Microsoft uncovers new variant of XCSSET macOS malware in targeted att

Data: 2025-09-26 20:00:49

Autor: Inteligência Against Invaders

Microsoft uncovers new variant of XCSSET macOS malware in targeted attacks

Microsoft Threat Intelligence researchers found a new XCSSET macOS malware variant used in limited attacks.

Microsoft Threat Intelligence researchers have discovered a new version of the macOS malware XCSSETthat has been employed in limited attacks.

Trend Micro first spotted the malware in 2020 when it was spreading through Xcode projects and exploiting two zero-day vulnerabilities to steal sensitive information from target systems and launch ransomware attacks.

The new XCSSET version can steal Firefox data and hijack the clipboard. It avoids detection using encryption and obfuscation techniques, and runs secret AppleScripts. The malware supports an additional persistence mechanism through*LaunchDaemon*entries.

“This variant features a submodule designed to monitor the clipboard and references a downloaded configuration file containing address regex patterns associated with various digital wallets.” reads the report*.“If a pattern match is detected, XCSSET is capable of substituting the clipboard content with its own predefined set of wallet addresses.”*

The updated stage also downloads and runs several new modules, extending the malware’s functionality compared with the older variant.

*“This new variant has added an info-stealer module to exfiltrate data stored by Firefox. TherunMe()function is invoked at first to download a Mach-O FAT binary, which is responsible for all info stealing operations, from the C2 server.” continues the report. “This downloaded binary appears to be a modified version of a GitHub project*HackBrowserData*, which is capable of decrypting and exporting browser data stored by browsers. Passwords, history, credit card information, and cookies are some of the key information it can extract from almost all popular browsers.”*

The new XCSSET variant implements a four-stage infection chain. The initial three stages are consistent with previous variants. Microsoft detailed the fourth stage, which includes the*boot()*function and its associated calls to download and run submodules.

The new XCSSET variant includes several focused submodules:

- **vexyeqj (info-stealer)**: downloads and runs a compiled AppleScript (bnk), decrypts C2 config

(AES), inspects and exfiltrates clipboard data, and can replace clipboard contents with attacker wallet addresses.

- **bnk (payload)**: run-only AppleScript that gathers serial/user info, validates/filters clipboard content, encrypts and posts data to C2.
- **neq_cdyd_ilvcmwx (file-stealer)**: fetches and runs additional AppleScripts from C2 to exfiltrate files.
- **xmyyeqjx (LaunchDaemon persistence)**: creates ~/.root, disables macOS auto/rapid updates, builds a fake System Settings app, writes a com.google.* LaunchDaemon plist, sets root ownership and loads it.
- **jey (obfuscation/persistence)**: shell-based payload decryption and execution with improved obfuscation.
- **iewmilh_cdyd (Firefox stealer)**: downloads a Mach-O binary (modified HackBrowserData) to export Firefox passwords, cookies, cards and uploads zipped results.

Across modules it uses run-only AppleScripts, AES-encrypted C2 configs, clipboard hijacking for crypto fraud, temp file cleanup, and chunked exfiltration to reduce local artifacts.

To mitigate this threat: keep OS and apps updated and promptly apply security patches; always inspect Xcode projects from repositories to avoid infected code; verify clipboard contents before pasting to prevent hijacking; use browsers like Microsoft Edge with SmartScreen to block malicious sites; install Microsoft Defender for Endpoint on Mac for malware detection and quarantine. Activate cloud protection, automatic sample submission, PUA protection, and network protection in Defender to block threats and unwanted applications, and restrict access to malicious domains.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,malware)