March 2023’s Most Wanted Malware: New Emotet Campaign Bypasses Microsoft Blocks to Distribute Malicious OneNote Files

blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/

April 10, 2023

Check Point Research reports that Emotet Trojan launched a new campaign last month to evade Microsoft’s macro block, sending spam emails containing malicious OneNote files. Meanwhile Ahmyth was the most prevalent mobile malware and Log4j took top spot once again as the most exploited vulnerability

Our latest Global Threat Index for March 2023 saw researchers uncover a new malware campaign from Emotet Trojan, which rose to become the second most prevalent malware last month.

As reported earlier this year, Emotet attackers have been exploring alternative ways to distribute malicious files since Microsoft announced they will block macros from office files. In the latest campaign, the attackers have adopted a new strategy of sending spam emails containing a malicious OneNote file. Once opened, a fake message appears to trick the victim into clicking the document, which downloads the Emotet infection. Once installed, the malware can gather user email data such as login credentials and contact information. The attackers then use the gathered information to expand the reach of the campaign and facilitate future attacks.

While big tech companies do their best to cut off cybercriminals at the earliest point, it’s near impossible to stop every attack from bypassing the security measures. We know that Emotet is a sophisticated Trojan and it’s no surprise to see it has managed to navigate Microsoft’s latest defenses. The most important thing people can do is make sure they have appropriate email security in place, avoid downloading any unexpected files and adopt heathy skepticism about the origins of an email and its contents.

Last month also revealed that “Apache Log4j Remote Code Execution” was the most exploited vulnerability, impacting 44% of organizations globally, followed by “HTTP Headers Remote Code Execution” with 43% of organizations worldwide and “MVPower DVR Remote Code Execution” with a global impact of 40%.

Top Malware Families

**The arrows relate to the change in rank compared to the previous month.*

Qbot was the most prevalent malware last month with an impact of more than 10% on worldwide organizations respectively, followed by **Emotet** and **Formbook** with a 4% global impact.

1. ↔ **Qbot** – Qbot AKA Qakbot is a banking Trojan that first appeared in 2008. It was designed to steal a user’s banking credentials or keystrokes and is often distributed via spam emails. Qbot employs several anti-VM, anti-debugging and anti-sandbox techniques to hinder analysis and evade detection.
2. ↑ **Emotet** – Emotet is an advanced, self-propagating and modular Trojan. Emotet used to be employed as a banking Trojan but has recently been used as a distributor to other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, it can be spread through phishing spam emails containing malicious attachments or links.
3. ↓ **FormBook** – FormBook is an Infostealer targeting Windows OS and was first detected in 2016. It is marketed as Malware as a Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. Formbook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes and can download and execute files according to orders from its C&C.
4. ↑ **AgentTesla** – AgentTesla is an advanced RAT functioning as a keylogger and information stealer, which is capable of monitoring and collecting the victim’s keyboard input, system keyboard, taking screenshots, and exfiltrating credentials to a variety of software installed on a victim’s machine (including Google Chrome, Mozilla Firefox and the Microsoft Outlook email client).
5. ↓ **XMRig** – XMRig is open-source CPU mining software used to mine the Monero cryptocurrency. Threat actors often abuse this open-source software by integrating it into their malware to conduct illegal mining on victims’ devices.
6. ↔ **GuLoader –** Guloader is a downloader that has been widely used since December 2019. When it first appeared, GuLoader was used to download Parallax RAT but has been applied to other remote access trojans and info-stealers such as Netwire, FormBook, and Agent Tesla.

7. ↑ **Remcos –** Remcos is a RAT that first appeared in the wild in 2016. Remcos distributes itself through malicious Microsoft Office documents, which are attached to SPAM emails, and is designed to bypass Microsoft Windows’s UAC security and execute malware with high-level privileges.
8. ↑ **NJRat** – NJRat is a remote accesses Trojan, targeting mainly government agencies and organizations in the Middle East. The Trojan first emerged in 2012 and has multiple capabilities: capturing keystrokes, accessing the victim’s camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim’s desktop. NJRat infects victims via phishing attacks and drive-by downloads, and propagates through infected USB keys or networked drives, with the support of Command & Control server software.
9. ↔ **Tofsee –** Tofsee is a Trickler that targets the Windows platform. This malware attempts to download and execute additional malicious files on target systems. It may download and display an image file to a user to hide its true purpose.
10. ↓ **NanoCore** – NanoCore is a Remote Access Trojan that targets Windows operating system users and was first observed in the wild in 2013. All versions of the RAT contain basic plugins and functionalities such as screen capture, crypto currency mining, remote control of the desktop and webcam session theft.

Top Attacked Industries Globally

Last month, **Education/Research** remained the most attacked industry globally, followed by **Government/Military** and then **Healthcare**.

1. Education/Research
2. Government/Military
3. Healthcare

Top Exploited Vulnerabilities

Last month, **“Apache Log4j Remote Code Execution**” was the most exploited vulnerability, impacting 44% of organizations globally, followed by **“HTTP Headers Remote Code Execution”** with 43% of organizations worldwide and **“MVPower DVR Remote Code Execution”** with a global impact of 40%.

1. ↑ **Apache Log4j Remote Code Execution (CVE-2021-44228)** – A remote code execution vulnerability exists in Apache Log4j. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the affected system.
2. ↑ **HTTP Headers Remote Code Execution (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756)** – HTTP headers let the client and the server pass additional information with an HTTP request. A remote attacker may use a vulnerable HTTP Header to run arbitrary code on the victim machine.

3. ↑**MVPower DVR Remote Code Execution –** A remote code execution vulnerability exists in MVPower DVR devices. A remote attacker can exploit this weakness to execute arbitrary code in the affected router via a crafted request.
4. ↑ **OpenSSL TLS DTLS Heartbeat Information Disclosure (CVE-2014-0160,CVE-2014-0346)** – An information disclosure vulnerability exists in OpenSSL. The vulnerability, aka Heartbleed, is due to an error when handling TLS/DTLS heartbeat packets. An attacker can leverage this vulnerability to disclose memory contents of a connected client or server.
5. ↓ **Web Servers Malicious URL Directory Traversal –** There exists a directory traversal vulnerability on different web servers. The vulnerability is due to an input validation error in a web server that does not properly sanitize the URI for the directory traversal patterns. Successful exploitation allows unauthenticated remote attackers to disclose or access arbitrary files on the vulnerable server.
6. ↑ **Dasan GPON Router Authentication Bypass (CVE-2018-10561)** – An authentication bypass vulnerability exists in Dasan GPON routers. Successful exploitation of this vulnerability would allow remote attackers to obtain sensitive information and gain unauthorized access into the affected system.
7. ↔ **PHP Easter Egg Information Disclosure –** An information disclosure vulnerability has been reported in the PHP pages. The vulnerability is due to incorrect web server configuration. A remote attacker can exploit this vulnerability by sending a specially crafted URL to an affected PHP page.
8. ↓ **Command Injection Over HTTP (CVE-2021-43936,CVE-2022-24086)** – A command Injection over HTTP vulnerability has been reported. A remote attacker can exploit this issue by sending a specially crafted request to the victim. Successful exploitation would allow an attacker to execute arbitrary code on the target machine.
9. ↑ **D-Link Multiple Products Remote Code Execution (CVE-2015-2051)** – A remote code execution vulnerability exists in multiple D-Link products. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the affected system.
10. ↓ **WordPress portable-phpMyAdmin Plugin Authentication Bypass (CVE-2012-5469)** – An authentication bypass vulnerability exists in WordPress portable-phpMyAdmin Plugin. Successful exploitation of this vulnerability would allow remote attackers to obtain sensitive information and gain unauthorized access into the affected system.

Top Mobile Malwares

Last month, **Ahmyth** moved to the top spot as the most prevalent mobile malware, followed by **Anubis** and **Hiddad.**

1. **AhMyth** – AhMyth is a Remote Access Trojan (RAT) discovered in 2017. It is distributed through Android apps that can be found on app stores and various websites. When a user installs one of these infected apps, the malware can collect sensitive information from the device and perform actions such as keylogging, taking screenshots, sending SMS messages, and activating the camera.
2. **Anubis** – Anubis is a banking Trojan malware designed for Android mobile phones. Since it was initially detected, it has gained additional functions including Remote Access Trojan (RAT) functionality, keylogger, audio recording capabilities and various ransomware features. It has been detected on hundreds of different applications available in the Google Store.
3. **Hiddad** – Hiddad is an Android malware which repackages legitimate apps and then releases them to a third-party store. Its main function is to display ads, but it can also gain access to key security details built into the OS.

Check Point’s Global Threat Impact Index and its ThreatCloud Map is powered by Check Point’s ThreatCloud intelligence. ThreatCloud provides real-time threat intelligence derived from hundreds of millions of sensors worldwide, over networks, endpoints and mobiles. The intelligence is enriched with AI-based engines and exclusive research data from Check Point Research, the intelligence and research Arm of Check Point Software Technologies.