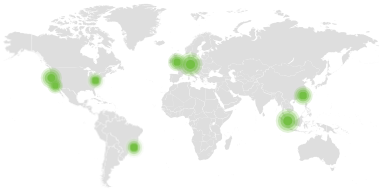

2023

APT Annual Landscape Report

Table of Contents

1. Executive Summary

In 2023, influenced by changes in the international political and economic landscape, downward pressure on the global economy deepened across major economies. Conflicts between nations escalated, and the tense international situation led to a record number of Advanced Persistent Threat (APT) cyberattacks.

Geopolitical conflicts became a major catalyst for APT incidents, with attacks concentrated in conflict or tension-prone regions such as Eastern Europe, the Middle East, the Korean Peninsula, and the South Asian subcontinent.

Due to the increasing visibility of international conflicts, greater media attention, and more standardized attribution practices for attackers, APT incidents were disclosed more frequently this year, showing a trend of persistent attacks throughout the year.

A small number of known active APT groups were responsible for most APT cyberattacks in 2023. Gamaredon in Eastern Europe, Kimsuky and Lazarus in East Asia, and Donot and Bitter in South Asia were the most active. The majority of APT activities were carried out via spear-phishing and exploitation of system vulnerabilities.

Driven by the ongoing Russia-Ukraine conflict and the outbreak of the Israel-Palestine conflict, the number of new APT groups increased significantly this year, with most new groups active in Eastern Europe or Palestinian territories.

APT actors increasingly leveraged publicly accessible vulnerable devices to gain initial access. Multiple APT groups launched extensive cyber espionage campaigns by compromising public-facing security devices to infiltrate internal networks. Additionally, many groups used compromised IoT devices as attack relays to conceal their true infrastructure.

China experienced a record high number of APT attacks this year, with threat sources including well-known and newly emerging APT groups from North America, South Asia, East Asia, Southeast Asia, and Europe. Targeted victims included government agencies, state-owned enterprises, and universities—representing critical infrastructure. The most severe incident was an attack campaign led by a new APT group named DoubleXorRat.

Looking ahead to 2024, cybersecurity professionals will face even more challenges from APT attackers. Defense efforts should prioritize countermeasures against supply chain attacks, zero-day vulnerabilities, and intrusions via public-facing devices.

2. Annual APT Trends

2.1 The number of APT attacks has reached a new high

In 2023, NSFOCUS's Fuying Lab observed that the number of global APT activities reached a new high, with a significant increase compared to last year.

This year, the Fuying Lab captured 607 APT attack leads from 81 groups through the Global Threat Hunting System, an increase of 26.9% compared to last year.

These clues, after being sorted out, can correspond to 362 APT incidents, among which 39 incidents were first disclosed by the Fuying Lab through research reports or social media.

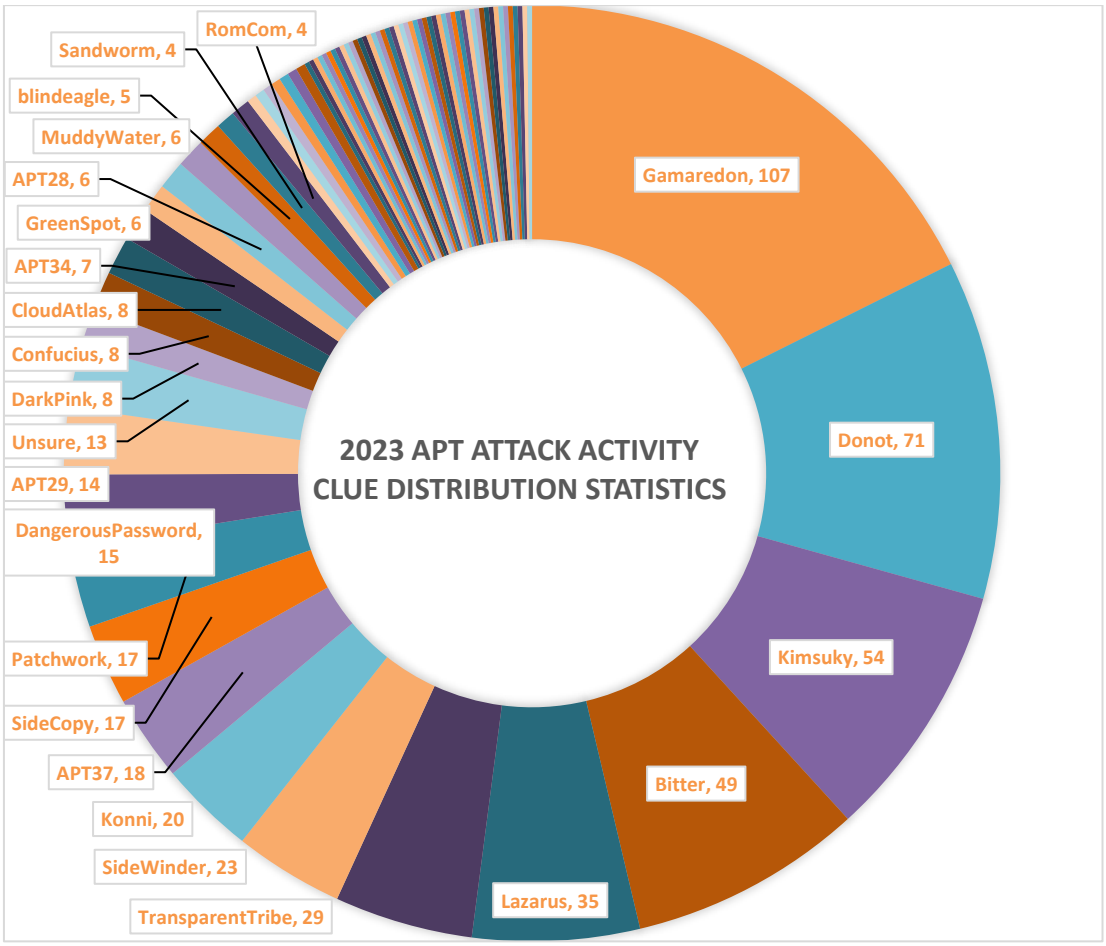

Figure 2.1 2023 APT Attack Activity Clue Distribution statistics

Overall, established APT groups such as Gamaredon, Donot, Kimsuky, and Bitter accounted for a larger number of detected attack clues. This trend indicates, on the one hand, that these groups are responsible for a higher volume of attack operations; on the other hand, it also suggests that their attack tools and behavioral patterns have been thoroughly studied and identified, making their activities easier to detect.

In addition, APT groups with nation-state hacker backgrounds—such as Gamaredon and Lazarus—received significantly more attention this year. Due to their direct ties to state-level intelligence agencies, these groups have become a primary focus in the field of APT threat detection.

2.2 APT attack activities persisted throughout the year without interruption

APT attack activities were consistently intense throughout 2023. Fuying Lab detected over 20 APT incidents each month, with the monthly distribution of attacks being relatively even. July saw the highest number of APT incidents at 39, while December had the lowest at 20.

This trend can be attributed to two main factors. On one hand, the intensification and growing visibility of global geopolitical conflicts in 2023 led many national APT groups to increase the frequency of their cyberattacks while reducing efforts to remain covert, resulting in a noticeable rise in exposed APT activities. On the other hand, the heightened international tensions significantly increased global attention on APT-related cyber threats. Security research institutions and media organizations around the world placed greater focus on APT activities, which in turn contributed to a higher frequency of publicly reported incidents.

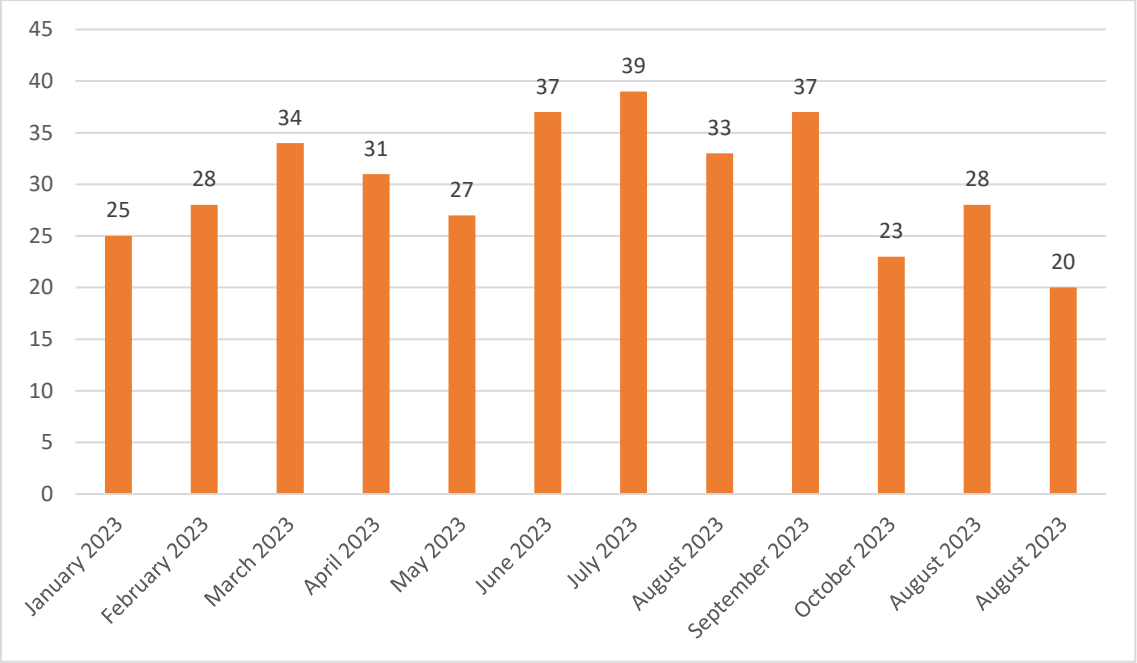

Figure 2.2 Timeline Distribution of APT Attack Detections in 2023

2.3 Geopolitical conflicts drive an increase in regional APT attacks.

In 2023, the continuous geopolitical conflicts have driven the number of APT group attacks to a new peak. The vast majority of APT incidents observed by the Fuying Lab this year are concentrated in conflict or tense areas such as Eastern Europe, the Middle East, the Korean Peninsula, and the South Asian subcontinent.

This year, due to the continuous tension in relations between India and its neighboring countries, APT groups in South Asia have been very active, with the number of incidents accounting for more than 30% (116 cases). In East Asia, affected by the escalation of the situation on the Korean Peninsula, there are more APT activities, with the number of incidents accounting for 26% (91 cases). In Eastern Europe and the Middle East, due to the persistence of the Russia-Ukraine conflict and the outbreak of the Palestine-Israel conflict, the number of APT incidents remains high, accounting for 21% (74 cases) and 8% (29 cases) respectively. Other sources of APT incidents also include Southeast Asia, South America, Central Asia, Western Europe and North America.

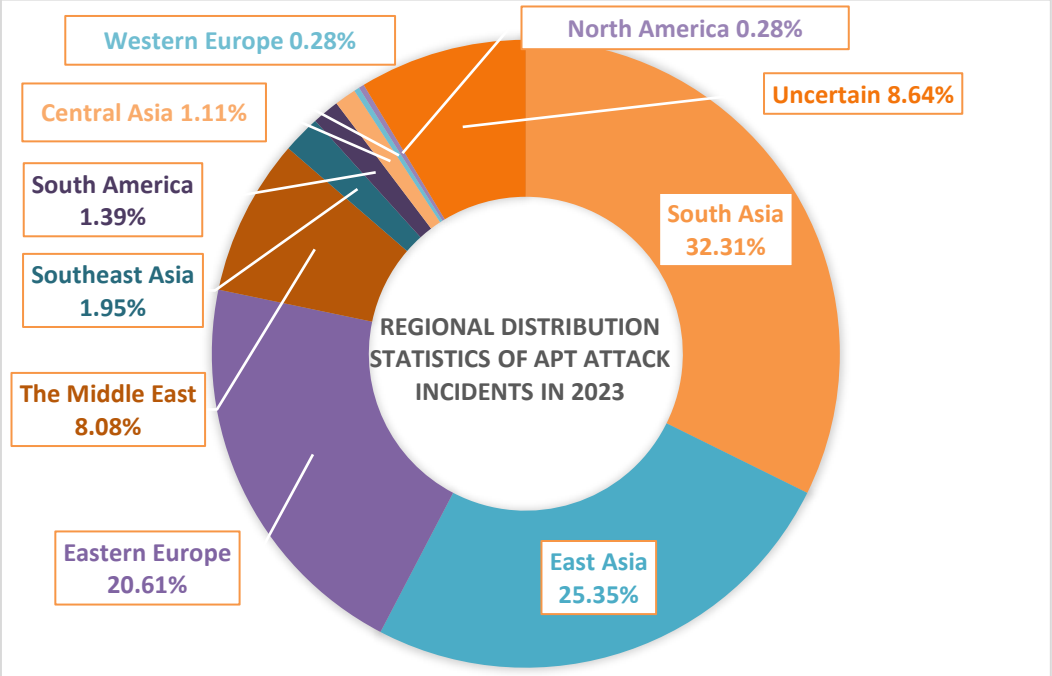

Figure 2.3 Regional Distribution Statistics of APT Attack Incidents in 2023

2.4 Active group activities constitute the core of APT cyber-attacks

The observation of the Fuying Lab has found that attack activities initiated by known APT groups remain the most important component of global APT attack incidents, and a few active APT groups continue to play the role of the "leader" in cross-border cyber-attacks.

Among the APT incidents discovered this year, nearly 80% (78.5%, 284 cases) were initiated by top APT groups, accounting for only 20% (27.5%, 22 cases). The most active attackers include groups such as Gamaredon, Kimsuky, Donot, and Bitter, which mainly use spear phishing as their attack method. This also includes groups such as Lazarus and APT29 that mainly exploit vulnerabilities as their means of intrusion. The number of active APT groups with more than 10 attack activities throughout the year has reached 12.

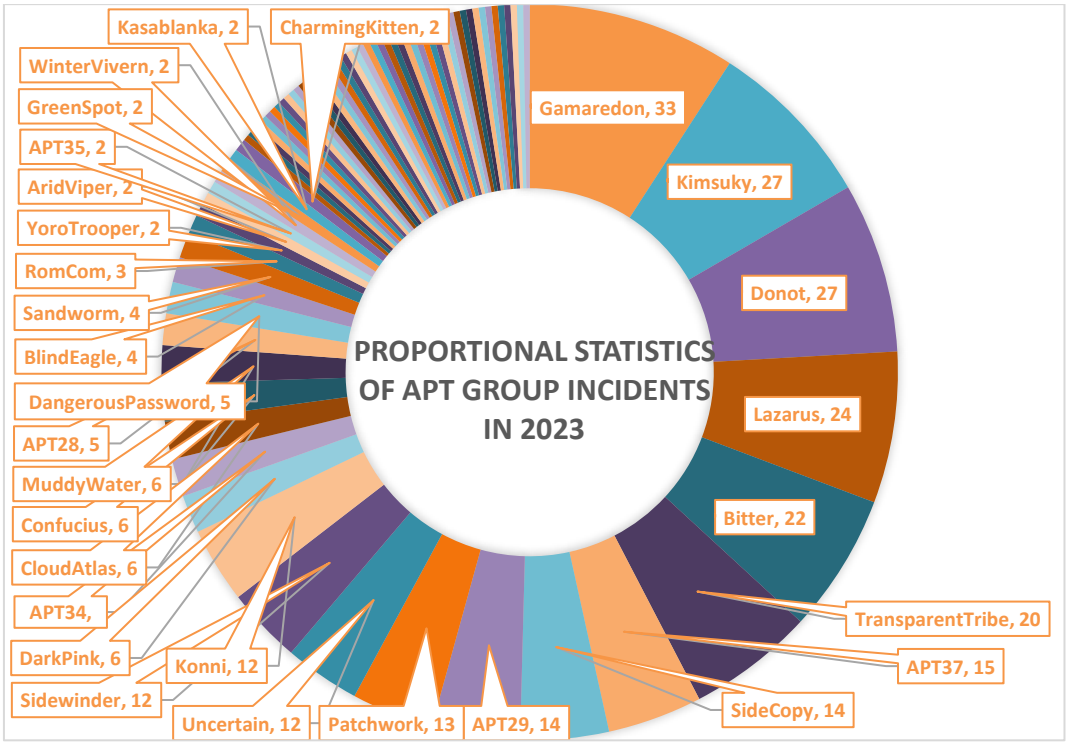

Figure 2.4 Proportional Statistics of APT Group Incidents in 2023

2.5 Explosive Growth in the Number of New APT Groups and Unattributed APT Activities

This year, the Fuying Lab has observed a total of 39 independently attributed APT attack incidents, which are respectively attributed to 27 newly named APT groups, among which 3 groups were independently discovered by the Fuying Lab. Most of these new APT groups operate in Eastern Europe and the Palestinian region. This phenomenon is directly related to the persistence of the Russia-Ukraine conflict and the outbreak of the Palestine-Israel conflict.

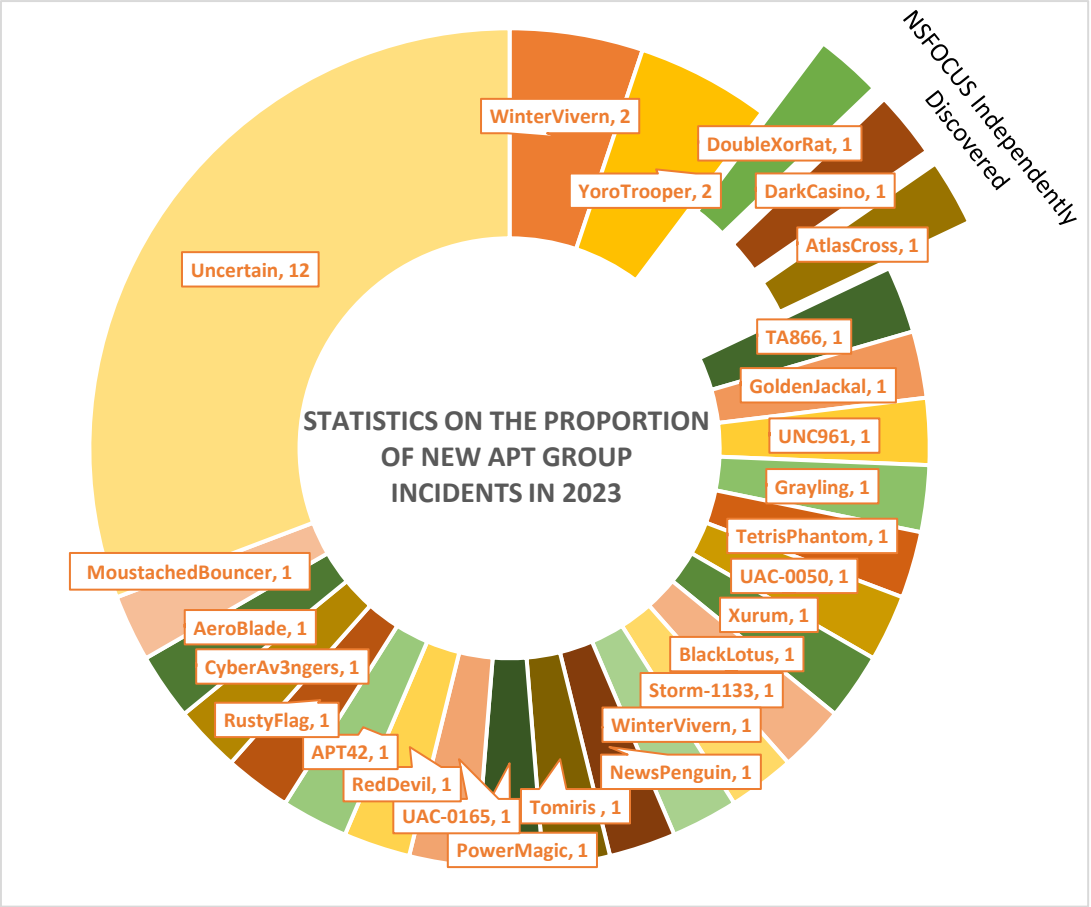

Figure 2.5 Statistics on the proportion of new APT group incidents in 2023

This year, in addition to newly identified APT groups, Fuying Lab has also observed and tracked multiple unattributed APT attack incidents. These unnamed emerging threat actors have targeted countries including Turkey, Indonesia, Argentina, Ukraine, Germany, and China. The affected sectors span government agencies, law enforcement, large enterprises, and academic research institutions.

2.6 Government Agencies and Research Institutions Become Major Targets of APT Attacks

Due to the continuous turmoil in the global situation, the number of APT attack activities oriented towards political purposes was relatively large in 2023, and government departments of various countries became the hardest-hit areas. In addition, the fields that have been more frequently attacked also include scientific research institutions, the defense military industry, financial institutions, the telecommunications industry, various enterprises and infrastructure, etc.

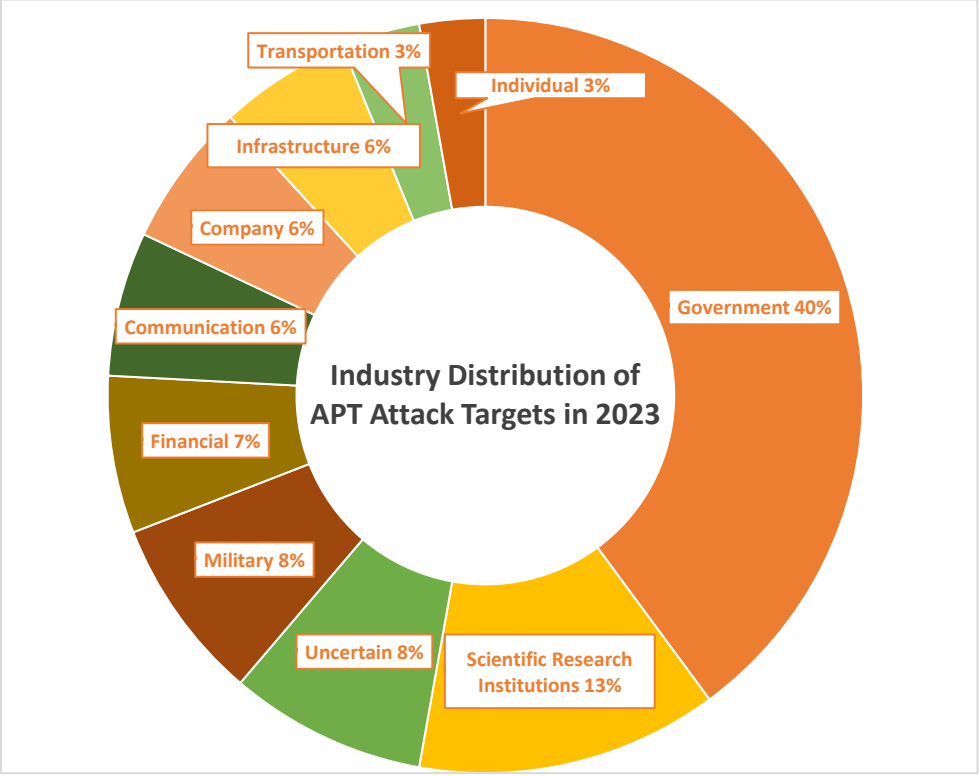

Figure 2.6 Industry Distribution of APT Attack Targets in 2023

2.7 Surge in APT Attacks Against China

In 2023, the number of APT attack operations targeting China further increased, and the associated APT groups also became more diverse. With the increase in the number of captures, the characteristics of these APT attack activities have become more obvious. A group attack pattern where multiple APT groups in the same area cover each other has emerged. The attack trajectory of a single operation by some APT groups has been extended to nearly a year.

This year, the Fuying Lab has been deeply involved in the investigation and evidence collection of multiple APT attacks on us by overseas groups. The APT groups involved include Equation in North America, Bitter, Patchwork, and Donot in South Asia, OceanLotus in Southeast Asia, and DarkHotel in East Asia. The Shathak from the European direction and the DoubleXorRat group were suspected to be from Asia. The vast majority of these APT incidents are driven by spyware information theft, and the target areas of attack cover key infrastructure such as government agencies, state-owned enterprises, and higher education institutions in China.

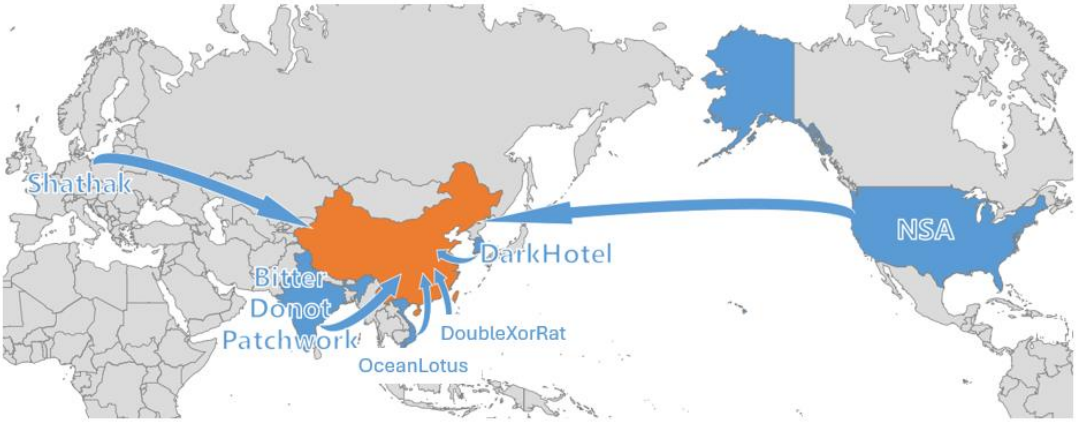

Figure 2.7 Source Distribution of APT Attacks Against China in 2023

For more information about the APT attack operations against China this year, please refer to Sections 3.2, 4.2 and 5.5 of this report.

3. Emerging APT Groups of the Year

3.1 Overview

In 2023, NSFOCUS Fuying Lab independently detected a large number of APT attack activities. Through analysis and retrospection of these incidents, Fuying Lab identified and classified three new APT groups: “DoubleXorRat”, which launched saturation-style attacks against a wide range of China’s public-facing infrastructure, “DarkCasino”, an extremely active group targeting online trading platforms, and “AtlasCross”, a cautious and highly prepared threat actor. Although their targets and objectives vary, all three groups demonstrate sophisticated capabilities and novel attack methods. These groups pose serious threats to key institutions worldwide, especially those in China, and warrant close monitoring by cybersecurity professionals.

3.2 DoubleXorRat

3.2.1 Group Profile

In 2023, during ongoing threat hunting operations, NSFOCUS Fuying Lab identified a large-scale cyberattack campaign against China that persisted for over six months, orchestrated by a newly emerged threat actor. The group demonstrated advanced hacking skills and high destructive capabilities, and its behavior suggests possible backing by nation-state interests.

Throughout the investigation, Fuying Lab observed multiple attack instances attributed to this actor and discovered two unique cyber weapons associated with its operations. One of the core tools used in the attacks featured a distinctive communication mechanism that applied XOR encryption twice during data exchange. Based on this unique technique, the tool was named “DoubleXorRat”, and the threat actor itself was designated with the same name.

Long-term tracking revealed that the DoubleXorRat group has a deep understanding of China’s national systems and cybersecurity infrastructure, is fluent in Chinese-language environments, and employs highly mature, bold, and sophisticated attack techniques. The group often uses a mix of zero-day and N-day vulnerabilities targeting security appliances, along with a combination of custom-built and open-source tools to conduct intrusions.

Its main targets include critical institutions in China, such as major central enterprises, state-owned companies, scientific research institutes, and government agencies.

The group’s signature tactic involves initially exploiting N-day vulnerabilities to gain persistent access to a wide range of internet-facing security devices. It then conducts internal reconnaissance to assess the value of each compromised target and designs custom follow-up attacks accordingly. High-value assets are prioritized for data exfiltration and targeted exploitation.

Figure 3.1 AI-generated concept image of the DoubleXorRat group

3.2.2 Attack Methodologies

Based on confirmed operations linked to the DoubleXorRat group, investigators have classified their main attack patterns into three primary categories. Each method is tailored based on the specific type of device being targeted. A visual summary is provided below.

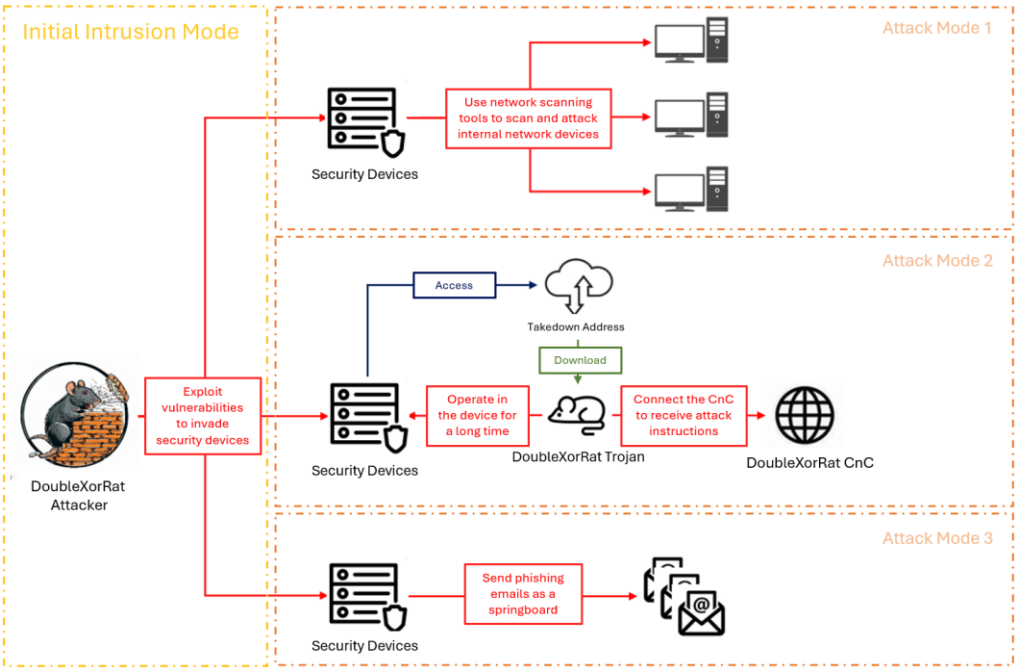

Figure 3.2 Schematic of DoubleXorRat Group Attack Patterns

The DoubleXorRat group initiates intrusions by targeting internet-facing security devices, primarily exploiting publicly disclosed N-day vulnerabilities to gain initial access. Upon successful exploitation, the attackers activate a Python-based HTTP server on the compromised security device, allowing them to upload and execute follow-up attack components.

Attack Pattern 1: Reconnaissance-Based Network Attack via NetBIOS Scanning

This is the most commonly observed method in the group's campaigns and is used as the initial phase in the majority of their intrusions. The DoubleXorRat group selects the appropriate scanner based on the victim device's CPU architecture, typically deploying either the NBTscan or Nextnet scanners. These tools are designed to identify Windows hosts within the internal network that have NetBIOS services enabled. By conducting this reconnaissance, the group builds a profile of the target network domain and evaluates the asset value of the compromised device, thereby informing decisions on follow-up attack strategies.

Attack Pattern 2: Surveillance-Based Attack via Custom Trojan

This pattern involves the deployment of a custom-developed trojan and is executed in most of the compromised devices that are deemed of strategic value. Following the reconnaissance phase in Pattern 1, if the target is assessed as worthwhile, the attacker remotely downloads and runs a specialized trojan on the device. This malware facilitates persistent access to the host, allowing the attacker to monitor its real-time status and issue arbitrary shell commands, effectively maintaining long-term control over the system.

Attack Pattern 3: Command-Based Attack Using Compromised Mail Servers as Phishing Relays

This pattern is only employed in rare cases where the compromised environment contains email service infrastructure. When such servers are identified during earlier reconnaissance phases, the DoubleXorRat group proceeds to compromise the mail server, which is then repurposed to distribute spear-phishing emails. Since these email servers typically belong to whitelisted domains, phishing campaigns launched via this method enjoy a higher success rate due to improved email deliverability and reduced suspicion from recipients.

3.2.3 Summary

The emergence of the DoubleXorRat group underscores a critical trend, as cloud computing continues to evolve rapidly, the security of network boundary devices has become a focal point in the landscape of APT offence and defense. APT groups are now leveraging this new attack vector to target internet-connected infrastructure, aiming to gain access to valuable data assets and orchestrate large-scale cyberattacks.

3.3 DarkCasino

3.3.1 Group Profile

DarkCasino is a financially motivated APT group whose activities were first observed in 2021. The group was initially discovered and named by NSFOCUS Fuying Lab.

DarkCasino primarily targets online trading platforms in economically developed regions worldwide. The industries it focuses on include cryptocurrency exchanges, online gambling sites, digital banking services, and online lending platforms. Its attacks typically involve stealing various types of credentials from compromised hosts to gain unauthorized access to victims' financial assets stored across different online accounts.

The group operates at a high frequency, demonstrating a strong and persistent desire to exfiltrate digital assets. In its early stages, DarkCasino was mostly active in countries surrounding the Mediterranean, as well as parts of Asia where users engaged heavily in online financial platforms. More recently, due to changes in its phishing techniques, the group's operations have expanded globally—now affecting cryptocurrency users across multiple regions, including non-English-speaking Asian countries such as South Korea and Vietnam.

DarkCasino exhibits strong technical capabilities and a high capacity for adaptation. The group actively researches zero-day vulnerabilities and repurposes techniques from other well-known APT operations. Its primary malware is a trojan known as DarkMe, written in Visual Basic, and typically packaged using an obfuscation framework also developed in Visual Basic to achieve antivirus evasion. The group has exploited high-profile zero-day vulnerabilities, such as CVE-2023-38831 and CVE-2024-21412, to obtain code execution privileges. These exploits are then combined with a wide variety of lure documents to carry out aggressive and high-frequency phishing campaigns.

Figure 3.3 AI-generated concept image of the DarkCasino group

3.3.2 Attack Methodologies

In its early stages, DarkCasino built its attack workflows by adopting and adapting techniques from well-known APT groups, achieving notable success in evading detection and resisting defensive measures. The group's typical attack chain consists of multiple components, including malicious shortcut (.LNK) files or executable payloads, registry files, steganographic image files, side-loaded loaders, and its core DarkMe trojan.

DarkCasino demonstrates exceptionally high variability in its tactics, techniques, and procedures (TTPs). According to research by Fuying Lab, between late 2021 and the second half of 2022, at least five distinct variations of its attack flow were identified, highlighting the group's adaptability and sustained focus on bypassing traditional security defenses.

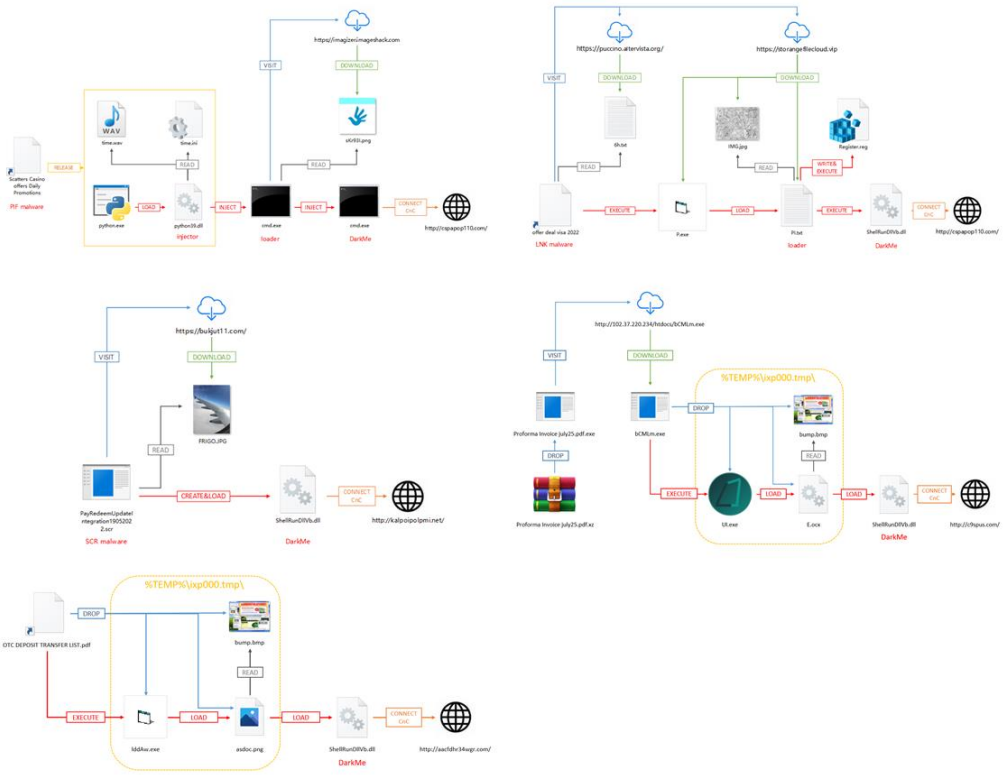

Figure 3.4 Primary Attack Flows Used by DarkCasino (DarkCasino) from Late 2021 to Mid-2022

In terms of technical detail, DarkCasino has demonstrated a strong capability in malicious code development and an acute awareness of offensive–defensive dynamics. Across its different campaigns, the group has employed a wide range of sophisticated techniques, including overwrite-based DLL side-loading, framework-based shellcode execution, custom-developed steganographic logic, socket window-based communication, and COM object implantation.

In April 2023, DarkCasino developed a new attack pattern, initiating a fresh wave of phishing campaigns specifically targeting users on online trading forums. In this campaign, the group exploited a previously unknown WinRAR vulnerability, later disclosed and assigned CVE-2023-38831 by the security community.

The attackers embedded malicious payloads within specially crafted archive files, which were then distributed via forum posts. When opened by unsuspecting users, these files triggered a multi-stage infection chain.

This newly adopted attack flow comprises the following elements: a CVE-2023-38831 exploit archive, CAB (Cabinet) compressed files, registry script (.reg) files, and ActiveX control components. The process unfolds in three main stages: vulnerability exploitation, payload deployment, and trojan execution.

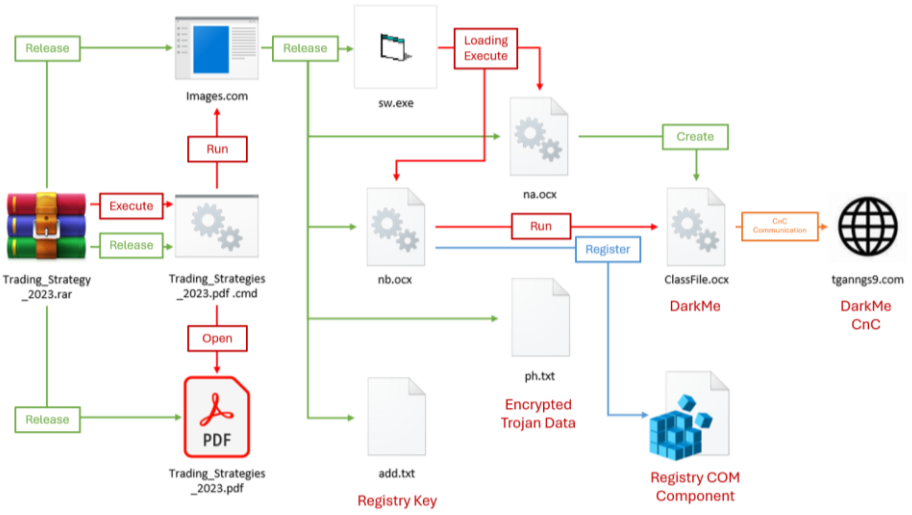

Figure 3.5 Primary Attack Flow Used by DarkCasino in 2023

3.3.3 Summary

DarkCasino is a highly adaptive and resilient APT group with clear internal role separation. Its developers consistently iterate on attack tools, enhancing their performance and resistance against detection. The group also proactively explores various methods to deliver trojans and rapidly refines its execution chains to achieve more effective outcomes.

To mitigate future threats from DarkCasino, users of online financial services—particularly those engaged in trading platforms—should exercise heightened caution when handling file types such as .LNK, .PIF, .SCR, and .COM received through any channel. Special attention should be paid to files containing keywords such as “offer”, “visa”, or “casino”, which are frequently used as bait in phishing campaigns.

3.4 AtlasCross

3.4.1 Group Profile

AtlasCross is a newly identified APT group discovered and confirmed by NSFOCUS Fuying Lab in the second half of 2023. The group exhibits a high level of technical sophistication and a highly cautious operational approach, conducting cyberattacks using two custom-developed trojans along with a range of uncommon attack techniques and tactics.

To date, AtlasCross has primarily targeted the American Red Cross. Its operations involve delivering tailored lures and malware designed to execute only on specific host configurations, enabling precision targeting of systems associated with the group. Observed activity has largely centered on intra-domain lateral movement, although the group’s initial access vector has not yet been confirmed.

Currently, AtlasCross’ s operations appear limited in scope, focusing on highly targeted attacks within specific network domains. However, the group’s attack flow demonstrates a high degree of maturity and robustness. Based on this, Fuying Lab assesses that AtlasCross is likely preparing to scale up its operations into broader campaigns in the near future.

Figure 3.6 AI-Generated Conceptual Illustration of the AtlasCross Group

3.4.2 Attack Methodologies

Analysis by Fuying Lab indicates that the AtlasCross group employs a wide range of techniques throughout its campaigns, with a primary focus on defense evasion, while also incorporating elements of resource development and persistence. This highlights the group’s deliberate awareness of operating in contested environments and its intent to evade detection at every stage.

Prior to launching its attack chain, AtlasCross had already exploited vulnerabilities to compromise a significant number of internet-facing hosts. These compromised machines were repurposed as statistical tracking servers or command-and-control (C2) servers to support subsequent stages of the campaign.

The group's main attack flow can be divided into three distinct phases:

- Lure Document Phase – The campaign begins with the delivery of specially crafted lure documents designed to trick targeted users into initiating the attack chain.
- Loader Phase – Upon successful engagement with the lure, a loader is executed. This component is responsible for staging and preparing the environment for malware deployment, often incorporating anti-analysis and anti-sandbox techniques.
- Trojan Phase – Finally, the core trojan is deployed, establishing persistent access and enabling command execution, surveillance, or data exfiltration based on tasking received from the C2 server.

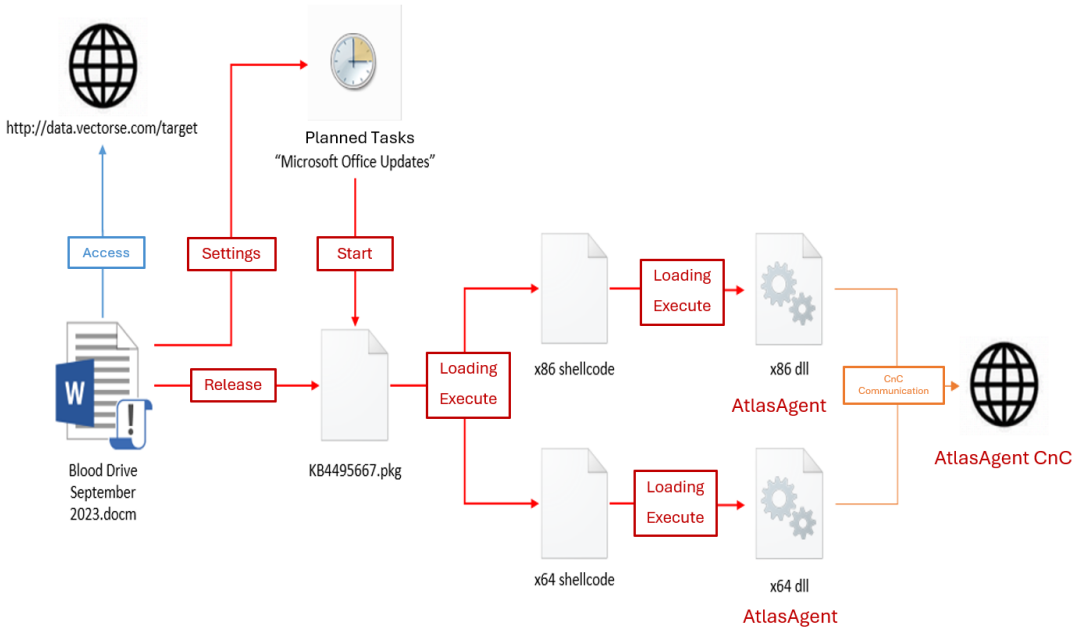

Figure 3.7 Primary Attack Flow of the AtlasCross Group

The main attack chain employed by the AtlasCross group consists of three stages, beginning with the execution of malicious macro code embedded within a lure document. This macro performs three core functions, inclusive extracts and drops the next-stage payload onto the victim host, establishes scheduled tasks to ensure persistence, collects and uploads basic information about the victim system.

In the loader phase, the attack relies on a custom-developed loader trojan known as DangerAds, designed by the AtlasCross group. This malware is configured to only execute malicious code if the victim's username or local domain name contains specific predefined strings. This conditional execution logic indicates that the campaign was designed for post-compromise domain-specific lateral movement, used only after the attackers had successfully infiltrated the target environment.

In the final phase, AtlasCross implants a backdoor trojan named AtlasAgent on the victim device. AtlasAgent establishes communication with pre-compromised command-and-control (CnC) servers and awaits instructions from the attackers. It enables a wide range of post-exploitation capabilities, including remote command execution and data exfiltration.

3.4.3 Summary

AtlasCross is a highly cautious and deliberate threat actor with strong capabilities in attack flow design and tool development. On the one hand, the group actively integrates a wide range of hacking techniques into its technical stack and malware engineering process. On the other, it consistently opts for conservative strategies in areas such as environmental detection, execution logic, and C2 infrastructure selection, willing to trade off efficiency in order to minimize the risk of exposure.

Moreover, the presence of debugging code fragments left within the AtlasAgent trojan suggests that the attacker is still in the process of refining and evolving its operational workflow.

4. Major APT Incidents of the Year

4.1 Overview

In 2023, the accelerating trend of de-globalization exacerbated tensions between nation-states, bringing cyberattacks orchestrated by state-sponsored threat actors into sharper focus. These activities received substantial exposure and analysis throughout the year.

Observations by NSFOCUS Fuying Lab indicate a clear trend toward increased sophistication and scale in international APT operations. Notable incidents under close scrutiny included: Large-scale cyber espionage campaigns launched by Indian APT groups against China, large-scale cyber espionage campaigns launched by Indian APT groups against China, the NSA's cyberattack targeting China's earthquake monitoring centers, the "Operation Triangulation" campaign targeting iOS device users, cyber warfare activities arising from the Israel–Palestine conflict and Lazarus Group's 3CX supply chain compromise, attributed to North Korea.

4.2 APT Attacks Targeting China

4.2.1 Cyber Espionage Campaigns by Indian APT Groups

In the first half of 2023, NSFOCUS Fuying Lab identified a series of APT campaigns originating from India and targeting Chinese entities. These operations were primarily attributed to several well-known Indian APT groups, including Bitter, Patchwork and Donot. By correlating and analyzing these seemingly independent attacks, Fuying Lab concluded that India had orchestrated a coordinated cyber espionage operation targeting key Chinese critical infrastructure, spanning from late 2022 through mid-2023. Each APT group exhibited clear division of roles within the campaign.

Bitter focused on infiltrating Chinese industrial personnel and government staff, Donot targeted diplomatic personnel, particularly those involved with China–Pakistan affairs, Patchwork extended its attack surface to include government departments and academic institutions within China.

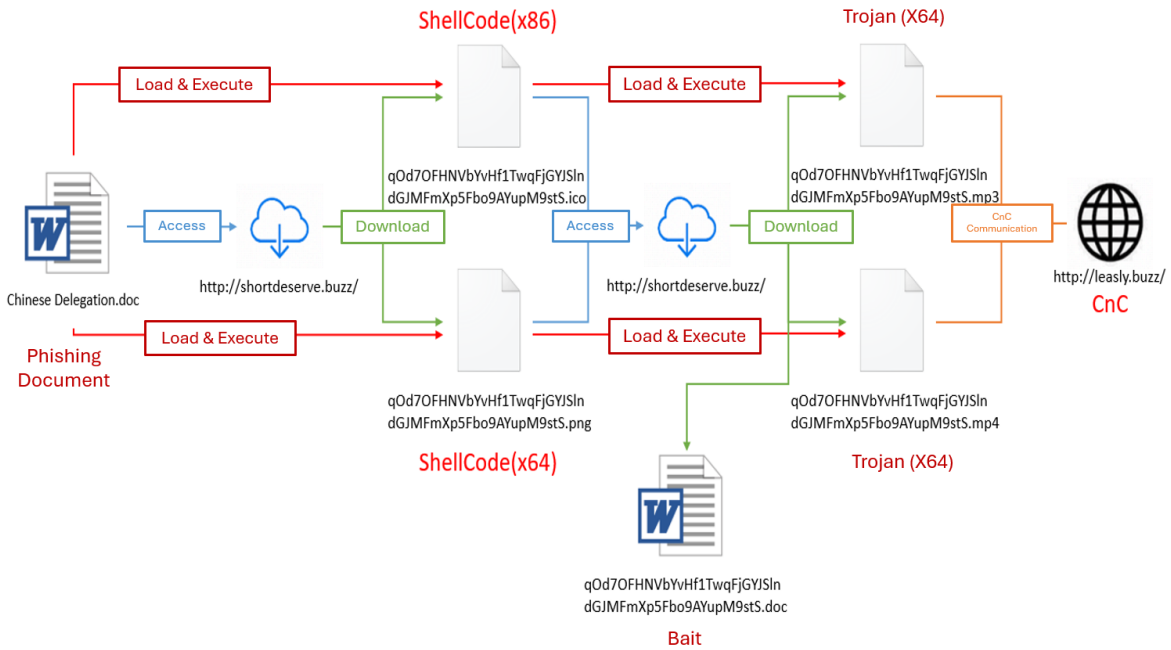

Figure 4.1 Attack Chain Used by the Donot Group in Operations Targeting China

In the captured incidents, most Indian APT groups utilized mature attack procedures and commonly used offensive tools, indicating that this was a broad-spectrum cyber operation aimed at maximizing efficiency and coverage. This clearly reflects India's strong desire for intelligence and data relating to China.

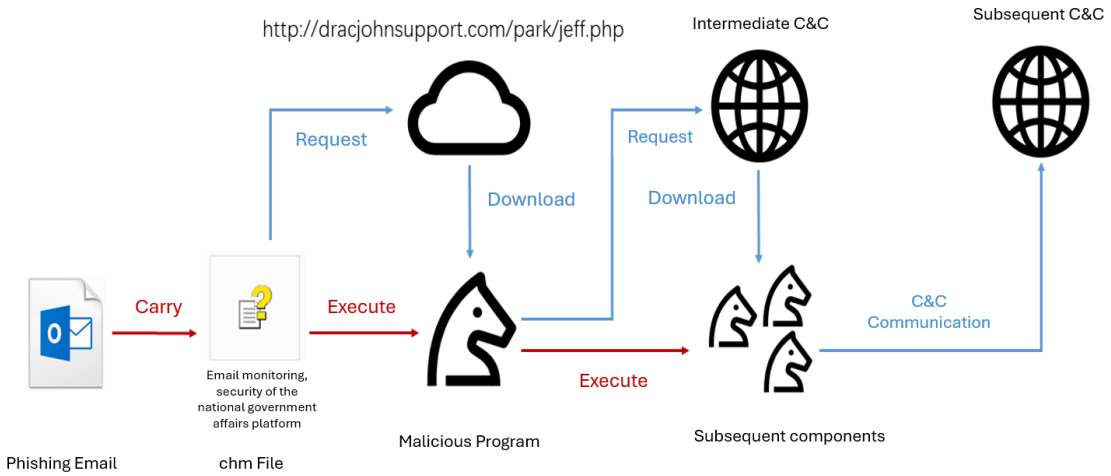

Figure 4.2 Attack Chain Used by the Bitter Group in Operations Targeting China

In the past, APT attacks against China occurred from time to time, but were mostly uncoordinated and isolated incidents. Sustained operations such as the Indian cyber espionage campaign observed this year have been relatively rare.

In the context of intensified de-globalization and escalating international frictions and conflicts, large-scale APT attacks organized and orchestrated by nation-state actors are expected to become increasingly frequent.

4.2.2 NSA's Cyberattack Operations Against China

In July 2023, a cyberattack unit under the United States National Security Agency (NSA) carried out a covert cyber operation against the Wuhan Earthquake Monitoring Centre. The attackers implanted backdoor program into the network equipment at certain seismic data acquisition stations, with the intent of stealing sensitive geological data related to earthquake monitoring, exhibiting clear characteristics of military reconnaissance.

The NSA's cyberattack on the Wuhan Earthquake Monitoring Centre posed a serious threat to China's data security. The stolen data may include seismic intensity information, which serves not only as a key indicator for measuring the destructive power of earthquakes, but also as an effective tool used by malicious actors to detect underground spatial structures. The NSA could use this data to infer information about China's geological, hydrological, and military conditions, thereby supporting U.S. strategic decision-making.

The NSA has a long history of conducting cyberattacks against China's critical infrastructure and was directly responsible for serious APT incidents such as the Northwestern Polytechnical University intrusion. As tensions between China and the United States continue to escalate, NSA-led APT groups are expected to persist in their infiltration activities against China. It is imperative that China enhance its preparedness for high-level cyber intrusions and improve its emergency response mechanisms.

4.2.3 Economically Motivated APT Attacks Against China

In the first half of 2023, the economically driven APT group Shathak launched cyberattacks targeting key Chinese enterprises. During this campaign, the attackers used social engineering lures to compromise an employee's work device at a critical enterprise. By implanting the IcedID trojan, the attacker maintained long-term surveillance over the system and exfiltrated high-value information. This attack campaign persisted for over a year. The attackers employed multiple technical methods to bypass the Endpoint Detection and Response (EDR) systems on the victim's device, enabling the persistent operation of the trojan. As a result, a large volume of internal corporate documents was stolen, causing severe data and asset losses.

Since 2018, with the rise of Ransomware-as-a-Service (RaaS) models and data-leak forums, hacker groups around the world have increasingly focused on corporate-side critical data, stealing it through cyberattacks and monetizing it via sale or extortion. This trend has intensified the threat landscape for Chinese enterprises. The Shathak incident highlights a troubling reality, financially motivated international APT groups have begun to regard China's key enterprises as high-value targets. These attackers have demonstrated the ability to identify, evaluate, and infiltrate critical assets within corporate networks. At the same time, the campaign exposes a gap between the current cybersecurity defenses of Chinese enterprises and the capabilities of mainstream international threat actors—allowing such groups to maintain prolonged, covert access to compromised systems and carry out their objectives with minimal resistance.

4.3 International APT Incidents

4.3.1 Operation Triangulation

The “Operation Triangulation” campaign targeting iOS device users in 2023 has been described as “the most complex cyberattack in history.”

The operation reportedly began as early as 2019 and was named after a unique fingerprinting technique used by the attackers during the reconnaissance phase. In this campaign, the hackers leveraged a chain of zero-day vulnerabilities in iOS to target prominent individuals using Apple devices. Once exploited, the attackers implanted a trojan named TriangleDB into victims' phones to monitor activities and steal data. Known victims of this campaign include officials from the Russian Ministry of Foreign Affairs and executives at Kaspersky Lab.

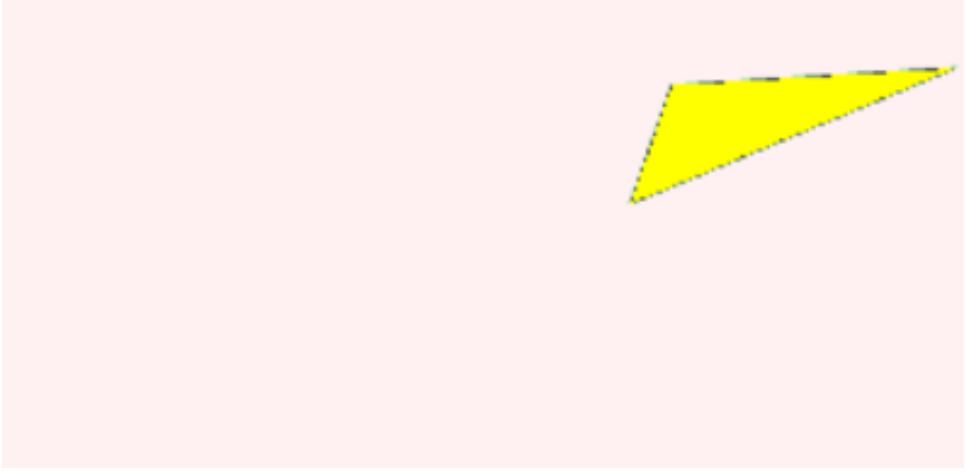

Figure 4.3 Output of Canvas Fingerprinting Code Used by Operation Triangulation Attackers

The full exploit chain used in Operation Triangulation comprises a series of zero-day vulnerabilities that work in sequence to enable remote access and control. These include a remote code execution vulnerability in the TrueType font engine (CVE-2023-41990), an integer overflow in the XNU memory mapping function (CVE-2023-32434), a page protection layer (PPL) bypass at the SoC level (CVE-2023-38606), and an arbitrary code execution vulnerability in the Safari browser (CVE-2023-32435). When combined, these exploits allow attackers to implant a trojan through a specially crafted iMessage attachment, achieving full compromise without any user interaction.

Although attribution remains inconclusive, the attacker’s demonstrated ability to exploit CVE-2023-38606—specifically tied to Apple’s System on Chip architecture—indicates possible access to internal Apple mechanisms or undisclosed backdoors. This suggests that the operation was likely state sponsored, backed by capabilities far beyond those of ordinary cybercriminal groups.

4.3.2 Cyber Warfare in the Israel–Palestine Conflict

On 7 October 2023, following the launch of thousands of rockets, Hamas. The Palestinian Islamic Resistance Movement, officially declared a military operation against Israel, marking the outbreak of the latest round of the Israel and Palestine conflict.

Alongside the physical conflict, hacker groups affiliated with various factions also began sustained operations in the cyber domain, engaging in a digital confrontation between both sides. These groups originated from several countries, including Russia, India, Indonesia, and Iraq. The predominant method of attack was distributed denial-of-service (DDoS), though other tactics such as data theft and website defacement were also observed. In addition to launching cyberattacks, these hacker groups, backed by different supporters, actively disseminated messages, images, and videos to promote narratives favorable to their respective sides, seeking to influence public opinion and steer online discourse in their favor.

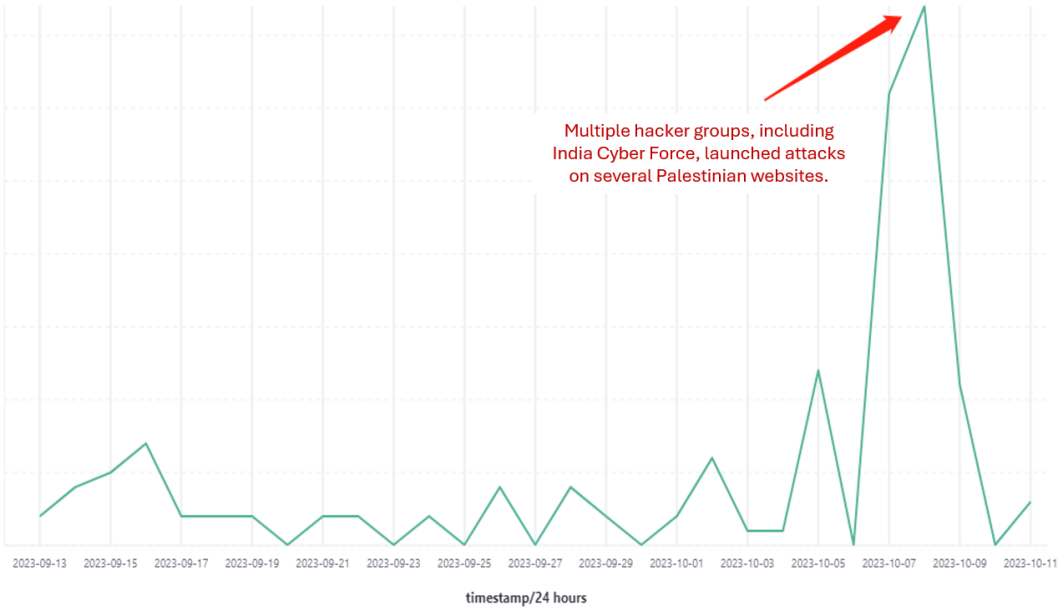

Figure 4.4 DDoS Attack Trends Targeting Palestine During the Outbreak of the Israel-Palestine Conflict

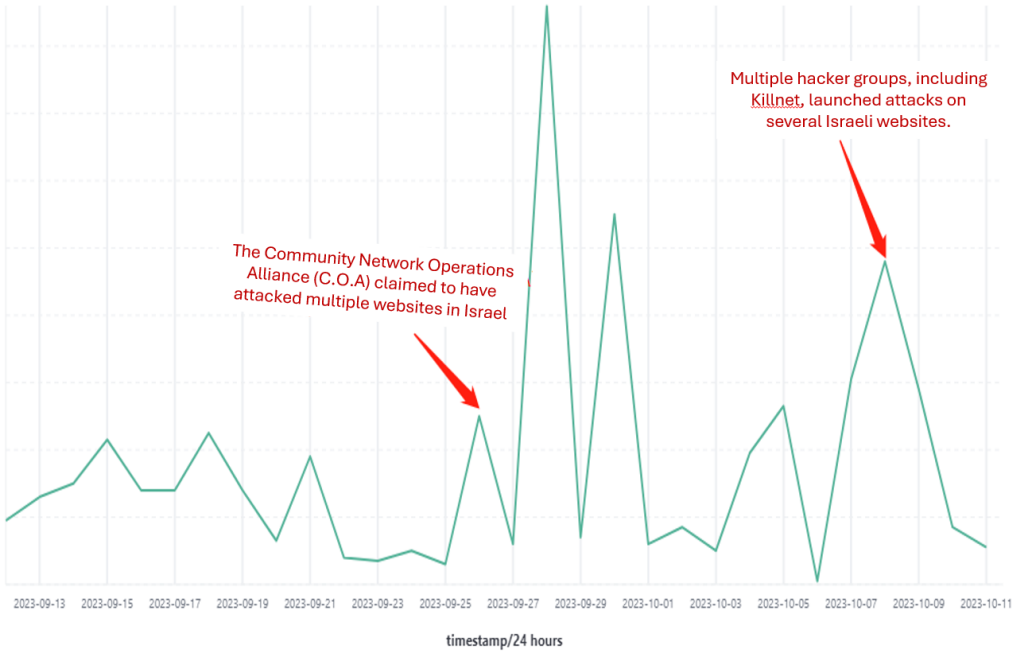

Figure 4.5 DDoS Attack Trends Against Israel During the Outbreak of the Israel–Palestine Conflict

According to monitoring by NSFOCUS Fuying Lab's global threat hunting system, a total of 55 groups were involved in cyberattacks during the Israel and Palestine conflict. The majority were pro-Palestinian hacker groups, with 43 cybercriminal groups, including Killnet launching attacks against Israel's critical infrastructure sectors, such as government, finance, and telecommunications. In contrast, only 12 groups were identified as pro-Israel, with India Cyber Force and UCC being among the most active. These groups mainly targeted Palestinian critical infrastructure in retaliation.

As the conflict intensified and became more protracted, several nation-state APT groups entered the fray, escalating the cyber dimension of the Israel–Palestine conflict into a complex, multi-national confrontation. Pro-Palestinian APT groups such as TA402 and Arid Viper conducted multiple cyber espionage campaigns targeting Israel and its allies before and after the outbreak of hostilities. Meanwhile, several Iranian APT groups—including Imperial Kitten and MuddyWater, launched cyberattacks on Israeli targets, focusing on sectors such as transportation, logistics, and technology.

Additionally, a suspected Israeli-backed group known as Predatory Sparrow carried out a cyberattack on Iran's national fuel distribution system, forcing 70% of gas stations across the country to switch to manual operation. Fuying Lab also observed several unattributed APT activities related to the ongoing conflict.

4.3.3 3CX Supply Chain Attack Operation

In the first quarter of 2023, Lazarus, a top-tier North Korean APT group, orchestrated what has become one of the widest-reaching supply chain attacks to date. By compromising the software supply chain of the international VoIP provider 3CX, Lazarus was able to implant malicious code into both the Windows and macOS desktop applications, allowing the software to download and execute arbitrary malicious payloads.

Investigations revealed that 3CX released a macOS desktop client containing malicious code on 23 January 2023, followed by a Windows version on 8 March 2023 that also carried embedded malware. The attack affected a large population of 3CX's global user base, which includes over 600,000 groups across various industries worldwide.


Security incident update - April 1, 2023, Saturday

Publisher: Nick Galea, CEO of 3CX, April 1st, 2023

We regret to inform you that our company has become a victim of attacks on our products and the larger supply chain. Our task is to transparently share the actions we have taken to address this incident and the detailed information we have learned so far. During this ongoing investigation, the information is being rapidly disseminated. We hope to ensure that we only share verified information and feasible steps that you can take. We will continue to work closely with Mandiant consultants to investigate how this incident occurred and take measures to prevent its recurrence.

What happened?

On March 29th, 3Cx received a report from a third party stating that there were individuals engaging in malicious activities exploiting the vulnerabilities in our products. We immediately took measures to investigate this incident and hired the world's leading cybersecurity expert, Mandiant. The preliminary investigation indicates that this incident was carried out by an experienced and knowledgeable hacker. We are currently cooperating closely with law enforcement agencies and other authorities.

Figure 4.6 Security Incident Notification Published by 3CX

It is worth noting that the 3CX supply chain attack was enabled through a prior supply chain operation targeting X_TRADER in 2022. Lazarus leveraged the X_TRADER campaign to successfully compromise the personal devices of 3CX employees, which ultimately led to the contamination of 3CX's software distribution channels.

The impact of the 3CX incident has proven to be long-lasting. For example, Lazarus reused parts of the network infrastructure obtained through the 3CX breach to conduct subsequent attacks, including a new supply chain attack that exploited a zero-day vulnerability in the MagicLine4NX software, primarily targeting enterprises in South Korea.

4.4 Summary

The major APT incidents observed by Fuying Lab this year, when assessed by their complexity, impact, and scale, demonstrate that nation-state threat actors are now capable of launching high-threat cyber-attacks that are cost-insensitive, indifferent to consequences, and precisely targeted.

These events also reflect the close interconnection between cybersecurity and global geopolitical dynamics. Cyberattacks often serve as extensions and manifestations of political, economic, or military interests between states or non-state actors. In cyberspace, various forces are competing for information dominance and access to data resources in pursuit of their strategic objectives. Responding to nation-state cyberattacks has evolved from simply managing occasional incidents into addressing the far more complex challenge of intercepting and mitigating sustained, large-scale offensive operations.

5. New APT Weapons of the Year

5.1 Overview

In 2023, zero-day and N-day vulnerabilities remain important weapons for APT groups to carry out intrusion activities. The Fuying Lab has found that APT groups have begun to widely exploit various types of vulnerability codes such as common software vulnerabilities, public network device vulnerabilities, and driver vulnerabilities in this year to build APT attack weapons and achieve highly efficient intrusion attack behaviors.

Fuying Lab has observed that the common software vulnerability that has been exploited on a large scale by APT groups this year is the logical RCE vulnerability CVE-2023-38831 targeting the WinRAR software. The most representative vulnerability of public network devices is the RCE vulnerability CVE-2023-42793 targeting TeamCity servers; There are also multiple driver vulnerabilities exploited by APT groups for BYOVD attacks.

In addition, APT groups have become increasingly proficient in using new weapon development tools. This year, the Shadow Lab has captured a variety of complex new APT Trojans, among which the representative one is ZSkyRAT written in rust.

5.2 CVE-2023-38831

CVE-2023-38831 is an arbitrary execution vulnerability in the WinRAR software. It was first exploited by Ghost Wheel attackers in April 2023 and was fixed in the new version v6.23 of WinRAR in August 2023.

The implementation of CVE-2023-38831 is based on the file operation mechanism of the WinRAR software. By constructing a decoy file, a folder with the same name as the decoy file, and a malicious file with the same name at the end of the folder with a space, it deceives the API function ShellExecuteExW called by WinRAR. Make it wrongly release the malicious file and execute it when the bait file should have been opened.

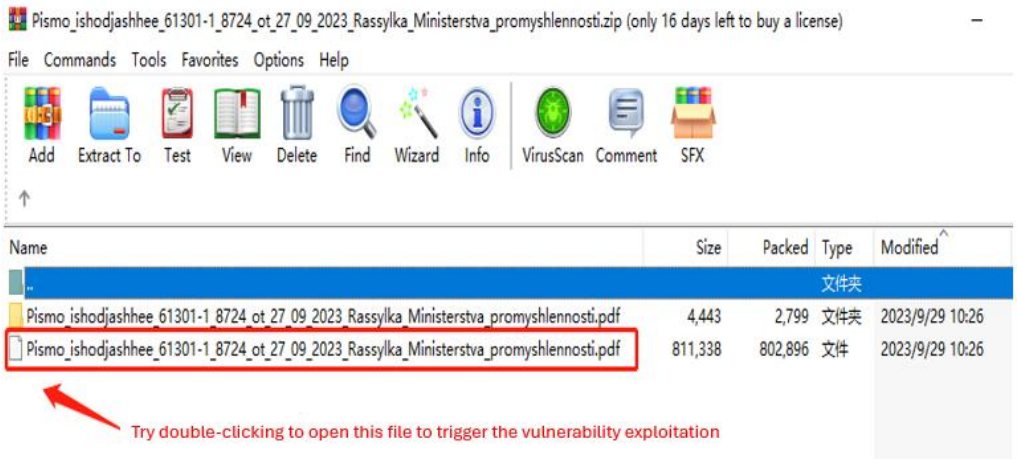

Figure 5.1 The CVE-2023-38831 vulnerability exploitation file constructed by the APT group

Fuying Lab has discovered that CVE-2023-38831 can be integrated into common phishing methods such as email or watering hole attacks, replacing typical malicious compressed file attachments in phishing emails to make them more deceptive. Untrained WinRAR users may find it difficult to detect and defend against such exploitation. Some variants of the CVE-2023-38831 exploit also possess certain evasion capabilities, allowing them to bypass endpoint protection software on target devices and achieve the intended attack objectives.

During its analysis of the impact scope of CVE-2023-38831, Fuying Lab found that since the vulnerability was disclosed in August 2023, multiple APT groups and unidentified attackers have exploited it in phishing attacks, with most of the targets being key government agencies in various countries. Over time, Fuying Lab has also detected a large number of exploit files created and distributed by international phishing actors, indicating a growing trend of large-scale exploitation of this vulnerability.

The first APT group to exploit CVE-2023-38831 in a zero-day attack was DarkCasino. Since then, several other APT groups have been observed leveraging this vulnerability in cyber operations, including the Southeast Asian group DarkPink, the East Asian group Konni, the South Asian group SideCopy, and Eastern European groups such as GhostWriter, Sandworm, and APT29.

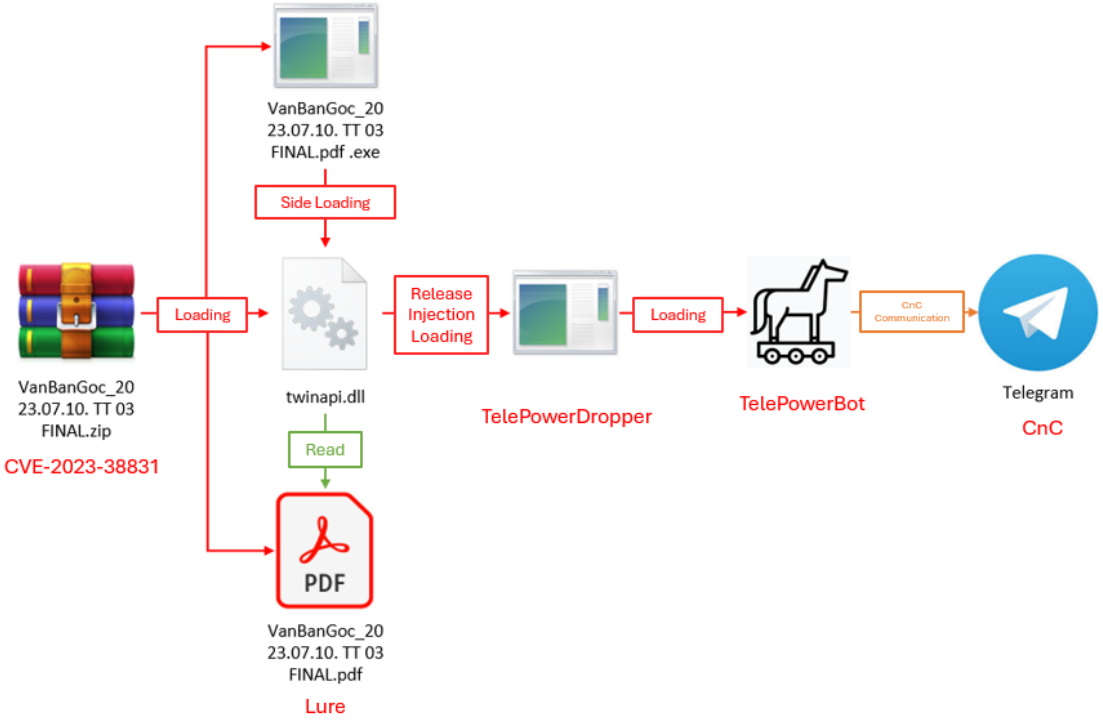

Figure 5.2 Attack Chain of APT Group DarkPink Using CVE-2023-38831

Due to the large installation volume, closed update channels and difficult maintenance of the WinRAR software, CVE-2023-38831 has a wide influence and attack power. It is expected that this vulnerability will become an important weapon for attackers to break through the target defense for a period of time.

5.3 CVE-2023-42793

CVE-2023-42793 is a critical security vulnerability with a CVSS 3.x score of 9.8, affecting the JetBrains TeamCity software. TeamCity is a software development tool used for managing and automating software compilation, build, testing and release. However, the CVE-2023-42793 vulnerability allows unauthenticated attackers to execute arbitrary code on TeamCity servers. Attackers can exploit this access to steal source code, service keys and private keys, control the build proxy on the server, and contaminate the build results. This kind of access rights can also be used by malicious actors to carry out supply chain attacks.

After the emergence of this serious RCE vulnerability, it immediately triggered a wave of attacks on TeamCity servers by global APT groups.

The first group to carry out the intrusion activity was APT29 (CozyBear). After scanning and locating the public network TeamCity server, they used a python script to construct the CVE-2023-42793 vulnerability exploitation payload for the intrusion. Subsequently, GraphicalProton malware was implanted in the successfully taken over TeamCity server to achieve residency and remote control. APT29 will conduct internal network probing on the already invaded TeamCity servers to determine their value, and then further penetrate and steal information from high-value targets. The APT29 attack was not a targeted attack. It is known that the victims are widely distributed in many countries around the world, affecting companies and institutions in multiple industries such as manufacturing, healthcare, finance, and entertainment.

The North Korean APT group Lazarus also promptly launched attack activities after the vulnerability was exposed. After using similar methods to invade the public TeamCity server, Lazarus carried out subsequent malicious activities with two approaches. The first idea of Lazarus is to use PowerShell commands to implant the ForestTiger malware in the victim device and use this program to steal the LSASS (Local Security Authority Subsystem Service) in the host. The local security agency subsystem serves the credentials and then uses these credentials for lateral movement within the domain. Another approach is to use the method of hijacking the search order of DLL to make the victim host load a Trojan program named FeedLoad. This Trojan will further install a remote-control Trojan, enabling the Lazarus attacker to fully control the host.

Another North Korean APT group, Andariel, has exploited this vulnerability even more specifically. After Andariel exploited a vulnerability to invade the TeamCity server, he created a new administrator account on the affected host and then used this account to execute commands to collect system information. Andariel will install a proxy-type backdoor program named HazyLoad on some of the victimized hosts, enabling Andariel attackers to continuously log in to the device.

CVE-2023-42793 is a rare RCE vulnerability for public network devices. This type of vulnerability has always been the focus of attention for various hacker groups and even APT groups. Fuying Lab believes that the ability to respond promptly and patch vulnerabilities in high-risk public network devices will become an important component of the overall APT confrontation capabilities in the future.

5.4 BYOVD

BYOVD (Bring Your Own Vulnerable Driver) is an advanced hacking technique where attackers implant a legitimate but vulnerable driver into a target environment. They then exploit the vulnerabilities in the driver to gain kernel-level privileges on the system, enabling them to carry out sophisticated attacks such as bypassing EDR (Endpoint Detection and Response) and executing malicious code at the kernel level. Originally adopted by high-level APT groups like Equation Group and Turla, BYOVD has in recent years become increasingly favored by a wide range of technically capable APT actors.

In 2023, the Lazarus Group began extensively leveraging the Dell driver vulnerability CVE-2021-21551 to conduct BYOVD attacks. CVE-2021-21551 is a privilege escalation vulnerability found in Dell's `dbutil_2_3. sys` driver. Due to Dell's incomplete remediation, this vulnerability has been actively abused by APT groups. Lazarus has been modifying and exploiting this vulnerability since as early as 2021, but their 2023 campaigns have frequently involved deploying rootkits that use this technique. Furthermore, their attack targets have expanded from high-end manufacturing to the cryptocurrency industry.

In one attack campaign earlier this year, Lazarus launched a phishing email operation targeting entities in the European Union. Upon successful compromise, the attackers implanted a rootkit tool named FudModule on victim hosts. This tool loads the vulnerable Dell driver `dbutil_2_3. sys` and leverages the CVE-2021-21551 exploit payload to gain kernel-level memory read/write access. Lazarus is also suspected of continuing to use BYOVD techniques in attacks against South Korean financial institutions and multiple cross-chain bridge platforms. Notably, their attacks on the Ronin and Harmony bridges resulted in financial losses totaling hundreds of millions of dollars.

Additionally, UNC2970, a suspected sub-group of Lazarus, also employed BYOVD in an operation earlier this year. The group used a trojan named LIGHTSHOW, which exploits a vulnerable `ene. sys` driver to perform kernel-level memory read/write operations, thereby disabling EDR software and evading detection.

The APT group Scattered Spider (UNC3944) also utilized BYOVD attacks this year by exploiting CVE-2015-2291, a vulnerability in Intel's `iqvw64. sys` Ethernet diagnostics driver. This flaw can be abused to execute arbitrary code or cause denial-of-service. Scattered Spider used the vulnerable driver to gain kernel code execution privileges, enabling them to load their custom malicious kernel drivers.

The widespread use of BYOVD techniques in APT campaigns this year has made detecting and defending against such threats significantly more challenging. Currently, the Windows operating system lacks an effective mechanism to manage vulnerable drivers, allowing many outdated drivers with known flaws to remain useful tools in modern cyber operations. Defenders must improve the ability of endpoint security solutions to monitor both user-level files and kernel-level activity in order to counter the growing threat of BYOVD-based APT attacks.

5.5 Rust Trojan ZSkyRAT

When developing new attack tools, APT groups often prefer to use foundational development components that reduce development complexity while increasing resistance to detection and analysis. This trend has made the Rust programming language increasingly popular among APT tool developers.

This year, during an investigation into a cyberattack attributed to the OceanLotus (APT32) group, Fuying Lab discovered a new APT attack tool named ZSkyRAT. Analysis revealed that this tool is highly sophisticated and well-constructed, demonstrating OceanLotus's advanced capabilities in developing Rust-based malware.

ZSkyRAT is written in Rust and is primarily designed for remote control, enabling data theft and the delivery of follow-up payloads. The malware decrypts a TOML-formatted configuration file to connect to its C\&C server and receive command instructions. Its supported functions include information gathering, reverse shell access, file read/write operations, execution of binaries and shellcode, as well as silent mode policies.

One of its notable features is the silent mode policy, which allows the attacker to remotely instruct the malware to suspend host and network activity within a specified time window. The attacker can insert, query, and delete these silent mode policies. The purpose of this feature is to enable the malware to lie dormant and evade detection by host- and network-based security systems while awaiting the optimal moment to launch further attacks.

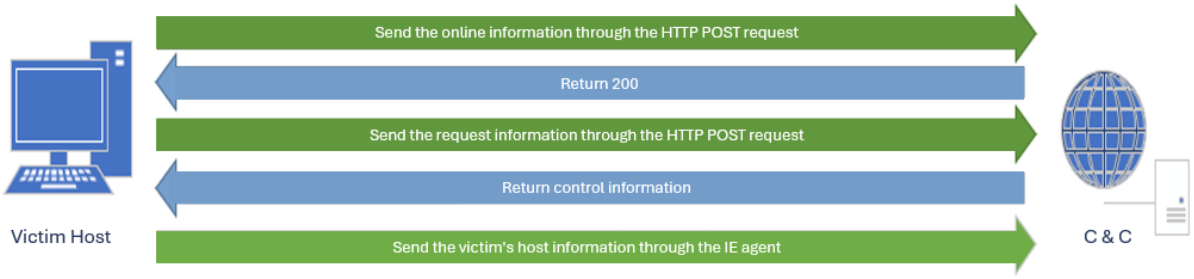

Figure 5.3 The communication process of the ZSkyRAT Trojan

6. Summary and Prediction

The turbulent year of 2023 has passed, and an even more unpredictable 2024 is approaching. In the realm of Advanced Persistent Threats (APT), existing threat forms are evolving rapidly, while emerging threat actors are becoming increasingly active. Driven by shifting geopolitical dynamics, APT activity is entering a period of profound transformation.

6.1 APT attack activities will remain closely bound to regional conflicts and disputes

APT conflicts have in fact become an important part of conflicts between countries. Countries embroiled in regional disputes have generally used APT attack weapons to gain leverage in competition with hostile countries. In 2024, the persistent unstable situations in regions such as the Middle East, Eastern Europe, and East Asia will surely give rise to the emergence of more APT activities.

6.2 APT groups will make broader use of zero-day vulnerability

In 2023, we have observed that multiple APT groups around the world have successfully planned cyber-attack operations using zero-day vulnerabilities. As precious attack resources, zero-day vulnerabilities targeting products from major network equipment manufacturers such as Apple, Microsoft, and Cisco are being removed from the arsenals of national-level APT groups and being thrown into cyber attacks against high-level targets at all costs.

In 2024, leading APT groups will continue to undertake a large number of attack tasks. It can be expected that these attackers will increasingly use zero-day vulnerabilities to achieve their set attack goals, and the resulting zero-day and N-day vulnerability attack risk management will also become an important task in APT attack governance.

6.3 Large-scale APT attacks targeting public network devices will emerge.

APT groups have discovered that cyber-attacks targeting public network facilities such as communication devices, security devices, and service devices can achieve good results. In the actual environment, these public network facilities generally have vulnerability problems or management issues, making them vulnerable to being controlled by attackers and turning them into high-quality attack resources or channels for invading the target's internal network.

In 2024, APT groups that have successfully carried out attacks on public network devices are likely to continue using this attack pattern, and other APT groups may also actively follow suit and try this approach. Today, as APT groups gradually ignore the concealment of their attacks, the greed and eagerness for advanced target data information will drive APT attackers to launch larger-scale intrusion operations into public network devices.

6.4 More APT operations will be carried out through indirect attacks

In the face of protected advanced targets that are difficult to invade, APT groups began to widely practice new attack patterns of achieving intrusion through indirect attacks in 2023. These indirect attacks include controlling software supply chains, controlling infrastructure, and invading boundary devices, etc.

At present, the thinking of mainstream APT groups in practicing indirect attacks has shifted from the previous goal-oriented approach to the current opportunity-oriented one. That is, they seize every opportunity to launch indirect attacks, quickly carry out large-scale cyber-attack operations, and then screen out high-value targets from the victims.

The key APT incidents that occurred in 2023 have demonstrated the high availability of the indirect attack pattern of APT groups. As APT groups further focus their attack targets on high-value devices and sensitive individuals, APT attackers will extensively practice indirect attack patterns in the future, posing a more severe test to the construction of cybersecurity systems. The future ideas for APT confrontation need to focus on considering the vulnerability risks of commonly used software, enterprise software, mail servers, security devices, communication equipment, business infrastructure, etc., to prevent them from becoming channels for indirect APT attacks.

Appendix A 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.

Appendix B About Fuying Lab

It focuses on research of security threat monitoring and countermeasure technologies, covering emerging fields such as APT advanced threats, Botnet, DDoS countermeasures, popular service vulnerability exploitation, black-gray industry chain threats and digital assets.

The research goal is to master the existing network threats, identify and track new threats, accurately trace and counter threats, reduce the impact of risks, and provide strong decision support for threat confrontation.

Adopting the research mode of combining cutting-edge technology exploration with actual combat confrontation, it has assisted national institutions in cracking several APT attack cases, taken the lead in discovering 8 new APT attack groups in the world and handled more than 40 APT attack incidents involving China, making outstanding contributions to major national cybersecurity.