Black Hole of Trust: SEO Poisoning in Silver Fox's Space Odyssey

Authors: Dillon Ashmore, Asher Glue

Key Findings

- NCC identified an exposed link management panel used by Silver Fox to track download activity for backdoor installer applications, including Microsoft Teams, revealing operational details and campaign telemetry.
- Analysis of the panel and related infrastructure uncovered a broader campaign that supports ReliaQuest's assessment of a false-flag operation, where Silver Fox employed Cyrillic file names to impersonate a Russian-speaking threat actor.
- Silver Fox leveraged SEO poisoning to distribute backdoor installers of at least 20 widely used applications, including communication tools, VPNs, and productivity apps. These primarily target Chinese-speaking individuals and organisations in China, with infections dating back to July 2025 and additional victims across Asia-Pacific, Europe, and North America.
- All observed samples delivered malware consistent with ValleyRAT's behaviour, a modular Remote Access Trojan linked to Silver Fox, with supporting infrastructure hosted in Asia.
- This research reinforces prior industry guidance: organisations with Chinese-speaking employees or operations in China, regardless of sector, face elevated risk from this campaign.

Introduction

Zero Trust is often touted as the ultimate defence for organisations, yet even threat actors sometimes leave the door unlocked, creating the perfect opening for us to walk through. This publication presents our findings on an ongoing campaign orchestrated by Silver Fox, uncovered through an insecure web panel identified as part of our Threat Intelligence operations.

Group Background

Silver Fox (also known as SwimSnake, Void Arachne, The Great Thief of Valley (Valley Thief) and UTG-Q-1000) is a China-based advanced persistent threat group that first emerged in 2022[1] and has been highly active since 2024. While classified as an APT by several Western cybersecurity companies, the group is tracked domestically in China as

[1] https://www.antiy.net/p/swimsnake-cybercriminal-operations-rampant-launch-special-inspection-and-handling-immediately/

a cybercrime actor. It is believed to operate in four sub-clusters: the Finance Group, the News and Romance Group, the Design and Manufacturing Group, and the Black Watering Hole Group[2].

Primarily focused on Chinese-speaking individuals and organisations, Silver Fox's victimology has expanded to include organisations operating in the public, financial, medical and technology sectors[3]. Its motives range from espionage and strategic intelligence collection to financial gain, cryptocurrency mining, and operational disruption [4].

Silver Fox leverages social engineering for initial access, primarily through phishing campaigns and SEO poisoning, to deliver .msi and .zip backdoor installers that masquerade as legitimate apps. These payloads have been observed delivering ValleyRAT, Gh0STCringe or HoldingHands RAT, a variant of Gh0st RAT. The group frequently rotates AV and EDR methods to maintain persistence and avoid detection.

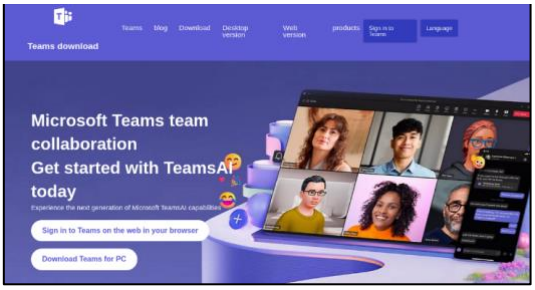
Most recently, as identified by ReliaQuest, the group has been using SEO to deliver backdoored installers of Microsoft Teams[5]. Notably, in this campaign, Silver Fox used false flags, including Cyrillic characters, to impersonate a Russian-speaking threat group. Our research at NCC has uncovered additional artefacts that reinforce this hypothesis and provide deeper insight into Silver Fox's operational patterns, as detailed in the following sections.

Infrastructure Breakdown

The research into Silver Fox APT's infrastructure began by investigating a domain already attributed to the group *teamscn[.]com*. Initial scanning of the URL in URLScan returned no similar sites. To uncover related infrastructure, the site was analysed manually, and several interesting strings of text were identified. The copyright text at the bottom of the page noticeably lacked a space between "Teams" and "Download": "*Copyright@2025 TeamsDownload*". Combining this string with an advanced search operator identified another impersonation domain: *teams-zh[.]net***.** WHOIS data for this site shows it was created on May 10th, 2025, and a historical scan of the domain from May 14th showed it was not hosting fake Teams content at that time. Although the exact date the site began impersonating Teams cannot be confirmed, several *Last-Modified* headers for Teams-related images on the site point to July 7, 2025. This suggests that the threat actor registers domains well in advance of their intended use.

---

[2] https://thehackernews.com/2025/09/silver-fox-exploits-microsoft-signed.html
[3] https://hackread.com/silver-fox-apt-valleyrat-trojanized-medical-imaging-software/
[4] https://levelblue.com/blogs/levelblue-blog/inside-silver-foxs-den-trustwave-spiderlabs-unmasks-a-global-threat-actor
[5] https://reliaquest.com/blog/threat-spotlight-silver-foxs-russian-ruse-fake-microsoft-teams-attack



Side-by-side comparison of teams-zh[.]net and teamscn[.]com

Although the sites' appearances differed visually, our suspicion that these domains were related was reinforced by the download of the advertised 'Teams' app. In the case of *teamscn[.]com*, as highlighted by ReliaQuest[6], when the fake Teams software is downloaded, a ZIP file is delivered from the Alibaba Cloud storage location "*shuangkg[.]oss-cn-hongkong[.]aliyuncs[.]com*" containing the ValleyRAT malware. Whereas on *teams-zh[.]net*, a ZIP is delivered from *cos[.]ap-seoul[.]myqcloud[.]com***.** At the time of analysis, the file had been removed from this bucket and couldn't be retrieved, however looking at the index.html file provided additional information on the actions performed when a download is attempted. The download link does not point directly to a file; instead, JavaScript intercepts the click, decodes the Base64-encoded URL stored in data-encrypted-url, and then opens the actual download URL in a new tab.

```
            <div class="topconZ3"><img src="static/picture/z1.png"></div>
            <div class="toptextwra"><h2>Microsoft Teams已准备好<br>立即使用TeamsAI</h2><p>经过Microsoft TeamsAI新一代的功能</p><a href="https://teams.microsoft.com/v2/">在浏览
器中打开Teams网页版</a><p><a class="download-link" href="#" data-encrypted-url="aHR0cHM6Ly9jZG4yLWRvd25sb2FkLnN0b3JlL2Rvd25sb2FkL3RlYW1zLmh0bWw=" title="teams下载"
id="dowurl">Teams桌面版下载</a></p></div>
            <div class="topPic">
                <img src="static/picture/t1.jpg" class="gt">
            </div>
```

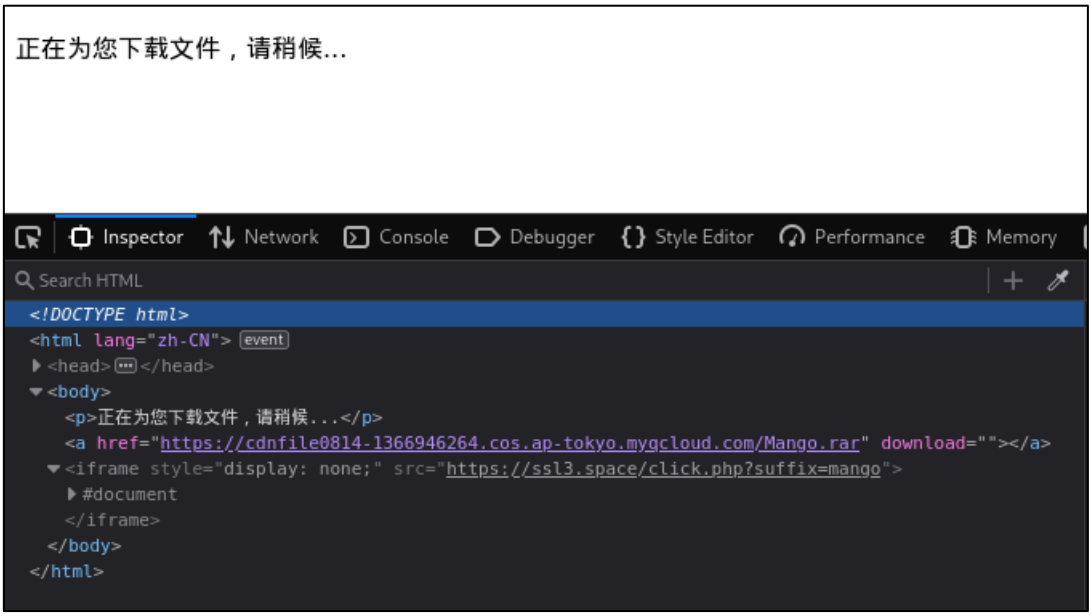
When decoded, the URL is *cdn2-download[.]store/download/teams.html*, which redirects to the previously mentioned QCloud file bucket. The domain *cdn2-download[.]store* was registered on Cloudflare on July 7th, 2025, and was observed on VirusTotal in two additional domains relating to mango and hello-gpt. Impersonation sites for neither app have previously been connected to Silver Fox; however, they align with the types of software the group is known to impersonate.

Scanned	Detections	Status	URL
2025-12-08	0 / 98	200	https://cdn2-download.store/
2025-07-10	0 / 97	200	https://cdn2-download.store/download/hello-gpt.html
2025-07-10	0 / 97	200	https://cdn2-download.store/download/mango.html

Both URLs were visited, and *cdn2-download[.]store/download/mango.html* initiated the file download. Like the Teams sample, the payload was hosted on Tencent Cloud (*myqcloud[.]com*) and delivered as *Mango.rar*, which contained an installer named *Mango.msi* (*cdnfile0814-1366946264[.]cos[.]ap-tokyo[.]myqcloud[.]com/Mango.rar*).

[6] https://reliaquest.com/blog/threat-spotlight-silver-foxs-russian-ruse-fake-microsoft-teams-attack

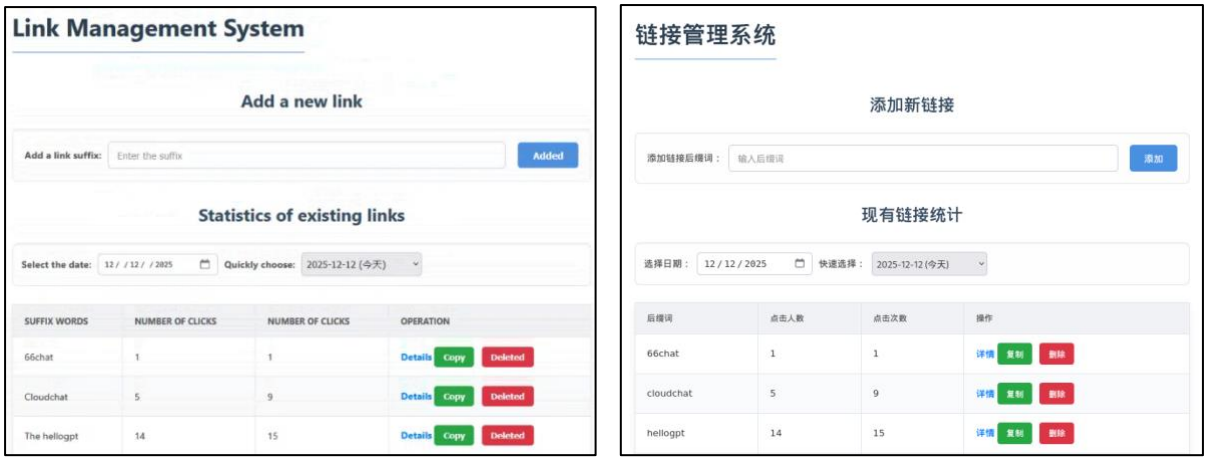
At the same time, the page triggered a secondary network request to *ssl3[.]space/click.php?suffix=mango*. This request originated from a hidden <iframe> embedded in the download page and served as a telemetry mechanism to log the click event. The screenshot confirms this behaviour, showing the outbound request and its JSON response indicating success.



Screenshot showing successful download and background request to ssl3[.]space

Admin Panel

Pivoting to *ssl3[.]space* showed an unsecured panel in Chinese that, when translated into English, indicated it was a link management interface for tracking users who clicked download links managed by the operators. The domain itself is hosted on *47.239.240[.]30* (Alibaba US Technology Co., Ltd.) alongside *ssl1[.]space* and *ssl2[.]space*, both of which were registered on the same day as *ssl3[.]space*. Leading us to believe that they are owned and operated by the same actor. This is further confirmed by a redirect from the file download link on *ssl1[.]space* to *ssl2[.]space/donw/qieqie.html*, which suggests a centralised infrastructure for tracking infection telemetry.



Screenshots showing the interface in English and Chinese

The table below describes the key sections of the panel.

Name	Chinese Name	Description
Suffixes	后缀词	Refers to webpages hosting backdoor installer applications.
Clicks	点击人数	Refers to the number of clicks a download button has received per day.
Clicks	点击次数	Refers to the cumulative number of clicks a download button has received since launch.
Date	快速选择	Operators can toggle dates for the past 7 days by the drop-down menu to review the performance. However, data from as early as July 08, 2025, was identified.
Operate	操作	From this column, the operator can add or remove suffixes and move to specific suffix pages.
Details	详情	Redirects the operator to ssl3[.]space/details.php?suffix=[NAME] where name is equal to the suffix it's associated with.

Reviewing the site's source code shows that the admin panel retrieves click-tracking data via background requests to PHP endpoints such as stats.php and details.php, using JavaScript fetch() calls that append the suffix value to the URL (e.g., *click.php?suffix=mango*). These PHP scripts take the suffix parameter, query the backend database for click and user-activity logs, and return the results as JSON. The browser then parses this JSON and populates the operator interface with the recorded click counts, timestamps, and victim metadata.

Inspecting each specific suffix page revealed the IP address, location, and time (set to China Standard Time) when a download link was clicked, as shown in the screenshot of the Hello-GPT page below. To protect victims, the IP column has been redacted.

Screenshot showing IP, location and date breakdown of Hello-gpt-related infections

From this admin panel, we were able to identify additional apps being impersonated by Silver Fox besides Teams, as shown in the table below:

CloudChat	QieQie
Mango	Telegram
HelloGPT	Xgram
Snipaste	Fantalks
Sigua	YeeYee/YeeChat
Safew	OpenVPN
Potato	FlyVPN
Teams	ToDesk
AweSun (Oray)	Youdao
WPS	Sogou
Signal	Santiao

Backdoored installers for several of these applications have previously been attributed to Silver Fox, according to research published by other organisations[7] [8] [9].

[7] https://dti.domaintools.com/chinese-malware-delivery-domains-part-iv/
[8] https://thehackernews.com/2025/12/silver-fox-uses-fake-microsoft-teams.html
[9] https://www.netskope.com/blog/deepseek-deception-sainbox-rat-hidden-rootkit-delivery

The table below shows a breakdown of IP addresses by country of origin for download clicks. This data covers one week and shows that infections in mainland China (217) were significantly higher than in other countries. During the same period, clicks on HelloGPT and Sigua impersonation sites were the highest.

Country	Count
China	217
United States	39
Hong Kong	29
Taiwan	11
Australia	7
Malaysia	7
Cambodia	5
Laos	5
Thailand	5
Singapore	4
Canada	3
South Korea	3
Netherlands	2
Philippines	2
United Kingdom	2
Japan	1
Myanmar	1
Taiwan	1
United Arab Emirates	1
Vietnam	1
Germany	1

Fake Sites

As the names of several apps being actively impersonated by Silver Fox were identified from the panel, we then set out to identify the domains and files they delivered. Reviewing pre-existing research on the group revealed the following pattern in their typosquat domain names:

- [app name]cn.com
- [app name]-hk.com
- [app name]-zhe.com
- ch-[app name].com
- cn-[app name].com

- [app name]cn.org
- zh.[app name].com

Using these patterns, keyword searches, and recently registered certificates, we focused on Cloudflare-hosted domains and enriched the dataset by pivoting on shared elements such as text strings and favicon hashes. The complete list of identified domains is provided in the IOCs section.

To illustrate this approach, we examined Sigua. First, by searching for recently registered certificates containing "sigua". As shown in the screenshot below, several domains were (re)registered in early December 2025 and follow the naming pattern identified earlier.

Subject CN	sigua.net
Valid From	2025-12-04
Valid To	2026-03-04
SAN	sigua.net, *.sigua.net

Subject CN	app-sigua-signal.com.cn
Valid From	2025-12-04
Valid To	2026-03-04
SAN	app-sigua-signal.com.cn

Subject CN	sigua-cn.icu
Valid From	2025-12-03
Valid To	2026-03-03
SAN	sigua-cn.icu, *.sigua-cn.icu

Subject CN	www.sigua.app
Valid From	2025-12-03
Valid To	2026-03-03
SAN	www.sigua.app

Subject CN	www.sigua.app
Valid From	2025-12-03
Valid To	2026-03-03
SAN	www.sigua.app

Subject CN	sigua-zq.com
Valid From	2025-12-03
Valid To	2026-03-03
SAN	sigua-zq.com, *.sigua-zq.com

Subject CN	sigua-zq.com
Valid From	2025-12-03
Valid To	2026-03-03
SAN	sigua-zq.com, *.sigua-zq.com

Subject CN	sigua.org
Valid From	2025-12-03
Valid To	2026-03-03
SAN	sigua.org, *.sigua.org

Subject CN	sigua.org
Valid From	2025-12-03
Valid To	2026-03-03
SAN	sigua.org, *.sigua.org

Subject CN	sigua.app
Valid From	2025-12-03
Valid To	2026-03-03
SAN	sigua.app

Screenshot of recently (re)registered domains containing "sigua"

Cn-sigua[.]com hosts a page advertising sigua downloads for Windows, Android, and iOS. Clicking any download button redirects the user to a cloud service hosting the payload. In this case: *xinjuiogh[.]oss-cn-hongkong.aliyuncs[.]com/SiGuчTalk.zip*. Although the file was removed, another sample from the same bucket was identified, also written in Cyrillic and impersonating Signal: SignчlSetup.exe. The file was delivered from the domain *zh-signal[.]com*. Both files are particularly interesting due to their likeness to the Cyrillic-named files delivered through similar sites that ReliaQuest reported on earlier this month[10].

[10] https://reliaquest.com/blog/threat-spotlight-silver-foxs-russian-ruse-fake-microsoft-teams-attack/

Screenshot showing cn-sigua[.]com

Analysis of Safew impersonation sites identified a new cluster of domains suspected of delivering ValleyRAT payloads. We attribute these domains to Silver Fox with high confidence based on multiple strong indicators: consistent domain naming patterns observed across prior campaigns, the use of redirects to cloud storage for payload delivery, and the subsequent behaviour of the retrieved files, which aligns with previously documented ValleyRAT infection chains.

Applying the same investigative approach to one Safew site (*safew[.]zip*) revealed a redirect to another domain distributing a backdoored version of Santiao, a Chinese messaging application. This secondary site, *3tiao[.]org*, featured a "Partners" section listing additional malicious domains masquerading as legitimate services such as Sogou, Oray, Aisi Assistant, Youdao Translate, Kuailian VPN, WPS Office, PaoPao, Telegram, Potato, Todesk, and Safew.

These domains ultimately redirected to cloud storage endpoints on Tencent Cloud (*myqcloud[.]com*), Alibaba Cloud OSS (*oss-cn-hongkong, oss-ap-southeast-1*), and Backblaze B2 (*s3[.]us-east-005[.]backblazeb2[.]com*), hosting payloads named after popular applications (e.g., telegamt_x64.1.7.zip, Potato_Desktop_x64.1.6.zip). While none of these samples contained Cyrillic strings, their execution behaviour mirrored the ValleyRAT infection chain previously documented by ReliaQuest, reinforcing our attribution. Further technical details on these samples are provided in the Malware section.

Malware Analysis

This analysis focuses on the *ToDesk_yuancheng_x64.1.3.zip sample*, which exhibits behaviours consistent with other fake remote-tool installers observed in our research. Across the wider set, multiple samples exhibit similar loader patterns, but the packaging visually differs to reflect the software they mimic. This ToDesk sample is *NSIS-based and reflects behaviour consistent with the Awesun and Youdao samples*. The observed behaviour shows overlap with publicly reported ValleyRAT activity, particularly those attributed to the current campaign, including installer-based delivery, abuse of legitimate system binaries and retrieval of additional payloads.

Where relevant, observations from the other related samples (Telegram, Awesun, Youdao, Potato) are referenced to highlight consistent patterns and key differences.

Execution Chain

ToDesk_yuancheng_x64.1.3.zip contains *Todesk_yuanCheng_x64.1.4.exe*, which executes as an *NSIS-based installer*. When run on a system, the installer extracts its internal runtime components (installer logic, configuration files, and NSIS plugins) into a temporary directory under %TEMP%, consistent with standard NSIS operation.

During execution, the installer decrypts and runs additional components, including *Verifier.exe* and Profiler.json, located in %LOCALAPPDATA%. Despite the name, the latter file is not a valid JSON and instead contains an embedded DLL, indicating deliberate payload masquerading (T1036.008). Static analysis of *Verifier.exe* indicates file I/O and memory-mapping functionality consistent with loading externally stored binary data, suggesting the embedded DLL is likely staged for execution at runtime.

Following execution of *Verifier.exe,* the installer decrypts and executes "AutoRecoverDat.dll" via rundll32.exe:

```
"rundll32.exe
C:\Users\Admin\AppData\Roaming\Embarcadero\AutoRecoverDat.dll,
DllRegisterServer"
```

Execution of this DLL initiates outbound network communication to a remote endpoint, after which the C2 returns a payload containing an embedded DLL. This payload exports the function `VFPower_32`. Notably, the embedded DLL within *Profiler.json* exposes a similarly named export (`VFPower`), indicating a potential linkage between these components.

This pattern was also observed in other samples such as *Awesun* and *Youdao*, indicating a shared loader design with rebranded decoy UI and branding (T1218.011, T1055).

Code Obfuscation

Static analysis of the next stage payload `AutoRecoverDat.dll` indicates the use of *ENIGMA Protector,* a commercial packer, to hinder static analysis and reverse engineering (T1027.002). Use of ENIGMA Protector is also observed in multiple related samples, including Youdao and Potato, indicating a shared payload-protection approach across the cluster rather than an installer-specific characteristic.

Defence Evasion

While the NSIS installer primarily serves as a delivery mechanism, logic embedded within the NSIS-based executable performs active defence evasion during execution.

Notably, the NSIS installer logic attempts to disable Windows Defender protections by executing an obfuscated PowerShell command to add broad filesystem exclusions:
`Add-MpPreference -ExclusionPath C:\, D:\, E:\, F:\`

Additional evasion techniques observed in later execution stages include:
- Abuse of legitimate Windows utilities such as `rundll32.exe` for payload execution (T1218.011) to execute the next stage `AutoRecoverDat.dll`,
- Anti-analysis behaviour by `Verifier.exe`, including hiding threads from debuggers via `NtSetInformationThread` (T1622),

Comparable defence evasion techniques are observed across related samples, including *Awesun*, *Potato*, and *Telegram*.

Persistence

No malicious persistence mechanism was observed in this sample. The ToDesk installer did not create Scheduled Tasks, Run or RunOnce registry keys, services, startup folder entries, or any other autorun-related modifications. This behaviour is observed in other samples that operate solely as first-stage loaders, without establishing a long-term foothold. If ValleyRAT is the final payload, it has been documented to include persistence mechanisms that can be deployed as needed during later stages of execution.

Command and Control

The payloads initiated an outbound connection to *118.107.43.131:18852* (T1071.001, T1095), an IP hosted by CTGSERVERLIMITED-AS-AP (AS152194) in Hong Kong. Multiple samples in our IOC set, as well as others identified on VirusTotal, attempted connections

to this host, reinforcing its role as active C2 infrastructure. From this server, a payload containing an embedded DLL, "VFPower_32.dll," was downloaded. Although a complete analysis was not performed at this time, strings were extracted, and some notable wide strings were identified and are shown in the table below. Using these strings 14 additional files on VirusTotal were identified, several of which contain artefacts consistent with indicators highlighted in Antiy's recent report on Silver Fox's ValleyRAT activity. In the case of the last two strings, these are the C2's IP and port suspected to be used in later stage communication.

Wide Strings of Interest
KEY_OFFLINE
KEY_START_RE
KEY_OFFLINE
YourSharedSecretKey
KEY_BOARD_DATA
KEY_BOARD_DATA_MD5
PLUGIN_RET_LOADE
PLUGIN_LOAD
KEY_BOARD_DATA_MD5
KEY_BOARD_DATA
PLUGIN_EVENT
LOADER_PLUGIN
118.107.43.131
9090

Further investigation of *118.107.43[.]131* in Censys confirmed that the service remained accessible on port 18852. Leveraging the banner hash as a pivot point, we identified 17 additional IP addresses: 15 hosted by the same AS and 3 by HKCICL-AS-AP (Hong Kong Communications International Co., Limited). Several of these were also listed as IOCs in ReliaQuest's report on the Silver Fox, thus expanding the known infrastructure linked to the group's campaigns.

Conclusion

We assess with moderate confidence that this malware is linked to ValleyRAT, based on overlapping behavioural indicators and infrastructure consistent with previously reported campaigns. The NSIS-based installers with decoy UIs, staged component drops, and DLL execution via rundll32.exe mirror patterns seen in previous ValleyRAT campaigns. Defence evasion techniques, including PowerShell-based Defender exclusions, anti-debugging, and use of legitimate Windows utilities, are consistent across related samples. The command-and-control infrastructure reinforces this assessment, with connections to hosts previously linked to Silver Fox activity. Wide strings extracted from VFPower_32.dll, such as PLUGIN_LOAD and PLUGIN_EVENT,

suggest a plugin-oriented architecture that aligns conceptually with ValleyRAT's modular design, though these specific strings have not been publicly attributed. Taken together, the loader design, evasion techniques, and infrastructure overlap indicate these samples likely belong to the ValleyRAT cluster used by Silver Fox.

Multiple high-confidence indicators support attribution to Silver Fox. The discovery of an exposed link management panel provided direct insight into campaign telemetry, confirming large-scale SEO poisoning and revealing infection metrics by geography. Data from this panel shows hundreds of clicks from mainland China and victims across Asia-Pacific, Europe, and North America, validating the campaign's scope and strategic targeting of Chinese-speaking users. Pivoting on TLS banner hashes expanded the known C2 footprint to multiple ASNs, supporting assessments that Silver Fox maintains a resilient, distributed infrastructure for ValleyRAT delivery.

And as for that exposed admin panel? It's a reminder that even the most sophisticated threat actors sometimes forget to lock their own doors, making it all the easier for us to walk right in.

Recommendations

- To identify malicious connections to the cloud services hosting the malicious file, monitor outbound traffic for unusual patterns such as direct downloads from cloud object storage domains (e.g., *.cos.ap-seoul.myqcloud.com, *.oss-cn-hongkong.aliyuncs.com) and correlate them with uncommon file types (.zip or .rar) or high-risk behaviours like execution of archives immediately after download.
- For organisations concerned about impersonation, monitor search engine results for brand impersonation and typosquatted domains or implement brand protection services to track SEO campaigns targeting your organisation.
- Use application allowlisting to prevent execution of unauthorised installers from Temp directories.
- Enable behavioural detection for RAT indicators (in the case of ValleyRAT patterns such as persistence via registry key, or rundl32 communicating to unusual ports like 18852).

TTPs

Phase	ID	Technique Title	Example from the Analysis
Resource Development	T1608.006	Stage Capabilities: SEO Poisoning	Silver Fox poisons search engine results to return fake applications to distribute malware
Initial Access	T1204.002	User Execution: Malicious File	User downloads the file from a fake website and runs NSIS installer Todesk_yuanCheng_x64.1.4.exe.

Execution	T1059.001	Command & Scripting Interpreter: PowerShell	Installer runs obfuscated PowerShell to modify Defender exclusions.
	T1055	Process Injection	Loader retrieves and executes embedded DLL stage (VFPower_32).
Defense Evasion	T1562.001	Impair Defenses: Disable/Modify Tools	PowerShell command to add WD exclusions: Add-MpPreference -ExclusionPath ....
	T1036.008	Masquerading: Masquerade File Type	Profiler.json contains an embedded DLL.
	T1622	Debugger Evasion	Verifier.exe uses NtSetInformationThread to hide debugger-visible threads.
	T1218.011	Signed Binary Proxy Execution: Rundll32	rundll32.exe C:\Users\Admin\AppData\Roaming\Embarcadero\AutoRecoverDat.dll, DllRegisterServer used to execute the next-stage DLL.
	T1027.002	Obfuscated/Compressed Files: Packed Payload	AutoRecoverDat.dll protected using ENIGMA Protector.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	Outbound connection to 118.107.43.131:18852 retrieving DLL stage.
	T1095	Non-Application Layer Protocol	C2 uses custom TCP on port 18852.

IOCs

Filename	**Hash**
Potato_Desktop2.47.28.exe	18a80813682b7ccc7428ab56e8c882ebeba94ae43df8993bd46c541d77fde56f
Potato_Desktop_x64.1.6.exe	3fb0fb8ec636e8ee47ad3b48827a5ffd9af39f0442bd5dd98ae9f659e3d65309
SignalSetup.exe	be62dc844ab234da9a29c6ba05aad1f323d30d163dd88002ac22a26508421435

Youdao_fanyi_x64.1.7.1.exe	822097f90504a419dd3e10ef91308f83606f4a6c80c95b7be786fe90a01e620c
Awesun_ yc_x64.3.2.5.exe	bd0ef6fbc7188c9434111e071751a244b79ea3ff9eac558d60b5d28ee480d87f
telegamt_x64.1.7.exe	f521e9a5cc0ab97b5b797e31bafdfe642aca95b4f8186ac6eb565d0395b0c430
i4Tools_Setup_x64.3.1.2.exe	40d69efcf04bb00c4411c1b8920bc35968e6b903f4f60c04b4e881e482672031
wps_bango_x64.1.6.2.exe	ada97bc3f0c142f50f006e19bf7e1d5fc25089334c782f4de0979bb0a9da7e35
sogou_guanwang_x64.1.2.exe	6ce6d863e55e2dfab3191e946b0449851d5a70bb118ca769c8c49c9793af42d0
Todesk_yuanCheng_x64.1.4.exe	3c7ef5d15d9b5429cd615900e2e50235db3badff75f6b66afa32dabd5167be15
Santiao_x64.1.2.7.exe	ae06a11574062a89ecdd7ee4293e0e4a4082d173866cf68c661ffc3f770c241c
Mango.msi	5ee4e4c8fcc00ea45aec5dda8cba27c090d115e287b4784867e3ce6d21239466
Paopaoim_x64.1.3.exe	3aa43350f17fb366174c77894a893d4e8d24c3b0f302190c16c2f62d5ab890b4
AutoRecoverDat.dll	bd5a0f1715ebe8c6d3d3d2d6ea31b7e84cc9c6021610509292648fca2e942d7b

Impersonation Domains
snipaste-cn.com
zh-snipaste.com
ivcduidnxudhwiucn.org
zh.snipaste.com
snipastesis.com
snipastesec.com
snipaste.net
snipaste.naifeiplus.com
cn-sigua.com
sigua-zq.com
sigua-cn.icu
sigua.tw
sigua.im
sigua.io
khjxvc.top
cn-safew.com
safew-zhe.com
safew-hk.com
ch-safew.com
safew.zip
safew-web.org

safew.love
3tiao.org
telegramk.org
telegramdld.com
shurufa-sougou.org
sunlogin-orayc.com
orayy.com
oryz.com
todesk.app
paopaoim.org
wps-excel.org
letsvpn-kl.org
vpm-kl.com
letsvpnm.com
aisi-i4.com
youdao-fy.org
potato-im.org
fantalks.cc
fantalks88.cc
zh-signal.com

Infrastructure

Value	Category	Description
ssl3.space	Domain	Link Management Panel
47.239.240.30	IP	Link Management Panel
officeline1.oss-cn-hongkong.aliyuncs.com	Domain	Alibaba Cloud Hosting ValleyRAT
myyonline2.oss-cn-hongkong.aliyuncs.com	Domain	Alibaba Cloud Hosting ValleyRAT
youline3.oss-cn-hongkong.aliyuncs.com	Domain	Alibaba Cloud Hosting ValleyRAT
xinjuiogh.oss-cn-hongkong.aliyuncs.com	Domain	Alibaba Cloud Hosting ValleyRAT
cdnfile0814-1366946264.cos.ap-tokyo.myqcloud.com	Domain	Tencent Cloud Hosting ValleyRAT
dfsdg44f5r.s3.us-east-005.backblazeb2.com	Domain	Backblaze Hosting ValleyRAT
118.107.43.131	IP	Suspected ValleyRAT C2
202.79.173.57	IP	Suspected ValleyRAT C2
118.107.43.141	IP	Suspected ValleyRAT C2
134.122.128.191	IP	Suspected ValleyRAT C2
27.124.43.12	IP	Suspected ValleyRAT C2
202.79.173.155	IP	Suspected ValleyRAT C2

202.79.173.70	IP	Suspected ValleyRAT C2
27.124.43.4	IP	Suspected ValleyRAT C2
202.79.173.194	IP	Suspected ValleyRAT C2
118.107.43.166	IP	Suspected ValleyRAT C2
27.124.43.7	IP	Suspected ValleyRAT C2
134.122.128.194	IP	Suspected ValleyRAT C2
202.79.173.139	IP	Suspected ValleyRAT C2
202.79.173.44	IP	Suspected ValleyRAT C2
134.122.128.183	IP	Suspected ValleyRAT C2
137.220.152.155	IP	Suspected ValleyRAT C2
137.220.152.199	IP	Suspected ValleyRAT C2
192.253.229.104	IP	Suspected ValleyRAT C2
143.92.63.190	IP	Suspected ValleyRAT C2
43.226.125.112	IP	Suspected ValleyRAT C2
192.253.229.50	IP	Suspected ValleyRAT C2
118.107.43.230	IP	Suspected ValleyRAT C2
118.107.43.248	IP	Suspected ValleyRAT C2
43.226.125.124	IP	Suspected ValleyRAT C2
143.92.63.147	IP	Suspected ValleyRAT C2
143.92.63.167	IP	Suspected ValleyRAT C2
43.226.125.125	IP	Suspected ValleyRAT C2
118.107.43.249	IP	Suspected ValleyRAT C2
154.86.19.89	IP	Suspected ValleyRAT C2
154.86.19.166	IP	Suspected ValleyRAT C2
154.86.19.17	IP	Suspected ValleyRAT C2
154.86.19.12	IP	Suspected ValleyRAT C2
154.86.19.177	IP	Suspected ValleyRAT C2
154.86.19.80	IP	Suspected ValleyRAT C2
202.95.16.102	IP	Suspected ValleyRAT C2
202.95.16.101	IP	Suspected ValleyRAT C2
202.95.16.100	IP	Suspected ValleyRAT C2
137.220.155.141	IP	Suspected ValleyRAT C2
137.220.155.134	IP	Suspected ValleyRAT C2
137.220.153.158	IP	Suspected ValleyRAT C2
137.220.153.42	IP	Suspected ValleyRAT C2
137.220.155.180	IP	Suspected ValleyRAT C2
137.220.155.39	IP	Suspected ValleyRAT C2
137.220.153.37	IP	Suspected ValleyRAT C2
137.220.155.16	IP	Suspected ValleyRAT C2
137.220.155.142	IP	Suspected ValleyRAT C2
137.220.153.147	IP	Suspected ValleyRAT C2