Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

New Face of ValleyRAT: Enhanced Commands and Infiltration Tactics

Date of Publication	Admiralty Code	TA Number
June 11, 2024	A1	TA2024225

Summary

First Seen: 2023
Malware: ValleyRAT
Attack Region: Worldwide
Attack: ValleyRAT, discovered in 2023 and linked to a China-based threat actor, is a Remote Access Trojan (RAT). This sophisticated malware employs a multi-stage infection process to execute various malicious activities. Its primary goal is to infiltrate and compromise systems, granting attackers unauthenticated remote access.

Attack Regions

Attack Details

#1 ValleyRAT is a sophisticated Remote Access Trojan (RAT) identified in 2023, developed by a China-based threat actor. It employs a complex multi-stage infection process to deploy its final payload, enabling various malicious activities.

#2 The ValleyRAT malware's primary objective is to infiltrate and compromise systems, granting unauthenticated remote access to attackers. Distribution typically occurs via phishing emails and malicious downloads. The latest version includes new commands for capturing screenshots, filtering processes, rebooting or forcing shutdowns, and clearing Windows event logs.

#3 The primary downloader in the attack sequence uses HTTP File Servers (HFS) to obtain five crucial files, employing techniques such as DLL sideloading and process injection. Additionally, the decrypted DLL is intricately crafted to identify and disable anti-malware solutions such as Qihoo 360 and WinRAR, thus avoiding detection. Subsequently, the downloader proceeds to retrieve three more files

#4 Injected shellcode contains configuration information and resolves APIs to connect with a command-and-control (C2) server, downloading the ValleyRAT payload as a DLL file. The final stage involves executing the payload, with the C2 server parsing data to determine the IP, port, and communication protocol, and implementing sleep duration before confirming the payload's presence on the victim host.

Recommendations

Deep Packet Inspection (DPI): Employ DPI technologies to inspect network traffic at the packet level, enabling the detection of malicious payloads or command-and-control communications associated with remote access trojans.

Access Control and Least Privilege Principle: Limit user privileges to only what is necessary for their roles and responsibilities. This helps reduce the impact of potential ValleyRAT infections by limiting attackers' access to critical systems and data.

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats like RAT by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0008** Lateral Movement	**TA0011** Command and Control	**TA0010** Exfiltration
T1036 Masquerading	**T1574.002** DLL Side-Loading	**T1055** Process Injection	**T1140** Deobfuscate/Decode Files or Information
T1010 Application Window Discovery	**T1057** Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1120 Peripheral Device Discovery	**T1518.001** Security Software Discovery	**T1071** Application Layer Protocol	**T1659** Content Injection
T1113 Screen Capture	**T1529** System Shutdown/Reboot	**T1087** Account Discovery	**T1135** Network Share Discovery
T1012 Query Registry	**T1106** Native API	**T1056** Input Capture	**T1566.001** Spearphishing Attachment
T1068 Exploitation for Privilege Escalation	**T1001** Data Obfuscation	**T1070.001** Clear Windows Event Logs	**T1070** Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	984878f582231a15cc907aa92903b7ab, 56384012e4e46f16b883efe4dd53fcb0, 8c0cde825ee2d3c8b60cd2c21d174d4c, 85f1c63c40918eb300420152eaf78e2c, 0b63f0b83f78dff04ae26fe6b1da3b29, 81ab4d6b9a07e354b52a18690f98b8aa, b79c69bb5d309b07e10a316ee9c2223e, ddb3c71de77a18421f6e86bc9fec6697, eb953e5f2a3eb68756f779b3fa4d5c4e, 8995fbb4679ddd1516eacb3e453cb1ba, 58f7311956c41e99f630286baa49d0ac, cc31928547ea412b9c7655ce958574bd, 043b4cbe238bcf0b242dc2874e275bbc, 019a5c4e67492e412f08758a06b3b354, abf0e40513a9d614266359e56ca54f90, 2c6a865a746ca9f37f9381aa64c2c1eb, 00296149b1ec62f8280ba0b3d08152ee, 02c1f92036278dfeabdc89d1a17da28f, c2ad2a683ff1898dd692e7d856c13d44, e9c4b65d39f73033d6ec3ee79bd39083, 4df3bf214daaaafee88c455a384a4421, 0d222e3084f9359a555acc3205c789fb, 92ae1aff368611d62afe51d43c91bf0b, 9aec2351a3966a9f854513a7b7aa5a13, 0a55af506297efa468f49938a66d8af9, 442f4ea7a33d805fb8944eb267b1dfad, c563f62191ea363259939a6b3ce7f192
URLs	hxxp[:]//hotshang[.]com/, 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/, hxxps[:]//2024aasaf[.]oss-cn-hongkong[.]aliyuncs[.]com/TARE961424[.]exe, hxxp[:]//wenjian2024[.]com/57683653%E5%87%BD%E6%95%B0[.]exe,

TYPE	VALUE
URLs	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, hxxps[:]//tzsxr[.]com/customer[.]exe, hxxp[:]//mtw[.]so/6oAUvN, hxxp[:]//kfurl[.]cn/kvukj, hxxp[:]//mtw[.]so/5Fytvq, hxxps[:]//fpwenj[.]zhangyaodong5[.]com/TARE985624[.]exe, hxxps[:]//2024aasaf[.]oss-cn-hongkong[.]aliyuncs[.]com/TARE967124[.]exe
File Path	C:\Program Files\TCLS, C:\Users\xig.ppt
File Name	client.exe, NTUSER.DXM, WINWORD2013.EXE, wwlib.dll, xig.ppt

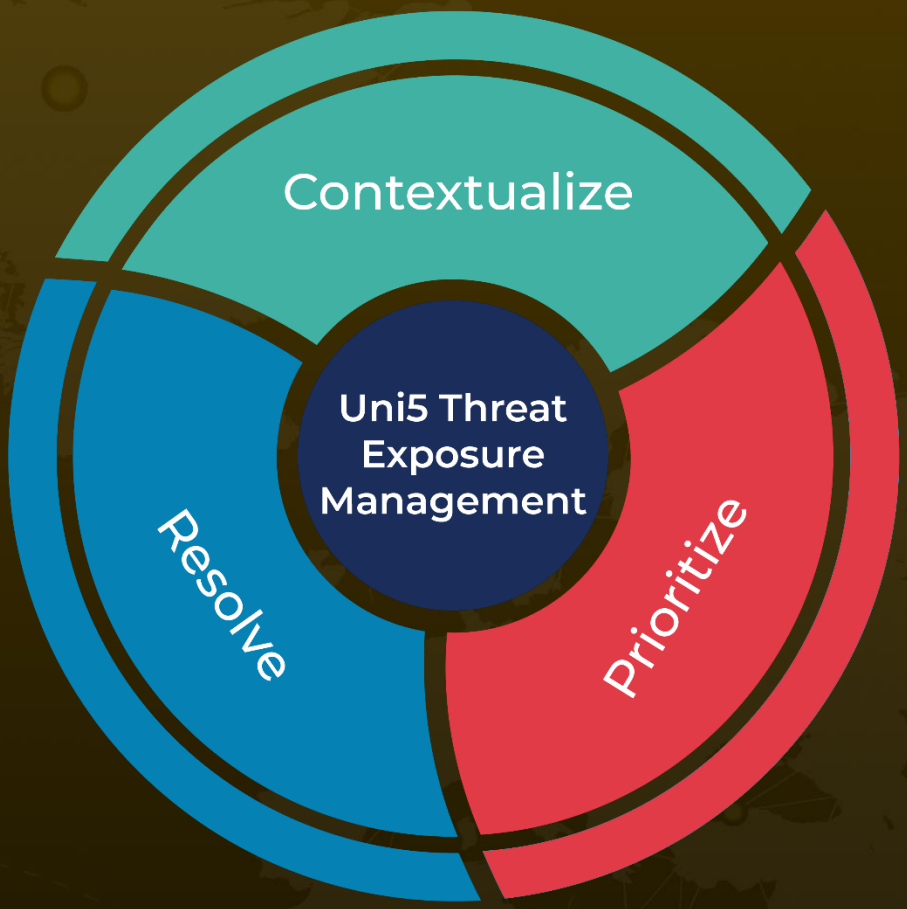
References

https://www.zscaler.com/blogs/security-research/technical-analysis-latest-variant-valleyrat

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 11, 2024 • 9:00 PM

More at www.hivepro.com