China-Linked ValleyRAT Malware Resurfaces with Advanced Data Theft Tactics

Date: 11th June 2024 | Severity: High

Summary

ValleyRAT is a remote access trojan (RAT) that was initially documented in early 2023. Its main objective is to infiltrate and compromise systems, providing remote attackers with unauthorized access and control over infected machines. ValleyRAT is commonly distributed through phishing emails or malicious downloads. In the latest version, ValleyRAT introduced new commands, such as capturing screenshots, process filtering, forced shutdown, and clearing Windows event logs. Zscaler ThreatLabz recently identified a new campaign delivering the latest version of ValleyRAT, which involves multiple stages.

Attack Vectors

- Zscaler ThreatLabz discovered a new campaign used to deliver ValleyRAT, which is developed by a China-based threat actor.
- The initial stage downloader utilizes an HTTP File Server (HFS) to download the files required for the subsequent stages of the attack.
- The downloader and loader utilized in the campaign employ various techniques, including anti-virus checks, DLL sideloading, and process injection.
- The configuration to communicate to the command-and-control (C2) server is identified by a specific marker. The configuration data is then parsed to identify the C2 IP, port, and communication (UDP or TCP-based) protocol.
- The ValleyRAT sample delivered within the campaign has modifications when compared to the previously documented version. These changes have been observed in areas such as device fingerprinting, bot ID generation, and the commands supported by the RAT.

Indicator of compromise

INDICATOR TYPE	INDICATORS
FileHash	• 984878f582231a15cc907aa92903b7ab • 56384012e4e46f16b883efe4dd53fcb0 • 8c0cde825ee2d3c8b60cd2c21d174d4c • 85f1c63c40918eb300420152eaf78e2c • 0b63f0b83f78dff04ae26fe6b1da3b29 • 81ab4d6b9a07e354b52a18690f98b8aa • b79c69bb5d309b07e10a316ee9c2223e • ddb3c71de77a18421f6e86bc9fec6697 • eb953e5f2a3eb68756f779b3fa4d5c4e • 8995fbb4679ddd1516eacb3e453cb1ba • 58f7311956c41e99f630286baa49d0ac • cc31928547ea412b9c7655ce958574bd • 043b4cbe238bcf0b242dc2874e275bbc • 019a5c4e67492e412f08758a06b3b354 • abf0e40513a9d614266359e56ca54f90 • 2c6a865a746ca9f37f9381aa64c2c1eb • 00296149b1ec62f8280ba0b3d08152ee • 02c1f92036278dfeabdc89d1a17da28f • c2ad2a683ff1898dd692e7d856c13d44 • e9c4b65d39f73033d6ec3ee79bd39083 • 4df3bf214daaaafee88c455a384a4421 • 0d222e3084f9359a555acc3205c789fb • 92ae1aff368611d62afe51d43c91bf0b • 9aec2351a3966a9f854513a7b7aa5a13
URLs	• hxxp[:]//119[.]28[.]41[.]143/ • hxxp[:]//124[.]156[.]134[.]223/ • hxxp[:]//101[.]33[.]117[.]200/ • hxxp[:]//43[.]129[.]233[.]146/ • hxxp[:]//43[.]132[.]212[.]111/ • hxxp[:]//43[.]129[.]233[.]99/ • hxxp[:]//119[.]28[.]32[.]143/ • hxxp[:]//43[.]132[.]235[.]4/ • hxxp[:]//wenjian2024[.]com/57683653%E5%87%BD%E6%95%B0[.]exe • hxxps[:]//2024aasaf[.]oss-cn-hongkong[.]aliyuncs[.]com/TARE965624%20[.]exe • hxxps[:]//2024fapiao[.]oss-cn-hongkong[.]aliyuncs[.]com/82407836%E5%87%BD%E6%95%B0[.]exe • hxxps[:]//scpgjhs[.]com/TARE965624[.]exe • hxxp[:]//mtw[.]so/6oAUvN • hxxp[:]//kfurl[.]cn/kvukj • hxxp[:]//mtw[.]so/5Fytvq

Recommendation

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Be cautious when clicking links or downloading files from unknown or suspicious websites.
- Stick to reputable sources for software downloads and content.
- Be wary of unexpected and irrelevant emails, especially those with attachments or links.
- Avoid opening attachments or clicking links from unfamiliar or unexpected sources (email addresses).
- Avoid interacting with shady ads (e.g., pop-ups) while visiting suspicious pages.
- Regularly update your operating system, software applications, and antivirus/anti-malware programs.
- If you believe that your computer is already infected, we recommend running a scan with Combo Cleaner Antivirus for Windows to automatically eliminate infiltrated malware.

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://www.zscaler.com/blogs/security-research/technical-analysis-latest-variant-valleyrat
- https://thehackernews.com/2024/06/china-linked-valleyrat-malware.html