KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emerging Post-Exploitation Kits - Havoc and EXFILTRATOR-22

Tracker ID: TN337 **Date:** March 02, 2023 **Category:** Malware **Industry:** All **Region**: Asia

Background

Threat actors are transitioning from expensive solutions such as Cobalt Strike and Brute Ratel and towards new tools such as "Havoc," an open-source command and control (C2) framework, and "EXFILTRATOR-22," which provides extensive defense evasion and anti-analysis capabilities. Havoc is used in the new campaign to target government organizations. It is a cross-platform program that employs sleep obfuscation, return address stack spoofing, and indirect syscalls to bypass Microsoft Defender on current Windows 11 systems, whereas EXFILTRATOR-22 appears to be the work of individuals from in North, East, or South-East Asia (China, Taiwan, Hong Kong, Malaysia, Singapore, Philippines, etc.). They likely used leaked source code from other post-exploitation frameworks to construct their post-exploitation-framework-as-a-service approach.

Pen testers (and hackers) have previously been seen using a variety of post-exploitation tools, such as Cobalt Strike and Brute Ratel, to perform a variety of operations on infected systems, such as running commands, controlling processes, downloading additional payloads, changing Windows tokens, and executing shellcode. These technologies can allow an attacker to view every one of their compromised devices, events, and task output utilizing a web-based administration console. Havoc and EXFILTRATOR-22 are the new additions to the long list of post-exploitation toolkits that aid in compromising a system with an ease to evade defenses and bypass anti-analysis capabilities. They offer a wide range of capabilities, making these a cakewalk for anyone purchasing the tool.

In early January, an unidentified threat group used the Havoc kit as part of an attack campaign against an unspecified government entity. The shellcode loader used in the campaign disables Event Tracing for Windows (ETW), and the final Havoc Demon payload is loaded without the DOS and NT headers to evade detection. Later, using the Havoc CnC framework, a DLL malware "Demon DLL" with standard RAT (remote access trojan) capabilities was constructed. It also supports generating malicious agents in several file types, including shellcode, Windows PE executables, and PE DLLs. The Havoc framework was also seen being deployed using a rogue npm package (Aabquerys) that typosquatted a legitimate module.

In comparison, EXFILTRATOR-22 (aka EX-22) is the most recent post-exploitation architecture to emerge in the wild for deploying ransomware within enterprise networks. Some of the major capabilities include establishing a reverse shell with elevated privileges, uploading and downloading files, monitoring keystrokes, launching ransomware to encrypt files, and launching a live VNC(Virtual Network Computing) connection for real-time access. It can also survive system reboots, propagate laterally through a worm, view running processes, produce cryptographic hashes of data, and extract authentication tokens. On Telegram and YouTube, it is advertised as entirely undetectable malware and is available for $1,000 per month or $5,000 for lifetime access. Criminals who purchase the toolkit are given a login panel through which they may access the EX-22 server and remotely operate the malware.

The appearance of these post-exploitation toolkits serves as a warning to technology vendors about the growing threat posed by malware identified in open-source repositories. The approaches used to conceal the dangerous features could be combined with more complex staging and social engineering techniques to install malicious programs on enterprise endpoints. These threat actors are incredibly sophisticated and will almost certainly continue to improve the evasiveness of the malware. With ongoing upgrades and support, Havoc, and EX-22 have emerged as viable option for any threat actor looking to acquire tools for the post-exploitation phase but hesitant to use standard tools due to high detection rates.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emerging Post-Exploitation Kits - Havoc and EXFILTRATOR-22

Tracker ID: TN337 **Date:** March 02, 2023 **Category:** Malware **Industry:** All **Region**: Asia

MITRE ATT&CK Tactics

Persistence, Privilege Escalation, Defense Evasion, Credential Access, Command and control, Discovery, Collection, and Impact.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Monitor for red flags in the code being downloaded and incorporated into internal development projects. That includes (but isn't limited to) the presence of obfuscated code as well as the use of known vulnerable components.
- Pay attention to links out to external sites and assets or infrastructure that could indicate communications with malicious command and control systems.
- To prevent servers from connecting arbitrarily to the internet to browse or download data, check your perimeter firewall and proxy and block suspicious activity. Such limitations aid in preventing the download of malware and C2 activity, including mobile devices.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Check that all security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- Organizations should verify that their security tools are running in optimum configuration and perform regular network scans to ensure a security product protects all systems.
- Prevent remote procedure call (RPC) and service message block (SMB) communication along endpoints whenever possible. This limits lateral movement and other attack activities.
- Ensure secure handling of emails that come from outside sources and data acquired from the Internet. Apply mail filtering settings to ensure blocking spoofed emails, spam, and emails with malware.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Emerging Post-Exploitation Kits - Havoc and EXFILTRATOR-22

Tracker ID: TN337 **Date:** March 02, 2023 **Category:** Malware **Industry:** All **Region**: Asia

References

- EXFILTRATOR-22 – An Emerging Post-Exploitation Framework, Cyfirma, February 28, 2023, External Link (www.cyfirma.com).
- Lucija Valentić, Open-source repository malware sows Havoc, ReversingLabs, February 09, 2023, External Lin (www.reversinglabs.com)
- Insights and Research, Havoc Across the Cyberspace, Zscaler, February 14, 2023, External Lin (https://www.zscaler.com)
- Cyware Alerts - Hacker News, Havoc Replaces Cobalt Strike and Brute Ratel, Cyware, February 19, 2023, External Link (cyware.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

*

Hash MD5	Hash SHA1	Hash SHA256	IP	Domain
5be4e5115cdf225871a66899b7bc5861	aa96e359daf6f90c2170c99a383f4f6b87e2154a	32746688a23543e674ce6dcf03256d99988a269311bf3a8f0f944016fe3a931d	3.136.16.137	hxxps://github[.]elemecdn.com
bfa5f1d8df27248d840d1d86121f2169	1f1aadda137e5f6d1d914f1c69160eed4dda8517		146[.]190[.]48[.]229	hxxp://zh[.]googlecdnb.tk
874726830ae6329d3460767970a2f805	36cce0d19253d08252d0d3ade1755d6b064786ae		23.216.147[.]76	ttwweatterarartgea[.]ga
	09a47a484c8e83f0d36772a445b4e6bc12dc247b		20.99.184[.]37	
	745f47e5349a99ee867fc1f5358462d176f97c6f			
	62036fd054bac1375fe1205dc595a246e9d94a83			
	4789cf9141da47fe265e3d646609d864e0074711			
	0dd0784b875183c5c8701ae4f46ed371a16fd6b3			
	4ae6fec8052a9648abaaa7b41625c911f355eaa7			
	a3dc96b5553606a039a68783989eba4cc0732b3a			
	4b0c13a054cadbfddf82686f4b4ff082e9cae428			
	eca49c8962c55bfb11d4dc612b275daa85cfe8c3			