ValleyRAT – Malware Trends Tracker by ANY.RUN

By Stanislav Gayvoronsky

Archived: 2026-04-05 23:15:11 UTC

What is Valley RAT malware?

ValleyRAT is a C++-based RAT first identified in early 2023. It is associated with the Silver Fox advanced persistent threat (APT) group, a suspected China-based threat actor.

It stands out of the plenty of RATs for its multi-stage infection chain, heavy reliance on shellcode for execution, and a focus on espionage and data theft. It is designed to infiltrate systems, maintain persistence, and provide attackers with extensive remote control. Including the ability to monitor activities, steal data, and deploy additional malicious plugins.

ValleyRAT employs a variety of distribution methods: phishing and spear-phishing emails, compromised websites, social engineering via instant messengers, fake downloads and DLL hijacking. For the initial infection, a loader disguised as a legitimate file is used, which triggers a multi-stage process to deploy the full payload discreetly.

The loader executes shellcode directly in memory thus minimizing its disk footprint and visibility to file-based detection tools.

Once rooted in the system, ValleyRAT provides attackers with its remote control (including keyboard, mouse, screen interaction via WinSta0), allows data exfiltration, file execution, and additional plugin deployment. Screenshot capture, keylogging, and activity monitoring are also performed.

ValleyRAT Ransomware’s Prominent Features

- **Targeted Espionage**: It focuses on high-value roles in finance, accounting, sales, and management, particularly within Chinese enterprises, to steal sensitive corporate data for financial fraud or insider threats.
- **Phased Deployment**: (loader → shellcode → C2 → payload) of ValleyRAT is more complex than many single-stage RATs, enhancing stealth.
- **Expanded Attack Surface**: By exploiting gaming software and other non-traditional vectors, it broadens its reach beyond typical enterprise targets.
- **Persistent Access**: ensures long-term control, enabling prolonged espionage campaigns.

- **Geopolitical Implications**: Linked to the Silver Fox APT, ValleyRAT aligns with state-sponsored tactics, suggesting potential use in cyber warfare or intelligence gathering against Chinese-speaking regions.

ValleyRAT Execution Process and Technical Details

The complicated behavior of ValleyRAT is observable in ANY.RUN's Interactive Sandbox. Let's explore its processes, IOCs, connections, and other activities.

View sandbox analysis

During the first stages, ValleyRAT may employ techniques such as DLL sideloading and exploiting legitimate signed executables that are vulnerable to DLL search order hijacking. Additionally, process injection is used to inject malicious code into processes like svchost.exe. This allows ValleyRAT to execute its payload, which may include shellcode that decrypts an encrypted PE file in memory for execution without leaving traces on the disk. The payload also includes hooks to bypass security mechanisms like AMSI (Antimalware Scan Interface) and ETW (Event Tracing for Windows).

To ensure persistence, ValleyRAT modifies registry settings under Software\Microsoft\Windows\CurrentVersion\Run or, in our analysis, in the startup directory %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ by using the Windows Command Shell (CMD). It also stores files in directories such as C:\ProgramData. Once established, ValleyRAT communicates with its Command-and-Control (C2) server using UDP or TCP protocols. The commands supported by ValleyRAT include capturing screenshots, executing files or DLLs, setting startup configurations, filtering processes, and clearing event logs.

To avoid running multiple instances of itself, the malware creates mutexes. In our case, the mutex " V‰°5i™þ«" contains non-standard characters.

It abuses Windows COM interfaces (e.g., CMSTPLUA, fodhelper.exe) to bypass User Account Control (UAC) and gain elevated privileges, often adjusting its security token to SeDebugPrivilege for deeper system access.

ValleyRAT employs multiple stealth mechanisms to evade detection. These include anti-VM checks to detect VMware environments and avoid analysis, as well as keylogging and screen monitoring capabilities to log keystrokes and collect screen data for remote control. Additionally, ValleyRAT injects DLLs into critical processes to prevent security applications from launching. This multi-layered execution chain highlights ValleyRAT's ability to infiltrate systems stealthily while maintaining persistence and evading detection.

ValleyRAT analysis in ANY.RUN *ValleyRAT sample analysis inside ANY.RUN's Interactive Sandbox*

Its famous arsenal of evasion tactics includes:

- **Memory-Based Execution**: It heavily relies on shellcode executed in memory rather than writing files to disk, reducing its traceable footprint.
- **Process Injection**: By injecting malicious code into legitimate processes, it masks its activities within normal system operations.

- **Sleep Obfuscation**: It uses sleep routines to alter memory permissions, evading memory scanners and sandbox analysis.
- **Encryption**: Shellcode is encrypted (e.g., XOR with keys like 0x27 or AES-256), making it harder for signature-based tools to identify.
- **Anti-VM and Sandbox Checks**: It terminates if it detects virtualized environments or common analysis tools (e.g., VMware, WeChat/DingTalk registry checks as a kill switch).
- **Security Tool Disruption**: ValleyRAT targets antivirus processes (e.g., Qihoo's ZhuDongFangYu) for termination and modifies registry settings or Windows Defender exclusions to disable defenses.
- **Legitimate Tool Abuse**: It leverages trusted Windows utilities (e.g., MSBuild.exe) and signed executables to blend in with normal activity.

What are the examples of the best-known ValleyRAT attacks?

While specific attacks are not always publicly detailed with victim identities due to the sensitive nature of espionage-driven attacks, cybersecurity researchers have documented key campaigns that highlight ValleyRAT's success in infiltrating systems, evading detection, and achieving its objectives.

1. **Impersonation of Chinese Telecom Companies (2024)**: Attackers created fraudulent websites mimicking legitimate Chinese telecom firms to distribute ValleyRAT. It employed DLL hijacking, utilizing legitimate game-related binaries to execute its payload stealthily. Users downloaded malicious software, leading to system compromises.
2. **Targeted Attacks on Chinese-Speaking Enterprises (August 2024)**: A campaign aimed at Chinese-speaking users of companies in e-commerce, finance, sales, and management sectors.
3. **Resume-Themed PDF Campaign (May 2023)**: Victims received PDFs mimicking job resumes, which, when opened, directed users to download ValleyRAT via malicious URLs. The RAT was deployed alongside a Rust-based loader, enhancing its stealth and delivery efficiency. This campaign successfully targeted high-value individuals, likely in corporate environments. The use of PDFs broadened its attack surface beyond traditional executable files, catching security systems off-guard.
4. **Trojanized Medical Imaging Software in Healthcare Sector (February 2025)**: The Silver Fox APT group embedded ValleyRAT within counterfeit versions of Philips DICOM viewer software.
5. **Fake Chrome Download Campaign (February 2025)**: Victims downloaded a ZIP archive containing "Setup.exe," which sideloaded malicious DLLs (e.g., "tier0.dll" from Valve games, "sscronet.dll") via legitimate executables like Douyin.exe. ValleyRAT then logged keystrokes, monitored screens, and established C2 communication, using Donut shellcode for in-memory execution.

The latter campaign's reuse of URLs, gaming software exploitation, and focus on key organizational roles demonstrated Silver Fox's strategic shift toward both wider and more precise targeting, cementing ValleyRAT's reputation as a versatile RAT.

Gathering threat intelligence on ValleyRAT malware

It would be a painful challenge to scrape ValleyRAT out of your system considering its persistence and evasion "talents". And, of course, losses calculation and mitigation would be even more painful. So, it's much better not to invite the digital culprit in.

Use threat intelligence to study and recognize ValleyRAT TTPs, and to gather IOCs, IOAs, and IOBs for tuning your monitoring and detection systems. You can also leverage ANY.RUN's TI Feeds to be updated with the new ValleyRAT's identificators automatically.

ValleyRAT has a habit of reusing the same URLs or IP addresses across campaigns, and besides, it often employs unique mutexes. Address ANY.RUN's Threat Intelligence Lookup and start your research with malware's name:

threatName:"valleyrat"


ValleyRAT search results in TI Lookup _ ValleyRAT samples in ANY.RUN's Sandbox_

ValleyRAT often leaves byte patterns that can be matched by custom or shared YARA rules. Suricata rules are also of much help in detecting the trojan's malicious processes. This is what the detalization of such process looks like in TI Lookup:


ValleyRAT process detailed *Details on ValleyRAT actions in the system*

Integrate ANY.RUN's threat intelligence solutions in your company

Contact us

Conclusion

ValleyRAT is an example of modern malware evolution, blending traditional RAT functionality with advanced evasion and persistence tactics. Its danger lies in its ability to quietly infiltrate networks, target valuable data, and maintain long-term access. Countering it demands a blend of cutting-edge detection tools, robust threat intelligence, and proactive security measures to stay ahead of its cunning Silver Fox operators.

Though it did start as a threat for Chinese enterprise and users, now, if you are on the opposite side of the world from China, you are not safe. APTs' appetites always grow, so be ready and proactive against ValleyRAT.

Gather IOCs on ValleyRAT with 50 trial requests in TI Lookup
