Fileless Revenge RAT Abuses Legitimate Tools to Hide Malicious Activity

Date: 18th April 2024 | Severity: High

Summary

- AhnLab SEcurity intelligence Center (ASEC) recently discovered the distribution of Revenge RAT malware that had been developed based on legitimate tools.
- It appears that the attackers have used tools such as ‘smtp-validator’ and ‘Email To Sms’. At the time of execution, the malware creates and runs both a legitimate tool and a malicious file, making it difficult for users to realize that a malicious activity has occurred.

Attack Vectors

- According to the reports shared with Cyber Security News, the malicious file “setup.exe” is used for generating additional malware by creating and running svchost.exe in the %appdata%Microsoft\Windows\Templates path with a hidden attribute.
- After this, the setup.exe program registers the svchost.exe file with the value “Microsoft Corporation Security” in the autorun registry. After establishing a connection with the C2 server, the HTML file is downloaded by the svchost.exe file and decompressed.
- The explorer.exe file in the %appdata%Microsoft\Windows\Templates path is created and executed by the HTML file that was downloaded. In the event that the initial C2 server URL was blocked or a new C2 was updated, two C2 servers were provided as a backup plan.
- In the %appdata%Microsoft\Windows\ path, this new explorer.exe file creates a version.exe file, and in the %temp% path, it creates a.inf file. This version.exe file is run as cmstp.exe (CMSTP defensive evasion) with an argument. Lastly, fileless malware is used to execute the Revenge RAT.
- To impede malware operation even more, version.exe is engineered to execute a PowerShell command that adds the files utilized by the Revenge RAT virus to the Windows Defender exception list.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Detection	• Trojan/Win.Generic.C4223332 • Trojan/Win.Generic.C5583117 • Dropper/Win.Generic.C5445718 • Dropper/Win.Generic.R634030 • Backdoor/Win.REVENGERAT.C5582863 • Backdoor/Win.REVENGERAT.R634026
File hashes	• 42779ab18cf6367e7b91e621646237d1 (smtp-verifier.exe) • fb34fe9591ea3074f048feb5b515eb61 (Email To Sms V8.1.exe) • 6d5ad2adce366350200958c37f08a994 (setup.exe) • 914ec5019485543bb2ec8edcacd662a7 (setup.exe) • 5e24e97bbc8354e13ee3ab70da2f3af6 (svchost.exe) • 1242c41211464efab297bfa6c374223e (svchost.exe) • 438817d3938ae5758d94bf2022a44505 (explorer.exe) • 304e264473717fad8f7c6970212eaaa7 (version.exe)
C&C	• qcpanel.hackcrack[.]io:9561

Recommendation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Emails from unknown senders should always be treated with caution.
- Employee Training and Awareness.
- Users must take extra caution when using open source or public tools.
- Always download them from the official website.

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://gbhackers.com/fileless-revenge-rat-legitimate-tools/
- https://asec.ahnlab.com/en/61584/