Digital Security
Progress. Protected.

APT Activity Report

WIPERS, PHISHING, AND UNPATCHED VULNERABILITIES

October 2024 – March 2025

(eset):research

Contents

Executive summary 3

Attackers and targets 5

China-aligned groups 6

China-aligned threat landscape in Europe 7

Boarding pass to cyberespionage: UnsolicitedBooker's phishing campaign 8

Some news from Worok 9

Iran-aligned groups 11

Clomping around the riverbank 12

Loading up on reverse tunnels 13

What's old is new again 13

Can you hear me now? 13

Interesting C&C communications channels 13

CyberToufan 14

North Korea-aligned groups 15

DeceptiveDevelopment diversifies 16

Bybit hack 17

Still offering dream jobs 17

Spearphishing in South Korea 18

Russia-aligned groups 19

Sednit has been mastering XSS exploitation tradecraft 20

RomCom deploys two zero days 21

Gamaredon's latest updates 21

Sandworm's use of RMM tools and data-wiping malware 22

Other 23

APT-C-60 in Japan 24

Davos-themed phishing campaign 24

Stealth Falcon 25

About ESET 26

Executive summary

Welcome to the latest issue of the ESET APT Activity Report!

This report summarizes notable activities of selected advanced persistent threat (APT) groups that were documented by ESET researchers from October 2024 through March 2025. The highlighted operations are representative of the broader threat landscape that we investigated during this period. They illustrate the key trends and developments, and contain only a small fraction of the cybersecurity intelligence data provided to customers of ESET APT reports.

During the monitored period, China-aligned threat actors continued engaging in persistent espionage campaigns with a focus on European organizations. Mustang Panda remained the most active, targeting governmental institutions and maritime transportation companies via Korplug loaders and malicious USB drives. DigitalRecyclers continued targeting EU governmental entities, employing the KMA VPN anonymization network and deploying the RClient, HydroRShell, and GiftBox backdoors. PerplexedGoblin used its new espionage backdoor, which we named NanoSlate, against a Central European government entity, while Webworm targeted a Serbian government organization using SoftEther VPN, emphasizing the continued popularity of this tool among China-aligned groups. Additionally, we believe that a ShadowPad cluster that may sporadically deploy ransomware for financial gain is primarily engaged in espionage. We also highlighted Worok's frequent use of shared espionage toolsets such as HDMan, PhantomNet, and Sonifake, addressing several inconsistent third-party attributions of campaigns involving these tools to other groups.

Iran-aligned threat actors remained highly active, led by MuddyWater, which frequently leveraged remote monitoring and management (RMM) software in spearphishing attacks. Notably, MuddyWater collaborated closely with Lyceum, an OilRig subgroup, to target an Israeli manufacturing company. BladedFeline revisited its earlier victim, a telecommunications company in Uzbekistan, coinciding with Iran's diplomatic outreach. CyberToufan conducted destructive operations, deploying a wiper attack against multiple organizations in Israel.

North Korea-aligned threat actors were particularly active in financially motivated campaigns. DeceptiveDevelopment significantly broadened its targeting, using fake job listings primarily within the cryptocurrency, blockchain, and finance sectors. The group employed innovative social engineering techniques, such as ClickFix attacks and bogus GitHub issue posts, to distribute the multiplatform WeaselStore malware. The Bybit cryptocurrency theft, attributed by the FBI to TraderTraitor, involved a supply-chain compromise of Safe{Wallet}, that caused losses of approximately USD 1.5 billion. Meanwhile, other North Korea-aligned groups saw fluctuations in their operational tempo: In early 2025, Kimsuky and Konni returned to their usual activity levels after a noticeable decline at the end of 2024, shifting their targeting away from English-speaking think tanks, NGOs, and North Korea experts to focus primarily on South Korean entities and diplomatic personnel; and Andariel resurfaced, after a year of inactivity, with a sophisticated attack against a South Korean industrial software company.

Russia-aligned threat actors, notably Sednit and Gamaredon, maintained aggressive campaigns primarily targeting Ukraine and EU countries. Sednit refined its exploitation of cross-site scripting (XSS) vulnerabilities in webmail services, expanding Operation RoundPress from Roundcube to include Horde, MDaemon, and Zimbra. We discovered that the group successfully leveraged a zero-day vulnerability in MDaemon Email Server (CVE-2024-11182) against Ukrainian companies, while RomCom demonstrated advanced capabilities by deploying zero-day exploits against Mozilla Firefox (CVE-2024-9680) and Microsoft Windows (CVE-2024-49039). All of these vulnerabilities were reported by ESET researchers to respective vendors. Gamaredon remained the most prolific actor targeting Ukraine, enhancing malware obfuscation and introducing PteroBox, a file stealer leveraging Dropbox, while the infamous Sandworm group intensified destructive operations against Ukrainian energy companies, deploying a new wiper named ZEROLOT via Active Directory Group Policy and utilizing RMM tools in early compromise stages.

Finally, notable activities by lesser-known groups included APT-C-60 focusing on individuals in Japan who are possibly linked to North Korea, and a highly targeted phishing campaign, conducted by an as yet unidentified threat actor, impersonating the World Economic Forum and election websites, aiming to obtain sensitive information from Ukrainian officials and diplomats. In addition, StealthFalcon conducted espionage focused operations in Türkiye and Pakistan.

ESET products protect our customers' systems from all the malicious activities described in this report. Intelligence shared here is based mostly on proprietary ESET telemetry data and has been verified by ESET researchers, who prepare in-depth technical reports and frequent activity updates detailing activities of specific APT groups. These threat intelligence analyses, known as ESET APT Reports PREMIUM, assist organizations tasked with protecting citizens, critical national infrastructure, and high-value assets from criminal and nation-state-directed cyberattacks.

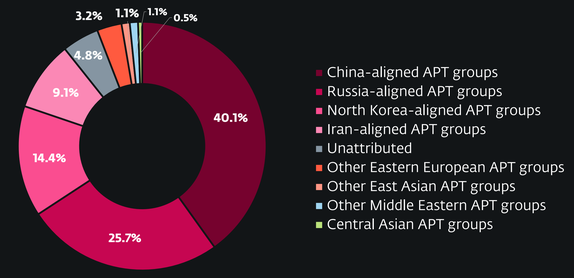
More information about ESET APT Reports PREMIUM and its delivery of high-quality, actionable tactical and strategic cybersecurity threat intelligence is available at the **ESET Threat Intelligence page**.

Attackers and targets

Across Europe, governmental entities remained a primary focus of espionage activities conducted by China-aligned APT groups. However, Ukraine was subjected to the greatest intensity of cyberattacks, driven largely by persistent campaigns from Russia-aligned threat actors against the country's critical infrastructure and governmental institutions. Among these adversaries, Gamaredon consistently emerged as the most active group operating within Ukraine, while Sandworm concentrated heavily on compromising Ukrainian energy infrastructure.

In Asia, China-aligned APT groups continued their campaigns against governmental and academic institutions. At the same time, North Korea-aligned threat actors significantly increased their operations directed at South Korea, placing particular emphasis on individuals, private companies, embassies, and diplomatic personnel.

Iran-aligned APT groups maintained their primary focus on the Middle East region, predominantly targeting governmental organizations and entities within the manufacturing and engineering sectors in Israel. Additionally, we observed a significant global uptick in cyberattacks against technology companies, largely attributed to increased activity by North Korea-aligned DeceptiveDevelopment.



Attack sources

Targeted countries and sectors

China

UnsolicitedBooker Worok Webworm PerplexedGoblin DigitalRecyclers Mustang Panda

Summary of China-aligned APT group activity

ESET researchers observed multiple campaigns targeting European organizations carried out by different China-aligned APT groups, highlighting their consistent and continuous effort against this region.

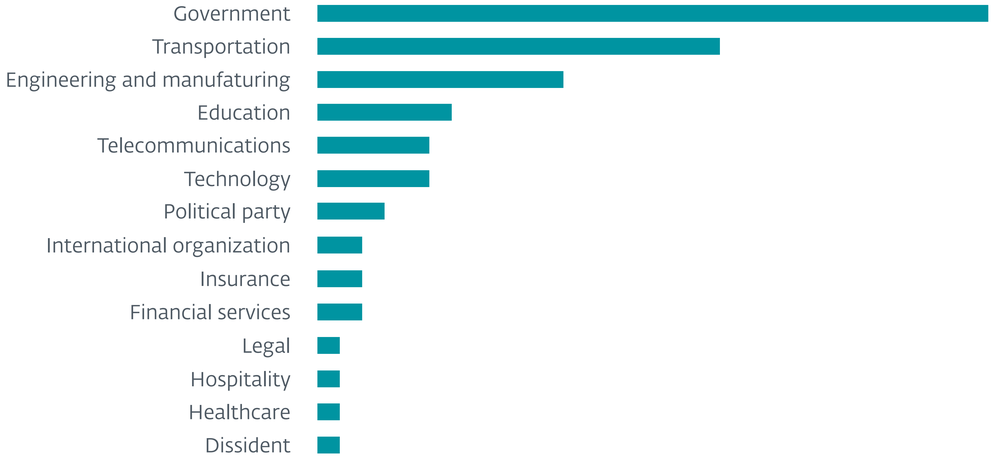
UnsolicitedBooker, a China-aligned threat actor that we discovered in 2023 and that often makes use of spearphishing emails using flight tickets as decoys to target governmental organizations, carried out a new spearphishing campaign using fake Saudia airline emails. The group targeted an international organization in Saudia Arabia with a backdoor it named MarsSnake.

ESET researchers continued to track the activity of Worok, a China-aligned cyberespionage group that was first observed in early 2021 exploiting ProxyShell, a Microsoft Exchange Server vulnerability. The group recently targeted academic institutions in the UK and governmental institutions in Cambodia. We also provide our assessment regarding several campaigns publicly documented by other security researchers that were inconsistently attributed and that we now link to Worok.

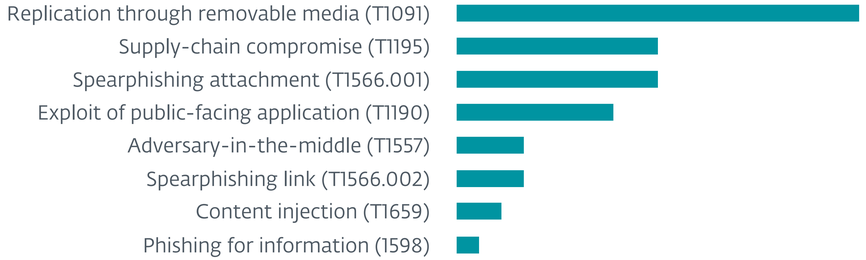
China-aligned threat landscape in Europe

Between October 2024 and March 2025, China-aligned APT groups continued to target European organizations, with multiple campaigns operated by various threat actors appearing in our telemetry.

In October, we detected suspicious SoftEther VPN activity on a machine belonging to a Serbian governmental entity. The threat actor deployed a SoftEther Bridge executable configured to connect to a SoftEther server that we attribute with high confidence to Webworm – one of the various China-aligned APT groups using SoftEther, such as Flax Typhoon and GALLIUM, as mentioned in **our APT Activity Report Q2–Q3 2024**.



Sectors targeted by China-aligned APT groups



Initial access techniques used by China-aligned APT groups (with MITRE ATT&CK IDs)

In December 2024, we observed PerplexedGoblin (whose TTPs overlap with APT31) on the network of a Central European government entity where the group deployed a new, full-fledged espionage backdoor that we named NanoSlate. Comparing NanoSlate to the previously known TurboSlate (which we consider to be used exclusively by PerplexedGoblin) shows marked similarities in the ways both operate and in their coding style, supporting our attribution of NanoSlate to PerplexedGoblin. Additionally, the victimology aligns with the group's commonly targeted vertical, further strengthening our attribution.

DigitalRecyclers, mentioned in **our APT Activity Report Q2–Q3 2023**, also continues to target European organizations. DigitalRecyclers is a China-aligned APT group that uses the RClient, HydroRShell, and GiftBox backdoors, and uses an **operational relay box** network, KMA VPN, to anonymize its network traffic. This is a common trend across China-aligned threat actors and multiple similar anonymization networks exist. Last March, we observed this threat actor at a governmental organization in an EU country, which it had also targeted in 2024.

In February, researchers at **Trend Micro** and **Orange Cyberdefense** published blogposts about a ShadowPad cluster that, in some cases, was seen deploying ransomware. Traditionally, ShadowPad had only been used for espionage operations, and only by China-aligned groups. We were also investigating this cluster and, in ESET telemetry, we found several governmental and private sector organizations across Italy, Romania, and France that had been targeted by this threat actor. However, we haven't observed any ransomware deployment, probably because ESET products are blocking earlier stages of the attack, preventing the threat actor from reaching the ransomware deployment phase. It is also likely that the operators of this activity cluster are mostly engaged in espionage but are moonlighting and, from time to time, deploy ransomware for their own profit. As ShadowPad is known to be sold only to China-aligned threat actors, we attribute this activity with high confidence to an as yet unidentified China-aligned group.

Last but not least, Mustang Panda continues to heavily target European organizations and is the most active China-aligned group we've seen operating in Europe. The group remains focused on the maritime transportation sector and government organizations. Mustang Panda continues to use malicious USB drives and to experiment with Korplug loaders based on various file formats and programming languages. We observed Delphi-, Go-, and Nim-based Korplug loaders as well as MSC downloaders, in Norway, the Netherlands, the UK, Bulgaria, Greece, Denmark, Poland, and Hungary.

Boarding pass to cyberespionage: UnsolicitedBooker's phishing campaign

We first discovered intrusions, by a China-aligned threat actor that we named UnsolicitedBooker, at an international organization in Saudi Arabia in March 2023 and then again in March 2024. The group deployed several backdoors, including Chinoxy, DeedRAT, Poison Ivy, and BeRAT. These backdoors are shared among multiple China-aligned groups. The group also deployed custom file stealers; therefore, we believe that the motivation of this threat actor is espionage and data theft. UnsolicitedBooker sends spearphishing emails, generally with a flight ticket as the decoy, and its targets include governmental organizations in Asia, Africa, and the Middle East. According to our investigation, UnsolicitedBooker overlaps with both **Space Pirates** and an unnamed threat actor that uses the **Zardoor** backdoor.

More recently, in January 2025, we detected a spearphishing campaign from UnsolicitedBooker. The threat actor sent a phishing email from `saudia.etickets@outlook[.]com` to the same organization in Saudi Arabia that was previously targeted by the group in 2023 and 2024. The subject of the email was `Your Saudia Flight Ticket is Ready for Download`, and Figure 1 is the body of the phishing email, which impersonates the Saudia airline.

> *Dear [redacted],*
> *I am pleased to inform you that your Saudia flight ticket has been successfully issued. Please find attached the corresponding air ticket for your upcoming journey.*
> *Thank you for choosing Saudia as your preferred airline. We look forward to welcoming you aboard and providing you with a comfortable and enjoyable travel experience.*
> *Should you have any further inquiries or require assistance, please do not hesitate to contact us.*
> *Warm regards,*
> *Saudia Customer Service Team*

Figure 1. Body of the phishing email

A Microsoft Word document is attached to the email, and the decoy content, shown in Figure 2, is a flight ticket that was modified but is based on a PDF that was available online on the Academia website, a platform for sharing academic research that allows uploading PDF files.

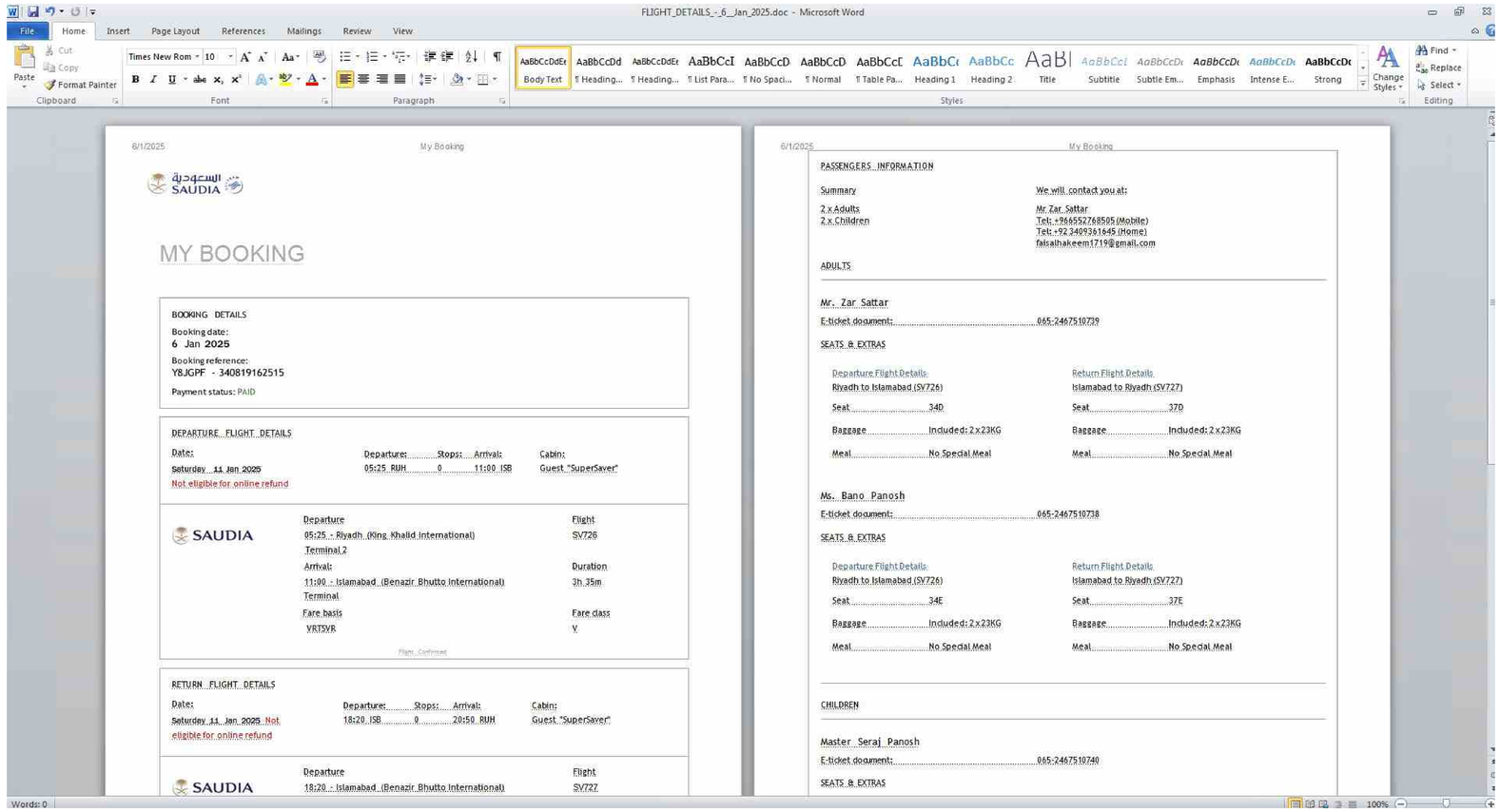


Figure 2. Decoy document used by UnsolicitedBooker

Interestingly, one of the decoy documents used by the group in 2024 was also based on the same original ticket.

The document contains a VBA macro that decodes a payload that it writes to `C:\ProgramData\smssdrvhost.exe`. This payload is a loader for a backdoor its developers call MarsSnake, based on the loader's PDB path `D:\yu_project\MarsSnake\bin_shellcode\load_http_64.pdb`, and that of the backdoor `D:\yu_project\MarsSnake\x64\http\MarsSnake.pdb`. The C&C domain is `contact.decenttoy[.]top`.

At the same organization, we detected two additional phishing attempts: one was sent from a likely compromised address and had the subject `How Saudi Arabia's new economic cities can make manufacturing more sustainable`, and the other had a subject of `Could you please check my file`.

The multiple attempts at compromising this organization in 2023, 2024, and 2025 indicate a strong interest by UnsolicitedBooker in this specific target.

Some news from Worok

In 2022, we published a **WeLiveSecurity blogpost** about Worok, a China-aligned cyberespionage group that we first observed in early 2021 exploiting the ProxyShell (**CVE-2021-34523**) vulnerability at the time of its disclosure. Worok has access to an arsenal of espionage-oriented toolsets with overlapping capabilities, probably obtained from different digital quartermasters. HDMan (aka EAGERBEE) and PhantomNet, well-known shared toolsets among China-aligned APT groups, are commonly deployed in tandem in Worok operations. Worok also uses a toolset that we named Sonifake, which is used by multiple China-aligned APT groups, including **BackdoorDiplomacy**. The highly obfuscated backdoors **Impersoni-fake-ator** and **RUDEBIRD** are part of this toolset.

Since the publication of our initial blogpost, we have continued to track this threat actor (see our **APT Activity Report Q2–Q3 2023**) and have observed Worok targeting various verticals in Mongolia, Kyrgyzstan, Türkiye, Taiwan, and Thailand. These targets include governmental and other organizations in the public sector, as well as private companies.

Last November, Worok targeted academic institutions in the UK with an undocumented backdoor, which we named XMLDoor, and that the group has been using since at least 2021. More recently, we have observed Worok deploying an updated version of the GoFighting backdoor against governmental institutions in Cambodia. GoFighting is a re-implementation of the group's PowHeartBeat backdoor that we documented in our WeLiveSecurity blogpost; this variant introduces a network communication method leveraging Dropbox. It should be noted that this is not the first time that Worok has deployed malware leveraging Dropbox, as documented by **Avast** in November 2022 with the DropboxControl C# backdoor.

Following an extensive review of our previous research and other published reports, we now also attribute to Worok, with medium confidence, several publicly documented campaigns that other researchers have attributed to various other groups:

- An attack against a Japanese consulting company in February 2023, **reported** by the Japanese company LAC, which was originally linked to LuckyMouse and TA428, both China-aligned groups.
- An attack against a Southeast Asian governmental organization, **reported** by Elastic in November 2023 under the codename REF5961. Elastic linked these activities to LuckyMouse and TA428.
- An attack, dubbed Operation Crimson Palace, against a Southeast Asian governmental organization between March 2023 and October 2023, **reported** by Sophos. The activities in question were tracked as Cluster Alpha, and linked to BackdoorDiplomacy, Worok, TA428, and REF5961 – all China aligned.

Our review of these reports indicates that these attacks actually align closely with Worok activities. The main reason for the attribution differences is Worok's frequent use of tools like PhantomNet and HDMan, which are shared by multiple groups. On the other hand, we agree with the attribution of Operation Crimson Palace to both Worok and BackdoorDiplomacy. This suggests that coordination between the Worok and BackdoorDiplomacy groups is possible: while we haven't observed any activities in our telemetry that would suggest the groups were sharing targets, publicly reported data shows that they both operated in the same network during Operation Crimson Palace, which we corroborate.

Iran

OilRig BladedFeline Lyceum GalaxyGato MuddyWater CyberToufan

Summary of Iran-aligned APT group activity

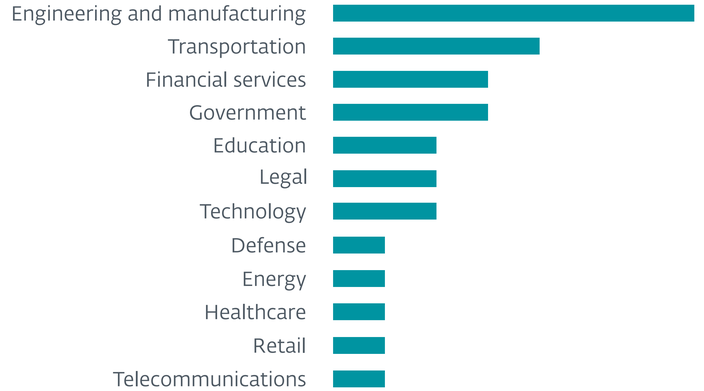
Over the course of Q4 2024 and Q1 2025, ESET researchers have tracked campaigns from Iran-aligned groups – OilRig (and its subgroups BladedFeline and Lyceum), GalaxyGato, MuddyWater, and CyberToufan.

Clomping around the riverbank

MuddyWater continues to be the most active of Iran-aligned APT groups that ESET researchers track. It also continues to be incredibly noisy and, generally, easily detected by ESET security software. In any given campaign, the group's default tool will be legitimate remote monitoring and management (RMM) software from **Atera**, **Level**, **PDQ**, **SimpleHelp**, **Syncro**, and **Tactical RMM**, which is generally deployed via spearphishing emails with a link to a file-hosting service (**OneHub** and **Mega**, in particular) that is often in an attached PDF.

We observed network infrastructure being refreshed at least every month, and we detected and reported on four distinct campaigns: two following typical MuddyWater patterns, one collaborative campaign with another Iran-aligned group, and one new and interesting campaign, in which we detected MuddyWater using an injector that reflectively loads a backdoor into memory and attempts to circumvent security software. The campaign lasted two months (September through October 2024) and targeted victims in Israel in the engineering and government verticals.

The two typical MuddyWater campaigns, which took place in February 2025 and did not use any new techniques or interesting malware, were curious in their targeting. Victims were in Cambodia and Kenya, and followed closely on the heels of **diplomatic entreaties** made by the government of Iran to these countries. It seems that Iran-aligned threat actors use their capabilities strictly for cyberespionage and have not been brought into the fold as support for any type of kinetic operation (to date). In **our APT Activity Report Q2–Q3 2024**, we discussed some targeting of the transportation vertical that could have been used to prepare for kinetic activity. That, however, did not turn out to be the case.



Sectors targeted by Iran-aligned APT groups

Initial access techniques used by Iran-aligned APT groups (with MITRE ATT&CK IDs)

The fourth campaign, in January and February 2025, was notable due to what appears to be cooperation and overlap between a MuddyWater compromise followed in rapid succession with Lyceum (an OilRig subgroup) gaining access to a system in the manufacturing vertical in Israel. MuddyWater created the initial compromise via a spearphishing email with a link to an RMM installer (Syncro). Subsequently, MuddyWater installed an additional RMM (PDQ, the RMM of choice recently for MuddyWater). A MuddyWater operator then engaged in a hands-on session of Windows shell commands, creating a bunch of noise and achieving very few operational objectives. Finally, MuddyWater deployed Mimikatz via a custom loader and injector. The same day, probably using credentials harvested using Mimikatz, Lyceum took control of adversarial activities within the organization. We have **previously noted** that MuddyWater may be acting as an access broker for other Iran-aligned groups.

Loading up on reverse tunnels

MuddyWater, a long-time user of Go-compiled reverse tunnels from GitHub, seems to have spread that tendency to Lyceum. However, Lyceum went to the trouble of writing its own reverse tunnel in C#/.NET. Lyceum used it to compromise an unidentified organization in Israel in January 2025 before pivoting to the jointly compromised victim in Israel in February 2025. The reverse tunnel was deployed via a loader that uses a separate configuration file (to avoid detection, as the configuration file does not contain any malicious content). This is a common tactic for OilRig and its subgroups, including BladedFeline.

Both campaigns used simple, custom encryption algorithms for data in motion, and reverse shells opening local ports 3389 (RDP) and 445 (SMB) to hardcoded remote ports 1500 or 10443 (paired with local port 3389) and 15475 (paired with local port 445). The second campaign (the joint effort with MuddyWater) featured a software update to its reverse tunnel, where Lyceum split the reverse tunnel's functionality from one module to two and changed the configuration file format. Both were probably a response to ESET security products detecting the original versions.

What's old is new again

In November 2024, we discovered, from a VirusTotal user in Lebanon, a new version of OilRig's old backdoor Karkoff, first reported on by **Talos** in 2019. This new version has added capabilities:

- obfuscation classes
- screen capture, and
- enumeration of files with specific filename extensions (`.pdf`, `.txt`, `.png`, and `.jpg`).

Previous versions of Karkoff were used by OilRig to target victims in Lebanon. That continues to be the case.

Can you hear me now?

BladedFeline previously (April 2022) compromised a telecommunications company in Uzbekistan. In March 2025, we detected activity consistent with BladedFeline TTPs targeting the same company with VBScripts that leverage PowerShell commands to enumerate victims' systems and provide backdoor-like functionality. It's possible that BladedFeline picked up this tactic from MuddyWater, as MuddyWater has a long history of using PowerShell scripts with backdoor-like functionality. Alternatively, this compromise could be the work of MuddyWater reacquiring access on behalf of BladedFeline (although we lack concrete evidence to support this supposition).

In addition to recompromising a previous victim, BladedFeline probably targeted and compromised a second telecommunications organization in Uzbekistan. Perhaps foreshadowing these compromises, Iran and Uzbekistan deepened their diplomatic ties in February 2025, by **lifting a USD 400 transit fee** for transportation fleets traveling between Iran and Uzbekistan (**and vice versa**). Again, diplomacy potentially foreshadows cyberespionage for Iran-aligned APT groups.

Interesting C&C communications channels

GalaxyGato stood up a new domain – `virgomarketingsolutions[.]com` – for C&C communications in September 2024. Approximately one week later, in October 2024, we detected a GalaxyGato ZIP archive uploaded to VirusTotal from Israel. The archive contained three files: a legitimate executable used to side-load one of the other files (a loader), which loads the third file (a backdoor). The backdoor, MINICHOPPER, shares similarities with MINIBIKE, first reported by **Mandiant**.

More interesting than the backdoor is the C&C communication method. MINICHOPPER uses specific URLs – `https://virgomarketingsolutions[.]com/news/photos/<victim_id>` – and POST requests for C&C communications. Neither is particularly novel, but when taken together and with similar activity seen from other Iran-aligned groups (e.g., MuddyWater), an interesting pattern emerges. It appears that Iran-aligned groups are trying to evade detection by blending into the background, mimicking legitimate traffic. Newly registered domains tend to trigger security operations center detections but nesting the C&C deeper into web server directories tends to lend credibility to the activity and may discourage responders from digging deeper.

CyberToufan

CyberToufan carried out a wiper attack against 50 organizations in Israel in January 2025. The wiper – that we named FlashFlood based on the use of "Flood" in Figure 3 and the sudden appearance of the wiper – used propaganda from the October 2023 attack by Hamas in Israel, as can be seen in Figure 3.

Interestingly, CyberToufan used the phrase `Saturday, October 07, 2023, 6:29:00 AM` as a decryption key for encrypted strings and API function names (which is, of course, when the attack in Israel started).

Figure 3. Desktop background set by the CyberToufan wiper

North Korea

DeceptiveDevelopment TraderTraitor Operation DreamJob Kimsuky Konni ScarCruft Andariel

Summary of North Korea-aligned APT group activity

The most interesting and visible activities in this region involve DeceptiveDevelopment and the Bybit hack. We observed less-than-usual activity from Kimsuky and Lazarus.

DeceptiveDevelopment diversifies

DeceptiveDevelopment is a North Korea-aligned group that focuses on financial gain. Its operators are primarily financially motivated, targeting software developers on Windows, Linux, and macOS to steal cryptocurrency, and with a possible secondary objective of cyberespionage.

During the last six months, we have observed this threat actor targeting an ever-widening range of individuals. In our investigation, we observed faux job listings for dozens of companies, both well-known industry leaders and relatively small startups, primarily related to cryptocurrency, blockchain, and finance (e.g., Coinbase, Binance, Etoro, Okcoin, Kraken, and RobinHood), but also investment firms (e.g., Barrow Wise, Bitwise, and Pantera) and disruptive technology startups (e.g., Halliday). We also observed the attackers targeting owners of cryptocurrency-related businesses, pretending to be investors interested in cooperation, as reported in a **post on X** from March 2025. The attackers seem to be picking their victims broadly without any specific selection criteria and without any regard for geographical location.

In addition to the trojanized codebase attack technique described in our previous APT Activity Report, we detected two additional attack vectors – a variation on the increasingly popular **ClickFix** social engineering technique and raising bogus issues in open-source projects.

In their ClickFix attack, the attackers direct the victim to a site impersonating a well-known video conferencing or hiring platform, attempt to convince the victim that the microphone is not working, and then instruct the victim to "fix" the issue by copying and pasting a series of commands into their terminal.

Sectors targeted by North Korea-aligned APT groups

Initial access techniques used by North Korea-aligned APT groups (with MITRE ATT&CK IDs)

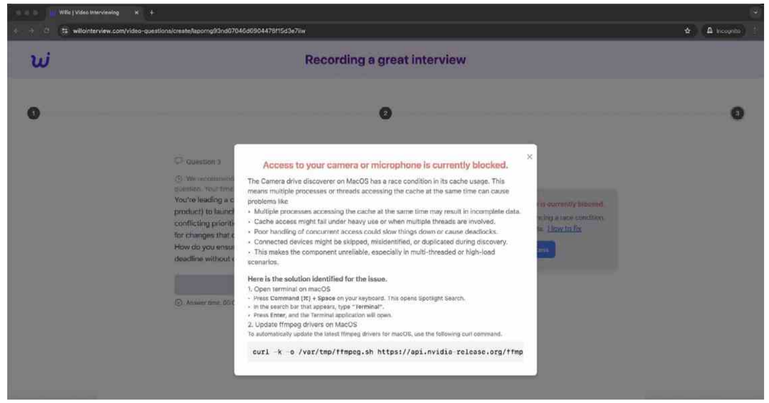


Figure 4. Fake Willo website displaying a job listing asking the candidate to record a video answer and displaying a ClickFix message attempting to convince the victim to execute a shell command to download and execute the WeaselStore malware (source: @tayvano_ **tweet**)

In the public lure approach, the attackers open issues on public GitHub repositories belonging to well-known projects, describing a generic bogus problem and also providing a supposed solution, again containing the same ClickFix instructions.

Both of these approaches were used to distribute a new multiplatform backdoor and infostealer written in Go, which we named WeaselStore. The WeaselStore malware has similar functionality to the **BeaverTail and InvisibleFerret infostealers** – which were used in past DeceptiveDevelopment campaigns – exfiltrating data saved in the Chrome browser, as well as data from the MetaMask wallet extension and the local keychain. A separate piece of malware, disguised as an app related to the browser or camera, is used to display a fake password prompt to the user and exfiltrate the account password on macOS, which can later be used to decrypt login information saved in macOS keychains.

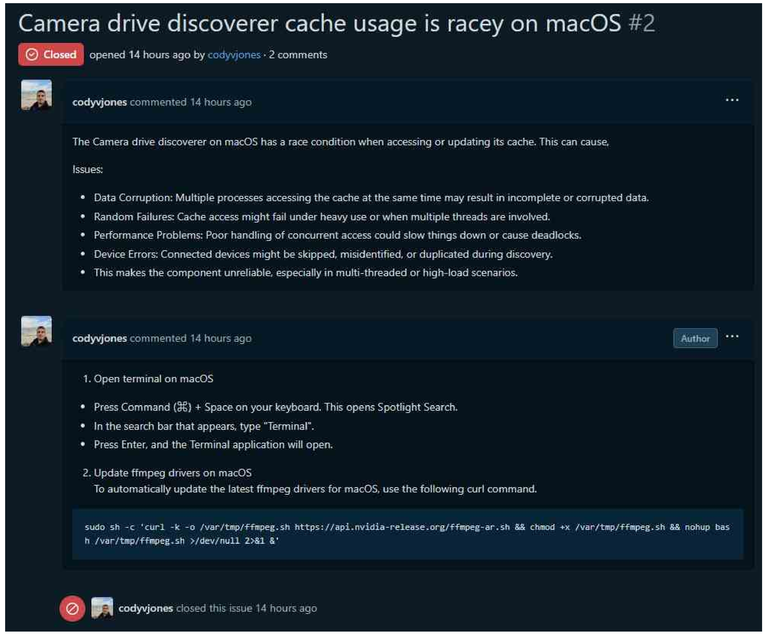


Figure 5. ClickFix-style malicious instructions posted by an attacker to a GitHub issue on a well-known repository

Bybit hack

On February 21, 2025 more than 400,000 ETH and other cryptocurrencies (worth approximately USD 1.5 billion at the time) were **stolen from Bybit**, the second largest cryptocurrency exchange in the world. The FBI publicly **attributed** this incident to the TraderTraitor group.

The threat actor was able to intercept and manipulate an ETH multi-signature transaction from Bybit's cold wallet to a hot wallet. The attackers managed to gain control of the affected cold wallet and transferred its holdings to a wallet under their control. The interesting part is how the attackers managed to do that.

Instead of compromising Bybit directly, attackers targeted the developers of Safe{Wallet} – a popular multi-signature wallet used by some of the largest companies in the cryptocurrency industry. According to a **Safe statement**, the attackers managed to compromise a machine belonging to one of the Safe{Wallet} developers. Using this access, the attackers made a change to a JavaScript file that was part of the `app.safe.global` frontend, used to sign transactions on the chain. The malicious implant was specifically crafted to only execute under specific conditions, in order to remain hidden. The attackers then used this malicious implant and combined with social engineering led Bybit employees to approve a smart contract upgrade that introduced malicious code that transferred ETH and ERC20 tokens to attacker-controlled wallets.

Supply-chain attacks continue to be some of the most challenging cyberthreats to detect and counter and the Bybit hack certainly ranks among the most impactful to date.

Still offering dream jobs

In the last six months we have observed continued activity from Operation DreamJob, mostly targeting employees of defense and aerospace companies in EU countries. The modus operandi and TTPs remain largely unchanged: the attackers use LinkedIn and other job platforms to reach out with lucrative job offers to prospective targets. After gaining the victim's trust, the attackers send the victim a malicious archive file, usually containing a trojanized PDF viewer and a decoy PDF document.

Spearphishing in South Korea

At the end of 2024 and beginning of 2025 we observed a decrease in activity from both Kimsuky and Konni. Their activity returned to usual levels in February and March 2025. However, we noticed a significant shift in campaign targeting and a change in the initial access vectors.

In our previous APT Activity Report we noted that Kimsuky was actively targeting, under the guise of interview requests, English-speaking think tanks, NGOs, and North Korea experts. These types of campaigns have decreased. Over the past six months, the majority of campaigns attributed to Kimsuky and Konni have been targeting South Korean individuals and companies, as well as embassies and diplomatic personnel located in South Korea.

Konni often uses relatively generic spearphishing emails with tax, police, and other government-related themes, whereas Kimsuky's emails are much more personalized, referring to current events and using real documents as decoys. These documents were most likely exfiltrated from previously compromised machines. The spearphishing emails are used to distribute Windows shortcut (LNK) files, leading to the next stages of compromise (a mix of PowerShell, JavaScript, and VBScript).

Kimsuky continued to use cloud services for C&C servers, with Dropbox and Google Drive being the most commonly abused. We also reported on a case where attackers used private GitHub repositories for the distribution of malicious scripts as well as for exfiltration of stolen data. On the other hand, Konni continued using compromised third-party web servers for C&C purposes, as well as deploying its own web servers in some cases.

ScarCruft continued to use HWP documents with embedded payloads and relied on social engineering in its attacks. In November 2024 we reported on a case of a compromised Korean-speaking entity in China, where RokRAT was probably used to install a more complex backdoor we named BirdCall. This backdoor was configured to use multiple compromised South Korean websites as C&C servers.

In February 2025 we observed a cyberattack by the Andariel group after a year of inactivity. A company developing industrial software in South Korea was attacked via unknown initial access methods. The attackers deployed NirSoft's WebBrowserPassView, a keylogger, a tool manipulating Windows event logs, and a TCP backdoor reminiscent of Andariel's TigerRAT. Changes in the code of the backdoor were significant compared to its previous variants, which suggests that, during this period, the group focused intensively on development efforts.

Russia

Sednit RomCom Gamaredon Sandworm

Summary of Russia-aligned APT group activity

Over the past six months, we have analyzed many activities carried out by Russia-aligned threat actors. These groups primarily target Ukraine and EU countries, relying on spearphishing email messages to gain initial access. Additionally, using XSS exploits, they target webmail servers, and in a newly discovered case they even used a zero-day vulnerability. Their usual goal is espionage, except for Sandworm, which focuses mainly on data destruction.

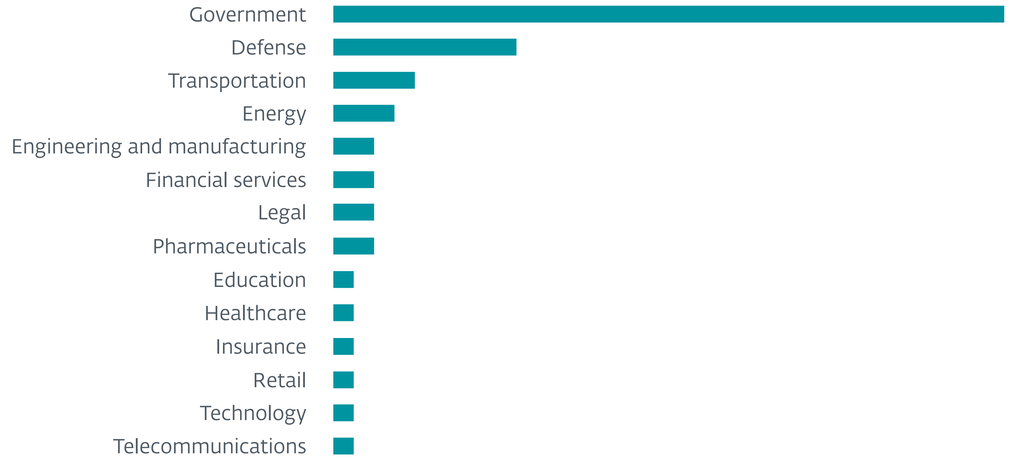
Sednit has been mastering XSS exploitation tradecraft

Russia-aligned cyberespionage groups continue to target self-hosted webmail servers. For instance, Sednit's Operation RoundPress campaign has broadened its scope to include several other webmail services such as **Horde**, **MDaemon**, and **Zimbra**, in addition to Roundcube. The attackers behind Operation RoundPress have been sending spearphishing emails containing XSS exploits, typically targeting vulnerabilities that have already been patched.

The exploits lead to the execution of malicious JavaScript code within the context of the webmail client web page running in a browser window. We identified several JavaScript payloads, such as SpyPress.HORDE, SpyPress.MDAEMON, SpyPress.ROUNDCUBE, and SpyPress.ZIMBRA. Most of these SpyPress payloads collect email messages and contact information from the victim's mailbox when a malicious email is received or viewed in a vulnerable webmail client. The data is then exfiltrated to a C&C server.

We detected several Sednit campaigns against defense companies located in Bulgaria and Ukraine.

For example, in November 2024 we detected a spearphishing email targeting a Bulgarian company. The email was sent from a compromised email address with the subject Путин се стреми Тръмп да приеме руските условия вдвустранните отношения (machine



Sectors targeted by Russia-aligned APT groups

Initial access techniques used by Russia-aligned APT groups (with MITRE ATT&CK IDs)

translation: Putin seeks Trump's acceptance of Russian conditions in bilateral relations). The message body (see Figure 6) contained excerpts (in Bulgarian) and links to articles from News.bg, a legitimate Bulgarian newspaper.

Figure 6. Content of Sednit's decoy email, which triggers an XSS vulnerability in the background

On November 1, 2024, we detected spearphishing emails targeting Ukrainian companies. These emails exploited a zero-day XSS vulnerability in **MDaemon Email Server**, specifically in the rendering of untrusted HTML code in email messages. We reported the vulnerability to the developers on November 1, 2024, and it was patched in **version 25.4.1**, which was released on November 14, 2024. We issued **CVE-2024-11182** for this vulnerability.

RomCom deploys two zero days

RomCom, also known as Storm-0978, Tropical Scorpius, or UNC2596, stands out from pure cyberespionage groups due to its dual focus on both cybercrime and espionage. This Russia-aligned group conducts both opportunistic campaigns against various business sectors and targeted espionage operations. Active since at least 2022, RomCom has been linked to the deployment of **Cuba ransomware** and has targeted the **Ukrainian government**, **Ukrainian defense sector**, NATO allies, and European governmental organizations. The group employs various tactics, including phishing campaigns and trojanized software, to deploy its malware, continually evolving its methods with new variants like **SnipBot** and exploiting vulnerabilities in popular software. For example, in June 2023, **RomCom exploited** a zero-day vulnerability (**CVE-2023-36884**) in Microsoft Word.

In October 2024, we identified previously unknown vulnerabilities in Mozilla products (**CVE-2024-9680**) and Microsoft Windows (**CVE-2024-49039**) used by the RomCom group. These zero-day vulnerabilities were used to deploy RomCom's eponymous backdoor without any user interaction required when visiting a web page containing the exploit. We published a **detailed analysis** of the chain of these vulnerabilities, specifically a use-after-free vulnerability in Firefox animation timelines and a privilege escalation vulnerability in Windows Task Scheduler. The exploits were used in a likely widespread campaign targeting up to 250 potential victims, according to ESET telemetry. This level of sophistication demonstrates the threat actor's determination and capability to develop or acquire stealthy techniques.

Gamaredon's latest updates

Gamaredon is the most active APT group targeting Ukraine. It continually improves its tools and makes numerous changes related to obfuscation, network-based detection bypass techniques, and main functionality.

To gain initial access, Gamaredon sends emails with either archive files (RAR, ZIP, 7z) or XHTML files that use HTML smuggling to simulate the download process of such archives. These archives contain HTA or LNK files that launch `mshta.exe` to download another HTA file, which includes a VBScript downloader called PteroSand for acquiring additional payloads. In October 2024, Gamaredon began heavily obfuscating HTA files by adding blank lines, unused string variables, and fake C&C servers in its spearphishing campaigns.

According to statistics from ESET telemetry and VirusTotal, Gamaredon conducted significantly larger campaigns in the second half of 2024. Notably, October 2024 was the busiest month for Gamaredon, with the highest number of new unique samples used in spearphishing campaigns.

In November 2024, we discovered a new malicious tool deployed by Gamaredon, which we named PteroBox. It is file-stealing malware written in PowerShell that exfiltrates data to Dropbox using the Dropbox API, refreshing its access token as needed. It monitors USB drives and common folders like Desktop and Documents for specific file types. The attackers are mostly interested in Microsoft Office documents, images, PDFs, archives, databases, certificates, and keys. The malware avoids certain files and uses a unique method to track already stolen files to prevent exfiltrating duplicates.

Sandworm's use of RMM tools and data-wiping malware

In October 2024, we detected Sandworm activity at several energy companies in Ukraine. In at least one case, we observed that Sandworm was using a remote monitoring and management (RMM) tool, specifically **Atera Agent**, in the early stages of the compromise.

Sandworm has intensified its operations involving data-wiping malware over the past six months. In December 2024, and again in February and March 2025, Sandworm deployed a new wiper named ZEROLOT[1] against different organizations in Ukraine. In all cases, the attackers used Active Directory Group Policy to deploy this wiper to computers in the affected organizations. Once executed, ZEROLOT wipes all files in the `C:\Users\` subdirectory and from the root on all logical drives except `C:`, skipping files with `.dll`, `.exe`, and `.sys` extensions. It uses `fsutil.exe` to overwrite file data and then deletes the files. Additionally, it deletes physical drive layouts using the `DeviceIoControl` Windows API.

[1] SHA-1: 4D4635D5DAB0E79AAEFAB0AD054627B9C154E051

Other

APT-C-60 Stealth Falcon

Other notable APT activities

ESET researchers also tracked campaigns from lesser-known groups. In this section, we highlight a recent APT-C-60 campaign in Japan, and a spearphishing campaign themed around the World Economic Forum.

In addition to Iran-aligned groups, we also observed activities from other Middle East-aligned threat actors such as Stealth Falcon in Türkiye and Pakistan.

APT-C-60 in Japan

On February 28, 2025 a VHDX file containing a malicious shortcut and an encrypted downloader, which we call RadialAgent, was uploaded to VirusTotal[2] from Japan. RadialAgent is a malware family that, we assess, is exclusive to **APT-C-60**, a South Korea-aligned cyberespionage group.

The root folder also contains interesting files such as `メールリスト.rtf` (machine translation: mail list) and `会社系.rtf` (machine translation: company department). The first is an old leak from the Anonymous group containing the **list of 3,667 members of the General Association of Korean Residents in Japan** (**Chongryon**), a group which is suspected to have ties with North Korea.

This suggests that APT-C-60 is operating against targets in Japan, possibly people with links to North Korea.

Davos-themed phishing campaign

In January 2025, Christo Grozev (an investigative journalist) published a **tweet** about a phishing message delivered via Signal to selected targets asking them to confirm their participation in the World Economic Forum at Davos, as shown in Figure 7.

If the potential victim clicks on this link, a phishing page, illustrated in Figure 8, asks for confirmation of some personal data.

If the target clicks on Continue, a phone number is requested, purportedly to validate the identity of the potential victim, as shown in Figure 9.

An allowlist to filter potential victims from nontargeted phone numbers was present on the website. This list contains the name, work title, birth date, and phone number of 25 potential victims, mostly Ukrainian officials and diplomats, also explaining the phishing page design.

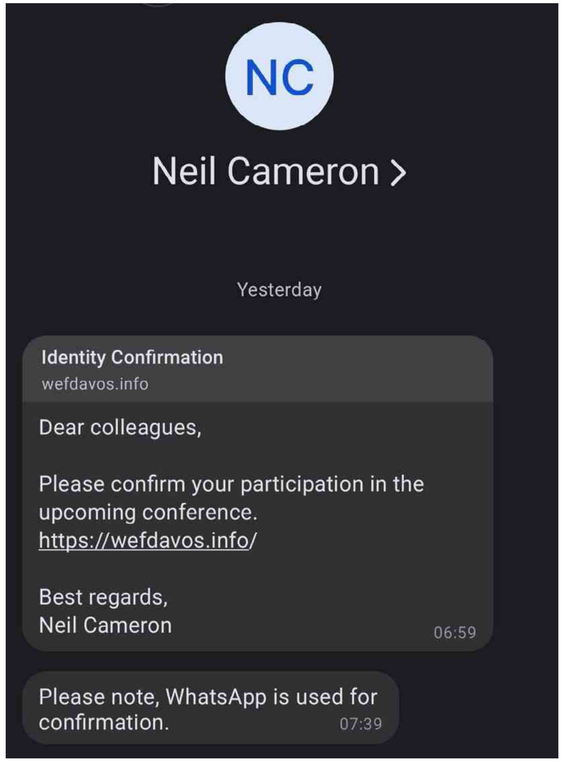


Figure 7. Phishing message received in Signal (source: Christo Grozev **tweet**)

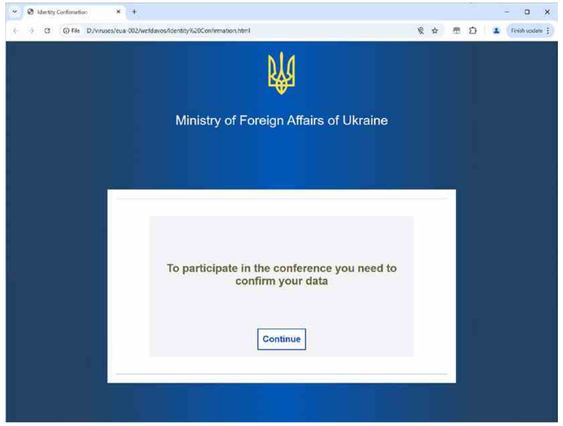


Figure 8. Request for personal data confirmation

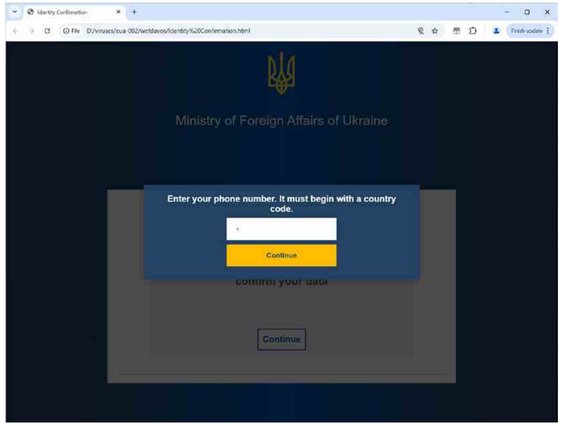


Figure 9. Phone number validation

[2] SHA-1: F32F07F2A4F019976B83088ED1D17B9D19A520CA

The website also has some user data collection in place, and sends the visitor's IP and geolocation to the C&C server controlled by this threat actor.

The following day in January, another similar phishing website (shown in Figure 10) was discovered, using the domain `gov-abh[.]site`, which impersonates `gov-abh[.]org`, the official website in Abkhazia, a partially recognized state in the South Caucasus officially belonging to Georgia.

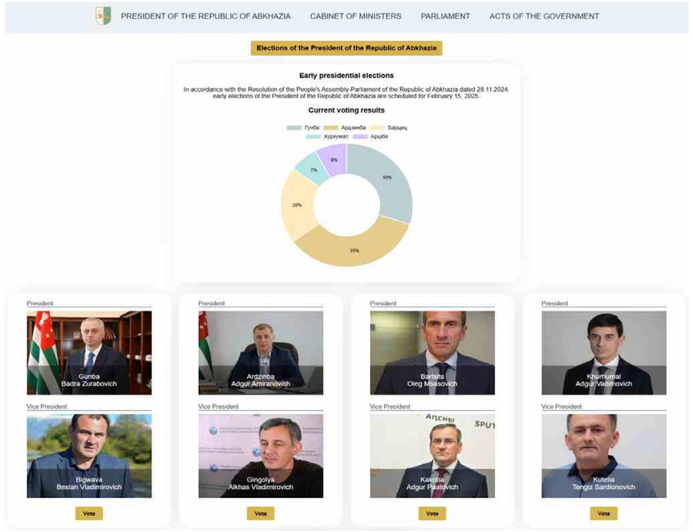


Figure 10. Election website of the Republic of Abkhazia

Both phishing websites were hosted on Cloudflare, but this time no phone number allowlist was in place. Clicking on a Vote button under a combination of president and vice president triggers the website to ask for confirmation of identity via phone number, as shown in Figure 11. Note that the country code

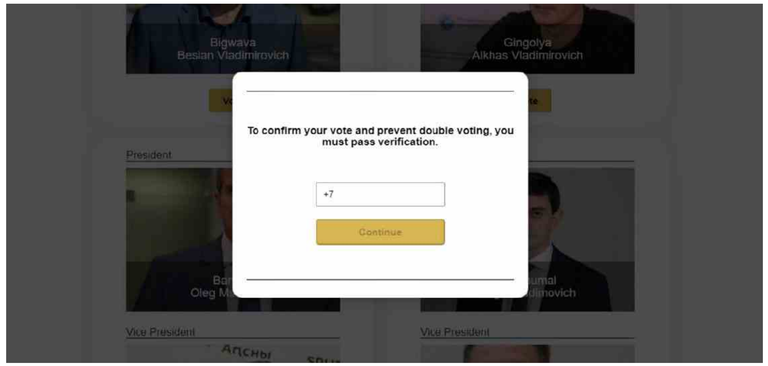


Figure 11. Request for phone number

`+7` belongs to Russia and Kazakhstan, but any valid phone number can be entered.

Just as on the World Economic Forum website, a message is sent to the victim with a code to enter.

These campaigns are examples of highly targeted phishing – especially the first one that verified the target against a predefined list – most likely aiming to steal sensitive information from the potential victims.

Stealth Falcon

In October 2024, Stealth Falcon deployed an injector to a victim in Türkiye, who uploaded the injector to VirusTotal. The injector is part of a multistage exploit chain that ends with a browser-data infostealer, which is quite popular with Middle East-based threat groups (among others). The infostealer is a C#/.NET creation targeting Chromium-based browsers like Chrome and Edge. The collected data is AES-256-CBC encrypted, base64 encoded, and written to a network storage location where it is staged for exfiltration by some other means (no part of the exploit chain contains backdoor-like functionality).

Separately, in January 2025, we detected an injector and keylogger in Pakistan that probably dates to sometime between 2020 and 2023. The keylogger parses keyboard layout information and properly converts virtual-key codes into characters, even considering cases such as ligatures and dead keys – probably with the intent of being able to target non-Latin-based languages such as Arabic. Again, Stealth Falcon split up its tools, probably to avoid detection, and some other means of exfiltration is employed.

About ESET

ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit **www.eset.com** or follow us on **LinkedIn**, **Facebook**, and **X**.

ESET Threat Intelligence

ESET Threat Reports and APT Activity Reports

ESET GitHub

@ESETresearch

WeLiveSecurity.com