Mphasis
The Next Applied

New Rust-based Fickle Malware Uses PowerShell for UAC Bypass and Data Exfiltration

Date: 20th June 2024 | Severity: High

Summary

A new Rust-based information stealer malware called Fickle Stealer has been observed being delivered via multiple attack chains with the goal of harvesting sensitive information from compromised hosts. it’s aware of four different distribution methods -- namely VBA dropper, VBA downloader, link downloader, and executable downloader -- with some of them using a PowerShell script to bypass User Account Control (UAC) and execute Fickle Stealer.

Attack Vectors

- The PowerShell script (“bypass.ps1” or “u.ps1”) is also designed to periodically send information about the victim, including country, city, IP address, operating system version, computer name, and username to a Telegram bot controlled by the attacker.
- The stealer payload, which is protected using a packer, runs a series of anti-analysis checks to determine if it’s running in a sandbox or a virtual machine environment, following which it beacons out to a remote server to exfiltrate data in the form of JSON strings.
- Fickle Stealer is no different from other variants in that it’s designed to gather information from crypto wallets, web browsers powered by Chromium and the Gecko browser engine (i.e, Google Chrome, Microsoft Edge, Brave, Vivaldi, and Mozilla Firefox), and applications like AnyDesk, Discord, FileZilla, Signal, Skype, Steam, and Telegram.
- In addition to some popular applications, this stealer searches sensitive files in parent directories of common installation directories to ensure comprehensive data gathering,” security researcher Pei Han Liao said. “It also receives a target list from the server, which makes Fickle Stealer more flexible.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• e9bc44cf548a70e7285499209973faf44b7374dece1413dfcdc03bf25a6c599c • a641d10798be5224c8c32dfaab0dd353cd7bb06a2d57d9630e13fb1975d03a53 • 1b48ee91e58f319a27f29d4f3bb62e62cac34779ddc3b95a0127e67f2e141e59 • ad57cc0508d3550caa65fcb9ee349c4578610970c57a26b7a07a8be4c8b9bed • 8e87ab1bb9870de9de4a7b409ec9baf8cae11deec49a8b7a5f73d0f34bea7e6f • 9ffc6a74b88b66dd269d006dec91b8b53d51afd516fe2326c6f9e3ed81d860ae • 48e2b9a7b8027bd03ceb611bbfe48a8a09ec6657dd5f2385fc7a75849bb14db1 • 6f9f65c2a568ca65326b966bcf8d5b7bfb5d8ddea7c258f58b013bc5e079308b • 2236ffcf2856d5c9c2dedf180654cf318596614be450f6b24621dc13d7370dbf
IP	• 144[.]208[.]127[.]230 • 185[.]213[.]208[.]245 • 138[.]124[.]184[.]210

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

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/new-rust-based-fickle-malware-uses.html
- https://www.fortinet.com/blog/threat-research/fickle-stealer-distributed-via-multiple-attack-chain