Digital Security
Progress. Protected.

APT Activity Report

ABUSING CLOUD SERVICES AND VPN PLATFORMS IN THE PURSUIT OF NEW PREY

April 2024 – September 2024

(eset):research

Contents

Executive summary

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

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

During the monitored period, we observed a notable expansion in targeting by China-aligned MirrorFace. Typically focused on Japanese entities, it extended its operations to include a diplomatic organization in the European Union (EU) for the first time while continuing to prioritize its Japanese targets. Additionally, China-aligned APT groups have been relying increasingly on the open-source and multiplatform SoftEther VPN to maintain access to victims' networks. We detected extensive use of SoftEther VPN by Flax Typhoon, observed Webworm switching from its full-featured backdoor to using the SoftEther VPN Bridge on machines of governmental organizations in the EU, and noticed GALLIUM deploying SoftEther VPN servers at telecommunications operators in Africa.

We also observed indications that Iran-aligned groups might be leveraging their cybercapabilities to support diplomatic espionage and, potentially, kinetic operations. These groups compromised several financial services firms in Africa – a continent geopolitically important to Iran; conducted cyberespionage against Iraq and Azerbaijan, neighboring countries with which Iran has complex relationships; and increased their interest in the transportation sector in Israel. Despite this seemingly narrow geographical targeting, Iran-aligned groups maintained a global focus, also pursuing diplomatic envoys in France and educational organizations in the United States.

North Korea-aligned threat actors persisted in advancing the goals of their regime, which has been accused by the United Nations and South Korea of stealing funds – both traditional currencies and cryptocurrencies – to support its weapons of mass destruction programs. These groups continued their attacks on defense and aerospace companies in Europe and the US, as well as targeting cryptocurrency developers, think tanks, and NGOs. One such group, Kimsuky, began abusing Microsoft Management Console files, which are typically used by system administrators but can execute any Windows command. Additionally, several North Korea-aligned groups frequently misused popular cloud-based services, including Google Drive, Microsoft OneDrive, Dropbox, Yandex Disk, pCloud, GitHub, and Bitbucket. For the first time, we saw an APT group – specifically ScarCruft – abusing Zoho cloud services.

We detected Russia-aligned cyberespionage groups frequently targeting webmail servers such as Roundcube and Zimbra, usually with spearphishing emails that trigger known XSS vulnerabilities. Besides Sednit targeting governmental, academic, and defense-related entities worldwide, we identified another Russia-aligned group, which we named GreenCube, stealing email messages via XSS vulnerabilities in Roundcube. Other Russia-aligned groups continued to focus on Ukraine, with

Gamaredon deploying large spearphishing campaigns while reworking its tools using and abusing the Telegram and Signal messaging apps. Sandworm utilized its new Windows backdoor, which we named WrongSens, and its advanced Linux malware: LOADGRIP and BIASBOAT. Additionally, we detected Operation Texonto, a disinformation and psychological operation primarily aimed at demoralizing Ukrainians, also targeting Russian dissidents. We also analyzed the public hack-and-leak of the Polish Anti-Doping Agency, which we believe was compromised by an initial access broker who then shared access with the Belarus-aligned FrostyNeighbor APT group, the entity behind cyber-enabled disinformation campaigns critical of the North Atlantic Alliance. Finally, from analyzing an exploit found in the wild, we discovered a remote code execution vulnerability in WPS Office for Windows. We attribute the attack leveraging the exploit to the South Korea-aligned APT-C-60 group.

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**.

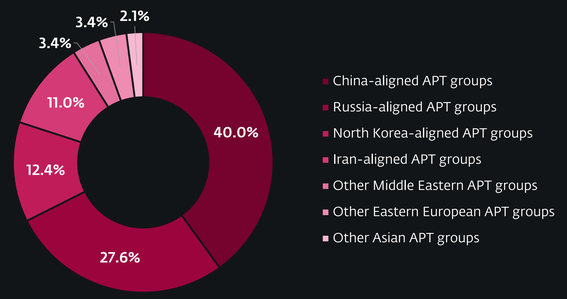
Attackers and targets

In Asia, we observed that campaigns continued to focus primarily on governmental organizations. However, we also noticed an increased emphasis on the education sector, particularly targeting researchers and academics focused on the Korean peninsula and Southeast Asia. This shift was driven by threat actors aligned with China's and North Korea's interests. Lazarus, one of the North Korea-aligned groups, continued to attack entities around the globe in the financial and technology sectors, where the adoption of cryptocurrencies has blurred the lines between the two industries. Additionally, China-aligned MirrorFace continued to target primarily governmental and political entities in Japan.

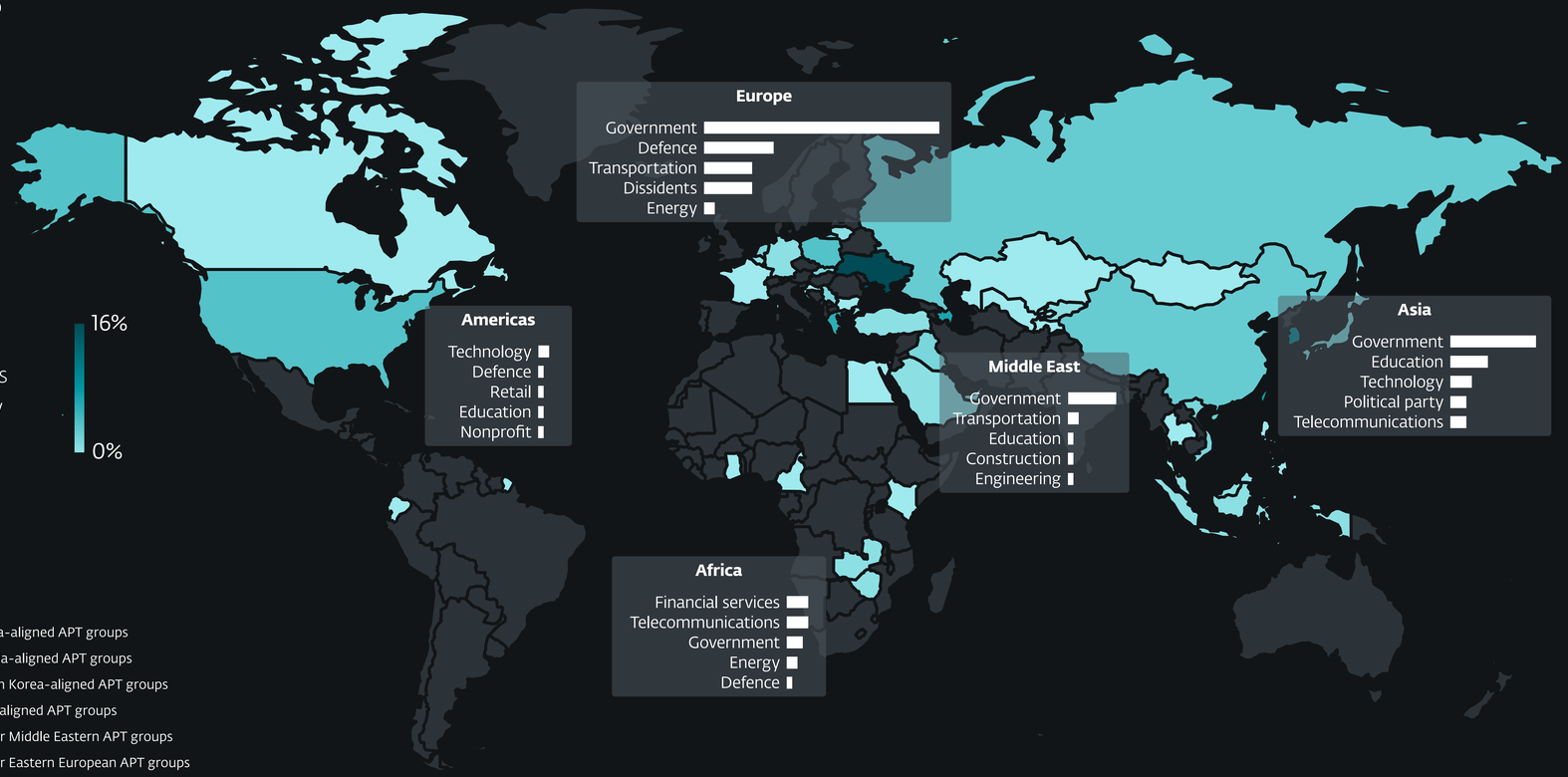
In the Middle East, several Iran-aligned APT groups continued to attack governmental organizations, with Israel being the most affected country.

Over the past two decades, Africa has become a significant geopolitical partner for China, and we have seen China-aligned groups expand their activities on that continent. Reflecting Iran's growing interest in Africa, we also detected that the MuddyWater APT group targeted financial institutions in several countries there.

For the first time, we observed MirrorFace targeting a diplomatic organization within the EU, which remains a focal point for several threat actors aligned with China, North Korea, and Russia, that focus on governmental entities and the defense sector. In Ukraine, Russia-aligned groups continued to be the most active, heavily impacting governmental entities, the defense sector, and essential services such as energy, water, and heat supply.



Attack sources



Targeted countries and sectors

China

Mustang Panda | MirrorFace | CloudSorcerer | GALLIUM | Webworm | Flax Typhoon

Summary of China-aligned APT group activity

As we noted in our previous APT activity report, Mustang Panda began targeting the European cargo shipping industry in early 2024. This campaign remains active, and its operations have since expanded to include targets in the Middle East and Asia. The tactics, techniques, and procedures (TTPs) remain unchanged: the group continues to deploy a Korplug loader, with initial access primarily achieved via removable media.

Our observation of Mustang Panda's heavy use of this method propelled it to the top spot in the chart of initial access techniques used by China-aligned groups, as illustrated in the graph at the bottom right.

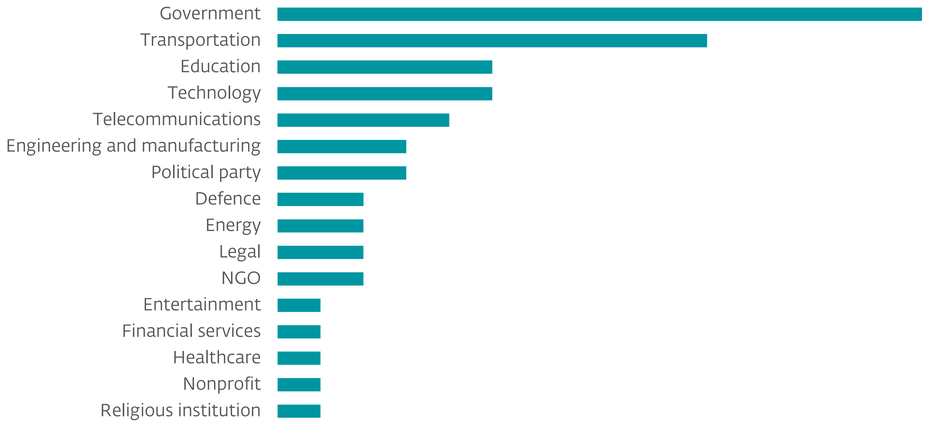
In contrast, other campaigns we've investigated revealed the exploitation of public-facing applications and spearphishing as the most commonly employed initial access techniques by China-aligned adversaries.

Since our last APT activity report, ESET researchers have noticed an increase in the use of SoftEther VPN by China-aligned APT groups, sometimes replacing the use of custom backdoors, to maintain their access to targeted organizations. For the first time, we observed MirrorFace targeting a diplomatic organization in the EU, outside the usual regional targeting in Japan. Finally, we provide additional insight into CloudSorcerer operations, which we traced back to 2022.

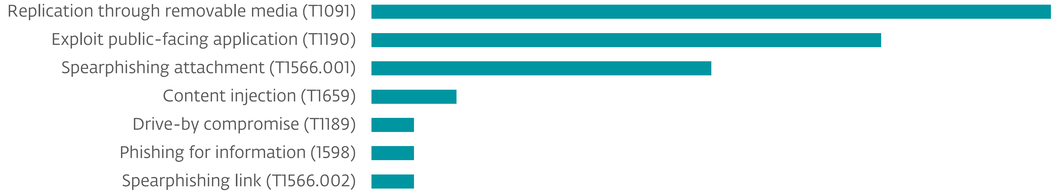
SoftEther VPN: A tool of choice for China-aligned APT groups

ESET researchers have observed several China-aligned APT groups relying more and more on **SoftEther VPN** to maintain access to their victims' networks. SoftEther VPN is open-source multiplatform VPN software that can use HTTPS to establish a VPN tunnel, facilitating firewall bypass while blending into legitimate traffic.

Since the beginning of the year, we have observed the Webworm APT group switching from full-featured



Sectors targeted by China-aligned APT groups



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

backdoors (such as the Trochilus RAT) to the use of SoftEther VPN Bridge on compromised machines of several governmental organizations in the EU. Such a VPN bridge allows the attacker to establish direct communication between the attacker-controlled infrastructure and the victim's local network, bypassing port filtering and accessing resources that might be blocked on the external router or firewall of the targeted organization.

Among the other China-aligned groups that we have observed making regular use of SoftEther VPN, we have seen GALLIUM deploying SoftEther VPN servers (instead of bridges) against several compromised telecommunications operators in Africa along with its usual toolset. Flax Typhoon, which we mentioned in our previous APT activity report, continues to make extensive use of SoftEther VPN by deploying SoftEther Bridge on compromised machines and maintaining an infrastructure of SoftEther servers. Note that we also observed MirrorFace making use of SoftEther VPN at the end of 2023.

MirrorFace expands its reach: Europe now in the crosshairs

In our **APT Activity Report Q2 2023–Q3 2023**, we documented continued MirrorFace (aka Earth Kasha) activity exclusively targeted toward Japanese entities. In a new development, this summer our team discovered that MirrorFace compromised a diplomatic organization in the EU. During this attack, the threat actor used as a lure the upcoming World Expo, which will be held in 2025 in Osaka, Japan. This shows that even considering this new geographic targeting, MirrorFace remains focused on Japan and events related to it. This is the first time we have detected MirrorFace targeting a European entity. Note that this January Trend Micro **reported on MirrorFace** targeting organizations in Taiwan and India.

In this attack, MirrorFace sent the victim a spearphishing email containing a link to a ZIP archive named `The EXPO Exhibition in Japan in 2025.zip` hosted on OneDrive and containing a single LNK file named `The EXPO Exhibition in Japan in 2025.docx.lnk`, masquerading as a Word document. Upon opening, the LNK file displays a decoy Word document, shown in Figure 1, ultimately leading to the deployment of version 5.5.5 of the ANEL backdoor. ANEL disappeared from the scene around the end of 2018 or the start of 2019, and it was believed that LODEINFO had succeeded it, appearing later in 2019. Therefore, it is interesting to see ANEL resurfacing after almost five years. The next day, the attackers deployed their flagship backdoor HiddenFace (aka NOOPDOOR), which we **documented at JSAC 2024**.

In the meantime, MirrorFace operations against its usual targets didn't stop. We continued to see the threat actor targeting various Japanese organizations, such as a research institute and a political party. In all instances the threat actor tried to deploy HiddenFace along with other implants.

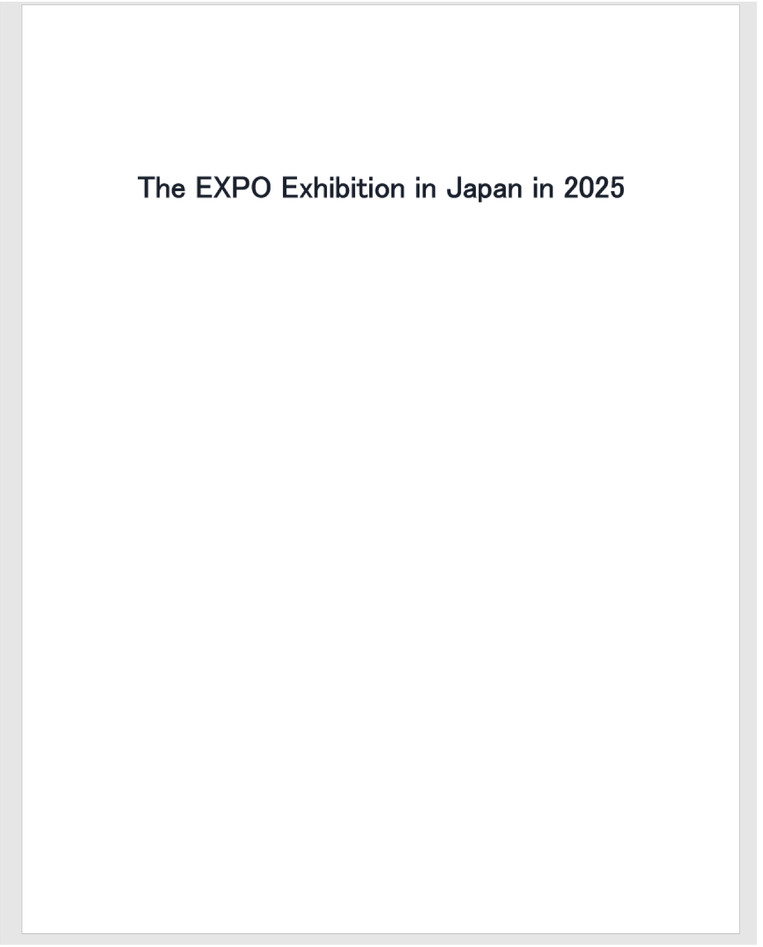


Figure 1. Malicious Word document used to deploy ANEL

CloudSorcerer's operations traced back to 2022

In July 2024, Kaspersky researchers published an **article** about CloudSorcerer, a new threat actor they observed targeting Russian government entities back in May 2024. Proofpoint **mentioned** on Twitter (now known as X) that a nonprofit organization in the US was targeted using similar TTPs. Lastly, in August 2024, Kaspersky released another **article** about the group, digging deeper into its modus operandi.

While some coverage has been done by our peers, we would like to add more information found during our own investigation of this threat actor.

In February and July 2024, two CloudSorcerer samples were uploaded to VirusTotal with PE timestamps of 2022-05-23 09:36:17 and 2022-03-28 02:56:17, respectively. ESET researchers believe with high confidence that these dates were not tampered with and establish the activity of the group back to at least early 2022.

Additionally, ESET researchers discovered a CloudSorcerer compromise chain similar to the one described by Proofpoint, whose decoy document, shown in Figure 2, suggests that the target is an individual in Ecuador.

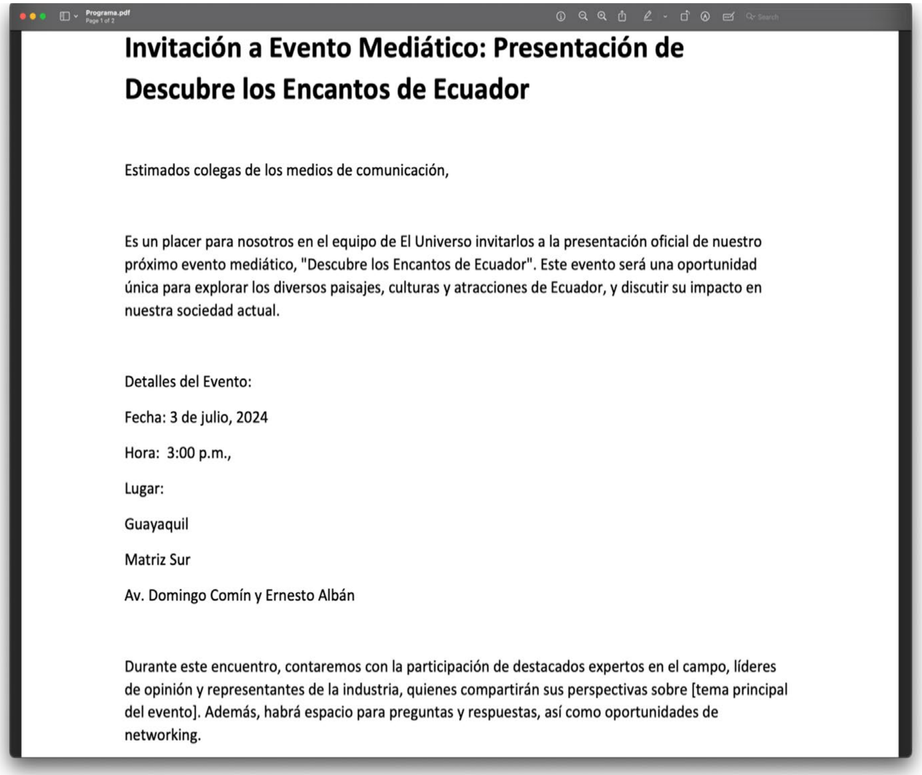


Figure 2. CloudSorcerer's decoy PDF document

Iran

MuddyWater BladedFeline Ballistic Bobcat

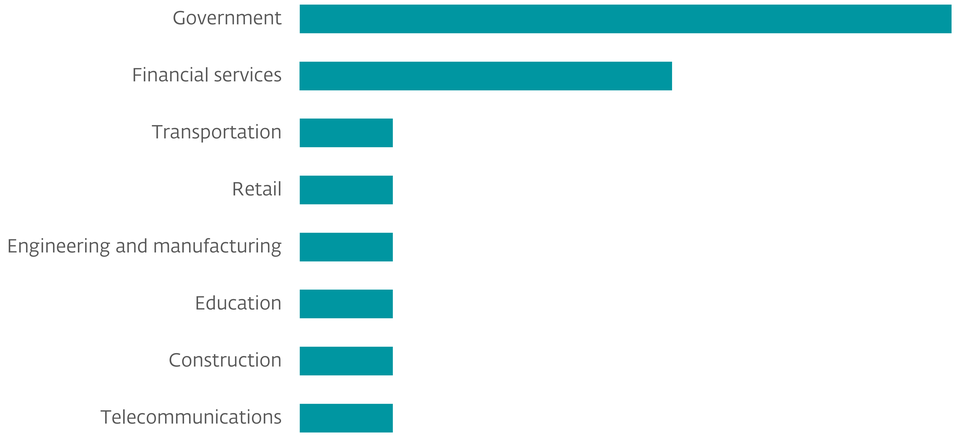
Summary of Iran-aligned APT group activity

Iran-aligned MuddyWater has spent considerable time moving laterally and performing hands-on-keyboard activities in several targeted environments, which marks an interesting departure from its typical TTPs that are generally focused on either credential theft or maintaining access to a specific system. In several instances, we have observed MuddyWater using internal network shares as intermediate C&C staging locations. MuddyWater operators are, often via command line access to systems, gathering reconnaissance info and dumping credentials to centralized network locations before exfiltrating that data from a single source. In one notable instance, MuddyWater operators spent 13 hours using various tools (e.g., MirrorDump, ProcDump, PowerSploit, and Impersonate) to attempt dumping LSASS process memory but without any apparent success. This shift to lateral movement likely indicates a better understanding of network defense capabilities and a maturing offensive cybercapability.

From cyber-support to diplomatic and kinetic operations

Examining the victimology of the network in which MuddyWater has been focused, we observed indications that Iran-aligned groups, and MuddyWater specifically, may be in the process of using their cybercapabilities to support diplomatic and kinetic operations. Iran has made no secret of the fact that its interests in Africa and the continent's natural resources are key components of its international policies. To that end, Iran-aligned groups spent significant time gaining access to, and moving laterally in, several financial services firms in Kenya and Zambia, and an unidentified victim in Ghana.

As for support or preparation for kinetic action, we have observed potential indicators that some Iran-aligned groups may be gathering information to support military activities. A transportation company



Sectors targeted by Iran-aligned APT groups

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

in Israel was targeted by MuddyWater, with many hours spent deploying various tools within the organization. Operators spent time moving laterally, using internal network shares, and gathering credentials and other information for exfiltration. Such activity, while not uncommon for many groups, is somewhat unusual for MuddyWater, indicating an increased interest in the transportation vertical. In light of the current tensions and conflicts in the Middle East, it makes sense that Iran-aligned groups would look to target critical industries like transportation.

Continued interest in being the intrusive neighbor

Separately, OilRig subgroup BladedFeline conducted cyberespionage against Iran's neighbors, with a high rate of malware development and deployment. Regional and national governmental organizations in Iraq, and diplomatic envoys from Iraq to various countries, have been the victims of multiple iterations of these custom backdoors: Whisper, Spearal, and Optimizer. BladedFeline has invested heavily in gathering diplomatic and financial information from Iraqi organizations, indicating that Iraq plays a large part in the strategic objectives of the Iranian government. Additionally, governmental organizations in Azerbaijan have been another focus of BladedFeline. Azerbaijan has a long history of abuse from Iran and is an important neighbor to Iran culturally and logistically.

The last point of interest is that Ballistic Bobcat (also known as APT35 and overlapping with APT42) has targeted diplomatic envoys in France and educational organizations in the US. Although the victimology is not novel, it does highlight the worldwide focus of Iran-aligned groups, despite their seemingly narrow focus (although Israel always holds a special place in Iran's mind). Whereas the aforementioned MuddyWater and BladedFeline activities in Africa and Azerbaijan were somewhat less sophisticated in tooling and modus operandi, the Ballistic Bobcat activities were more so. Ballistic Bobcat attempted to circumvent security software, such as EDR, by injecting malicious code into innocuous processes and using multiple modules to evade notice. This indicates that the targets are highly valuable to Iranian interests and, when coupled with credential theft, point to a long-term plan and additional cyberincursions.

North Korea

Lazarus Kimsuky ScarCruft Citrine Sleet

Summary of North Korea-aligned APT group activity

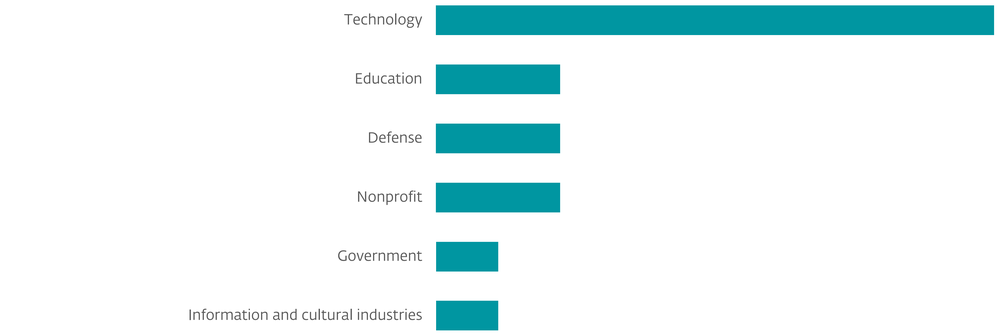
In this reporting period, we noted ongoing persistent efforts from North Korea-aligned groups to infiltrate critical sectors, gather intelligence, and exploit vulnerabilities for both financial gain and strategic advantage. Lazarus continued its espionage efforts, known as Operation DreamJob, by targeting defense and aerospace companies both in Europe and the US. Lazarus also targeted developers working with cryptocurrencies by using fake job offers and setting up a fake cryptocurrency platform. Kimsuky was also quite active in the reporting period, targeting mostly think tanks, NGOs, and North Korea experts – under the guise of requests for interview, thesis advisory, or requests for a public presentations. On the other hand, we noticed limited activities from other North Korea-aligned groups, like Konni and ScarCruft.

Abusing cloud services

One of the noteworthy trends in this period is the abuse of popular cloud-based services. Network traffic to these services is less likely to be detected as anomalous, giving attackers a small window of opportunity to stay undetected in the corporate environment.

Specifically, Kimsuky frequently abused Google Drive and Microsoft OneDrive to host decoy documents and as C&C servers. For data exfiltration, Kimsuky used Dropbox accounts. Interestingly, ScarCruft uses various cloud services for its backdoors. We detected RokRAT instances using Yandex Disk and pCloud as C&C servers, and BirdCall – a publicly undocumented backdoor – abusing Zoho WorkDrive and pCloud. This is the first time we have seen Zoho cloud services being abused by an APT group.

We also saw abuse of code and package repositories for deploying initial malware masked as coding projects and hiring challenges. We observed Lazarus using GitHub and Bitbucket to share trojanized projects with its victims. We also observed a subgroup of Lazarus,



Sectors targeted by North Korea-aligned APT groups

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

which we named Moonstone, uploading trojanized packages to the npm registry with a similar goal.

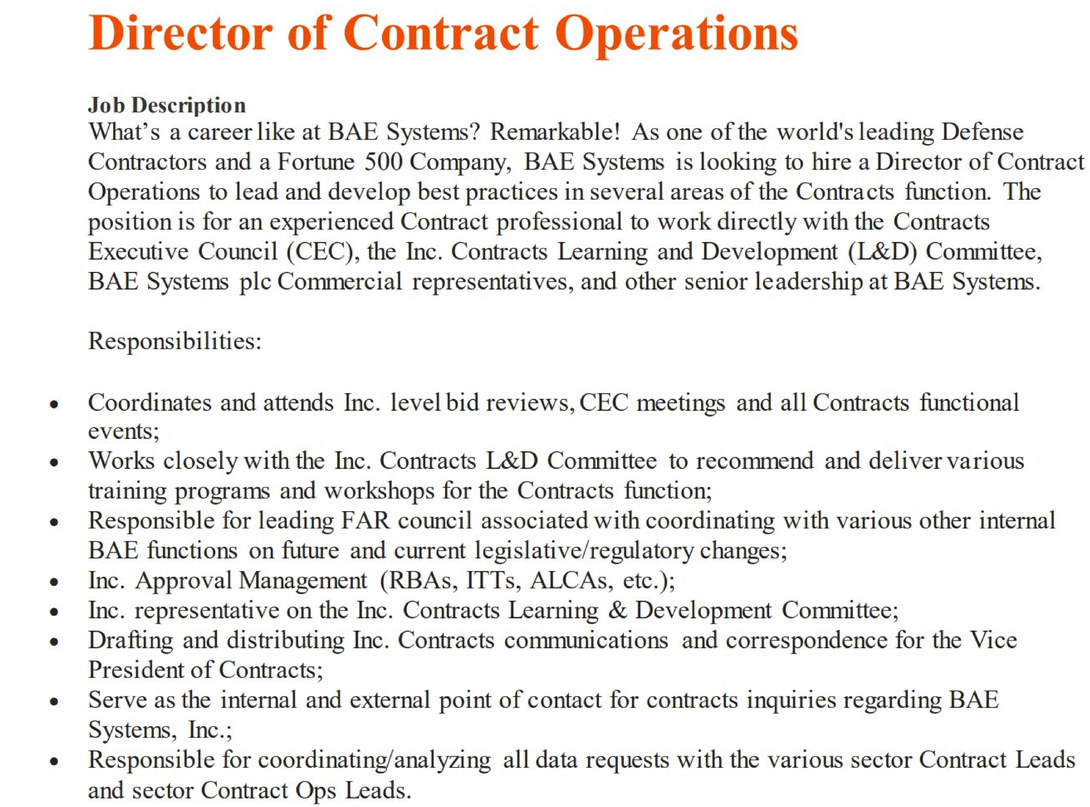
We are pleased to be able to report that most service providers are reacting quickly and promptly terminate the abused accounts.

Building relationships before the attack

Another distinctive feature of many attacks that we attribute to North Korea-aligned groups is the gradual building up of the relationship with the victim. Both Lazarus and Kimsuky used fake job offers to approach the targeted individuals. Only after the victim responds and a relationship is established, is a malicious package sent to the victim.

For example, we observed Lazarus's Operation DreamJob cluster focus on defense contractors and media companies in Europe and Asia. It used fake job offers for desirable positions at large companies (like Airbus or BAE Systems) and delivered trojanized PDF viewers along with decoy PDF documents, as well as many new malicious tools. Figure 3 shows an example of such a decoy PDF.

We also identified a new cluster of Lazarus activity that we've named DeceptiveDevelopment, targeting freelance developers around the world with the aim of cryptocurrency theft. To this end, the attackers impersonated recruiters on professional networks and work platforms, distributing trojanized codebases under the guise of job assignments and hiring challenges, or distributing trojanized remote conferencing tools. They focused heavily on the theft of cryptocurrency wallets and stored login information using simple, yet effective, multiplatform malware named BeaverTail and InvisibleFerret.



Director of Contract Operations

Job Description
What's a career like at BAE Systems? Remarkable! As one of the world's leading Defense Contractors and a Fortune 500 Company, BAE Systems is looking to hire a Director of Contract Operations to lead and develop best practices in several areas of the Contracts function. The position is for an experienced Contract professional to work directly with the Contracts Executive Council (CEC), the Inc. Contracts Learning and Development (L&D) Committee, BAE Systems plc Commercial representatives, and other senior leadership at BAE Systems.

Responsibilities:

- Coordinates and attends Inc. level bid reviews, CEC meetings and all Contracts functional events;
- Works closely with the Inc. Contracts L&D Committee to recommend and deliver various training programs and workshops for the Contracts function;
- Responsible for leading FAR council associated with coordinating with various other internal BAE functions on future and current legislative/regulatory changes;
- Inc. Approval Management (RBAs, ITTs, ALCAs, etc.);
- Inc. representative on the Inc. Contracts Learning & Development Committee;
- Drafting and distributing Inc. Contracts communications and correspondence for the Vice President of Contracts;
- Serve as the internal and external point of contact for contracts inquiries regarding BAE Systems, Inc.;
- Responsible for coordinating/analyzing all data requests with the various sector Contract Leads and sector Contract Ops Leads.

Figure 3. A decoy job offer document discovered in an attack at a defense contractor in Poland

Speaking of cryptocurrency theft, we also observed the Citrine Sleet threat actor setting up a fake cryptocurrency trading and investment platform in order to distribute a trojanized cryptocurrency trading app to compromise its victims and steal cryptocurrency. We assume the victims were lured via social networks and targeted communications by the attacker pretending to advertise the platform.

Another approach used mostly by Kimsuky is a request for a media interview or giving a presentation. These attacks mostly target North Korea experts working for NGOs, and researchers in academic circles whose research is related to the Korean peninsula. We observed lure emails in both English and Korean, praising the target's expertise and asking for help. Once the relationship is established, a malicious package is delivered, usually disguised as a list of questions that should be answered before the event.

Abuse of Microsoft Management Console

One of the most interesting technical developments in the period was the abuse of Microsoft Management Console (MSC) files. MSC files are normally used by system administrators to perform tasks, like managing Windows users or system policies. However, MSC files are not limited to performing just system administration tasks – they can be used to run any Windows command. It's also possible to change the icon of an MSC file, so that it resembles a PDF or Word document – making it more likely that a victim will be successfully deceived.

The first publicly documented use of malicious MSC files was reported by Genians in May 2024. In that case, Kimsuky targeted individuals in South Korea and Japan with MSC files masquerading as essays or materials for a media interview. A certain amount of social engineering is required to persuade the victim to open the MSC file, ignore a warning message displayed by Windows, and then click on the Open link. However, the previously established relationship between the attacker and the victim makes this task easier.

Since then, we have observed multiple attacks by Kimsuky, targeting mostly Western academics and NGOs. For example, in September 2024 we detected a malicious MSC file that looks like an interview request from The Wall Street Journal (see Figure 4).

Other threat actors quickly recognized the potential of MSC files: we have observed malicious MSC files being used by China-aligned Mustang Panda, and by parties involved in the Russia–Ukraine conflict.

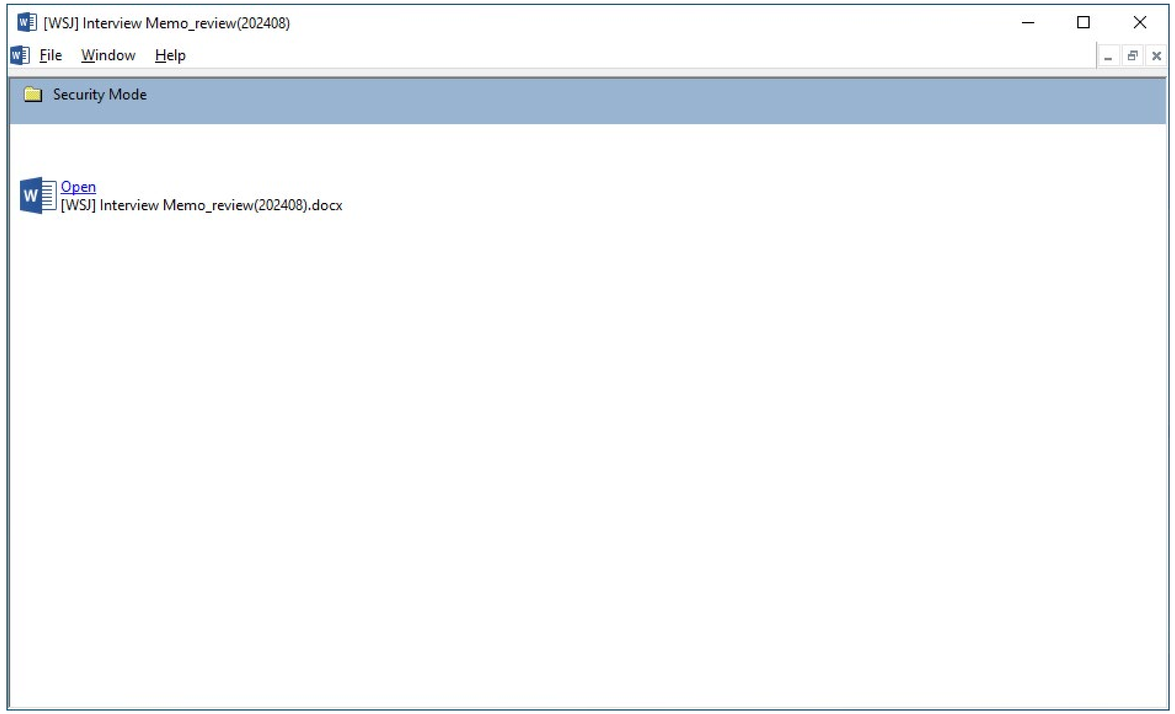


Figure 4. A malicious MSC file, from the victim's perspective

Russia

Sednit GreenCube Gamaredon Sandworm Operation Texonto

Summary of Russia-aligned APT group activity

Over the past six months, ESET researchers have analyzed campaigns led by Russia-aligned threat actors, primarily targeting Ukraine and several EU countries. These adversaries have predominantly relied on spearphishing emails to gain initial access. However, we have also observed a growing focus on exploiting webmail servers by using one-day vulnerabilities, broadening their attack surface.

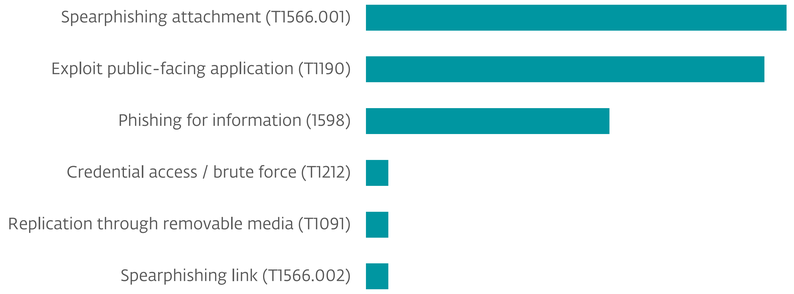
An increase in XSS spearphishing attacks against Zimbra and Roundcube

Russia-aligned cyberespionage groups have frequently targeted webmail servers such as Roundcube and Zimbra. The initial access vector for such attacks is usually a spearphishing email, which triggers a known XSS vulnerability and enables the execution of arbitrary JavaScript payloads. Those payloads can access webmail users' data; therefore the main goal is to steal emails or add persistent forwarding rules. It is very common for such webmail servers to be updated infrequently.

We discovered new Sednit spearphishing waves, which are part of the already known Operation RoundPress campaign directed against Roundcube webmail servers. In the past several months, we observed such spearphishing waves against governmental, academic, and defense-related entities in Cameroon, Cyprus, Ecuador, Indonesia, Romania, and Ukraine. Sednit used a wide range of lures, from legitimate news articles to a commercial brochure for thermal optics, as shown in Figure 5.

We identified another Russia-aligned group, which we named GreenCube, that has been active since at least 2022. This group specializes in credential-stealing spearphishing campaigns and stealing email messages via XSS vulnerabilities in Roundcube. From 2022

Sectors targeted by Russia-aligned APT groups



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

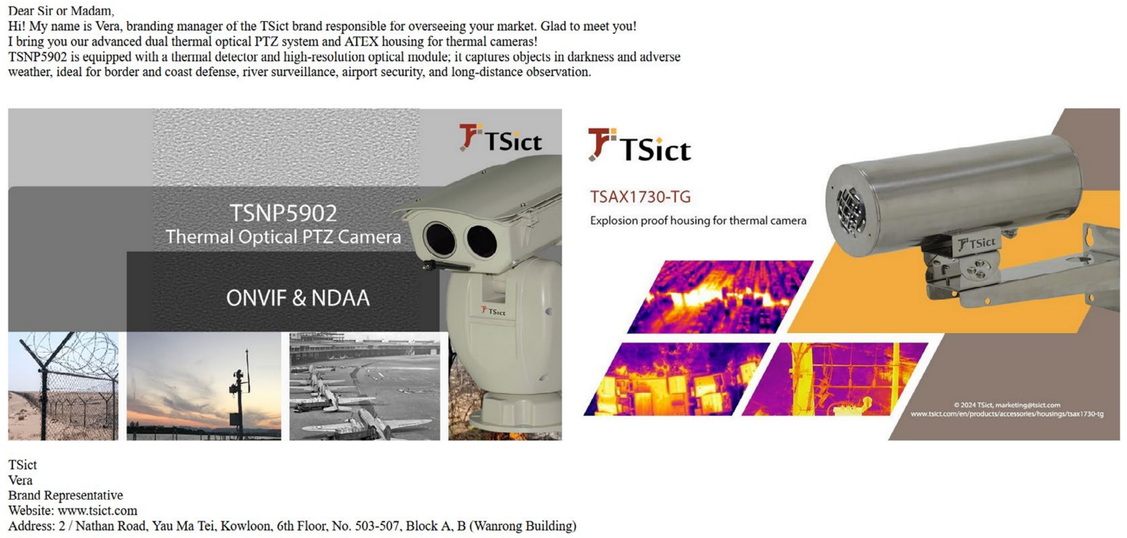


Figure 5. Decoy email, which triggers an XSS vulnerability in the background

to 2024, GreenCube has been repeatedly targeting governmental and defense-related organizations in Greece, Poland, Serbia, and Ukraine. GreenCube overlaps with a cluster tracked by CERT-UA as UAC-0102 (see this first **notification** and this second **notification**) and with a cluster tracked by Mandiant as UNC3707.

We observed four different types of payloads that GreenCube can deploy once XSS exploitation has been successful: adding a Sieve rule to forward incoming emails, stealing webmail credentials, exfiltrating account metadata, and exfiltrating email messages.

Russia-Ukraine war

Gamaredon

Gamaredon continues to be the most active APT group targeting Ukraine. Recently, we published a detailed **white paper** thoroughly describing the TTPs used by this group in 2022–2023. Most of the mentioned TTPs haven't changed significantly in 2024. For example, in the past few months, we detected a number of large spearphishing campaigns with attachments utilizing HTML smuggling – a typical initial compromise vector for Gamaredon.

During this period, Gamaredon improved already existing malicious tools and deployed new ones. Specifically, in August 2024 we discovered a new PowerShell tool, which we named PteroGraphin; it is a persistent downloader that delivers an encrypted payload via telegra.ph – the Telegram publishing platform. In addition, Gamaredon significantly reworked one of its backdoors written in PowerShell – PteroPSDoor – making it stealthier by adding multiple layers of obfuscation and hiding its parts in the Windows registry. Finally, Gamaredon improved its data exfiltration tool for **Signal's desktop application** – PteroSig. This adjustment was made **due to recent changes** in Signal Desktop. Now PteroSig is able to parse and decrypt the DPAPI-protected key used by the Signal application, allowing PteroSig to again decrypt and exfiltrate data from Signal.

In July 2024, we discovered an unusual payload deployed by Gamaredon; it merely opens a Telegram channel named Хранители Одессы (translation: Guardians of Odessa) in the default browser. This channel, which can be found at `https://t[.]me/s/hraniteli_odessi`, is full of Russian propaganda focused on the Odessa region.

Sandworm

In April 2024, CERT-UA published a **notification** about disrupted Sandworm group activity. According to the notification, Sandworm targeted about twenty organizations, including energy, water, and heat supply enterprises, in ten regions of Ukraine.

During this activity, Sandworm used a Windows backdoor, which we track under the name WrongSens (CERT-UA named it QUEUESEED). Additionally, Sandworm used custom Linux malware named LOADGRIP and BIASBOAT. After performing an in-depth analysis of LOADGRIP and BIASBOAT samples, we concluded that they are advanced Linux malware, created by developers with a good understanding of Linux internals. This malware is designed to work only on targeted machines, using their machine-specific IDs for payload decryption.

Researchers from WithSecure independently discovered and analyzed the WrongSens backdoor, which they named **Kapeka**.

Operation Texonto

In February 2024, we published a **blogpost** about a disinformation and psychological operation (PSYOP) campaign we named Operation Texonto. This campaign primarily aims to raise doubts in the minds of Ukrainians and Ukrainian speakers abroad; however, we also observed a campaign targeting Russian dissidents. Attackers primarily use email as the main distribution method for their PSYOP messages.

In September 2024, we detected an Operation Texonto email sent from `DCHC@headlineinteresting[.]pro`,

likely targeting individuals residing in the Sumy region of Ukraine. The body of the email contains the following message in Ukrainian:

> *Шановні жителі Сумської області!*
>
> *Через російські авіаудари в регіоні почалися серйозні перебої з електроенергією та водопостачанням. Води і електрики не передбачається в найближчі три тижні.*
>
> *Просимо вас в найближчі 48 годин придбати все необхідне для життя в екстрених умовах. У вкладенні - рекомендації, які допоможуть вам пережити цей складний період. Обов'язково перепишіть їх на папір.*

A machine translated version of the body is:

> *Dear residents of Sumy region!*
>
> *Due to Russian airstrikes in the region, serious interruptions in electricity and water supply began. Water and electricity are not expected in the next three weeks.*
>
> *We ask you to purchase everything necessary for life in emergency conditions in the next 48 hours. The attachment contains recommendations that will help you survive this difficult period. Be sure to write them down on paper.*

As is evident from the message, the goals of Operation Texonto appear to still be the same, trying to demoralize Ukrainians via war-related topics.

Other

FrostyNeighbor Beregini APT-C-60

Other notable APT activities

ESET researchers also tracked campaigns from lesser-known groups. In this section, we highlight a recent FrostyNeighbor campaign in Poland, a Linux toolset probably used to target an ISP in Yemen, and the exploitation of a zero-day vulnerability in WPS Office for Windows by APT-C-60.

FrostyNeighbor

FrostyNeighbor, also known as UNC1151, is a Belarus-aligned threat group that performs influence and disinformation campaigns (like the **Ghostwriter information operations**), but has also compromised a variety of governmental and private sector entities, with a focus on Ukraine, Poland, and Lithuania.

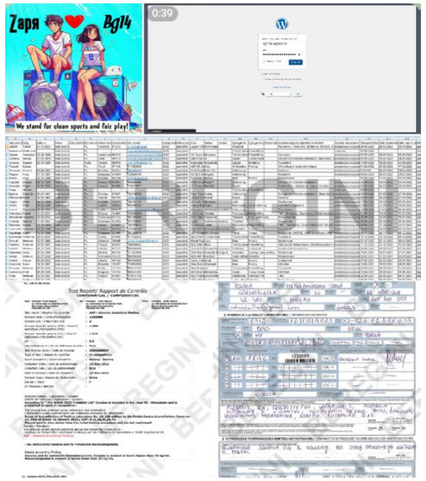
FrostyNeighbor compromised the Polish Anti-Doping Agency (POLADA), and documents were stolen in a **hack-and-leak operation** in July 2024, then made available by the Beregini hacking group via its Telegram channel `https://t[.]me/hackberegini` in August 2024. As shown in Figure 6, the post contains screenshots of stolen documents, a video showing access to the WordPress admin dashboard of the agency website (`antidoping[.]pl`), and links to download archives containing the stolen data.

Machine translation of the post:

> *Well, here we go! In the run-up to the 2024 Olympic Games, we were uninvited guests of the Polish Anti-Doping Agency (POLADA). And we liked it so much that we decided to stick around and take their entire base for a look. And according to the old tradition we give our loyal subscribers to read it.*
>
> *And so, we present to your attention the full database on Polish athletes with the results of doping tests, where the whole bouquet of banned substances, including drugs. Well, those who can and can dig deeper, will find a lot of other interesting information, which will pull on the investigation of criminal distribution of banned drugs in the EU countries, where the donkey ears of Ukrainian and Polish businessmen stick out!*
>
> *The whole database is here:*
>
> *In the archives named dump.part1.rar – dump.part8.rar there is service information from computers. Archives dump.part1.rar – dump.part4.rar can be downloaded and unpacked independently of each other. Archives dump.part5.rar – dump.part8.rar can be unpacked only after downloading all parts of the archive.*
>
> *The password for these archives is doping.*

The leaked documents contained, among other things, athletes' personal data, medical data, failed doping controls, investigations of illegal chemical laboratories, and a plethora of plaintext passwords saved within text and Microsoft Excel documents.

After analyzing the compromise chain and links found to potential compromises that were not linked with FrostyNeighbor, we think that the initial compromise was done by an initial access broker who made some opportunistic hacks and shared access with FrostyNeighbor when the victim was interesting or a high-value target. At a later stage, the Beregini group got access to the stolen documents and, in a disinformation effort, leaked them to discredit authorities.



Ну, что поехали! В преддверии Олимпийских игр 2024 мы побывали в незваных гостях у Польского антидопингового агентства (POLADA). И нам так понравилось, что мы решили подзадержаться и забрать на посмотреть всю их базу. И по старой традиции даем почитать и нашим преданным подписчикам.

И так, представляем вашему вниманию полную базу данных на польских спортсменов с результатами допинг-тестов, где весь букет запрещенных веществ, в том числе и наркотики. Ну а те, кто может и умеет копать глубже, найдут много другой интересной информации, которая потянет на расследование преступного распространения запрещенных препаратов в странах ЕС, где торчат ослиные уши украинских и польских бизнесменов!

Вся база тут:
В архивах с названием dump.part1.rar - dump.part8.rar находится служебная информация с компьютеров. Архивы dump.part1.rar - dump.part4.rar можно скачать и распаковать независимо друг от друга. Архивы dump.part5.rar - dump.part8.rar можно распаковать только после скачивания всех частей архива.
Пароль от этих архивов – doping.
Это с копьютеров
https://archive.bg14.world/dump.part1.rar
https://archive.bg14.world/dump.part2.rar
https://archive.bg14.world/dump.part3.rar
https://archive.bg14.world/dump.part4.rar
https://archive.bg14.world/dump.part5.part1.rar
https://archive.bg14.world/dump.part5.part2.rar
https://archive.bg14.world/dump.part6.part1.rar

Figure 6. Message with links, published on Telegram

Linux toolset in Yemen

On August 10, 2024, a user from Yemen uploaded to VirusTotal an archive named `files.zip`[1] that contains multiple samples of various Linux malware. Specifically, it contains modified versions of publicly available Linux tools, such as **Tiny SHell** and **Srelay**, and custom malware, such as SLAPSTICK and STEELCORGI. Additionally, we discovered several other Linux binaries uploaded from Yemen within a close time frame, leading us to believe that they are probably related to the discovered activity. It should be noted that this toolset matches that publicly described by Mandiant as part of the activity of **UNC1945** and **UNC2891**.

In addition to the listed malware families, the archive contains an obfuscated shell script named `hactrl.txt`. This shell script establishes a reverse SSH tunnel at specific times of the day. The attackers disguised the SSH private key file by using the location `/opt/VRTSvcs/bin/hacoconfig`, which suggests that **Veritas Cluster Server** is likely the targeted system.

We believe with medium confidence that a telecommunications company in Yemen was targeted. Our assessment is based on some other Yemeni users who uploaded related malicious files and also uploaded legitimate binaries belonging to software used in the telecommunications industry. Specifically, a user from Yemen who uploaded related malware samples also uploaded the file `_mh_av.txt`[2], which is a non-malicious Linux binary from **NewStart Carrier-Grade Server Linux** by Guangdong ZTE NewStart Technology Co., Ltd.

At this point, we are unable to determine the specific objectives of the threat actor, whether being a financially motivated operation or cyberespionage.

WPS Office for Windows vulnerability – APT-C-60

ESET researchers discovered a code execution vulnerability in WPS Office for Windows (**CVE-2024-7262**), as it was being exploited in the wild by APT-C-60, a South Korea-aligned cyberespionage group. WPS Office is an "Office Suite for Docs, Sheets, Slides and PDFs" and has over 500 million active users worldwide, which makes it a good target to reach a substantial number of individuals.

Upon analyzing the root cause, we subsequently discovered another way to exploit the faulty code (**CVE-2024-7263**). Following a coordinated disclosure process, we shared our findings with Kingsoft. Both vulnerabilities were silently patched around the end of May 2024.

The exploit was delivered via a malicious document[3] that is an MHTML export of the commonly used XLS spreadsheet format. However, this document contains a specially crafted and hidden hyperlink, designed to trigger the execution of an arbitrary DLL if clicked on when using the WPS Spreadsheet application. The rather unconventional MHTML file format allows a file to be downloaded as soon as the document is opened; therefore, leveraging this technique while exploiting the vulnerability provides remote code execution.

A root cause analysis of these vulnerabilities can be found on our blog **WeLiveSecurity**.

[1] SHA-256: 0012C49FAC5EAB8FF1BCB7EFAB62CB1D29E6CCEA2F272C968CA7C4BC2FE011B7
[2] SHA-256: AA6F6A50271A1D63896971C2759A619E651D94D475B504200C1A0F2E5F623EFF
[3] SHA-256: 6174276F94219BC386BDC628CA18EAEC261998B7BD03077562FE93C268B42446

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