Executive Summary

BlackBerry | Cybersecurity

NOV | 23

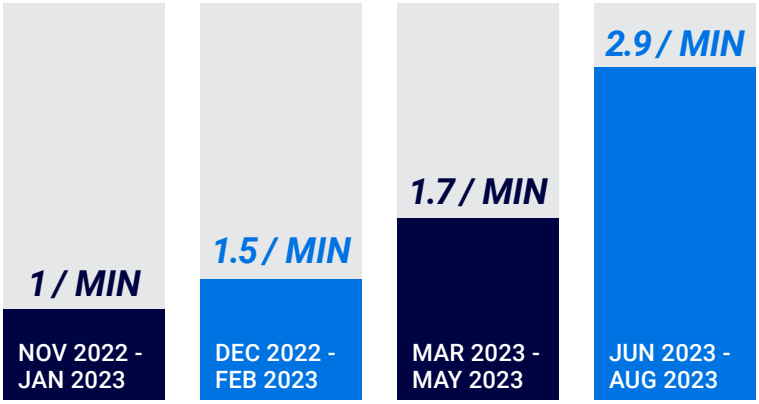
GLOBAL THREAT INTELLIGENCE REPORT

REPORTING PERIOD JUNE 1 - AUGUST 31, 2023

Cyberattacks rose significantly from June through August 2023, according to data from the* BlackBerry Global Threat Intelligence Report–November 2023. *During those months, BlackBerry Cybersecurity solutions stopped over 3.3 million attacks. That's an average of 26 attacks per minute—more than double the number in our previous report, which recorded 1.5 million attacks.

The latest *Report* also records a 70% jump in unique malware samples, which equates to 2.9 unique malware samples per minute. That volume of unique malware can overwhelm some cybersecurity filters. It also indicates how attackers have diversified their tactics and techniques to thwart cybersecurity processes such as those used in legacy, signature-based solutions.

Malware Samples Per Minute Over Time



As in previous reporting periods, malware-based distributed denial of service (DDoS) attacks were the most prevalent type of attacks this reporting period according to BlackBerry telemetry. The Mirai and Gafgyt botnets were used to launch DDoS attacks, both of which share a similar code base and commonly target unpatched and vulnerable IoT devices.

Ransomware groups like LockBit, Clop, and ALPHV caused tens-of-millions of dollars in damages worldwide, as they have learned to evade security by rapidly changing their tactics, techniques, and procedures (TTPs).

Other commonly found threats were remote access tools (RATs) and infostealers, such as RedLine, Lumma Stealer, and Vida, which were very active over the summer.

BlackBerry telemetry also showed a rise in reverse shell-based backdoor malware such as GetShell and BPFDoor. Reverse shell backdoor malware allows attackers to control a remote system by remotely connecting to a Linux shell, then creating a covert communications channel to issue commands and exfiltrate data.

The industries that received the greatest volume of attacks this reporting period were finance, healthcare, government, and critical infrastructure.

Finance: BlackBerry telemetry blocked more than 420,000 attacks on financial institutions during this period. In July, four European banking giants were breached by cyberattackers exploiting a vulnerability in Progress Software's MOVEit file transfer software.

Healthcare: BlackBerry Cybersecurity solutions detected more than 179,000 attacks against the healthcare industry. These attacks were spread across Canada, the U.S., Australia, Japan, India, and several South American and Latin American countries. Infostealers and ransomware attacks were common. Perhaps the most damaging healthcare attack, in terms of outcome, was on Spring Valley St. Margaret's Hospital in Illinois. After a ransomware attack, the hospital was forced to close its doors to the public.

Government: More than 100,000 attacks were launched at government agencies, nearly 50% higher than the previous report. A number of U.S. government agencies, including the U.S. Department of Energy (DOE), were breached by attackers exploiting a vulnerability in Progress Software's MOVEit file transfer application. Clop ransomware, which is sold largely as ransomware-as-a-service, was actively targeting governments. Likewise, infostealers including RedLine, RacconStealer v2, Vidar, and Lumma Stealer were also common this reporting period.

Critical infrastructure: Critical infrastructure is increasingly a target of both state-sponsored and financially motivated threat actors. BlackBerry Cybersecurity solutions thwarted over 75,000 attacks against critical infrastructure around the world. The LockBit ransomware group was particularly active. In July, LockBit claimed responsibility for an attack on the Japanese port of Nagoya, the country's largest port, which disrupted operations for 48 hours. LockBit also targeted the Montreal Commission des Services Electriques (CSEM), forcing the 100-year-old municipal electricity provider to rebuild its infrastructure.

Cyberattackers also abused software tools—both legitimate commercial tools and malicious tools. Metasploit and Cobalt Strike, two popular penetration testing tools, have been heavily impacted by different threat actors ranging from financially motivated groups to hacktivists to nation-state threat actors. Ransomware groups also use those tools to exfiltrate data before encrypting it.

The report also lists threats against specific operating systems, including Windows, Linux, Android, and Mac/iOS. Windows attracted the widest range of threats, with the dominant one being RedLine, which is a .NET compiled infostealer that has been a continuously active in 2023. Android devices were also heavily targeted, especially by phishing campaigns.

The goal of the *BlackBerry Global Threat Intelligence Report* is to provide exceptional cybersecurity data as well as actionable and contextual cyber threat intelligence. To further our goal of providing actionable intelligence, we have included sections on "Common MITRE Techniques" and "Applied Countermeasures and Remediation", as well as the most effective Sigma rules to detect malicious behaviors exhibited by malware. Finally, we have a section on "Common Vulnerabilities and Exposures Impact" (CVE). It includes new vulnerabilities found in popular software such as MOVEit, Barracuda ESG, and Citrix.

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–November 2023*.

Number of Attacks Per Industry

420k

FINANCE

179k

HEALTHCARE

100k

GOVERNMENT

75k

CRITICAL INFRASTRUCTURE