BlackBerry® | Cybersecurity

EXECUTIVE SUMMARY

GLOBAL THREAT INTELLIGENCE REPORT

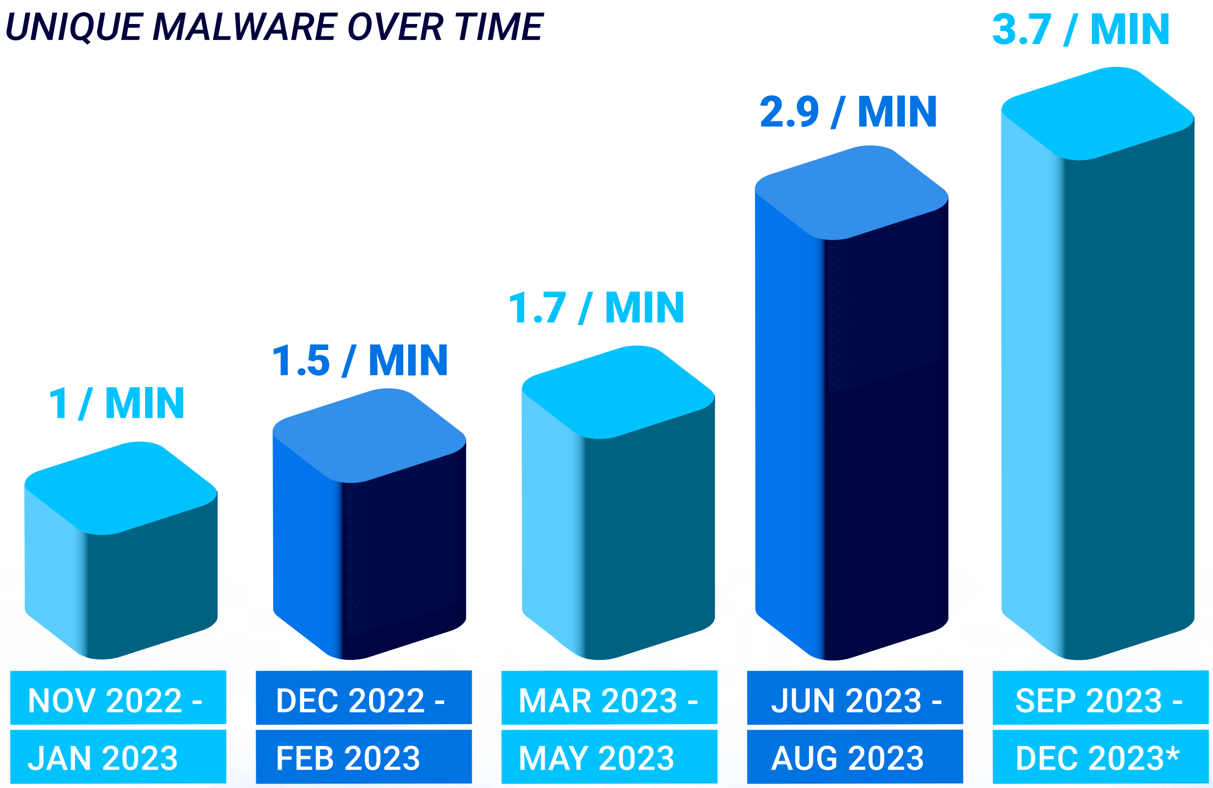
MARCH 2024

Reporting Period: September – December 2023

The latest *BlackBerry® Global Threat Intelligence Report* is hot off the press and records a busy period for threat actors. This edition of the BlackBerry report covers four months, from September 1 to December 31, 2023, instead of the usual three-month period. However, the results are adjusted for per-day and per-minute comparisons.

This reporting period, BlackBerry® cybersecurity solutions stopped over **5.2 million cyberattacks** in total. On a per-minute basis, attacks rose from 26 per minute in the prior period to **31 per minute** this period, which is a **19 percent increase** in cyberattacks per minute compared to the last report.

In terms of new malware samples, an average of around **5,300 *unique* samples per day** targeted BlackBerry customers. That's an **increase of 27 percent** over the previous reporting period.



* Represents a four-month time frame, rather than previous three-month periods.

Figure 1: Unique malware samples per minute over time.

Critical infrastructure attracted the largest volume of cyberattacks this reporting period, as the chart on the next page indicates. Critical infrastructure includes industries such as communications, defense, energy, finance, government, healthcare, transportation and utilities. Facilities within these sectors received over **62 percent of all cyberattacks**, or over two million attacks, with financial organizations receiving half of those attacks.

Cyberthreats have emerged as a new and highly destructive weapon, capable of disrupting or destroying a region's heating and water treatment plants, transportation hubs, hospitals and government centers. With the increased digitization of critical infrastructure, threat actors today can attack a facility by exploiting security misconfigurations and other vulnerabilities — all remotely. The World Economic Forum's 2024 Global Risk Report[1] ranks the threat of cyber insecurity as among the "most severe global risks anticipated over the next two years."

Financial incentives can also be a motive for an infrastructure attack. Threat actors can use information stealing malware (infostealers) to access a system and covertly download data such as defense plans, financial accounts, healthcare records or facility schematics to sell to other threat actors on the dark web.

The most commonly seen cyberthreats used against critical infrastructure include:

- **PrivateLoader:** A malicious downloader family written in C++ and observed continuously since being first discovered in 2021. It is often used to deploy infostealers onto a victim's computer or device.
- **RisePro:** A commodity infostealer that has been in the wild since 2022.
- **SmokeLoader:** A downloader malware that often spreads through phishing documents or links, targeting energy and government organizations.
- **PikaBot:** It has been a prominent threat throughout the year. This modular malware shares many similarities with the QakBot Trojan and has the ability to receive various commands from its C2.
- **Artificial intelligence (AI):** It may increasingly be used to target critical infrastructure, particularly government and election processes, as well as spread false information. Jen Easterly, director of CISA, warned,[2] "Generative AI will amplify cybersecurity risks and make it easier, faster, and cheaper to flood the country with fake content."

CRITICAL INFRASTRUCTURE FACILITIES EXPERIENCED OVER ***2 MILLION CYBERATTACKS.***

Commercial enterprises were also heavily targeted, mostly for financial gain. The commercial enterprise category includes retailers, manufacturing, wholesale distributors and professional services. More than **one million attacks** targeted the commercial enterprise sector which is nearly **33 percent of all attacks** blocked by BlackBerry cybersecurity solutions. Ransomware was a common attack method against commercial enterprise, as were infostealers. In terms of new malware, **53 percent of all unique hashes** this period were launched against businesses. Unique malware is typically used when the attacker has a very specific interest in a particular organization or sector.

Top threats to commercial enterprises included SmokeLoader and PrivateLoader (described above), as well as Formbook/XLoader, OriginLogger and Remcos. Commonly seen threats against commercial enterprises during the reporting period were:

- **Formbook:** A veteran infostealer that was rebranded as XLoader, grabs data off web forms and browsers and logs keystrokes.
- **Remcos:** Remote control and surveillance software that are commercially sold RATs. Though also used as legitimate surveillance tools, Remcos are often abused by cybercrime groups.
- **OriginLogger:** It is part of the Agent Tesla family, which consists of RATs with info-stealing capabilities. It can grab data from web browsers, capture keystrokes and even take a screenshot from the victim's device.

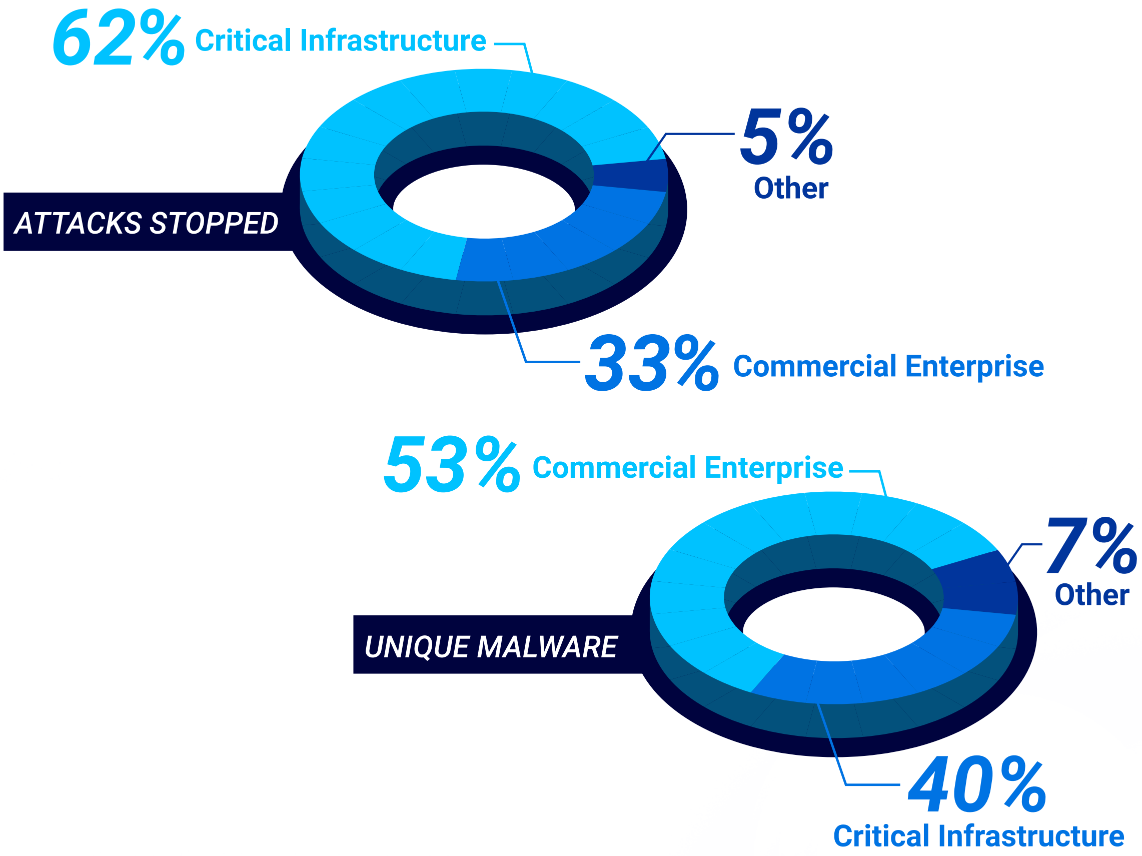


Figure 2: Industry-specific attacks stopped and unique malware hashes, September to December, 2023.

FIGHTING BACK

In positive news, a multinational effort by the U.S., France, Germany, the U.K. and other countries successfully shut down Qakbot, a major malware botnet. Operation Duck Hunt also remotely removed Qakbot malware from 700,000 infected devices, including 200,000 computers[3] in the United States. Qakbot had stolen more than $8.6 million in illicit cryptocurrency profits, which Operation Duck Hunt seized.

The *BlackBerry Global Threat Intelligence Reports* aim to provide actionable and contextual cyber threat intelligence. To aid cybersecurity professionals in their efforts to fight back against cybercrime, the report has several sections devoted to identifying and blocking the dominant threats observed this period. The report describes the most prevalent threats by operating systems as well as the threat actors and their tools.

In addition, we've included sections on:

- **Incident Response and Analysis.** BlackBerry® Cybersecurity Services Incident Response (IR) team provides key observations about the threats they've responded to this reporting period. The IR service develops rapid response plans to help mitigate the impact of cyberattacks and ensure that digital recovery follows best practices.
- **Common Vulnerabilities and Exposures (CVE).** CVE is a MITRE program that informs on publicly known vulnerabilities and exposures in commercial software. This reporting period has seen the rise of new vulnerabilities found within Cisco®, Apache®, Citrix® and JetBrains® products.
- **Common MITRE Techniques.** BlackBerry recorded the top 20 techniques (from the MITRE ATT&CK® framework of 300) that were used for cyberattacks this period.
- **Applied Countermeasures.** BlackBerry analyzed the top five MITRE techniques observed this period and provided countermeasures to them.
- **CylanceGUARD Data and Observations.** CylanceGUARD® is a subscription-based MDR service that provides 24x7x365 monitoring and helps organizations stop sophisticated cyberthreats seeking gaps in the customer's security program. The BlackBerry MDR team tracked thousands of alerts over this reporting period.

Our goal is to enable readers to translate our findings into practical threat hunting and detection capabilities. For more information, read the complete *BlackBerry Global Threat Intelligence Report* – March 2024.

[1] https://www.weforum.org/publications/global-risks-report-2024/

[2] https://www.foreignaffairs.com/united-states/artificial-intelligences-threat-democracy

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

BlackBerry | Cybersecurity

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

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