Cybercriminals Exploit Free Software Lures to Deploy Hijack Loader and Vidar Stealer

Date: 19th June 2024 | Severity: High

Summary

The attackers trick users into downloading password-protected archive files containing trojanized copies of a Cisco Webex Meetings App. When victims run the “Setup.exe” file, it covertly loads the malware loader.

Attack Vectors

- Threat actors are luring unsuspecting users with free or pirated versions of commercial software to deliver a malware loader called Hijack Loader, which then deploys an information stealer known as Vidar Stealer.
- “The malware employs a known technique for bypassing User Account Control (UAC) and exploiting the CMSTPLUA COM interface for privilege escalation,” Houspanossian said. “Once privilege escalation had succeeded, the malware added itself to Windows Defender’s exclusion list for defense evasion. “The attack chain, besides using Vidar Stealer to siphon sensitive credentials from web browsers, leverages additional payloads to deploy a cryptocurrency miner on the compromised host.
- The PowerShell script then serves as a launchpad for Hijack Loader, which ultimately delivers the Lumma Stealer malware. The stealer is also equipped to download three more payloads, including Amadey Loader, a downloader that launches the XMRig miner, and a clipper malware to reroute crypto transactions to attacker-controlled wallets.
- The message also features two options, “How to fix” and “Auto-fix.” If a victim selects the first option, a Base64-encoded PowerShell command is copied to the computer’s clipboard followed by instructions to launch a PowerShell terminal and right-click the console window to paste the clipboard content and execute code responsible for running either an MSI installer or a Visual Basic Script (VBS). Similarly, users who end up selecting the “Auto-fix” are displayed WebDAV-hosted files named “fix.msi” or “fix.vbs” in Windows Explorer by taking advantage of the “search-ms:” protocol handler.

Indicator of compromise

INDICATOR TYPE	INDICATORS
SHA Hash Value	• CA53407B356FCDEA51A6D536447ED6B88AD14C87FACF421080D141CAE837EEDC • 8103F2CCE6A864CEEFE6C5B0C05087AC85AB04A2ABF150E93BC9DB90C54D9D20 • 725F50650CB9490027B633A1FF0AE166CB6FC42037DBE72D9A09DD65BE323A1F
Domains	• keningsberguersfax[.]com • pixeldrain[.]com
URLs	• 78[.]47.78.87 • 185[.]172.128.87 • 144[.]76.154.59 • 139[.]99.16.105 • 185[.]172.128.212 • 1[.]1.1.1

Recommendation

- Block all threat indicators at your respective controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Deploy WAF so that helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- Block transaction to IOC and block transaction to malicious URL by using secure socket layer (SSL or TLS) and Ensure any communication towards public facing network is happening via SSL and TLS (Secure Socket Layer and Transport layer security latest version).

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/06/cybercriminals-exploit-free-software.html
- https://www.redpacketsecurity.com/cybercriminals-exploit-free-software-lures-to-deploy-hijack-loader-and-vidar-stealer/