Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

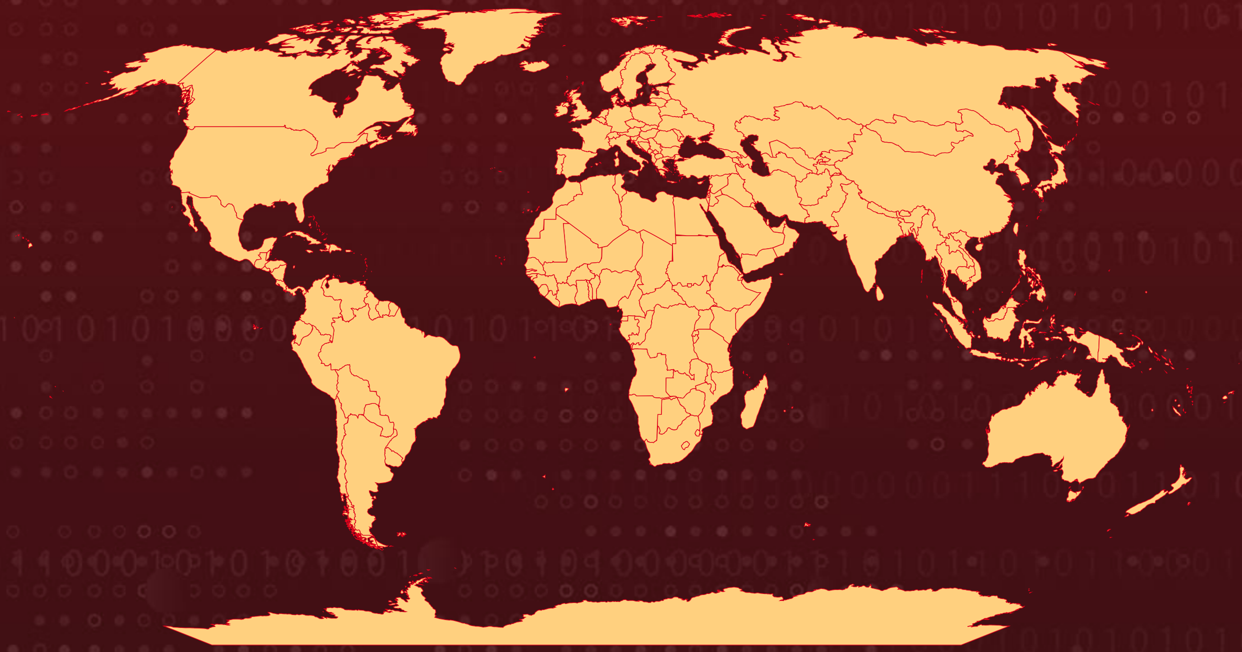
ValleyRAT Strikes Organizations with Stealthy DLL Hijacking Attack

Date of Publication	Admiralty Code	TA Number
February 7, 2025	A1	TA2025034

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Affected Platform: Windows
Malware: ValleyRAT
Attack: ValleyRAT, a remote access trojan (RAT) first discovered in 2023, has evolved with a multi-stage infection process and enhanced evasion tactics to ensure persistent access and control over compromised systems. Attackers are actively distributing the malware through fake websites impersonating official Google Chrome download pages, deceiving users into unknowingly installing ValleyRAT. To maximize the campaign's effectiveness, they continuously refine their tactics, recycle URLs, and adapt their techniques, making detection and mitigation increasingly challenging.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 ValleyRAT, a remote access trojan (RAT) linked to the Silver Fox APT, has evolved with new attack techniques and enhanced stealth tactics this year. The group employs multiple distribution methods, including phishing emails, fake websites, and instant messaging platforms, to deliver the malware. In earlier campaigns, they disguised malicious installers as legitimate software, using scripts to execute their payloads.

#2 Previous versions of ValleyRAT featured capabilities such as screenshot capture, process filtering, forced system reboots or shutdowns, and Windows event log deletion. In its latest iteration, the operators have created a fake website impersonating a Chinese telecom company, distributing malware through a deceptive installer.

#3 The attack begins when a victim unknowingly downloads a fake Chrome installer from a phishing website. This .NET-based setup file first checks for administrator privileges before downloading four files into the C:\Program Files (x86)\Common Files\System\ directory. The malware then loads a DLL into memory and executes a legitimate TikTok executable, exploiting DLL side-loading to execute malicious code discreetly.

#4 A key evasion technique used by ValleyRAT is injecting a DLL into SVCHOST.exe, enabling it to monitor and terminate specific processes while avoiding detection. Additionally, tier0.dll, a library commonly associated with Valve's Source Engine, is manipulated to establish persistence on the infected system.

#5 Once inside, ValleyRAT interacts directly with the Windows Station, granting it control over screen, keyboard, and mouse inputs. It leverages Windows API functions to access the user's interactive session while suppressing error messages to remain hidden. The malware also monitors connected displays, allowing attackers to capture on-screen activity in real time.

#6 Before establishing communication with its command-and-control (C2) server, ValleyRAT first checks for virtualized environments by scanning for VMware tools and processes. If no VM is detected, it attempts to reach www.baidu.com as a network connectivity test. The final objective of the malware is to establish persistent access, exfiltrate data, and enable remote control over compromised systems while maintaining a low profile.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Strengthening Defenses: Limit script execution by disabling the automatic running of .BAT, .PS1, .DLL, and other script files from untrusted sources to prevent malware from installing itself. At the same time, keep a close watch on network traffic identify and block any unusual outbound connections, especially those reaching unknown IPs or domains, to cut off communication with command-and-control (C2) servers.

Limit Administrative Access: Apply the principle of least privilege to prevent malware from gaining high-level permissions and making critical system changes.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1566 Phishing	**T1566.002** Spearphishing Link	**T1204** User Execution	**T1204.002** Malicious File
T1056 Input Capture	**T1056.001** Keylogging	**T1082** System Information Discovery	**T1140** Deobfuscate/Decode Files or Information
T1027 Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1497** Virtualization/Sandbox Evasion	**T1057** Process Discovery

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading
T1036 Masquerading	**T1055** Process Injection	**T1548** Abuse Elevation Control Mechanism	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	149[.]115[.]250[.]19, 149[.]115[.]052[.]91, 8[.]217[.]244[.]40, 154[.]82[.]85[.]79, 149[.]115[.]250[.]19, 118[.]107[.]44[.]219, 43[.]250[.]172[.]42, 202[.]146[.]222[.]208, 103[.]183[.]3[.]10
URLs	hxxps[:]//anizom[.]com/, hxxps[:]//karlost[.]club/
SHA256	53A6735CE1ECA68908C0367152A1F8F3CA62B801788CD104F53D037811284D71, 6ED466A2A6EEB83D1FF32BA44180352CF0A9CCC72B47E5BD55C1750157C8DC4C, 311f2d4ef2598e4a193609c3cd47bf4ff5fb88907026946ecffe6b960d43d5b2, a87745682da20ddfd6eac7ff2d27fec73ff56c6e9b4438121dcb6ba699c5cb3c, 1db77692eaf4777f69ddf78c52424d81834572f1539ccea263d86a46f28e0cea, 3989f7fa8d1d59ebc6adea90e3958a892b47d94268bf9d5c9c96811f3fb65b00, 7c2a1b09617566ff9e94d0b1c15505213589f7fd3b445b334051d9574e52e0f5, bb89e401560ba763d1c5860dd51667ba17768c04d00270bf34abebac47fd040e, 51a9d06359952f6935619e8cf67042d2cec593788c324b72cffc0d34b1762bb0, 968b976167b453c15097667b8f4fa9e311b6c7fc5a648293b4abd75d80b15562

References

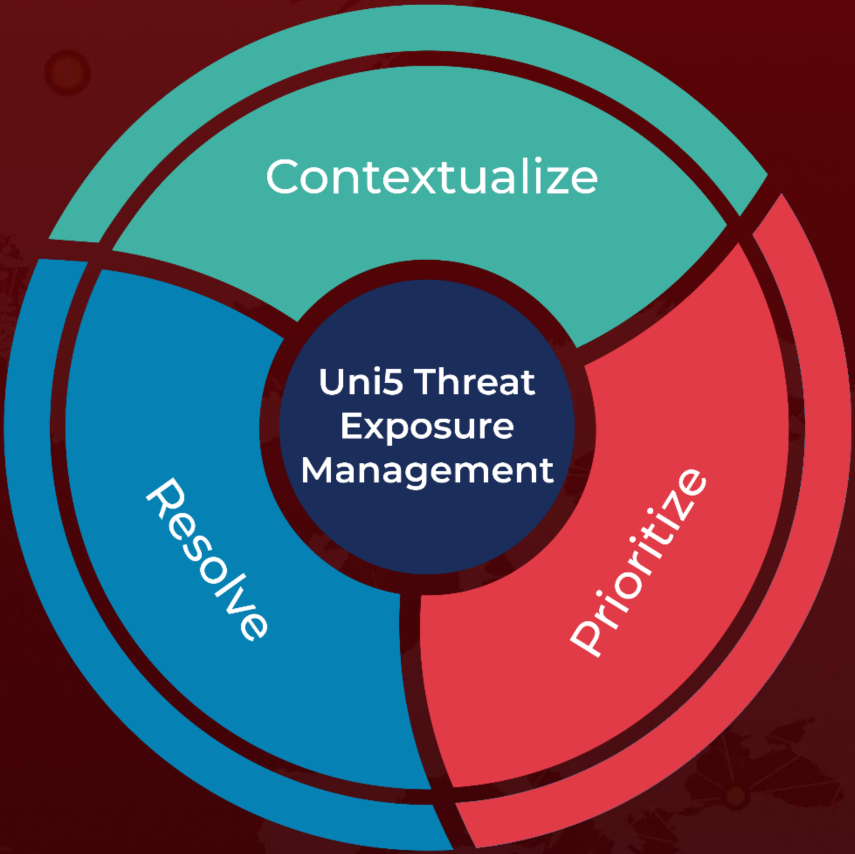
https://www.morphisec.com/blog/rat-race-valleyrat-malware-china/

https://www.hivepro.com/threat-advisory/new-face-of-valleyrat-enhanced-commands-and-infiltration-tactics/

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

February 7, 2025 • 7:00 AM

More at www.hivepro.com