Digital Security
Progress. Protected.

# APT Activity Report

## IRAN-ALIGNED CYBERATTACKS: RISE IN DISRUPTIVE OPERATIONS

October 2023 – March 2024

(eset):research

# Contents

**Executive summary** 3

**Attackers and targets** 4

**China-aligned groups** 5

Mustang Panda targets the cargo shipping industry in Europe 6

Activities against Taiwan 7

Our assessment of the I-SOON leaks 7

**Middle East-aligned groups** 9

BladedFeline 10

POLONIUM 10

Summary of Iran-aligned APT group activity 11

Access brokering 11

Impact attacks with wipers and ransomware 12

**North Korea-aligned groups** 13

Supply-chain attacks and trojanized installers 14

Evolving attackers' toolset 15

**Russia-aligned groups** 16

Spearphishing as initial access 17

Cyberespionage operation against European governments 18

Russia-Ukraine war 18

**Other** 20

SturgeonPhisher 21

Unlucky Kamran 21

Winter Vivern 22

**About ESET** 23

# Executive summary

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

This report summarizes notable activities of selected advanced persistent threat (APT) groups that were documented by ESET researchers from October 2023 until the end of March 2024. The highlighted operations are representative of the broader landscape of threats we investigated during this period, illustrating the key trends and developments, and contain only a fraction of the cybersecurity intelligence data provided to customers of ESET's private APT reports.

In the monitored timeframe, several China-aligned threat actors exploited vulnerabilities in public-facing appliances, such as VPNs and firewalls, and software, such as Confluence and Microsoft Exchange Server, for initial access to targets in multiple verticals. Based on the data leak from I-SOON (Anxun), we can confirm that this Chinese contractor is indeed engaged in cyberespionage. We track a part of the company's activities under the FishMonger group. In this report, we also introduce a new China-aligned APT group, CeranaKeeper, distinguished by unique traits yet possibly sharing a digital quartermaster with the Mustang Panda group.

Following the Hamas-led attack on Israel in October 2023, we detected a significant increase in activity from Iran-aligned threat groups. Specifically, MuddyWater and Agrius transitioned from their previous focus on cyberespionage and ransomware, respectively, to more aggressive strategies involving access brokering and impact attacks. Meanwhile, OilRig and Ballistic Bobcat activities saw a downturn, suggesting a strategic shift toward more noticeable, "louder" operations aimed at Israel. North Korea-aligned groups continued to target aerospace and defense companies, and the cryptocurrency industry, improving their tradecraft by conducting supply-chain attacks, developing trojanized software installers and new malware strains, and exploiting software vulnerabilities.

Russia-aligned groups have focused their activities on espionage within the European Union and attacks on Ukraine. Furthermore, the Operation Texonto campaign, a disinformation and psychological operation (PSYOP) uncovered by ESET researchers, has been spreading false information about Russian-election-related protests and the situation in Ukrainian Kharkiv, fostering uncertainty among Ukrainians domestically and abroad.

Additionally, we spotlight a campaign in the Middle East carried out by SturgeonPhisher, a group we believe to be aligned with the interests of Kazakhstan. We also discuss a watering-hole attack on a regional news website about Gilgit-Baltistan, a disputed region administered by Pakistan, and lastly, we describe the exploitation of a zero-day vulnerability in Roundcube by Winter Vivern, a group we assess to be aligned with the interests of Belarus.

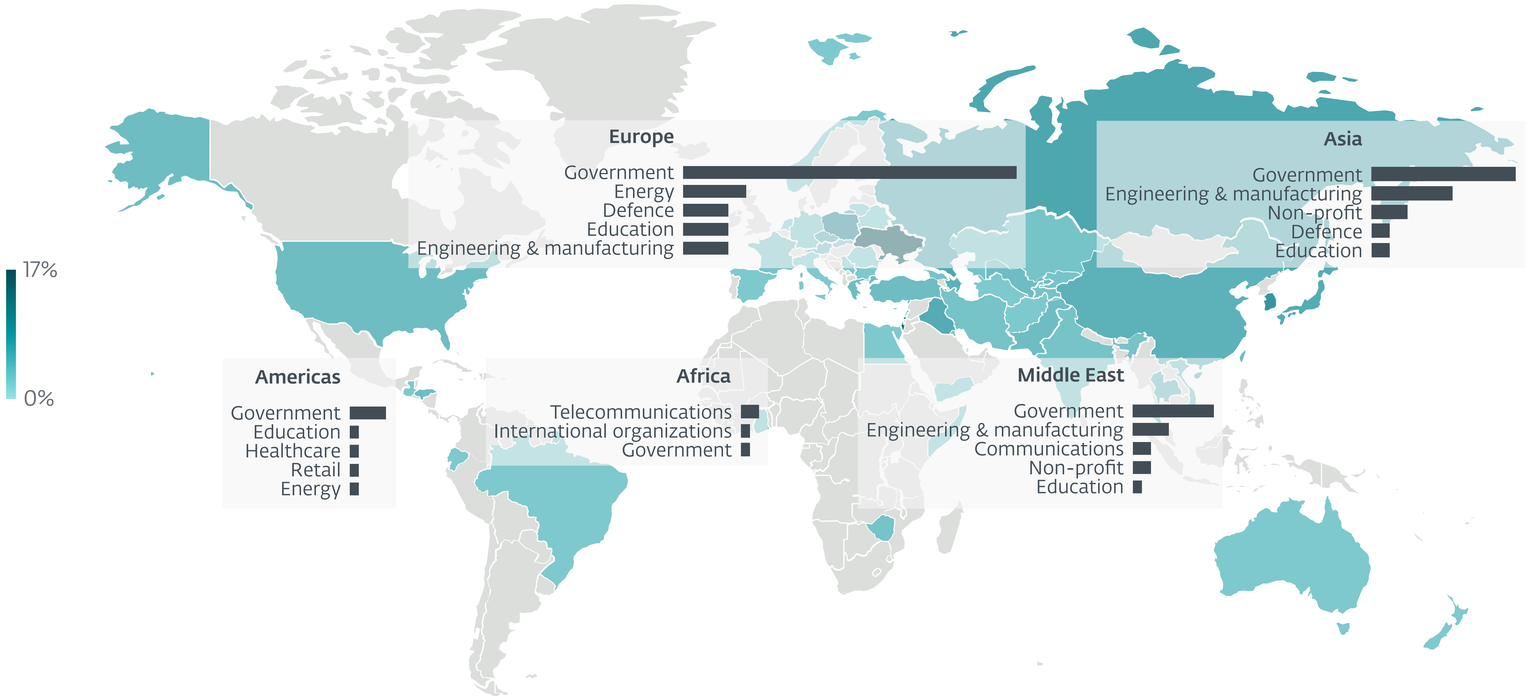
ESET products protect our customers' systems from the malicious activities described in this report. Intelligence shared here is based mostly on proprietary ESET telemetry data and has been verified by ESET researchers, who prepare in-depth technical reports and frequent activity updates detailing activities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

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

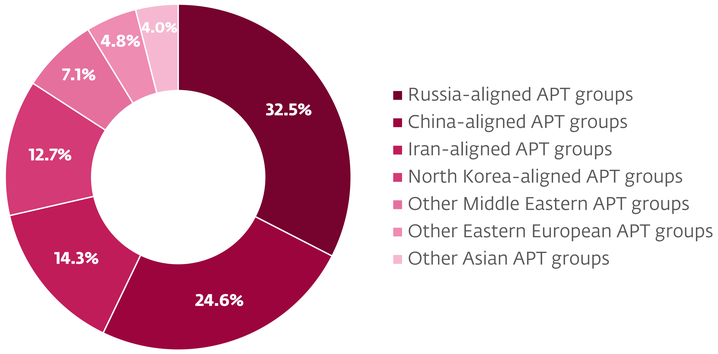
# Attackers and targets

In Asia, the focus of the described campaigns was primarily on government organizations, non-profit entities such as Tibetan groups or dissidents, and the engineering and manufacturing sectors. In Japan, China-aligned MirrorFace showed a marked persistence in its attacks on government institutions, indicating a specialized focus within this geographical area. Similarly, in the Middle East, threat actors aligned with Iran primarily targeted government organizations and other verticals. The most significant attention was directed towards Israel, suggesting a geopolitical motive behind the threat activity in this region.

Europe experienced a more diverse range of attacks from various threat actors. Russia-aligned groups continued to relentlessly target Ukrainian infrastructure, with Gamaredon standing out as the most active APT group operating in Ukraine, and Sandworm focusing on Ukrainian energy infrastructure. Russia-aligned groups also expanded their focus on espionage in the European Union, where China-aligned threat actors maintain a consistent presence, indicating a continuous interest in European affairs by both Russia- and China-aligned groups.




Targeted countries and sectors




Attack sources

# China

Mustang Panda | CeranaKeeper | Flax Typhoon | Operation ChattyGoblin | FishMonger | I-SOON

# Summary of China-aligned APT group activity

This section provides highlights of various cyberespionage campaigns carried out by China-aligned APT groups tracked by ESET researchers.

China-aligned threat actors predominantly exploit public-facing applications for initial access, targetting a variety of verticals. In the campaigns we investigated, these groups mostly used one-day vulnerabilities against a variety of appliances (e.g., VPNs, firewalls) and software (e.g., Confluence, Microsoft Exchange Server) on internet-facing devices.

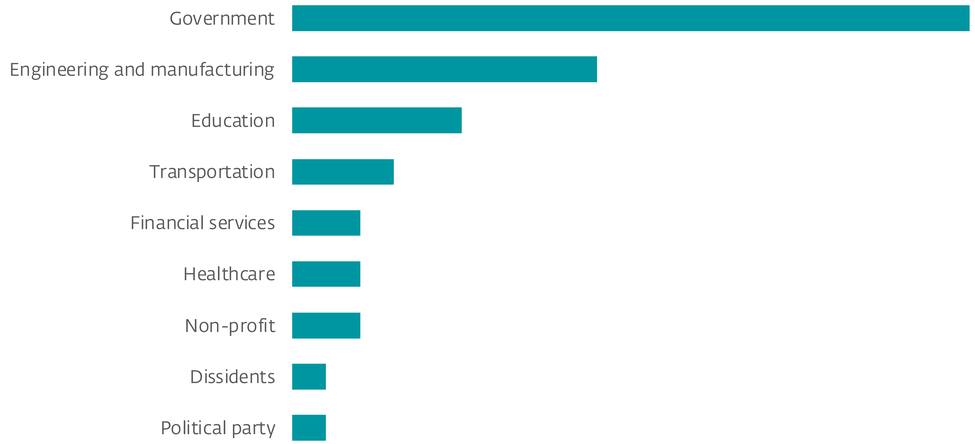
In Europe, the Mustang Panda group targeted the cargo shipping industry, deploying Korplug loaders onto victim's systems. Some of these samples used DLL search-order hijacking against an outdated version of Nero WaveEditor and used invalid Authenticode signatures.

We provide below a summary of various cyberespionage campaigns carried out by China-aligned APT groups against multiple different targets in Taiwan.

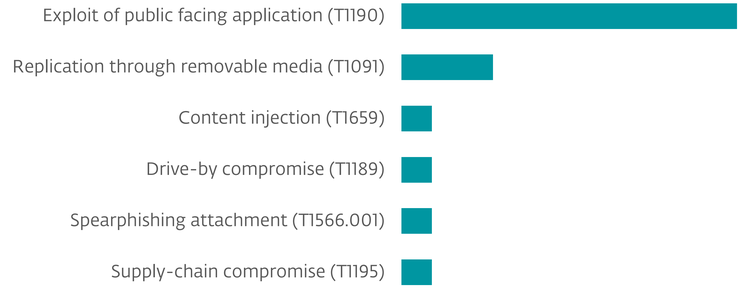
Finally, we share our assessment about the I-SOON leaks that occurred this February and discuss the links between the company, FishMonger, and Operation ChattyGoblin.

## Mustang Panda targets the cargo shipping industry in Europe

In the first quarter of 2024, our team identified the presence of Mustang Panda's Korplug loaders on computer systems belonging to cargo shipping companies based in Norway, Greece, and the Netherlands, including some that appeared to be aboard the cargo ships themselves. We were already familiar with these samples, as they have been utilized in previous campaigns, suggesting that Mustang Panda operators are reusing samples across




**Sectors targeted** by China-aligned APT groups




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

multiple campaigns. It's worth noting that in certain instances, the initial dropper appears to have been launched from a USB drive and had filenames such as `Usb Disk(29GB).exe` or `SONY_8GR.exe`.

All working samples were blocked, but others were non-functional due to them having been packed with a modified version of UPX that prevented their execution.

Some of the samples deployed at these cargo shipping companies have invalid Authenticode signatures and probably used DLL search-order hijacking against an old version of Nero WaveEditor. One invalid signature was copied from a binary legitimately signed by Klaas Nekeman. Another sample utilized a signature copied from a binary legitimately signed by AVG Technologies USA, a firm specializing in computer security.

**A note about the attribution of the recent TONESHELL campaigns**

Since mid-2022, campaigns using a new toolset, including the TONESHELL backdoor, have been attributed to Mustang Panda. However, after extensive analysis, we have decided to track this activity as the work of a separate threat actor that we have named CeranaKeeper. Despite some similarities, such as the use of the same DLL hijacking targets and some shared tooling, we are tracking this as a distinct threat actor due to organizational and technical differences. Mustang Panda and CeranaKeeper seem to operate independently, each with its own toolset. They may, however, rely on the same digital quartermaster or have some level of information sharing, which would explain the observed similarities. We will continue to track and report on both groups.

## Activities against Taiwan

During the last six months, ESET researchers observed numerous campaigns carried out by China-aligned APT groups against various targets in Taiwan, where a presidential election was held this January.

We observed the compromise of the network of a Taiwanese television broadcasting company that we attribute with high confidence to the SparklingGoblin group (which we documented in **several publications** on WeLiveSecurity).

Flax Typhoon, a group **documented by Microsoft**, remains very active in Taiwan. During the last six months we observed Flax Typhoon compromising multiple Microsoft Exchange servers and deploying China Chopper webshells. Even though focused exclusively in Taiwan, Flax Typhoon's targeting seems opportunistic and the victimology is broad: the group targeted several government organizations, but also a consulting firm, a travel booking software company, and the pharmaceuticals and electronics verticals. As mentioned by Microsoft, Flax Typhoon operators deploy the legitimate SoftEther VPN client and VPN bridge, and establish a persistent VPN connection on compromised systems, allowing them to RDP directly to the compromised systems.

ESET researchers also discovered two undocumented Linux backdoors used by Gelsemium (a group that we documented in a **white paper on WeLiveSecurity**) against Linux servers in Taiwan, probably exploiting an Apache Tomcat vulnerability. One of these backdoors, which we named WolfsBane, is a Linux variant of the Gelsevirine backdoor. The second backdoor, which we named FireWood, is connected to Project Wood (which we documented in a **WeLiveSecurity blogpost**), previously used by Gelsemium during Operation TooHash, as **documented by G Data**.

Finally, considering Linux malware, we observed the tentative deployment of the Linux variant of the Winnti malware against a computer science department of a Taiwan university. Unfortunately, since the Winnti malware is shared among several China-aligned APT groups, we cannot conclusively attribute this attack.

## Our assessment of the I-SOON leaks

On February 16, 2024, a leak containing internal data of the I-SOON (Anxun) company was posted on GitHub at **https://github.com/I-S00N/I-S00N/**.

We believe the leak is authentic. While it's not possible for us to validate every single document, we can corroborate enough of the documents as authentic to be highly confident in this assessment.

We can also independently confirm that I-SOON is indeed a Chinese contractor engaged in cyberespionage. What we are tracking under the group name FishMonger corresponds to part of the company's activities (note that the link was also confirmed by **PwC analysts**). While I-SOON is based in Shanghai, most of the R&D is located in Chengdu. This city also hosts the infamous **Chengdu 404 network company**, but both should not be mixed. In October 2023, it was **revealed** that the two companies are opponents in a court case. I-SOON's website is not accessible anymore since the release of the leak, but it was **archived** before it was taken offline. On this website, I-SOON publicly advertised having China's **Ministry of Public Security** as a customer and of carrying out offensive and defensive operations.

Interestingly, one IP address mentioned in the leaked chat logs (`8.218.67[.]52`) was used during Operation ChattyGoblin – a series of attacks against Southeast Asian gambling companies that we documented in our **Q4 2022-Q1 2023 APT activity report on WeLiveSecurity.** According to ESET telemetry, that server was hosting the web interfaces for the NPS and Maisui network proxying tools in June 2022. During

our research, we could not tie that activity to a known group. In the leaked I-SOON chat logs shown in Figure 1, an employee asks for access to a machine, apparently for a third party, and another employee provides the credentials to log into that server. Note that this dialog also happened in June 2022.

```
2022-06-13 07:39:19 user_1: Asking about personal PC access in Yangzhou

2022-06-13 07:39:23 user_1: Can I give it now

2022-06-13 07:40:26 user_2: 8.218.67[.]52:27011 [account] admin [password] 88888888
```

**Figure 1.** Extract of I-SOON leaked chat logs (machine translated)

Therefore, we now attribute Operation ChattyGoblin's activity to I-SOON, with medium confidence.

The leak offers some interesting perspective on the motivations behind these attacks against gambling companies. In particular, I-SOON provides to its customers a platform to investigate gambling cases – gambling is an illegal activity in the People's Republic of China – named the Falcon Anti-Gambling Platform. That platform relies on "backend data of domestic and foreign gambling websites", according to its leaked documentation, and allows its users to search for data on gamblers and gambling companies. This very likely explains the purpose of Operation ChattyGoblin: to hack into gambling companies to exfiltrate data to feed to the Falcon platform.

Overall, the leak offers an unprecedented view of the internals of the company, including some of its products, its HR challenges, its customers, and its victims. Our analysis reveals a few global points:

- I-SOON works mostly for the Chinese **Ministry of Public Security** (MPS), not only by providing stolen data and ready-to-use malware, but also by training MPS employees in several provinces.
- I-SOON resells ShadowPad (internal name: SecuritySystem), Winnti for Linux (internal name: Threadstone), and an unknown Linux implant named Hector.
- I-SOON also has iOS and Android implants that are probably related to the **POISON CARP** group.
- The list of victims reveals the targeting of universities in Hong Kong in 2019. This is in line with **our findings published on WeLiveSecurity.** We initially attributed the incident to Winnti Group but have since revised our attribution to FishMonger.

# Middle East

BladedFeline POLONIUM MuddyWater OilRig Ballistic Bobcat Agrius

# Summary of Middle Eastern APT group activity

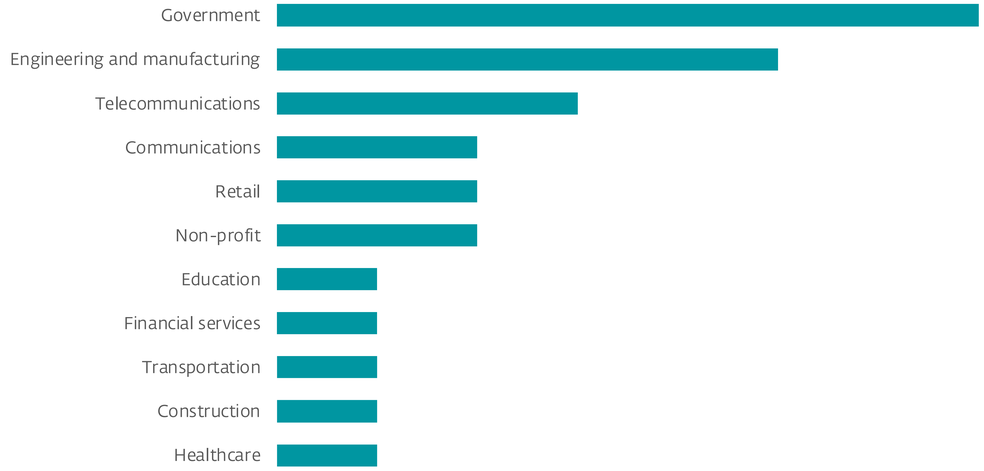
## BladedFeline

During the past two quarters, BladedFeline continued to exploit a governmental organization from the Kurdistan region of Iraq. The coding capabilities of this group, which has interests that align with Iran, specifically targeting longtime rival Iraq, display a breadth of skill, deploying payloads written in Python, C#/.NET, and C++, which makes them something of an oddity amongst Middle East-aligned (and Iran-aligned) groups. The group is also quite proficient in PowerShell and VBScript, having deployed tools using both in what are best characterized as well-written scripts that are a notch above other groups in the region.

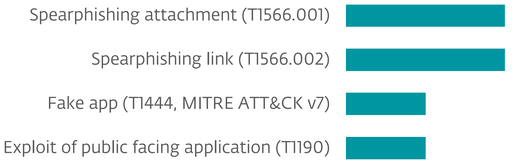
The group has gone to some lengths to maintain access to this governmental organization, having breached it at several layers and reinforcing access by innovating new backdoors and tunneling applications. In addition to the governmental organization, BladedFeline also compromised a telecommunications provider in Uzbekistan. We detected the attack during this reporting period; however, the initial compromise time probably dates back to May 2022. Targeting this victim is interesting in the timing, particularly if the links to Iran-aligned groups pan out, as Iran has recently been noted to be considering **rapprochement with Central Asian countries**. Having followed Middle Eastern groups for some time, we can say that cyberespionage goes hand in hand with diplomatic efforts, particularly when it comes to Iran.

## POLONIUM

During this reporting period, we observed **POLONIUM**, a threat actor aligned with Hezbollah's interests, continue to be avid Python coders. In November 2023, POLONIUM used a Python backdoor, MegaPy, and an exfiltrator to exploit four Israeli organizations in the technology and social services verticals. The




**Sectors targeted** by Middle Eastern APT groups




**Initial access techniques** used by Middle Eastern APT groups (with MITRE ATT&CK IDs)

backdoor uses **MEGA** and Nextcloud for C&C communications and, for the exfiltrator, for data storage. An interesting feature of the exfiltrator is that the WebDAV protocol is used, which is not something we commonly see in malware communications.

Then in January 2024, POLONIUM deployed an update of its Python backdoor to construction, manufacturing, and healthcare companies in Israel. This iterative update employs encrypted payloads with per-victim, customized content, probably to mask some of the exploit chain from defenders and to make tracking more difficult for researchers. During this campaign, POLONIUM changed the service providers used for its C&Cs: **Supabase** and **Backendless**. Initial payload hosting was done, in one particular case, on a typo-squatting domain: `yutube.com[.]de`.

MuddyWater OilRig Ballistic Bobcat Agrius

# Summary of Iran-aligned APT group activity

ESET researchers, while tracking Iran-aligned threats, have observed a sharp uptick in activity following the attack on Israel on October 7, 2023. The increased activity has been focused on two primary pursuits: access brokering, typified by access development immediately followed by credential theft; and, subsequent attacks seeking to damage, destroy, or otherwise harm organizations, with the occasional name-and-shame post-impact activity on social media. Commensurate with the uptick in operational tempo has been a marked decline in attack efficacy and overall quality of operations and tooling (particularly with MuddyWater, which has not historically been a powerhouse in APT circles).

This increase in operational tempo and focus on access brokering in conjunction with impact malware has likely led to a decrease in typical cyberespionage. We have noted a downturn in OilRig activities, beginning in November and culminating in December. Since then, OilRig has been unusually quiet, whereas we would typically expect to see the group updating existing tooling to maintain previously established accesses and deploying new, often novel, malware to target mostly governmental entities in the Middle East – with a heavy focus on Israel.

**Ballistic Bobcat**, which also has generally been a steady purveyor of malware, also seemed to wind down operations in September and October. Although, in that timeframe, we did see Ballistic Bobcat employing TTPs we associate with MuddyWater, including the use of remote access tools (**RemCom**), PowerShell scripts, and manual operator command line execution of a variety of commands. Overall, we assess that a great many Iran-aligned threat actors have shifted focus to support efforts to attack Israel with loud attacks and have largely eschewed quieter operations.

## Access brokering

The group doing the bulk of the yeoman's work in this area is, perhaps unsurprisingly, MuddyWater. The primary initial access method has been phishing emails with maliciou link that, when clicked, download a remote access tool (RAT), also referred to as a remote management and monitoring (RMM) tool. A less seen but equally successful initial access tactic is a phishing email with an attached document that includes a malicious link that, when opened, downloads the same or similar RAT/RMM. This extra step was only adopted by MuddyWater at the end of Q1 2024, probably to evade defenders from blocking the previously employed method that was publicly reported by **Proofpoint**.

In addition to MuddyWater, we also observed Agrius both attempting access brokering activities and deploying impactful malware to victims in

Israel. This represents a departure from typical Agrius activity, which has historically been focused on wipers, ransomware, or some variation of the two, without any credential theft endeavors.

Subsequent to the initial access, MuddyWater has employed a variety of tools and techniques attempting to obfuscate C&C servers. Typical RATs/RMMs include **Atera**, **SimpleHelp**, and **TacticalRMM**. Beyond that, though, MuddyWater operators have literally been scraping GitHub and the internet for any and all tooling they can find that offers reverse-shell-like capabilities. Aside from old MuddyWater staples like **Ligolo**, **frp**, and **Venom**, they have also used **Bore**, **GoSocks5**, **Koblas**, **rathole**, **ReSocks**, ReSocks-5 (in C++ and **Go**), **Revsocks**, and **Yamux**. Many would-be victims received more than a handful of these tools, which were quite often blocked by ESET software…leading to several comical instances of operators attempting to execute the same tools repeatedly.

Finally, MuddyWater deployed additional tooling to establish persistence (occasionally) and gather credentials. For the former, MuddyWater continued looking for resources on the internet, including **AutodialDLL** (which was publicly reported on by **Palo Alto**). As to the former, MuddyWater deployed an LSASS dumper disguised as 7-Zip and a credential stealer masquerading as a Java update. In several cases, MuddyWater used a tool, **RunPEinMemory**, to attempt to bypass ESET security tooling (unsuccessfully) by loading malware into memory, then executing it.

## Impact attacks with wipers and ransomware

We observed three distinct impact attacks (e.g., wipers, ransomware) during this period. The first occurred at the end of October, which we dubbed BiBiGun Wiper, based on the file extension that was used to overwrite files (`.bibi`). Initially reported by **Security Joes**, we quickly pivoted on the Linux version to find a Windows variant. It is not clear to us whether any of the aforementioned access brokering was used to facilitate access to victims, as we did not see any victims with ESET software installed.

The second occurrence took place at roughly the same time. Agrius deployed a wiper to victims in Israel in the communications vertical (among others we could not identify). **Palo Alto** and the **Israeli CERT** each published an article about this attack. The version of the wiper observed in our telemetry is a BIOS wiper based on the **Red Petya wiper**. Perhaps more interesting than the wiper, though, is the use of a modified version of Plink that Agrius used like a reverse tunnel: it requires base64-encoded runtime arguments. In addition, Agrius also deployed several LSASS dumpers to victims before deploying the wiper, likely to add access brokering for future attacks. One additional tidbit we saw is that both Agrius (during this incident) and Ballistic Bobcat (in previous attacks) have used the same SQL dumping tool, perhaps indicating tool sharing across these previously unlinked groups.

The final occurrence was in March 2024 and was perpetrated by an as-yet-unattributed group with goals that coalesce with Iran-aligned threat actors. The wiper targeted at least 19 organizations in Israel over a wide range of verticals. The group's TTPs align with other Iran-aligned groups, most notably MuddyWater, in that several remote access tools were used to drop files on victim systems, including **AnyDesk**, **N-Able**, and **UltraVNC**. Additionally, the string `AaronBushnell` is included in all wiper samples discovered. Aaron Bushnell was an enlisted member of the United States Air Force prior to his self-immolation in front of the Israeli embassy in Washington, DC on February 25, 2024. In the days following his death, many pro-Iranian figures – including Ayatollah Ali Khamenei – have used Bushnell as a talking point supporting Iranian interests. It follows that groups with interests aligned with Iran would also use Bushnell's name.

While we cannot definitively state that access broker operations were involved in this last wiper attack, it does seem highly plausible based on the suddenness of the attack (carried out over two days), and the large number of victims with seemingly no indicators of compromise leading up to the wiper's deployment.

[1] SHA-1: C9D18D01E1EC96BE952A9D7BD78F6BBB4DD2AA2A

# North Korea

Andariel Lazarus ScarCruft Kimsuky Konni

# Summary of North Korea-aligned APT group activity

In the current reporting period period, we noticed several interesting trends. All groups continued to improve their tradecraft by either developing new malware strains or using techniques successfully used in the past by North Korea-aligned groups.

Lazarus continued to target aerospace and defense companies, with the presumed goal of espionage. At the same time, we noticed that Lazarus appears to be putting a larger effort into targeting the cryptocurrency industry, both organizing crypto heists and compromising developers working on cryptocurrency projects. According to a Microsoft report, cryptocurrency worth between $600 million and $1 billion was stolen by North Korea-aligned threat actors in 2023.

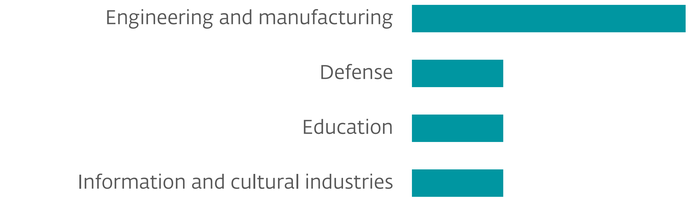
Both ScarCruft and Konni ran spearphishing campaigns targeting individuals and organizations in South Korea. In addition, Konni apparently targeted selected Russian government employees in a campaign we investigated in December 2023. We also detected activity of different Kimsuky clusters worldwide.

The primary compromise vector remains spearphishing. Lazarus continued using fake job offers in its Operation DreamJob, whereas ScarCruft and Konni often used cryptocurrency, Know Your Customer, or business agreement lures, to target selected individuals. Andariel used several publicly disclosed vulnerabilities in web applications as the initial access vector.

## Supply-chain attacks and trojanized installers

In this period, there was a noticeable increase in broadscale campaigns using supply-chain compromises and trojanized software installers.

In November 2023, Microsoft uncovered a Lazarus-linked attack on CyberLink – a Taiwanese multimedia software company. Attackers compromised the




**Sectors targeted** by North Korea-aligned APT groups


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

company, inserted malicious code into its software build and delivery process, hence any resulting binaries would be trojanized and be signed by the company's digital certificate and released via official channels to the company's users.

In December 2023, ESET detected Kimsuky malware on several machines belonging to a construction-related entity in South Korea. The analysis of the attack revealed that the malware was downloaded and executed, by employees, on the entity's compromised servers that were running the WIZVERA VeraPort solution. According to our data, the attack continued until January 2024. Interestingly, the malware was available for download only in specific timeframes. Outside of these timeframes, the compromised servers served legitimate binaries. This was confirmed in an AhnLab **report**, published in February 2024. Additionally, AhnLab estimated that the total number of afflicted machines was over 3,000, showing that this attack had a relatively large number of victims.

Konni used a trojanized installer of a very niche application to target employees of Russian embassies as seen in Figure 2. The same approach was also used by Lazarus in its DreamJob campaigns. Trojanized PDF viewers and trojanized VNC applications were delivered to victims as a part of a job application process, which served as the initial compromise vector.

Last but not least, Lazarus was observed uploading trojanized JavaScript and Python packages to open-source package repositories like NPM and PyPI, imitating popular package names in order to trick people into installing them. These packages would act as downloaders for further malicious components and were targeting three major operating systems – Windows, Linux, and macOS.

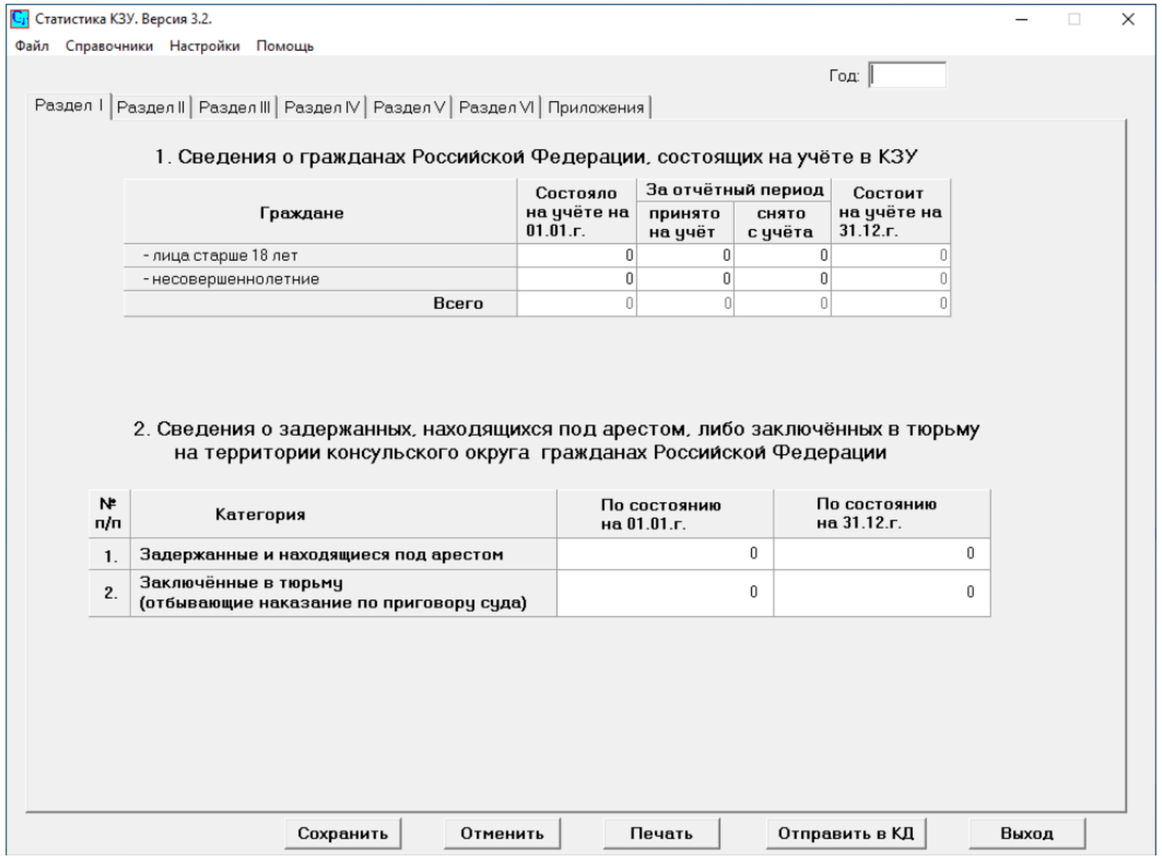



**Figure 2.** Screenshot of the custom reporting software

## Evolving attackers' toolset

Speaking of attacker's tools and techniques, we noticed a shift towards the use of malicious LNK (Windows shortcut) files. ScarCruft, Konni, and Kimsuky all started using v"very similar LNK files with artificially inflated sizes. PowerShell emerged as the favorite scripting language for these threat actors – long PowerShell command lines are used to extract and decrypt malicious payloads embedded in the shortcut file itself. Previously, these actors used CHM (Compiled Windows Help) files and the MSHTA engine to achieve their goals.

Lazarus developed a new backdoor that we named WebLogTea. We were able to analyze both macOS and Linux versions of the backdoor, which were distributed via trojanized PyPI packages in February 2024. WebLogTea was also independently analyzed and **described** by researchers at Vipyr Security.

In the middle of 2023, Kimsuky was observed using **AlphaSeed**, which is newly developed malware written in Go, as well as **proxy malware**. Throughout the rest of 2023 and the beginning of 2024, Kimsuky continued with the trend of developing new malware strains in Go. In particular, various security vendors described and named **TrollAgent**, **Endoor**, and **Nikidoor**. We attribute all this new malware to the Kimsuky AppleSeed cluster.

# Russia

Sandworm Gamaredon Turla Sednit

# Summary of Russia-aligned APT group activity

Over the last six months, ESET researchers have consistently monitored the operations of Russia-aligned APT groups, primarily directing their activities towards Ukraine and countries within the European Union.

Russia-aligned threat actors predominantly relied on spearphishing emails against a variety of verticals for initial access. In a campaign we investigated, emails sent to targets contained either malicious links or malicious attachments. When successful, these were ultimately used to harvest credentials from the targets or directly install malicious payloads onto their systems.

## Spearphishing as initial access

Since the end of February 2024, we observed a wave of spearphishing emails targeting European governmental entities and attempting to exploit the CVE-2024-21413 vulnerability in Outlook, aka the Moniker Link bug.

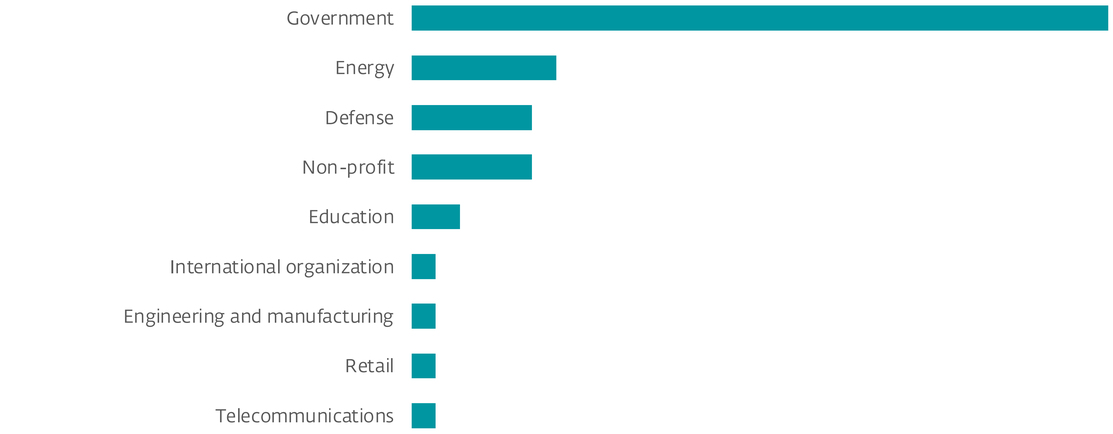
Figure 3 shows an example of one of these emails, using the European Council calendar as a lure. Note that the sender email address and the email's signature impersonate a real person who works as a press officer for the Council.

Examining the victimology of the incidents, it becomes evident that the pattern of targeting aligns with the modus operandi commonly associated with Sednit.

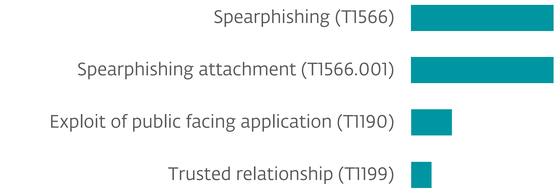
### Callisto

In December 2023, the UK government publicly attributed Callisto to the FSB's 18th Center for Information Security of the Russian Federation, establishing a strong link between the group and the Russian government.

In February 2024, an article was published by The Record, in which they explain how Callisto targeted Keir Giles, a well-known researcher and fellow at the Chatham House think tank. The Callisto group primarily uses phishing emails sent from Proton Mail addresses




**Sectors targeted** by Russia-aligned APT groups




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

From Maria Daniela Lenzu <maria.daniela.lenzu@outlook.com>
To [redacted]
2/25/2024, 9:55 PM
Subject **Meeting calendar - Consilium**

Hi!

The schedule of upcoming European Council events has been published.
Official Council meetings are organised by the Council of the EU and chaired by the Council presidency.
Check out the upcoming events and we will be glad if you take part in them, all detailed information is in the description of the events

https://www.consilium.europa.eu/en/meetings/calendar/?daterange=future

Best Regards,
**Maria Daniela Lenzu**

*Foreign Affairs, Security & Defence Issues*
*Rue de la Loi/Wetstraat 175*
*B-1048 Bruxelles/Brussel*
*Belgique/Belgie*
*Tel: +32 470 88 04 02*
*Email: maria-daniela.lenzu@consilium.europa.eu*

**Figure 3.** Body of a phishing email using the European Council calendar as a lure

```
On <redacted> James Sherr <jamessherr77@protonmail[.]com> wrote:
Dear [redacted],
I hope you're well. Please find attached a private paper concerning
Russian sanctions. The doc is password protected (below).

Just thought you might enjoy this.

Sincerely,
James

Bruce W. McConnell
Distinguished Fellow and Board Member
The Stimson Center <http://www.stimson.org/
+359.0217

<Attachments: Russian sanctions.pdf
------- Original Message -------
On <redacted>, Sherwood, Jacob<jwcompany@protonmail.com[.]com> wrote:
Subject: Jacob Sherwood has shared "Russian sanctions.pdf" with you

Dear All,
Please find attached private report which I mentioned earlier. Usual
password - <redacted>
Best,
JW
```

**Figure 4.** Callisto phishing email

and attaches a blurred PDF to entice the target to log into a fake webmail page. We have detected similar phishing emails: see Figure 4.

Note that the attackers tried to convince the victim that they were replying to an existing email, while both were actually created by the attackers. In this case, Callisto impersonated **James Sherr**, a fellow at Chatham House and specialist in Soviet and Russian military matters. Note that he was **sanctioned** by the Russian government in February 2024.

## Cyberespionage operation against European governments

In 2023, we detected two previously unknown backdoors that we call LunarWeb and LunarMail. They were used in compromises of a European ministry of foreign affairs and its diplomatic missions abroad.

Both backdoors share a loader that uses the DNS domain name for decryption of the payload, have code overlaps, and support similar commands, but differ in C&C communication methods. LunarWeb, deployed on servers, uses HTTP(S) and attempts to blend in by mimicking the traffic of legitimate services such as Windows Update. LunarMail, deployed on workstations, piggybacks on Outlook and communicates via email messages. The backdoors hide commands and data in images and documents and both have the unusual capability of being able to execute Lua scripts.

We believe with high confidence the backdoors have been used for years – since at least 2020 and possibly earlier. Based on similarities with past activity, we attribute the compromises to Turla with medium confidence.

## Russia-Ukraine war

### Gamaredon

Gamaredon remains the most active APT group operating in Ukraine, with thousands of daily detections, as illustrated in Figure 5 below. It uses spearphishing emails as one of its initial access vectors. The emails contain an XHTML file attachment that utilizes **HTML smuggling** to deliver a ZIP archive containing an HTA file. This HTA file then downloads another HTA file that contains a VBScript downloader that can deliver various payloads.

During this period, we discovered a new version of commonly used downloaders written in PowerShell that we call PteroPSLoad. This time PteroPSLoad has been using the Cloudflare Tunnel client and ngrok utility in order to communicate with its C&C servers.


**Figure 5.** Gamaredon tool detection statistics

### Sandworm

In December 2023, Kyivstar, a major telecommunications operator in Ukraine, **disclosed** that it had fallen victim to a cyberattack. The same month, the pro-Russian Telegram channel @solntsepekZ, which has been used to amplify Sandworm's attacks, claimed that Sandworm is responsible for the cyberattack against Kyivstar.

In January 2024, we detected Sandworm activity directed against a regional power supply company in Ukraine.

In March 2024, the same Telegram channel announced a cyberattack against four small internet providers in Ukraine. SentinelLabs analyzed **AcidPour**, a Linux wiper, which might have been used in this cyberattack.

Note that in addition to Sandworm, we have detected the group UAC-0099 targeting energy companies in Ukraine in the last few months. This, along with the ongoing physical destruction of Ukrainian energy infrastructure with missile barrages, underscores the energy vertical as one of the primary targets for Russia.

### Operation Texonto

In February 2024, we published a **blogpost** about a disinformation and psychological operation (PSYOP) campaign we named Operation Texonto. This campaign is trying to raise doubts in the minds of Ukrainians and Ukrainian speakers abroad. Attackers primarily use emails as the main distribution method for their PSYOP messages.

In March 2024, we observed new Operation Texonto activity directed against various individuals in Russia, most likely Russian dissidents. Attackers were trying to impersonate **Alexey Navalny**'s team in order to disorganize the **noon voting protest** of Navalny's supporters during Russia's 2024 presidential election.

Привет, это команда Навального!

Мы запустили акцию Полдень против Путина.

Алексея больше нет с нами, но в его стиле всегда было переиграть эту власть. Власть уже тратит огромные ресурсы, чтобы противодействовать вашему приходу на участки 17 марта в 12:00.

Из-за этого акция переносится на конец дня!

Наша цель - сделать всё, чтобы международное сообщество не признало эти выборы. В условиях манипуляций и пропаганды единственный законный способ показать нашу силу - прийти на участки 17 марта в 17:00! Мы должны создать такие очереди, чтобы многие не успели проголосовать, и УИК не смог закрыться в 20:00. Не спешите расходиться! Инструкции о дальнейших действиях после закрытия будут отправлены 17 марта! Ждите!

Давайте вместе переиграем их!

Теперь у нашей акции есть бот!

https://t[.]me/protiv_new_12_bot

Проходите по ссылке и сообщайте, куда придете голосовать всей семьей!

Через бот вы получите дальнейший план действий. Все анонимно и защищено.

Нас много и правда на нашей стороне!

**Figure 6.** Email body (original version in Russian)

Hello, this is Navalny's team!

We launched the Noon campaign against Putin.

Alexey is no longer with us, but his style has always been to outplay this power. The authorities are already spending enormous resources to counteract your arrival at the polling stations on March 17 at 12:00.

Because of this, the campaign is postponed until the end of the day!

Our goal is to do everything to prevent the international community from recognizing these elections. In the conditions of manipulation and propaganda, the only legal way to show our strength is to come to the polling stations on March 17 at 17:00! We must create such queues that many will not have time to vote, and the PEC will not be able to close at 20:00. Don't rush to leave! Instructions for further actions after closure will be sent on March 17th! Wait!

Let's beat them together!

Now our campaign has a bot!

https://t[.]me/protiv_new_12_bot

Follow the link and let us know where you will come to vote with your whole family!

Through the bot you will receive a further action plan. Everything is anonymous and protected.

There are many of us and the truth is on our side!

**Figure 7.** Email body (machine translation from Russian to English)

The email was sent from `info@information2024[.]com` with text trying to convince people to go vote at 17:00 instead of noon. The email content is provided in Figure 6 (and see Figure 7 for the English translation).

In April 2024, we detected a new Texonto PSYOP spam wave directed against people living in the Kharkiv region of Ukraine. The email content is provided in Figure 8 (and see Figure 9 for the English translation).

У зв'язку з можливим оточенням російськими військами Харкова, переконливо просимо вас в термін до 15 квітня 2024 року тимчасово покинути місто. Можливі маршрути евакуації додаються у вкладенні до даного повідомлення.

**Figure 8.** Email body (original version in Ukrainian)

In connection with the possible encirclement of Kharkiv by Russian troops, we strongly ask you to temporarily leave the city by April 15, 2024. Possible evacuation routes are attached to this message.

**Figure 9.** Email body (machine translation from Ukrainian to English)

# Other

SturgeonPhisher Unlucky Kamran Winter Vivern

# Other notable APT activities

In this section, we review notable activities from groups with as yet unknown alignments.

ESET researchers also track campaigns from lesser-known groups. In this section, we highlight a recent SturgeonPhisher campaign in the Middle East, a watering-hole attack on a regional news website that delivers news about Gilgit-Baltistan (a disputed region administered by Pakistan), and the exploitation of a zero-day vulnerability in Roundcube by Winter Vivern.

## SturgeonPhisher

SturgeonPhisher (also known as YoroTrooper) is a cyberespionage group that we believe is aligned with the interests of Kazakhstan. The group mainly targets governments in Central Asia, but campaigns in recent months suggest that they are also tasked with intelligence gathering operations worldwide.

In particular, we noticed that in November 2023, a month after the start of the armed conflict between Israel and Hamas, SturgeonPhisher created phishing websites targeting ministries of foreign affairs in Iran and Yemen. It is the first time that we have noticed any Middle Eastern countries to be of interest to the group.

Figure 10 shows an **Axigen WebMail** phishing page hosted at `mail.mofa.middleast-gov[.]com`.

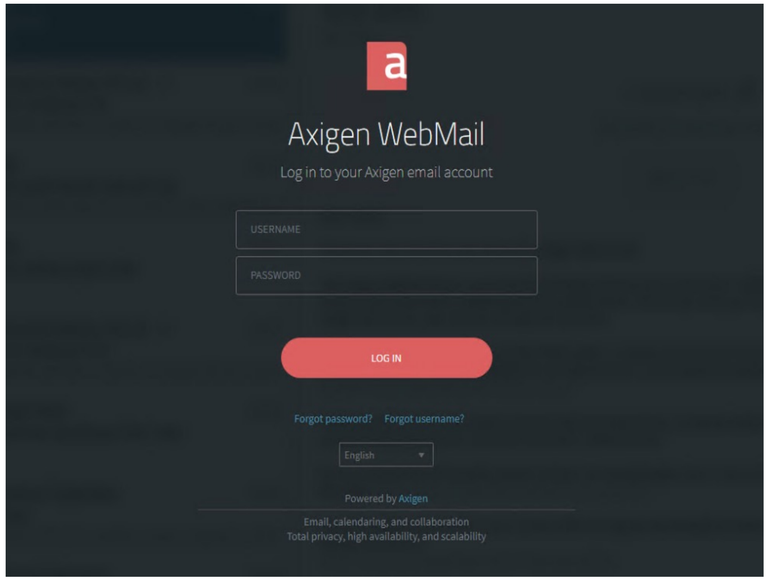



**Figure 10.** Axigen WebMail phishing page

We believe that a spearphishing email, with a link to the fake webmail page, was sent to the targets leading them to believe that they need to authenticate to view a document. After the victim is enticed into submitting credentials, a PDF is displayed (see Figure 11). This document is about alleged crimes during Israel's occupancy of Palestine.

## Unlucky Kamran

In activity reported in November 2023, **ESET researchers** have identified a watering-hole attack on a regional news website that delivers news about Gilgit-Baltistan, a disputed region administered by Pakistan. When opened on a mobile device, the Urdu version of the Hunza News website offers


الخارجية والمغتربين//

جرائم الاحتلال تستهتر بحياة المدنيين الفلسطينيين وبالمطالبات الدولية والأمريكية لحمايتهم

تدين وزارة الخارجية والمغتربين بأشد العبارات انتهاكات وجرائم قوات الاحتلال وميليشيات المستوطنين ضد شعبنا في عموم الضفة الغربية المحتلة بما فيها القدس الشرقية، بما في ذلك التصعيد الحاصل في الاجتياحات والاقتحامات شبه اليومية التي تخلف المزيد من الشهداء والجرحى وعمليات التجريف والتخريب المتعمدة للبنية التحتية في المناطق الفلسطينية خاصة في المخيمات، كما حصل مؤخرا في مخيمات طولكرم وبلاطة وعقبة جبر وبلدة عزون شرق قلقيلية وغيرها، كما تدين الوزارة بشدة اقتحام قوات احتلال مستشفى ثابت ثابت بمدينة طولكرم وانتهاك حرمة سيارة الإسعاف واعتقال مصاب من داخلها في انتهاك صارخ للقانون الدولي والقانون الإنساني الدولي.

تنظر الوزارة بخطورة بالغة لهذه الانتهاكات المتواصلة وتعتبرها محاولات إسرائيلية مستمرة لتسخين الاوضاع في الضفة الغربية المحتلة على طريق تفجيرها وخلق حالة من العنف والفوضى كبيئة مواتية لتمرير المزيد من المشاريع الاستيطانية والاستعمارية العنصرية على حساب ارض دولة فلسطين والوجود الفلسطيني فيها، في استهتار إسرائيلي رسمي بحياة المدنيين الفلسطينيين وبالمطالبات الامريكية والدولية لحمايتهم.

تطالب الوزارة بتدخل دولي حقيقي يجبر دولة الاحتلال على وقف تصعيد عدوانها ضد شعبنا في قطاع غزة والضفة الغربية المحتلة.

22/11/2023

@MOFA.PNA @PMOFA PALESTINE.MOFA @PMOFA PMOFA

**Figure 11.** `Palestine_MOFA.pdf`

readers the possibility to download the Hunza News Android app directly from the website, but the app has malicious espionage capabilities.

The developer certificate of the malicious app was issued on January 10, 2023 and the app appeared on the website sometime between January 7 and March 21 that year. During that time, protests were being held in Gilgit-Baltistan for various reasons encompassing land rights, taxation concerns, prolonged power outages, and a decline in subsidized wheat provisions. The region, shown in the map in Figure 12, is under Pakistan's administrative governance, consisting of the northern portion of the larger Kashmir region, which has been the subject of a dispute between India and Pakistan since 1947, and between India and China since 1959.

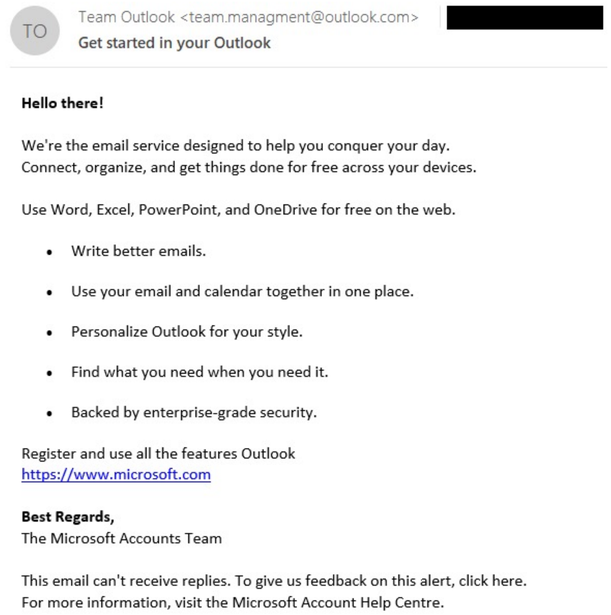
The Kamran spyware automatically gathers sensitive user data, including SMS messages, the contacts list, call logs, calendar events, device location, list of installed applications, and images.

**Figure 12.** Gilgit-Baltistan region

## Winter Vivern

In October 2023, **ESET researchers discovered** a zero-day vulnerability used in the wild by Winter Vivern, a cyberespionage group that we believe is aligned with the interests of Belarus.

Exploitation of the XSS vulnerability, assigned CVE-2023-5631, can be done remotely by sending a specially crafted email message. In this Winter Vivern campaign, the emails were sent from `team.managment@outlook[.]com` and had the subject `Get started in your Outlook`.



TO Team Outlook <team.managment@outlook.com> [redacted]

**Get started in your Outlook**

**Hello there!**

We're the email service designed to help you conquer your day.
Connect, organize, and get things done for free across your devices.

Use Word, Excel, PowerPoint, and OneDrive for free on the web.

- Write better emails.
- Use your email and calendar together in one place.
- Personalize Outlook for your style.
- Find what you need when you need it.
- Backed by enterprise-grade security.

Register and use all the features Outlook
https://www.microsoft.com

**Best Regards,**
The Microsoft Accounts Team

This email can't receive replies. To give us feedback on this alert, click here.
For more information, visit the Microsoft Account Help Centre.

**Figure 13.** Email sample exploiting CVE-2023-5631

# 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**

Digital Security
**Progress. Protected.**



(eset):research