BlackBerry | Cybersecurity

GLOBAL THREAT INTELLIGENCE REPORT

Reporting Period:
March–May 2023

EXECUTIVE BRIEF

In this reporting period, Cylance® Endpoint Solutions by BlackBerry stopped over 1.5 million attacks. On average, threat actors deployed approximately 11.5 attacks per minute, including approximately 1.7 novel malware samples per minute. This represents a 13 percent increase in novel samples from the previous reporting period's average of 1.5 new samples per minute, demonstrating that attackers are diversifying their tooling in an attempt to bypass defensive controls. Known threat actors APT28 and the Lazarus Group, believed to be a North Korean state-sponsored cyberthreat group, were active this quarter, and tools including AdFind, Extreme RAT, and the legitimate tools Mimikatz (an open-source penetration-testing framework) and Cobalt Strike (a commercial adversary-emulation solution) were observed.

The following industries and sectors were frequently targeted this reporting period:

- **Government and public services:** BlackBerry® cybersecurity solutions stopped more than 55,000 individual attacks against the government and public services sector during this reporting period, up nearly 40% from the previous period. Attacks against government entities were stopped in North America and the Asia-Pacific (APAC) region, where Australia, South Korea, and Japan were heavily targeted. The complete threat report discusses the most commonly seen malware, potential motives for government attacks, and a review of the global threat landscape for this sector.
- **Healthcare:** Ransomware gangs continued targeting healthcare organizations, where confidential personal data and critical service present a lucrative target. In this reporting period, BlackBerry detected and stopped 13,433 unique malware binaries and prevented over 109,922 separate attacks across the healthcare sector. Notable attacks in the global healthcare landscape included disruptions at hospitals and pharmaceutical manufacturers and suppliers in Spain and India. North-Korean-based hackers' breach of a South Korea hospital was also disclosed.
- **Finance:** Financial institutions face persistent threats due to their economic significance and wealth of sensitive data. During this reporting period, BlackBerry cybersecurity technologies and services stopped over 17,000 attacks targeting financial institutions. The United States was the most-targeted country, followed by countries located in South America and Asia. Android-based threats this period include a Trojan that masquerades as a legitimate banking app and a new variant of existing malware that stole credentials from hundreds of banks around the world.

- **Critical infrastructure:** Cylance Endpoint Security solutions stopped over 25,000 attacks against critical infrastructure during this reporting period, most frequently targeting customers in the United States, India, Japan, and Ecuador. In fact, the number of threats to Western-based critical infrastructure were so high that the UK National Cyber Security Center issued an alert calling for heightened awareness and vigilance because of increased activity targeting infrastructure by state-aligned threat actors sympathetic to Russia's invasion of Ukraine.

During this reporting period, the industries attacked were a more diverse group than in the last report. The figure below shows the distribution of cyberattacks among the top three industries. It also shows that there's an inverse relationship on how the industries rank from 1 to 3 in attacks stopped vs. unique hashes stopped:

Geopolitically motivated attacks in all sectors are predicted to rise. In the face of escalating attacks, governments are increasing collaboration to help investigate, respond to, and recover from incidents. The report discusses global response to both state-sponsored and non-state-sponsored geopolitically motivated threats.

The most frequently seen malware for major operating systems are discussed in this report. Malware targeting Microsoft® Windows® includes droppers and downloaders (Emotet, PrivateLoader, and SmokeLoader), infostealers (RedLine, RaccoonStealer, Vidar, and IcedID), the Agent Tesla RAT, and ransomware from the BlackCat/ALPHV group.

For Android™ devices, the most common malware includes SpyNote, which can monitor location, access a device's camera, intercept SMS text messages (which

CYBERATTACKS STOPPED BY INDUSTRY

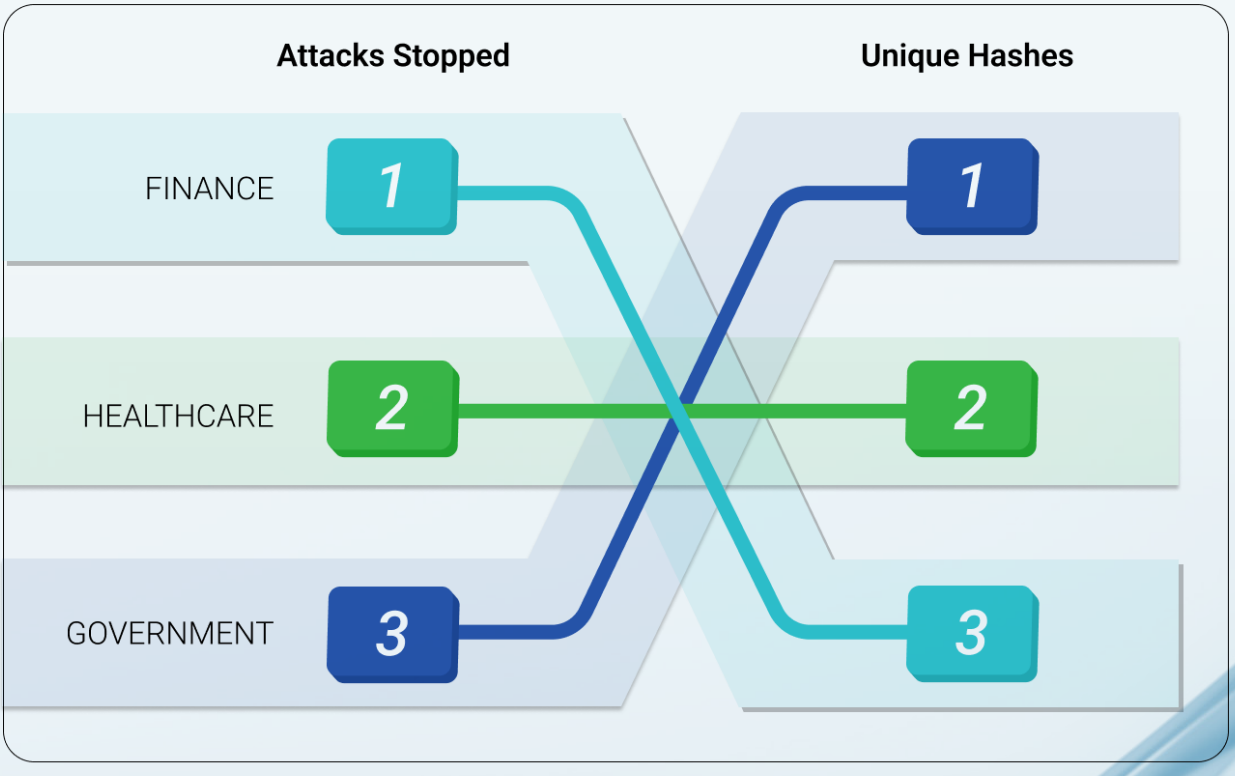

Figure 1: The three industries with the highest distribution of stopped cyberattacks and of stopped unique/different samples during this period.

helps threat actors bypass two-factor authentication), and record phone calls as well as extract valuable information like logon credentials and credit card data.

Because Linux® is primarily deployed in enterprise systems, the most popular infection vectors are via brute-forcing passwords to gain Secure Shell (SSH) access or by exploiting vulnerabilities in public-facing services. Linux threats during this reporting period included distributed denial of service (DDoS) attacks, cryptominers that hijack system resources to mine cryptocurrency, and ransomware.

While typical macOS malware displays adware or hijacks web browser searches, a growing number of threat actors last period used cross-platform programming languages to develop malware targeting macOS itself. This period's threats included Atomic macOS (AMOS), a new strain of infostealer based on the cross-platform programming language GoLang (aka Go). Adware and browser hijacking attacks were also observed.

Notable cybersecurity events during the reporting period include a significant blow to Russian cyber espionage capabilities. In early May, the U.S. Department of Justice announced that they had dismantled the infrastructure used by the threat actor Turla, which is publicly attributed to a Russian intelligence agency. Other noteworthy events include the following:

- In early March, BlackBerry researchers observed campaigns targeting European entities by the Russian state-sponsored threat actor NOBELIUM (APT29), which is publicly linked to the Russian foreign intelligence service.
- At the end of March, the business communication supplier 3CX announced a security breach that resulted in worldwide distribution of Trojanized versions of their VOIP software 3CXDesktopApp, a voice and video conferencing product widely used for calls, video, and live chat.
- In April, a malvertising campaign using Google Ads to trick victims into downloading fake, Trojanized versions of popular software and a large-scale spearsphishing campaign against Spain's national tax agency were observed.
- In early May, the BlackBerry Threat Research and Intelligence team published findings uncovering a campaign focusing on Pakistani government targets by the SideWinder group, which is believed to have originated in India.
- In late May, a ransomware attack against Chile's army by the new threat actor Rhysida was revealed.

Finally, the report provides a complete list of countermeasures and Sigma rules to detect the malicious behaviors exhibited by novel malware 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 report.

BlackBerry | Cybersecurity

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 235M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

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

BB23 | 071223