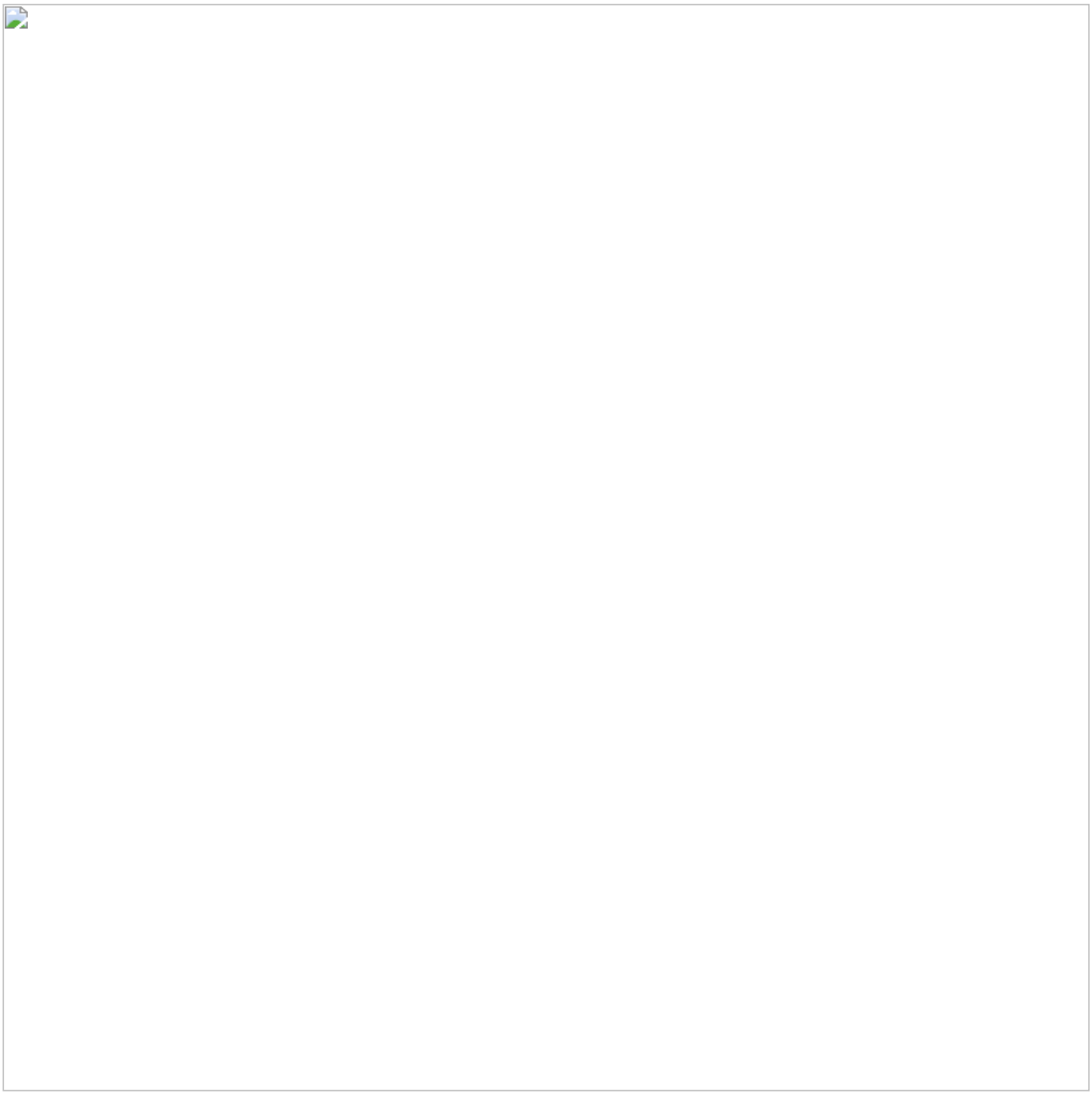
November 2023’s Most Wanted Malware: New AsyncRAT Campaign Discovered while FakeUpdates Re-Entered the Top Ten after Brief Hiatus

blog.checkpoint.com/research/november-2023s-most-wanted-malware-new-asyncrat-campaign-discovered-while-fakeupdates-re-entered-the-top-ten-after-brief-hiatus/

December 12, 2023



Researchers reported on a new AsyncRAT campaign where malicious HTML files were being used to spread the stealthy malware. Meanwhile, downloader FakeUpdates jumped straight into second place after a short break from the top

ten list

Our latest Global Threat Index for November 2023 saw researchers discover a AsyncRAT campaign where malicious HTML files were used to spread the covert malware. Meanwhile, JavaScript downloader, FakeUpdates, jumped straight into second place after a two-month hiatus from the top ten list, and Education remained the most impacted industry worldwide.

AsyncRAT is a Remote Access Trojan (RAT) known for its ability to remotely monitor and control computer systems without detection. The malware, which came in sixth place on last month's top ten list, utilizes various file formats such as PowerShell and BAT to carry out process injection. In last month's campaign, recipients received an email containing an embedded link. Once clicked, the link triggered a malicious HTML file to be downloaded, which then prompted a sequence of events that meant that the attacker could hide within trusted system applications to avoid detection.

Meantime, downloader, FakeUpdates, re-entered the top malware list after a two-month break. Written in JavaScript, the malware distribution framework deploys compromised websites to trick users into running fake browser updates. It has led to further compromise through many other malwares including GootLoader, Dridex, NetSupport, DoppelPaymer, and AZORult.

November's cyber threats demonstrate how threat actors leverage seemingly innocuous methods to infiltrate networks. The rise of the AsyncRAT campaign and the resurgence of FakeUpdates highlight a trend where attackers use deceptive simplicity to bypass traditional defenses. This underscores the need for organizations to adopt a layered security approach that doesn't just rely on recognizing known threats, but also has the capability to identify, prevent and respond to novel attack vectors before they inflict harm.

CPR also revealed that "Command Injection Over HTTP" was the most exploited vulnerability, impacting 45% of organizations globally, followed by "Web Servers Malicious URL Directory Traversal" with 42%. "Zyxel ZyWALL Command Injection (CVE-2023-28771)" came in third with a global impact of 41%

Top malware families

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

Formbook was the most prevalent malware last month with an impact of **3%** worldwide organizations, followed by **FakeUpdates** with a global impact of **2%,** and **Remcos** with a global impact of **1%.**

1. ↔ **Formbook** – Formbook is an Infostealer targeting the 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 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.
2. ↑ **FakeUpdates** – FakeUpdates (AKA SocGholish) is a downloader written in JavaScript. It writes the payloads to disk prior to launching them. FakeUpdates led to further compromise via many additional malwares, including GootLoader, Dridex, NetSupport, DoppelPaymer, and AZORult.
3. ↔ **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 UAC security and execute malware with high-level privileges.
4. ↔ **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.

5. ↑ **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).
6. ↑ **AsyncRat –** Asyncrat is a Trojan that targets the Windows platform. This malware sends out system information about the targeted system to a remote server. It receives commands from the server to download and execute plugins, kill processes, uninstall/update itself, and capture screenshots of the infected system.
7. ↓ **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.
8. ↓ **Mirai –** Mirai is an infamous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive Distributed Denial of Service (DDoS) attacks. The Mirai botnet first surfaced in September 2016 and quickly made headlines due to some large-scale attacks including a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's infrastructure.
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 in an effort to hide its true purpose.
10. ↓ **Phorpiex** – Phorpiex is a botnet (aka Trik) that has been active since 2010 and at its peak controlled more than a million infected hosts. It is known for distributing other malware families via spam campaigns as well as fueling large-scale spam and sextortion campaigns.

Top Attacked Industries Globally

Last month, **Education/Research** remained in first place as the most attacked industry globally, followed by **Communications** and **Government/Military**.

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

Top exploited vulnerabilities

Last month, **"Command Injection Over HTTP"** was the most exploited vulnerability, impacting **45%** of organizations globally, followed by **"Web Servers Malicious URL Directory Traversal"** with **42%**. **"Zyxel ZyWALL Command Injection (CVE-2023-28771)"** came in third with a global impact of **41%**.

1. ↑ **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.

2. ↑ **Web Servers Malicious URL Directory Traversal (CVE-2010-4598,CVE-2011-2474,CVE-2014-0130,CVE-2014-0780,CVE-2015-0666,CVE-2015-4068,CVE-2015-7254,CVE-2016-4523,CVE-2016-8530,CVE-2017-11512,CVE-2018-3948,CVE-2018-3949,CVE-2019-18952,CVE-2020-5410,CVE-2020-8260) –** 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.
3. ↓ **Zyxel ZyWALL Command Injection (CVE-2023-28771) –** A command injection vulnerability exists in Zyxel ZyWALL. Successful exploitation of this vulnerability would allow remote attackers to execute arbitrary OS commands in the effected system.
4. ↑ **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.
5. ↑ **HTTP Headers Remote Code Execution –** 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.
6. ↓ **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 to the affected system.
7. ↑ **PHP Easter Egg Information Disclosure (CVE-2015-2051)** – 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. ↓ **MVPower CCTV DVR Remote Code Execution (CVE-2016-20016)-** A remote code execution vulnerability exists in MVPower CCTV DVR. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the affected system.
9. ↓ **PHPUnit Command Injection (CVE-2017-9841) –** A command injection vulnerability exists in PHPUnit. Successful exploitation of this vulnerability would allow remote attackers to execute arbitrary commands in the affected system.
10. ↔ **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 the memory contents of a connected client or server.

Top Mobile Malwares

Last month **Anubis** remained in first place as the most prevalent mobile malware, followed by **AhMyth** and **SpinOk**.

1. **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.
2. **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, which is usually used to steal sensitive information.

3. **SpinOk** – SpinOk is an Android software module that operates as spyware. It collects information about files stored on devices and can transfer them to malicious threat actors. The malicious module was found present in more than 100 Android apps and downloaded more than 421,000,000 times until May 2023.

Check Point's Global Threat Impact Index and its ThreatCloud Map are 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.