AL2025_37 Silver Fox Exploits Microsoft-Signed WatchDog Driver to Deploy ValleyRAT Malware (September 19th , 2025)

Description

The cybercrime group Silver Fox (aka SwimSnake, UTG-Q-1000, Void Arachne) has been linked to a Bring Your Own Vulnerable Driver (BYOVD) campaign that abuses a previously undisclosed flaw in the WatchDog Anti-malware driver (amsdk.sys). The vulnerable driver, which was Microsoft-signed but not blocklisted, allows attackers to disable security solutions and escalate privileges.

This campaign primarily targets Chinese-speaking victims through phishing, SEO poisoning, and trojanized software masquerading as popular applications (Chrome, Telegram, DeepSeek, WPS Office). The end goal is to deliver ValleyRAT (Winos 4.0), a modular remote access trojan capable of espionage, persistence, and financial fraud.

Attack Details

The Silver Fox campaign leverages a dual-driver exploitation strategy, using the known vulnerable zam.exe Zemana driver against Windows 7 systems and the previously undetected amsdk.sys WatchDog driver against Windows 10 and 11 machines. Through these drivers, attackers gain the ability to terminate arbitrary processes bypassing Protected Process Light (PPL) and achieve local privilege escalation (LPE) via weak access control. In a sophisticated evasion technique, the group abuses Microsoft's signing process by flipping a single byte in the timestamp field, preserving the valid digital signature while bypassing hash-based blocklists. The attack chain also incorporates anti-analysis features, enabling the malware to detect virtual environments, sandboxes, and hypervisors, and abort execution if flagged. The final payload is ValleyRAT, a modular remote access trojan delivered through a custom loader embedding two vulnerable drivers, antivirus-killer logic, and a DLL downloader. ValleyRAT provides attackers with full remote control, supports data theft from platforms like WeChat and online banking systems, captures screenshots, and harvests credentials. Silver Fox operates through multiple sub-groups, including the Finance Group, which targets enterprise financial staff with phishing lures related to taxes, invoices, and personnel transfers, as well as the News & Romance Group, Design & Manufacturing Group, and Black Watering Hole Group, which focus on espionage, trojanized software distribution, and watering hole attacks.

Remediation

Patch vulnerable drivers:

1. Update WatchDog Anti-malware to **v1.1.100** or later.
2. Enforce the **Microsoft Vulnerable Driver Blocklist (HVCI-enabled systems)**.

Detection & Monitoring:

3. Monitor for the presence of amsdk.sys and zam.exe.
4. Flag attempts to load unsigned or suspiciously modified signed drivers.
5. Watch for **anti-analysis behavior** and fake system error messages during execution.

Endpoint Protection:

6. Deploy **EDR solutions** capable of detecting BYOVD techniques.
7. Enable **Protected Process Light (PPL)** enforcement where possible.

Network Defense:

8. Block access to **known Silver Fox C2 servers** and cloud storage links distributing malware.
9. Monitor **outbound traffic** for suspicious communications to Alibaba Cloud OSS / Youdao Cloud Notes.

User Awareness & Training:

10. Educate staff about **phishing risks** (fake invoices, tax forms).
11. Warn against downloading apps from unofficial websites or search engine ads.

Incident Response:

12. If infected, isolate systems immediately.
13. Perform forensic analysis to identify persistence mechanisms.
14. Rotate credentials and audit for financial fraud attempts.
    a.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2025, August 15). Researcher to release exploit for full auth bypass on FortiWeb. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/researcher-to-release-exploit-for-full-auth-bypass-on-fortiweb/all-confirms-patched.html?m=1
- PSIRT | FortiGuard Labs. (n.d.). Retrieved from FortiGuard Labs. https://fortiguard.fortinet.com/psirt/FG-IR-25-448