*February 07, 2025*

# Fake Google Chrome Sites Distribute ValleyRAT Malware via DLL Hijacking

## Overview

Fake Google Chrome websites are being used to distribute ValleyRAT, a remote access trojan (RAT) linked to the Silver Fox threat actor. The malware primarily targets Chinese-speaking regions and high-value corporate roles in finance, accounting, and sales. Attackers use DLL hijacking via bogus Chrome installers to execute ValleyRAT stealthily, enabling keystroke logging, screen monitoring, and remote command execution.

## CTI Analysis

Silver Fox has been active since 2023, previously using Purple Fox and Gh0st RAT in attacks. The infection chain involves drive-by downloads, where users searching for Chrome are redirected to fake installer sites. The downloaded Setup.exe installs multiple payloads, leveraging DLL hijacking through Douyin.exe to execute ValleyRAT. The malware communicates with a remote C2 server for further instructions and persistence.

## Impact Analysis

Organizations face risks of data theft, credential compromise, and network-wide infections, particularly affecting high-value roles with access to sensitive financial data. Individuals are vulnerable to identity theft, keylogging, and unauthorized remote access, increasing the risk of financial fraud and personal data leaks. ValleyRAT's persistence and execution of arbitrary DLLs and binaries make it a long-term threat.

**Mitigation**

- Download software only from official sources (e.g., Google's website).
- Enable application whitelisting to block unauthorized executables.
- Monitor network traffic with Suricata IDS to detect suspicious connections.
- Deploy endpoint security solutions (e.g., Wazuh for behavioral analysis).
- Block access to malicious websites via DNS filtering.

**Conclusion**

The ValleyRAT campaign highlights the dangers of malware-laden fake software installers, exploiting user trust and DLL hijacking techniques. Organizations and individuals must adopt strict cybersecurity measures, including network monitoring, endpoint protection, and software integrity verification, to prevent infection and mitigate potential damage.

**Source**

- https://thehackernews.com/2025/02/fake-google-chrome-sites-distribute.html