Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

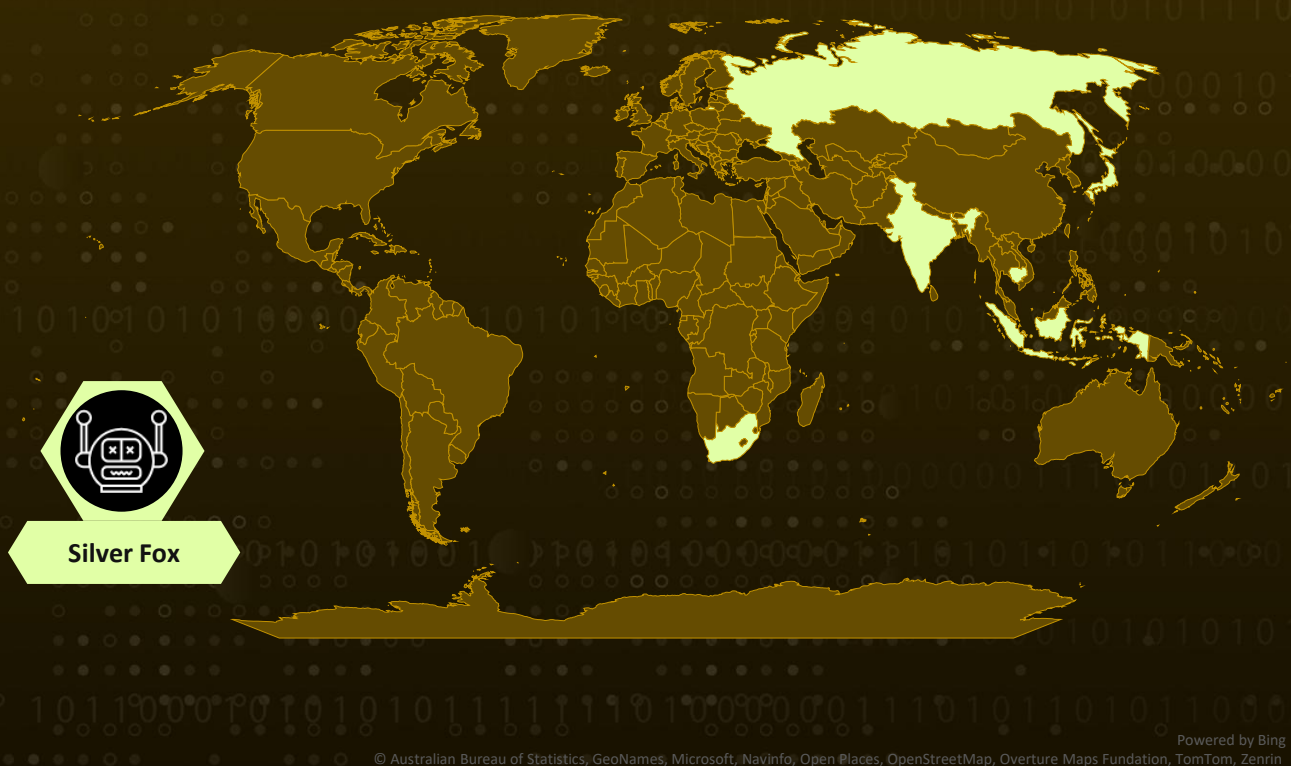
Tax Trap to Full Takeover: Inside the Silver Fox Multi-Stage Intrusion Chain

Date of Publication	Admiralty Code	TA Number
May 05, 2026	A1	TA2026120

Summary

First Seen: December 2025
Targeted Regions: India, Russia, Indonesia, South Africa, Cambodia, Japan
Targeted Platforms: Windows
Targeted Industries: Industrial, Consulting, Retail, Transportation
Threat Actor: Silver Fox (aka Void Arachne)
Malware: ValleyRAT, ABCDoor, RustSL
Attack: Silver Fox, a China-based threat group, conducted a large-scale phishing campaign impersonating tax authorities in India and Russia to deliver ValleyRAT and a previously undocumented Python-based backdoor called ABCDoor. Over 1,600 malicious emails were distributed between early January and early February 2026, using PDF attachments with embedded malicious links or directly attached archives containing a modified Rust-based loader (RustSL) to execute the infection chain.

Attack Regions



Attack Details

#1

The China-based cybercrime group known as Silver Fox launched a campaign that begins with what appears to be a routine tax notice but quickly unfolds into a carefully orchestrated intrusion. First observed in December 2025, the operation targeted Indian organizations using phishing emails crafted to mimic official communication from the Income Tax Department. By January 2026, the campaign expanded to Russian entities, this time impersonating the national tax authority. In both waves, the attackers exploited trust in government messaging, using lures such as audit notifications or downloadable lists of alleged tax violations. Some emails were even distributed via SendGrid, adding a layer of legitimacy. Delivery methods included PDFs with embedded malicious links and RAR archives carrying executables disguised as familiar document formats, with the PDF-based approach helping bypass email security controls.

#2

Once the user engages, the attack chain quietly escalates. The disguised executable deploys a modified version of RustSL, an open-source Rust-based shellcode loader adapted under the Silver Fox toolkit. This variant integrates custom modules for stealth, including multi-layer XOR decryption for payload extraction and geofencing checks to evade sandbox and virtualized environments. The payload itself may be embedded within the loader, fetched from attacker-controlled infrastructure disguised as an image, or bundled with benign-looking files. After decryption, the loader retrieves ValleyRAT (Winos 4.0), enabling command-and-control communication, remote execution, and modular expansion. A later iteration introduced “Phantom Persistence,” a technique that manipulates the Windows restart process to relaunch the malware under the pretense of a system update.

#3

With a foothold established, the attackers extend control through additional ValleyRAT plugins. These modules perform further geolocation checks before delivering a secondary payload containing the ABCDoor backdoor, a portable Python environment, and a legitimate ffmpeg binary for screen capture. The files are staged in a directory mimicking the Tailscale VPN service, making detection more difficult during forensic analysis. Execution is handled through pythonw.exe via a batch script, blending malicious activity with legitimate processes. The operation also demonstrates resilience by leveraging multiple fallback download methods, including native Windows APIs and command-line tools like PowerShell and curl.

#4

At its core, ABCDoor is a Python-based backdoor compiled with Cython, built for persistent and covert access. It communicates over HTTPS using asynchronous networking, enabling operators to monitor and control infected systems in real time. Rather than relying on a traditional shell, it emphasizes visual surveillance through screen capture while supporting file execution, clipboard exfiltration, process management, and user input control. Persistence is maintained through registry modifications and scheduled tasks, ensuring continued access. Over time, ABCDoor has steadily evolved within the Silver Fox arsenal, transitioning from earlier C++ and Go-based delivery methods to more adaptable and evasive techniques, reflecting a clear progression in both tooling and operational sophistication.

Recommendations

- **Implement Email Gateway Filtering for PDF Link Analysis:** Configure email security gateways to perform deep inspection of PDF attachments for embedded URLs, particularly those linking to external download sites, rather than relying solely on attachment scanning. Flag emails impersonating tax authorities with external download links for manual review.

- **Monitor for Phantom Persistence Artifacts:** Deploy detection rules that monitor for abuse of the RegisterApplicationRestart API, unexpected SetProcessShutdownParameters calls with non-standard priority values (e.g., 0x4FF), and anomalous shutdown-reboot sequences that may indicate Phantom Persistence exploitation.

- **Restrict PowerShell and Script Execution Policies:** Enforce constrained language mode for PowerShell and restrict the execution of unsigned scripts, particularly those that download and install NodeJS or invoke remote scripts via Invoke-WebRequest or irm (Invoke-RestMethod) piped to iex (Invoke-Expression).

- **Block Unauthorized Software Installations:** Implement application control policies that prevent unauthorized installation or execution of portable Python environments, NodeJS runtimes, and ffmpeg binaries from user-writable directories such as %LOCALAPPDATA%, %TEMP%, and %USERPROFILE%\.node\.

Conduct Security Awareness Training on Tax-Themed Phishing: Educate employees through regular training sessions on the risks of tax-themed phishing lures, emphasizing the need to verify all emails purporting to be from tax authorities through official channels before opening attachments or clicking embedded links.

Implement Geolocation-Based Anomaly Detection: Since the malware performs geofencing checks using public IP geolocation services (ip-api.com, ipwho.is, ipinfo.io, ipapi.co, geoplugin.net), monitor for unusual outbound requests to these five services from endpoint devices, which may indicate an active infection in the pre-execution phase.

Segment Network and Enforce Least Privilege: Ensure proper network segmentation to limit lateral movement, and enforce least-privilege access policies to reduce the impact of credential compromise. Monitor for unexpected outbound HTTPS connections to unfamiliar domains from internal hosts, particularly connections using the Socket.IO protocol.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1059.007: JavaScript
		T1059.006: Python

Tactic	Technique	Sub-technique
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
		T1036.008: Masquerade File Type
	T1140: Deobfuscate/Decode Files or Information	
	T1622: Debugger Evasion	
Discovery	T1016: System Network Configuration Discovery	T1016.001: Internet Connection Discovery
	T1082: System Information Discovery	
Collection	T1115: Clipboard Data	
	T1113: Screen Capture	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
	T1571: Non-Standard Port	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	abc[.]fetish-friends[.]com, abc[.]3mkorealtd[.]com, abc[.]sudsmama[.]com, abc[.]woopami[.]com, abc[.]ilptour[.]com, abc[.]petitechanson[.]com, abc[.]doublemobile[.]com, mcagov[.]cc, roldco[.]com, vnc[.]kcii2[.]com, abc[.]haijing88[.]com
IPv4:Port	45[.]118[.]133[.]203[:]5000
IPv4	108[.]187[.]37[.]85, 108[.]187[.]42[.]63, 207[.]56[.]138[.]28, 108[.]187[.]41[.]221, 154[.]82[.]81[.]192, 139[.]180[.]128[.]251, 192[.]229[.]115[.]229, 207[.]56[.]119[.]216, 192[.]163[.]167[.]14, 45[.]192[.]219[.]60, 192[.]238[.]205[.]47, 45[.]32[.]108[.]178, 57[.]133[.]212[.]106, 154[.]82[.]81[.]205
MD5	1AA72CD19E37570E14D898DFF3F2E380, 79CD56FC9ABF294B9BA8751E618EC642, 0B9B420E3EDD2ADE5EDC44F60CA745A2, 6611E902945E97A1B27F322A50566D48, 84E54C3602D8240ED905B07217C451CD, 2B92E125184469A0C3740ABCAA10350C, 043E457726F1BBB6046CB0C9869DBD7D, 6495C409B59DEB72CFCB2B2DA983B3BB, B500E0A8C87DFFE6F20C6E067B51AFBF, 90257AA1E7C9118055C09D4A978D4BEE, F8371097121549FEB21E3BCC2EEEA522, 814032EEC3BC31643F8FAA4234D0E049, B53E3CC11947E5645DFBB19934B69833, 0C3B60FFC4EA9CCCE744BFA03B1A3556,

TYPE	VALUE
MD5	039E93B98EF5E329F8666A424237AE73, B6DF7C59756AB655CA752B8A1B20CFFA, 5390E8BF7131CAAAA98A5DD63E27B2BC, 44299A368000AE1EE9E9E584377B8757, E5E8EF65B4D265BD5FB77FE165131C2F, 3279307508F3E5FB3A2420DEC645F583, 1020497BEF56F4181AEFB7A0A9873FB4, B23D302B7F23453C98C11CA7B2E4616E, A234850DFDFD7EE128F648F9750DD2C4, 4FC5EC1DE89CE3FCDD3E70DB4A9C39D1, A0D1223CA4327AA5F7674BDA8779323F, 70AE9CA2A285DA9005A8ACB32DD31ACE, DD0114FFACC6610B5A4A1CB0E79624CC, 891DE2FF486A1824F2DB01C1BDF1D2E9, B0E06925DB5416DFC90BABF46402CD6F, AD39A5790B79178D02AC739099B8E1F4, D1D78CD1436991ADB9C005CC7C6B5B98, 2C5A1DD4CB53287FE0ED14E0B7B7B1B7, E6362A81991323E198A463A8CE255533, CB3D86E3EC2736EE1C883706FCA172F8, A083C546DC66B0F2A5E0E2E68032F62C, 70016DDBCB8543BDB06E0F8C509EE980, 8FC911CA37F9F451A213B967F016F1F8, 202A5BCB87C34993318CFA3FA0C7ECB0, 06130DC648621E93ACB9EFB9FABB9651, F7037CC9A5659D5A1F68E88582242375, 8AC5BEE89436B29F9817E434507FEF55, 5ED84B2099E220D645934E1FD552AE3A, 27A3C439308F5C4956D77E23E1AAD1A9, 53B68CA8D7A54C15700CF9500AE4A4E2, 1D1F71936DB05F67765F442FEB95F3FD, 3C6AEC25EBB2D51E1F16C2EEF181C82A, 7F27818E4244310A645984CCC41EA818, A75713F0310E74FFD24D91E5731C4D31, 4FC8C78516A8C2130286429686E200ED, 3417B9CF7ACB22FAE9E24603D4DE1194, 933F1CB8ED2CED5D0DD2877C5EA374E8, B5CA812843570DCF8E7F35CACAB36D4A, 4A5195A38A458CDD2C1B5AB13AF3B393, E66BAE6E8621DB2A835FA6721C3E5BBE, 04194F8DDD0518FD8005F0E87AE96335, F15A67899CFE4DECFF76D4CD1677C254, 11705121F64FA36F1E9D7E59867B0724, 4D343515F4C87B9A2FFD2F46665D2D57,

TYPE	VALUE
MD5	DFC64DD9D8F776CA5440C35FEF5D406E, EEFC28E9F2C0C0592AF186BE8E3570D2, 6CF382D3A0EAE57B8BAAA263E4ED8D00, 32407207E9E9A0948D167DCA96C41D1A, D17CAF6F5D6BA3393A3A865D1C43C3D2, 13669B8F2BD0AF53A3FE9AC0490499E5, 5B998A5BC5AD1C550564294034D4A62C, C50C980D3F4B7ED970F083B0D37A6A6A, DE8F0008B15F2404F721F76FAC34456A, 9BF9F635019494C4B70FB0A7C0FB53E4, A543B96B0938DE798DD4F683DD92A94A, FA08B243F12E31940B8B4B82D3498804

References

https://securelist.com/silver-fox-tax-notification-campaign/119575/

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 demo of **HivePro.**

REPORT GENERATED ON

May 05, 2026 • 8:00 AM

More at www.hivepro.com