EncryptHub abuses Brave Support in new campaign exploiting MSC EvilTw

Data: 2025-08-16 09:36:33

Autor: Inteligência Against Invaders

EncryptHub abuses Brave Support in new campaign exploiting MSC EvilTwin flaw

EncryptHub actor exploits Windows flaw CVE-2025-26633 (“MSC EvilTwin”) with rogue MSC files and social engineering to drop malware.

The threat actor EncryptHub exploits the now-patched Windows flaw CVE-2025-26633 (“MSC EvilTwin”) using rogue MSC files and social engineering to deliver malware, warns Trustwave SpiderLabs.

The flaw is an improper neutralization issue in Microsoft Management Console that lets unauthorized attackers bypass security features locally.

*“The SpiderLabs Research team recently observed an EncryptHub campaign that combines social engineering and the exploitation of the Microsoft Management Console (MMC):*CVE-2025-26633*. This vulnerability, dubbed MSC EvilTwin, allows the attacker to execute malicious .msc files. While the tactics observed align with previously reported methods, deeper investigations uncovered additional new tools used in EncryptHub campaigns.”* reads the advisory*. “These activities are part of a broad, ongoing wave of malicious activity that blends social engineering with technical exploitation to bypass security defenses and gain control over internal environments.”*

EncryptHub (aka LARVA-208/Water Gamayun) is knonw for attacks targeting Web3 developers and abusing platforms like Steam. By February, at least 618 organizations worldwide had been compromised.

The attack chain starts with fake IT messages on Microsoft Teams to gain remote access. A PowerShell loader fetches runner.ps1, which drops two .msc files to exploit CVE-2025-26633 (“MSC EvilTwin”). Attackers exploit the MSC EvilTwin to allow mmc.exe loading an identically named .msc from the MUIPath (e.g., *en-US*) and execute the attacker’s copy. Runner.ps1 then inserts the C2 URL into that file, which downloads build.ps1. Build.ps1 steals system info, establishes persistence, and runs AES-encrypted commands from the C2, including deploying Fickle Stealer.

Researchers also detailed SilentCrystal, a Golang loader by EncryptHub, that replaced earlier PowerShell scripts. It abuses Brave Support to host payloads, creates a fake Windows directory to bypass defenses, and exploits MSC EvilTwin to execute malware. The researchers also detailed another tool in the threat actor’s arsenal, a Golang SOCKS5 backdoor that works in client or server mode. The tool sends stolen system details via Telegram, and sets up C2 infrastructure with TLS. Both tools show EncryptHub’s shift to stealthier, resilient tactics.

The experts observed EncryptHub setting up a fake video call platform, RivaTalk, as cover for its new C2 server. The site, registered in July 2025, requires an access code to download its malicious Windows app, limiting exposure to targets. The installer abuses a Symantec ELAM binary to sideload a DLL, which runs a PowerShell script pulling further payloads. While showing a fake setup pop-up, it generates fake web traffic to mask activity, then maintains C2 contact, executing AES-encrypted commands for full control.

“The EncryptHub threat actor represents a well-resourced and adaptive adversary, combining social engineering, abuse of trusted platforms, and the exploitation of system vulnerabilities to maintain persistence and control. Their use of fake video conferencing platforms, encrypted command structures, and evolving malware toolsets underscores the importance of layered defense strategies, ongoing threat intelligence, and user awareness training.” concludes the report. “As their campaigns grow more targeted and stealthier, proactive detection and swift incident response are critical in mitigating the risks posed by this emerging threat group.”

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,EncryptHub)