BlackBerry | Cybersecurity

EXECUTIVE SUMMARY

GLOBAL THREAT INTELLIGENCE REPORT

JUNE 2024

Reporting Period: January 1 – March 31, 2024

This newly released BlackBerry® Global Threat Intelligence Report covers everything a security operations center (SOC) manager or CISO needs to stay abreast of the latest cyberthreats and defensive measures.

Along with extensive data on cyberattacks, listed by industry and geographical region, the report includes the following from both internal reporting and external sources:

- Leading malware types
- Dominant threat groups
- The most abused software tools
- Vulnerabilities in commonly used software
- MITRE countermeasures your SOC team can use to identify and remediate cyberthreats

The number of cyberattacks rose again in the first three months of 2024; BlackBerry logged **3.1 million cyberattack attempts** against its customers, with a **17 percent increase in cyberattacks per day** compared to our last report.

In addition, our telemetry recorded a total of **630,000 unique malware hashes** targeting our customers, **a per-minute increase of over 40 percent** compared to the previous reporting period in late 2023.

Whether an attacker uses known malware or creates a unique malware hash depends on the type of attack and the target. For example, an attacker wanting to broadly target major companies in a particular industry might send floods of phishing emails with off-the-shelf malware attachments to their intended victims' employees.

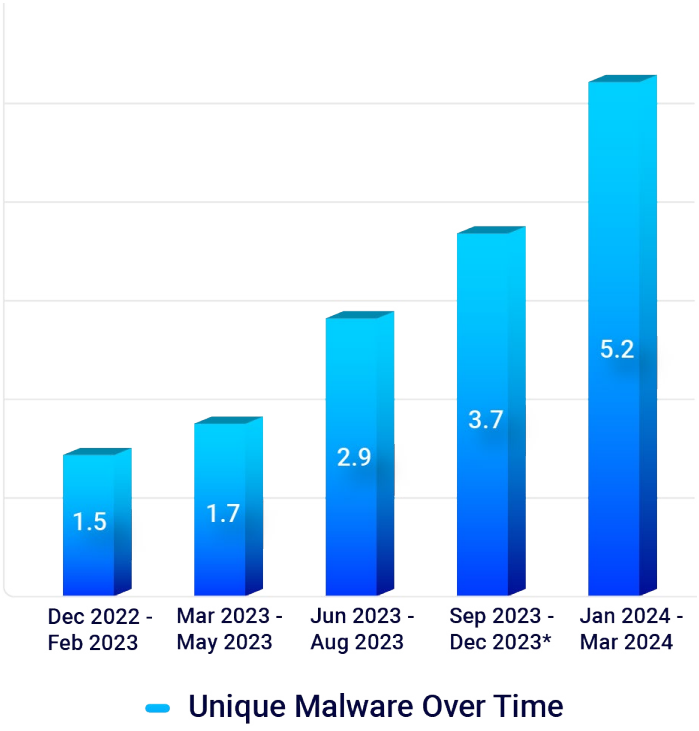

Figure 1: Unique malware hashes per minute encountered by BlackBerry cybersecurity solutions. (*The Sept. 2023 - Dec. 2023 period covered 120 days.)

Conversely, a highly resourced cyber-criminal gang with their sights set on a specific, high-value target like a CFO may develop custom malware in the hopes of circumventing their target's security measures.

KEY FINDINGS

Here are the key findings from our June 2024 report:

- Critical infrastructure bore the brunt of cyberattacks in the first three months of 2024, receiving 60 percent of total attacks. BlackBerry® cybersecurity solutions **stopped over 1.1 million attacks** against critical industry sectors, with the greatest percentage targeting finance, healthcare and government organizations.

  Critical infrastructure, as defined by the Cybersecurity and Infrastructure Security Agency (CISA), encompasses 16 sectors including healthcare, government, energy, agriculture, finance and defense. The increasing digitization of these sectors makes them more vulnerable to cybercrime. Threat actors often exploit newly revealed vulnerabilities or use social engineering against employees to steal credentials and spread malware within these sectors.

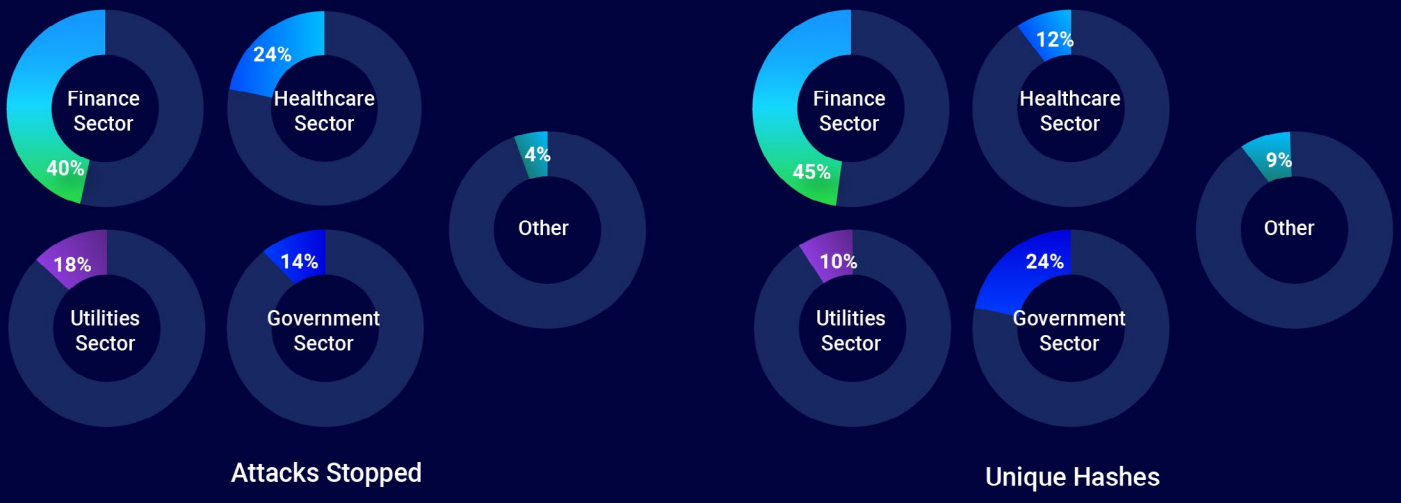

Figure 2: Industry-specific attacks versus unique malware hashes.

- **Cybercriminals are increasingly exploiting vulnerabilities** in common software tools and utilities. BlackBerry recorded nearly **9,000 new Common Vulnerabilities and Exposures (CVEs)** in the first three months of 2024. For example, the legitimate software ConnectWise ScreenConnect as well as several genuine Ivanti IT management products have been weaponized by threat actors to deliver malware.

- **Ransomware attacks on healthcare are rising.** Healthcare is an extremely profitable sector for ransomware groups to target, as few hospitals can afford to have their systems down for any length of time. Healthcare data also has a high financial value on the dark web. Attacks on healthcare can have serious knock-on effects, such as crippling hospitals, clinics, pharmacies and drug dispensaries, that prevent patients from obtaining vital medications and medical procedures. For this reason, we predict healthcare will continue to be heavily targeted throughout 2024.

- **New "Who's Who in Ransomware" section** details the top ransomware-based threat actors and identifies new emerging groups. For example, Hunters International has been in operation since late 2023 and is already a prominent ransomware-as-a-service (RaaS) crime syndicate, active around the globe. Ransomware groups are adept at finding new ways to evade traditional cybersecurity defenses and will immediately exploit any new security vulnerabilities — a factor that makes ransomware a critical threat to every organization.

- **Politically motivated cyberattacks top the list in our "Geopolitical Analysis" section.** International politics and regional strife have caused a rise in spyware, data theft and espionage attacks. In February, for example, European Parliament members on the European Parliament's security and defense subcommittee discovered spyware on their cellphones. In March, Russian cybercriminal groups intercepted conversations between German military officials about potential military support to Ukraine. Also in March, the U.S. Department of Justice (DoJ) and the FBI revealed that Chinese threat actors had targeted several UK, EU, U.S. and Canadian members of the Interparliamentary Alliance on China. Israeli, Palestinian and Iranian groups have also targeted each other's infrastructure and commercial enterprises.

- **56 percent** of CVEs were assigned a severity rating of 7 or higher on the Common Vulnerability Scoring System (CVSS) of 1 to 10. CVEs have been rapidly weaponized by malware developers — especially for use in ransomware and information stealers.

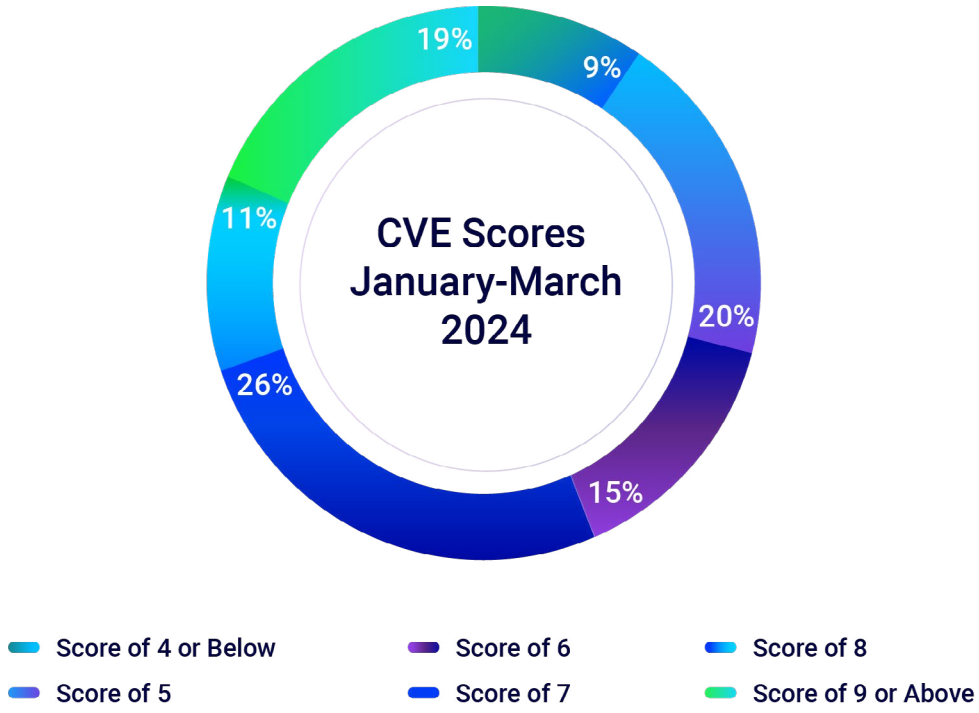

Figure 3: CVE scores recorded in the first three months of 2024.

- Finally, our section on **Common MITRE Techniques and Applied Countermeasures** will help SOC teams better recognize and defend against malicious tactics and techniques. BlackBerry recorded the top 20 techniques (from the MITRE ATT&CK® framework of over 300) that were used by attackers. BlackBerry® analysts have developed countermeasures for the top five.

The BlackBerry Global Threat Intelligence Report is the culmination of the research, analysis, and conclusions of our Cyber Threat Intelligence (CTI) team, our Incident Response (IR) team, and specialists in our CylanceMDR™* division, providing expert analysis on today's critical cybersecurity topics and challenges.

For more information, read the complete *BlackBerry Global Threat Intelligence Report – June 2024.*

*Formerly known as CylanceGUARD®.

BlackBerry Intelligent Security. Everywhere.

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 and follow @BlackBerry.