SILVER FOX

[/ 'sil.vɪr faks /]

Silver Fox, a China-aligned APT active since 2022, conducts espionage and financially motivated attacks. Evolving from simple RATs to advanced kernel-level evasion, it abuses signed drivers and fake websites to spread malware. Assessed as high risk, it targets government, tech, telecom, and financial sectors across Europe, East Asia, and global enterprises.

IDENTITY

Attribution	: China-aligned cybercrime/APT group
Active Since	: At least 2022, with major campaigns documented through 2025
Aliases	: Silver Fox, Void Arachne, Valley Thieves, UTG-Q-1000, The Great Thief of the Valley
Motivation	: Mixed: cyberespionage against government and enterprises, financially motivated malware and ransomware distribution

TTPs

Initial Access	: Phishing with weaponized Google Translate pages, fake software websites (WPS Office, DeepSeek), exploitation of vulnerable file transfer software
Persistence	: Abuse of scheduled tasks, credential theft, rootkit deployment, use of Microsoft-signed vulnerable drivers for stealth persistence
C2 Infrastructure	: TOR-based infrastructure, proxy botnets, commercial VPN fallback
Malware & Tools	: ValleyRAT, Sainbox RAT, Hidden Rootkit, PlugX variants, credential stealers
Techniques	: Kernel-level evasion, lateral movement in hybrid cloud and enterprise networks, supply chain targeting of IT and telecom providers

TARGET PROFILE

Target Sectors	: Government and diplomatic entities, technology and telecom providers, cloud service companies, financial and corporate enterprises
Geographies Targeted	: *Primary:* Europe, East Asia, multinational corporate environments, *Secondary:* Africa and broader APAC via telecom and IT supply chain intrusions

THREAT ASSESSMENT

Risk Level	: High: capable of bypassing EDR/AV and rapidly adapting to defensive measures
Most Recent Activity	: 2025, Microsoft driver abuse (WatchDog, Zemana) for evasion and ValleyRAT deployment 2025, Fake WPS Office and DeepSeek websites distributing Sainbox RAT with Hidden Rootkit 2025, Weaponized Google Translate phishing delivering Windows malware
Evolution	: Transition from commodity RAT distribution to advanced kernel-level and supply chain operations, indicating maturity into a hybrid APT and cybercrime actor

NOTABLE OPERATIONS

- **2024:** Telecom intrusions in Europe using VPN zero-days for espionage
- **2024:** Finance sector compromise in APAC with data exfiltration and resale on dark web
- **Q1 / 2025:** Supply chain attack leveraging Cleo file transfer software vulnerabilities
- **Q2 / 2025:** Credential harvesting against government ministries in the Middle East