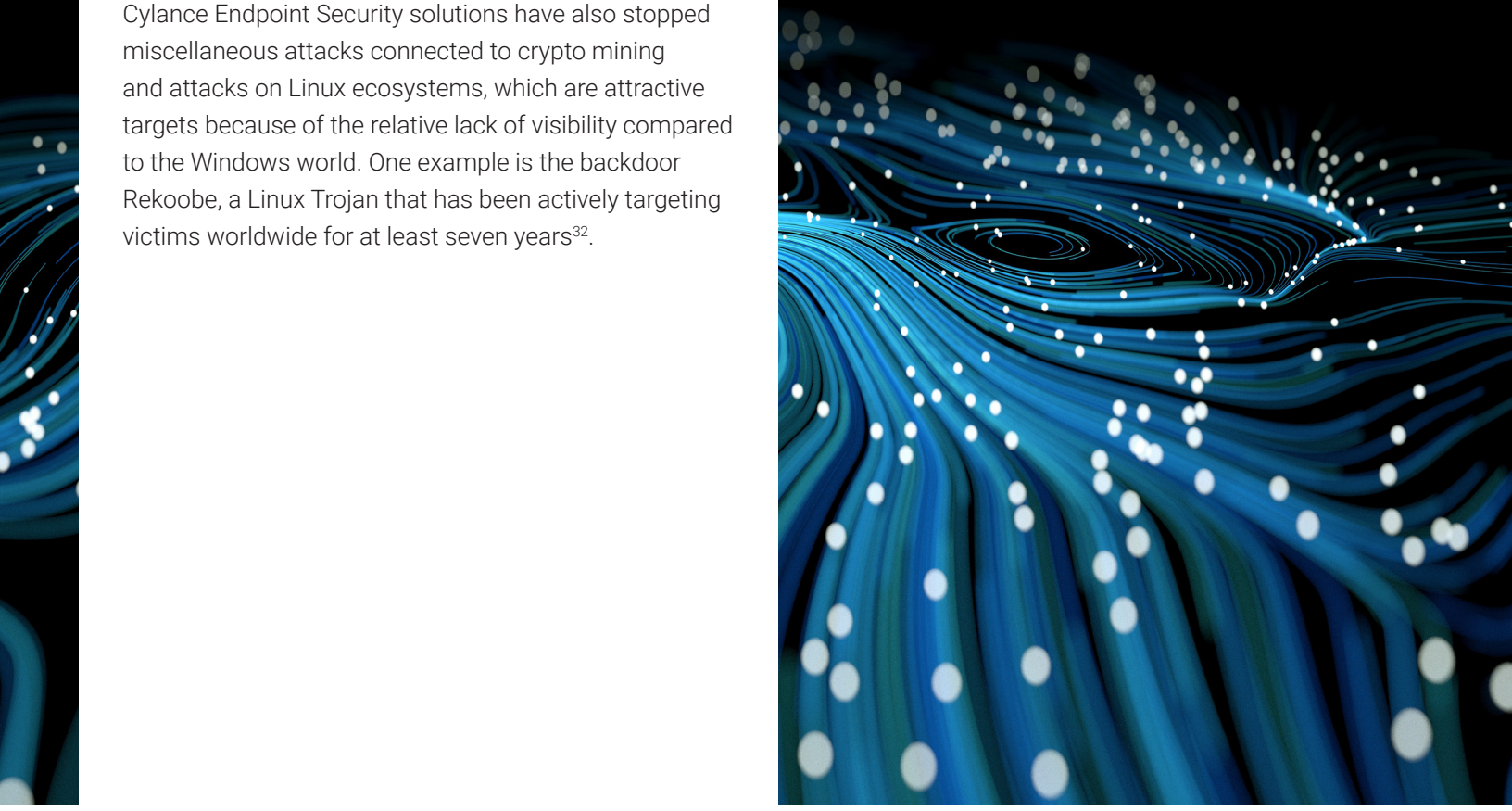
Among other top threats, we stopped initial-access infostealers such as Redline Stealer. It is publicly known that initial access tools are in high demand because they gain access to victims' networks that can then be sold. Many threat actors, including the Lapsus$ group, rely on infostealers to gain access to enterprises. (The Lapsus$ group is an international extortion-focused threat group known for numerous cyberattacks against companies and government agencies.)

Cylance Endpoint Security solutions have also stopped miscellaneous attacks connected to crypto mining and attacks on Linux ecosystems, which are attractive targets because of the relative lack of visibility compared to the Windows world. One example is the backdoor Rekoobe, a Linux Trojan that has been actively targeting victims worldwide for at least seven years[32].

CYLANCE ENDPOINT SECURITY SOLUTIONS STOPPED

9,721

UNIQUE MALWARE SAMPLES LAUNCHED AGAINST TARGETS IN THE FINANCIAL INDUSTRY.



MOST ACTIVE THREAT ACTORS

Our telemetry revealed the activities of many different threat actors. Some of the attackers included in this section were mentioned in the preceding sections about specific types of attacks or industry sectors.

TA505

TA505 is an active and influential cybercrime group with significant impact in the world of financially motivated cyberthreats. The group's targets include education, finance, healthcare, hospitality, and retail worldwide.

They are known for sending large volumes of malicious email and have a wide range of malware at their disposal, indicating strong connections to underground malware networks. Currently, the group continues to use Locky ransomware as their primary tool for attacks, but it has also been known to experiment with other types of malware.

TA505's toolset includes Cl0p ransomware, the FlawedAmmyy RAT (which was based on leaked source code for a version of legitimate tool Ammyy Admin), and banking Trojans like Dridex.

ALPHV

ALPHV is a relatively new and rapidly growing cybercrime group that has gained attention for innovative extortion tactics and unconventional attack methods. Despite its relatively short history, the group has made a significant impact in the cybercrime community and is likely to continue to evolve and expand its operations[33].

ALPHV is well known for using Rust, a powerful programming language that allows the threat operator to use one code base on many different operating systems. The group uses multiple LotL binaries, scripts, and libraries (LOLBins) to achieve their objectives.

BlackCat RaaS is deployed as part of the final stage of ALPHV hacking campaigns after the group has completed lateral movements within specific hosts and collected all the information they were seeking. ALPHV then begins financial extortion, and has even threatened to carry out DDoS attacks to coerce victims to pay the ransom. With the release of BlackCat ransomware as a RaaS, the hacking group has joined the rapidly growing malware trend of double-extortion attacks that both exfiltrate data and encrypt data for ransom.

The ALPHV group does not appear to target a specific sector or country. Because ALPHV allows other threat actors to use BlackCat ransomware, the presence of the malware does not necessarily indicate a direct attack by ALPHV. To date, BlackCat ransomware has struck retail, financial, manufacturing, government, technology, education, and transportation in countries that include the U.S., Australia, Japan, Italy, Indonesia, India, and Germany[34].

APT32

APT32 is believed to be based in Vietnam and has conducted malicious cyber activities since at least 2014. Its targets have included various private industries, foreign governments, and individuals like dissidents and journalists, with a particular focus on Southeast Asian nations including Vietnam, the Philippines, Laos, and Cambodia. APT32 frequently employs tactics such as strategic web compromise to gain access to victims' systems. This sophisticated group has also attacked defense organizations, high-tech companies, healthcare, and manufacturing.

The BlackBerry Threat Research and Intelligence team has analyzed multiple APT32 intrusions. The group has used a suite of RATs dubbed Ratsnif to leverage new network attack capabilities. We also identified the group's use of steganography (the technique of hiding secret data within an ordinary, non-secret file or message) to embed a malicious payload in a PNG image.

APT29 (THE DUKES)

APT29, also known as the Dukes, are a well-funded and highly organized group suspected of conducting cyber espionage on behalf of the Russian government since at least 2008. The group particularly targets governments and non-governmental organizations in North America and Europe; however, entities across Asia, Africa, and the Middle East have also been attacked.

The group frequently uses Cobalt Strike, Mimikatz, and AdFind (a free command-line query tool that can be used to gather information from Active Directory). The group has also developed a set of custom tools that includes CloudDuke, CozyDuke, and FatDuke, among others. In addition, APT29 is known to exploit vulnerabilities affecting some products to access their victims' systems.

MUSTANG PANDA

Mustang Panda is a China-based APT group that has been identified as a cyber espionage threat actor. The group was first detected in 2017 and may have been active since 2014[35]. Mustang Panda has targeted a wide range of organizations including government agencies, nonprofits, religious institutions and non-governmental organizations (NGOs) in countries around the world including the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam.

The group frequently uses China Chopper and PlugX for its operations. PlugX is a modular RAT that can be configured to use both HTTP and DNS for command-and-control (C2) activities. China Chopper is malicious software hosted on web servers that allows unauthorized access to an organization's network and does not require an infected device to communicate with a remote C2 server.

The BlackBerry Threat Research and Intelligence team has also discovered recent activity in which Mustang Panda used global interest in the Russian-Ukrainian war to attack targets in Europe and Asia Pacific regions.

TA542

The cybercriminal group TA542 is believed to have played a significant role in creating the Emotet malware. This malware was first discovered in mid-2014 and shares certain characteristics with the Bugat (also known as Feodo) banking Trojan, enhanced with the addition of an RSA key exchange for C2 communication and a modular design. TA542 does not follow the typical behavior patterns of cybercriminal organizations and generally carries out attacks for a short period of time, after which they take a break for several months before returning with a new version or variant of the malware. Targets of TA542's campaigns include the education, financial, retail, and healthcare industries.

COMMON MITRE TECHNIQUES

The BlackBerry Threat Research and Intelligence team utilizes multiple MITRE techniques, event analysis and telemetry to analyze threats. Common MITRE techniques used during this reporting period are listed in the following table. A full list of MITRE techniques used by the BlackBerry team is located in the MITRE ATT&CK® Navigator Layer.

TABLE 1: COMMON MITRE TECHNIQUES AND TACTICS

MITRE Technique	Technique ID	Tactic
System Information Discovery	T1082	Discovery
Process Injection	T1055	Defense evasion
Virtualization/Sandbox Evasion	T1497	Defense evasion
Remote System Discovery	T1018	Discovery
Masquerading	T1036	Defense evasion
Application Layer Protocol	T1071	Command-and-control
Software Packing	T1027.002	Defense evasion
Security Software Discovery	T1518.001	Discovery
Process Discovery	T1057	Discovery
Disable or Modify Tools	T1562.001	Defense evasion
Application Window Discovery	T1010	Discovery
Windows Management Instrumentation	T1047	Execution
Query Registry	T1012	Discovery
Obfuscated Files or Information	T1027	Defense evasion
Modify Registry	T1112	Defense evasion
File and Directory Discovery	T1083	Discovery
Encrypted Channel	T1573	Command-and-control
Command and Scripting Interpreter	T1059	Execution
Rundll32	T1218.011	Defense evasion
Regsvr32	T1218.010	Defense evasion

Most of the techniques listed are related to defense evasion and discovery tactics. In general, these tactics and related techniques are uncovered during a post-mortem after an infection—use of these techniques requires knowledge of previously identified intrusions. Sample behaviors associated with the five most common techniques are listed below.

SAMPLE BEHAVIORS OF COMMON TECHNIQUES

The following table lists the behaviors associated with the most common MITRE techniques.

TABLE 2: SAMPLE BEHAVIORS OF COMMON TECHNIQUES

Technique	Behaviors
System Information Discovery - T1082	> wmic csproduct get UUID > query user > tasklist | findstr "dll" > systeminfo >> output > date /t
Process Injection - T1055	> dllhost.exe > rundll32.exe > explorer.exe > MSBuild.exe
Virtualization/Sandbox Evasion - T1497	> timeout 5000 > Start-Sleep -s 100 > Check for registries of VMWare and VirtualBox
Remote System Discovery - T1018	> net group /domain admins > nltest /domain_trusts /alltrusts > net view /all
Masquerading - T1036	> Renaming the malware filename as a legitimate-sounding filename > Use of .jpg extension for binaries > Use scheduled tasks with legitimate names like win32times and others

MITRE D3FEND COUNTERMEASURES

Understanding common countermeasures can help organizations improve their defensive strategies and determine whether adequate visibility and/or detection techniques are in place. Countermeasures can be based on OS events (such as process events that occur in the system) or file events (such as creating, modifying, or deleting files).

A complete list of attack techniques and associated countermeasures is located in our GitHub repository. We recommend choosing only countermeasures that you can fully implement and that best meet your organization's needs.

MOST SOUND ATTACKS

FOR A COMPLETE LIST OF ATTACK TECHNIQUES AND ASSOCIATED COUNTERMEASURES VISIT THE BLACKBERRY GITHUB REPOSITORY.

Between September 1 and November 30, 2022, the BlackBerry Threat Research and Intelligence team tracked, uncovered, researched, and published the latest information about the cyberthreat landscape around the world. The world economy is still recovering in the aftermath of the COVID-19 pandemic, and current geopolitical events in Eastern Europe and East-West relations continue to be uncertain. These factors converge to create fertile soil for threat actors that attempt both politically motivated and financial exploits.

This quarter, we saw state-affiliated APT groups, financially motivated ransomware gangs, and many other threat actors of all sizes, capabilities, and motivations conducting multiple campaigns. Below is a selection of some of the most consequential attacks across the global landscape and our own most significant finds during the quarter.

DJVU: STRANGELY FAMILIAR RANSOMWARE

DJVU ransomware masquerades as legitimate services or applications and is often bundled with decoy files to appear benign. An evolution of the notorious STOP ransomware, DJVU has seen many iterations since its creation back in 2018. The ransomware uses cryptography stream cipher Salsa20 for its encryption routine. After carrying out numerous anti-analysis and

anti-sandbox checks to confirm that it's running on a real system, the malware encrypts multiple file types before generating a ransom note with instructions for the victim to recover their files. The threat recently became even more damaging when the threat actors added pre-encryption downloader capabilities to the ransomware.

This quarter, DJVU downloaded and deployed infostealer malware in apparent collaboration with the threat groups behind Arkei variant Vidar Stealer and Redline Stealer, creating additional paths for threat actors to benefit at victims' expense.

MUSTANG PANDA ABUSES LEGITIMATE APPS TO TARGET VICTIMS IN MYANMAR

In early October, we published the results of several months of tracking the Mustang Panda APT group. Also known as Bronze President, Red Delta, and Honeymyte, this group is publicly attributed to China.

During our investigation, we uncovered a campaign targeting Myanmar. The campaign impersonated popular Myanmar news outlets and targeted multiple entities including a government VPN portal. The infection vector in this campaign used phishing lures with malicious attachments that fool users into executing them, which allows the attackers to gain a foothold on the system.

The execution chain contained several components, including a legitimate benign utility that is susceptible to DLL search order hijacking, plus a malicious DLL loader and an encrypted DAT payload. After the malicious DLL loader is sideloaded, a PlugX payload is loaded into memory. The infection vector, execution chain, and use of PlugX and overall TTPs conform to Mustang Panda's tried-and-tested campaign methodology.

BIANLIAN RANSOMWARE ENCRYPTS FILES IN THE BLINK OF AN EYE

BianLian is an extremely fast-acting ransomware written in the Go programming language (GoLang). In this white paper, we predicted the current rise in the malicious use of less commonly used languages like GoLang. Threat actors recognize these languages' potential to create malware, especially bespoke ransomware. GoLang offers particularly robust support for concurrency, which can speed attacks by enabling multiple malicious functions to run independently at the same time.

BianLian is a relatively new threat that has targeted a wide range of industries. The group behind the malware appears to be purely financially motivated, and attacks related to BianLian continued through the end of 2022. The group appears to heavily exploit the systems and networks that they access. Their typical deployment method is manual infiltration of systems to gain initial access, followed by abuse of LOLBins to explore the networks and systems. After gathering this information, they deploy their ransomware for financial gain.

UNATTRIBUTED ROMCOM THREAT ACTOR SPOOFING POPULAR APPS NOW HITS UKRAINIAN MILITARY

In October, BlackBerry uncovered the previously unknown RomCom RAT targeting Ukrainian military institutions. The same threat actor was known to deploy spoofed versions of the popular Advanced IP Scanner software before switching their efforts to PDF Filler (another popular application) and may have developed these exploits themselves.

The RomCom RAT attempts to take malicious control of affected devices. The initial infection vector we observed was an email with an embedded link to a fake Ukrainian-language document called Наказ_309.pdf (Order_309.pdf in English) that dropped the next-stage downloader.

During this reporting period, this threat actor was observed actively developing new techniques targeting victims worldwide.

ROMCOM THREAT ACTOR ABUSES POPULAR SOFTWARE BRANDS TO TARGET UKRAINE AND POTENTIALLY THE UNITED KINGDOM

After a series of attacks on Ukraine, the same group launched new attack campaigns that took advantage of popular software brands. The BlackBerry Threat Research and Intelligence team uncovered the campaigns while analyzing network artifacts identified during our earlier research into RomCom RAT.

Our researchers found the threat actor impersonating SolarWinds Network Performance Monitor, KeePass Open-Source Password Manager, and PDF Reader Pro in their campaigns. The campaigns used these legitimate companies as fronts and designed fake websites that mimic the real ones to coax victims into downloading the Remcos RAT malware. The RomCom threat actor has continued to actively deploy new campaigns targeting victims in Ukraine, and may be expanding to English-speaking targets worldwide in their latest string of attacks.

ARCRYPTER RANSOMWARE EXPANDS ITS OPERATIONS FROM LATIN AMERICA TO THE WORLD

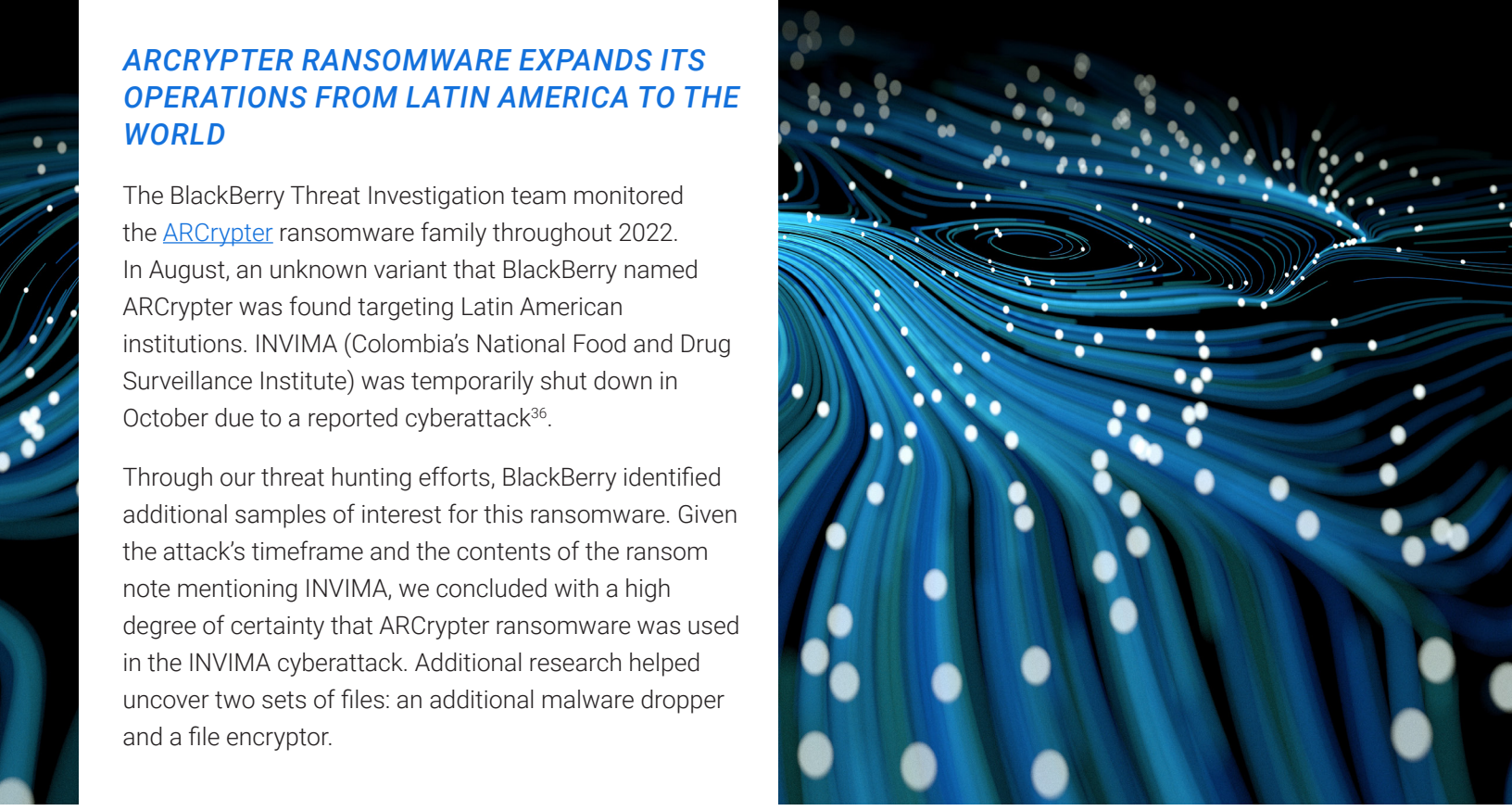
The BlackBerry Threat Investigation team monitored the ARCrypter ransomware family throughout 2022. In August, an unknown variant that BlackBerry named ARCrypter was found targeting Latin American institutions. INVIMA (Colombia's National Food and Drug Surveillance Institute) was temporarily shut down in October due to a reported cyberattack[36].

Through our threat hunting efforts, BlackBerry identified additional samples of interest for this ransomware. Given the attack's timeframe and the contents of the ransom note mentioning INVIMA, we concluded with a high degree of certainty that ARCrypter ransomware was used in the INVIMA cyberattack. Additional research helped uncover two sets of files: an additional malware dropper and a file encryptor.

THE GLOBAL RANGE OF THE CAMPAIGNS INDICATES THAT THE MUSTANG PANDA GROUP HAS

POWERFUL

RESOURCES AND CAPABILITIES. WE DO NOT EXPECT THIS TO BE THEIR LAST ATTACK.



MUSTANG PANDA USES THE RUSSIAN-UKRAINIAN WAR TO ATTACK EUROPE AND ASIA PACIFIC TARGETS

In December, our continuous monitoring of Mustang Panda uncovered a campaign targeting entities across multiple countries and continents.

This campaign relied on thematic lures (such as a file titled "Political Guidance for the New EU Approach Towards Russia.rar") related to current geopolitical events. The lure contained a decoy document and LNK file that followed the same naming convention as the lure RAR file. Additional components included legitimate utilities that are susceptible to DLL search order hijacking, malicious DLL loaders, and DAT payloads similar to components that the group has used in the past.

The goal of the execution chain is to deliver a PlugX payload into the host system's memory that provides full remote access capabilities to compromised hosts.

Although the core execution chain and TTPs in this campaign have been seen before, these attacks demonstrated subtle changes, including a small alteration in execution flow so that the function EnumSystemCodePagesW was used for shellcode execution instead of EnumThreadWindows. This modest modification required adjustments to defensive awareness and countermeasures to ensure the most effective protection.

By pivoting off a unique domain SSL certificate, we were able to uncover 15 additional IP addresses, five of which were C2 servers for the Mustang Panda group that serve similar files conforming to the same attack chain and TTPs to additional locations and victims.

The global range of the campaigns indicates that the group has powerful resources and capabilities. We do not expect this to be their last attack.

ADDITIONAL ATTACKS

EMOTET

Emotet is an elaborate and continually evolving malware family that recently returned to the spotlight in November 2022. Attributed to the criminal entity TA542 and also known as Heodo or Geodo, the malware has seen many iterations since its conception in 2014[37].

Delivered via email, Emotet's initial stager is often a Trojanized Microsoft® Excel® document. It relies on deception to persuade the victim to open the attachment and disregard pop-up security warnings. Emotet targets can vary widely and its lure documents masquerade as a range of topics across multiple languages and regions. When a victim ignores warnings and allows the execution of the fake documents, the malware's intended payload attempts to download. After the malware is installed, it can carry out a wide range of functions including dropping and deploying additional malware.

CRYWIPER

In early December, details emerged about CryWiper, a new malware wiper. CryWiper is unique because it was specifically designed and deployed to target entities in Russia, including courts and mayors' offices[38].

At first glance, CryWiper behaves like typical ransomware, including removing system shadow copies to prevent recovery of affected files; encrypting and appending the .CRY extension to affected files; and dropping a README.txt ransom note that contains instructions for paying the ransom to recover the files. However, CryWiper is not ransomware: it's a wiper. Like all wipers, CryWiper's goal is to corrupt and destroy files on the target systems so that they are unrecoverable by any means, even if the ransom is paid.

CryWiper achieves this level of file devastation with the use of Mersenne Vortex, a pseudo random number generator (PRNG) algorithm that overwrites and destroys the original contents of the files with no hope of recovery.

CONCLUSIONS AND FORECAST FOR Q1 2023

The past quarter (and 2022 in general) revealed significant cybersecurity trends that are likely to continue throughout 2023 and beyond. The number of politically motivated threat actors continues to grow, with threats including the distribution of misinformation and disinformation through fake news sites, tracking the actions and behaviors of journalists and dissidents, and attempted direct attacks on government and military organizations.

Across the board, threat actors used an array of methods that include newly identified tools and techniques as well as modifications to existing tools that enable them to better evade detection. The growth of targeted attacks in the automotive, healthcare, and financial industries cast a harsh light on the critical need to protect these sectors' expansive and vulnerable threat surfaces.

Defending your organization against malware and cyberattacks requires in-depth knowledge of how threat actors are targeting your industry, the tools that they use, and their possible motivations. This detailed knowledge provides contextual, anticipative, and actionable cyberthreat intelligence that can reduce the impact of threats on your organization.

LESSONS LEARNED / TAKEAWAYS

- In addition to financial motivation, increasing numbers of threat actors are now targeting individual and institutional victims based on economics, geopolitics, and societal circumstances. Defenders must proactively consider the possible impact of economic and political developments on cybersecurity.
- Threat actors are increasingly using less common or exotic programming languages such as GoLang and Rust to develop new malware. Threat hunters must remain vigilant and learn how the use of novel programming languages can manifest in attacks. Because GoLang supports cross-platform coding, more attacks on Linux and macOS may occur in the future.
- Wider access to initial access tools resulted in major incidents in 2022, as did the availability of ransomware as a managed service to groups without sufficient technical skills to create their own malware. As a result, use of ransomware by nation-state threat actors grew.
- The automotive industry was heavily impacted by a wide variety of cyberattacks in 2022. The compromise of large-scale manufacturers and industry suppliers resulted in stoppages across a number of production lines. These strings of attacks are likely to continue into 2023.
- Supply chain attacks that abuse legitimate apps to deliver malicious payloads can be mitigated and even prevented by implementing zero-trust policies that require continual authentication and authorization to access networks and applications.

Q1 2023 FORECAST

- To date, 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.
- Ransomware operations targeting hospitals and medical organizations will continue, especially in countries that support or fund Ukraine.
- Cyberattacks on critical infrastructure will continue. AI may be increasingly used not only for attack automation, but also to develop advanced deepfake attacks.
- Attacks on European financial institutions, like the September 2022 attack on U.K.-based Revolut (a popular fintech company and app) that compromised more than 50,000 customer records, may also continue.
- In the Americas, we predict an explosion of commercial mobile spyware attacks. We expect that threat actors in Brazil will further expand Trojan banking attacks from desktop systems to mobile devices and continue targeting victims in Latin America. In fact, December 2022 revealed the BrasDex malware family[39], which specifically targets Brazilian banking including PIX, a payment system similar to Zelle in the U.S.
- Attacks on Linux systems may continue to fly under the radar, especially those that virtualize systems, drop ransomware and install backdoors on target systems.
- We expect more targeted attacks on cloud infrastructure in every industry, as threat actors seek to gain additional visibility into the organizations that they seek to undermine or extract profit.

RESOURCES

The following BlackBerry Threat Research and Intelligence resources are available.

PUBLIC INDICATORS OF COMPROMISE (IOCS)

The BlackBerry Threat Research and Intelligence team publishes the 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 & Intelligence Team 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 here.

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 generated by the BlackBerry team.

MITRE D3FEND COUNTERMEASURES

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

REFERENCES

1 https://www.uber.com/newsroom/security-update/

2 https://www.computerworld.com/article/3604601/macs-reach-23-share-in-us-enterprises-idc-confirms.html

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

4 https://sysdig.com/blog/malware-analysis-shellbot-sysdig/

5 https://threatpost.com/sysrv-k-botnet-targets-windows-linux/179646/

6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22947

7 https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/

8 https://sandflysecurity.com/blog/log4j-kinsing-linux-malware-in-the-wild/

9 https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228

10 https://cyware.com/news/kinsing-operators-target-weblogic-servers-and-docker-apis-for-cryptomining-5ce39d4b

11 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14882

12 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

13 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725

14 https://twitter.com/MsftSecIntel/status/1542281836742729733

15 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009

16 https://www.reuters.com/business/autos-transportation/continental-investigates-cyberattack-after-report-says-data-up-sale-2022-11-15/

17 https://www.juniperresearch.com/press/in-vehicle-commerce-opportunities-exceed-775mn

18 https://www.lv.com/insurance/press/keyless-technology-drives-rise-in-theft-over-past-four-years

19 https://www.europol.europa.eu/media-press/newsroom/news/31-arrested-for-stealing-cars-hacking-keyless-tech

20 https://www.bbc.com/news/uk-england-39906534

21 https://attack.mitre.org/groups/G0050/

22 https://resources.infosecinstitute.com/topic/biggest-data-breaches-of-2019-so-far/

23 https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

24 https://www.zdnet.com/article/europes-biggest-car-dealer-hit-with-ransomware-attack/

25 https://www.broshuis.com/news/ransomware-attack

26 https://www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/

27 https://europe.autonews.com/automakers/toyota-suspend-output-japan-after-supplier-hit-cyberattack

28 https://www.nhtsa.gov/press-releases/nhtsa-updates-cybersecurity-best-practices-new-vehicles

29 https://www.bleepingcomputer.com/news/security/commonspirit-health-ransomware-attack-exposed-data-of-623-000-patients/

30 https://www.cisa.gov/emergency-directive-21-02

31 https://asec.ahnlab.com/en/27346/

32 https://malpedia.caad.fkie.fraunhofer.de/details/elf.rekoobe

33 https://www.computerweekly.com/news/252525240/ALPHV-BlackCat-ransomware-family-becoming-more-dangerous

34 https://www.securitymagazine.com/articles/97489-blackcat-alphv-ransomware-breaches-60-organizations

35 https://attack.mitre.org/groups/G0129/

36 https://twitter.com/invimacolombia/status/1577455552954712064?s=20&t=JYJsQ6PFhxBv3YHim_PQrw

37 https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider

38 https://www.bleepingcomputer.com/news/security/new-crywiper-data-wiper-targets-russian-courts-mayor-s-offices/

39 https://thehackernews.com/2022/12/beware-cybercriminals-launch-new.html

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.

January 2023 Edition