Digital Security
Progress. Protected.

APT Activity Report

GOVERNMENT ESPIONAGE AND UNPATCHED VULNERABILITIES

April 2023 – September 2023

(eset):research

Contents

Executive summary

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

This report summarizes the activities of selected advanced persistent threat (APT) groups that were observed, investigated, and analyzed by ESET researchers from April 2023 until the end of September 2023. In the monitored timespan, we observed a notable strategy of APT groups utilizing the exploitation of known vulnerabilities to exfiltrate data from governmental entities or related organizations. Russia-aligned Sednit and Sandworm, North Korea-aligned Konni, and geographically unattributed Winter Vivern and Sturgeon Phisher seized the opportunity to exploit vulnerabilities in WinRAR (Sednit, SturgeonPhisher, and Konni), Roundcube (Sednit and Winter Vivern), Zimbra (Winter Vivern), and Outlook for Windows (Sednit) to target various governmental organizations in Ukraine, Europe, and Central Asia. Regarding China-aligned threat actors, GALLIUM probably exploited weaknesses in Microsoft Exchange servers or IIS servers, extending its targeting from telecommunications operators to government organizations around the world; MirrorFace probably exploited vulnerabilities in the Proself online storage service; and TA410 probably exploited flaws in the Adobe ColdFusion application server.

Iran- and Middle East-aligned groups continued to operate at high volume, primarily focusing on espionage and data theft from organizations in Israel. Notably, Iran-aligned MuddyWater also targeted an unidentified entity in Saudi Arabia, deploying a payload that suggests the possibility of this threat actor serving as an access development team for a more advanced group.

The prime target of Russia-aligned groups remained Ukraine, where we discovered new versions of the known wipers RoarBat and NikoWiper, and a new wiper we named SharpNikoWiper, all deployed by Sandworm. Interestingly, while other groups – such as Gamaredon, GREF, and SturgeonPhisher – target Telegram users to try to exfiltrate information or at least some Telegram-related metadata, Sandworm uses this service for active measure purposes, advertising its cyber-sabotage operations. However, Gamaredon remained the most active group in Ukraine, significantly enhancing its data-collecting capabilities by redeveloping existing tools and deploying new ones.

North Korea-aligned groups continued to focus on Japan, South Korea, and South Korea-focused entities, employing carefully crafted spearphishing emails. The most active Lazarus scheme observed was Operation DreamJob, luring targets with fake job offers for lucrative positions. This group consistently demonstrated its capability to create malware for all major desktop platforms. Finally, our researchers uncovered the operations of three previously unidentified China-aligned groups: DigitalRecyclers, repeatedly compromising a governmental organization in the EU; TheWizards, conducting adversary-in-the-middle attacks; and PerplexedGoblin, targeting another government organization in the EU.

ESET APT Activity Reports contain only a fraction of the cybersecurity intelligence data provided to customers of ESET's private APT reports. ESET researchers prepare in-depth technical reports and frequent activity summaries detailing activities of specific APT groups, in the form of ESET APT Reports PREMIUM, to help organizations tasked with protecting citizens, critical national infrastructure, and high-value assets from criminal and nation-state-directed cyberattacks. Comprehensive descriptions of activities described in this document were therefore previously provided exclusively to our premium customers. 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**.

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.

Targeted countries and verticals

TARGETED COUNTRIES AND REGIONS

- Armenia
- Bangladesh
- Central Asia
- China
- Czechia
- European Union
- French Polynesia
- Greece
- Guyana
- Hong Kong
- Israel
- Japan
- Kuwait
- Mali
- Pakistan
- Philippines
- Poland
- Saudi Arabia
- Serbia
- Slovakia
- South Korea
- Tajikistan
- Türkiye (aka Turkey)
- Ukraine
- United Arab Emirates
- United States
- Uyghurs and other Turkic ethnic minorities

TARGETED BUSINESS VERTICALS

- Gambling companies and their customers
- Governmental organizations and entities
- Hosting providers
- Industrial networks
- IT companies
- Local governments and institutions
- Media organizations
- Political entities
- Private companies
- Scholars and journalists specializing in North Korea
- Research institutes
- Telecommunication operators
- Universities

China

Mustang Panda FishMonger TA410 GREF MirrorFace GALLIUM DigitalRecyclers TheWizards PerplexedGoblin Worok

Summary of China-aligned APT group activity seen by ESET Research in April 2023 – September 2023

During the past six months, ESET researchers continued to observe several China-aligned APT groups targeting European government organizations, including Mustang Panda and a group we named DigitalRecyclers. We also observed a governmental entity in Guyana being targeted by a cluster of activity we named **Operation Jacana**, a governmental entity in Kuwait and a hosting provider targeted by TA410 and, finally, a watering hole attack by FishMonger against a Pakistani government website. In the same period, MirrorFace continued to heavily target Japanese organizations. We also uncovered a China-aligned APT group, which we named TheWizards, spying on Chinese speakers in mainland China and abroad using adversary-in-the-middle (AitM) attacks. We also discovered that the Worok APT group has developed a new Go backdoor that we have named GoFighting.

Mustang Panda

In August, ESET researchers identified a campaign by Mustang Panda targeting a governmental organization in Slovakia. There is no indication leading us to think that this organization was successfully compromised. It is worth noting that this Mustang Panda spearphishing operation happened amidst the **political campaigns for the Slovak parliamentary elections**.

Targets first received a spearphishing email with a tracking pixel, enabling the attacker to know when the target opens the email. A malicious link is then sent in a second email. We believe the goal is to identify users who are more likely to open phishing emails and target them specifically in order to reduce the risk of the payload being reported to IT or security services.

That malicious link leads to a ZIP archive containing a LNK file that downloads and executes an HTA script, which then deploys the group's **classic trident Korplug loader**. The only significant difference here being that the malicious DLL is written in **Nim**. While this is the first instance we could find of Mustang Panda using Nim, it is consistent with the group's recent exploration of new programming languages and technology.

Over the last months, we also observed Mustang Panda increasingly relying on Cloudflare to hide its actual C&C and distribution servers.

FishMonger

In July, ESET researchers detected a watering-hole attack on a legitimate, but presumably compromised, Pakistani government website. If the visitor is using a computer, not a smartphone, the script displays an alert box (see Figure 1) and if the visitor clicks on `OK`, a Windows executable is downloaded onto the device.

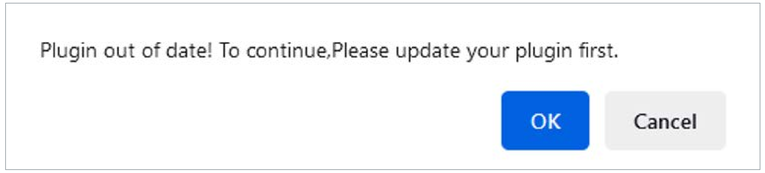

Figure 1. Malicious alert box

The downloaded executable is a backdoor named Trochilus, which is commonly used by other China-aligned APT groups such as Webworm. However, the C&C server had typical characteristics of the ShadowPad servers deployed by FishMonger. Therefore, we believe with medium confidence that FishMonger is behind this watering-hole attack and is a Trochilus backdoor user.

TA410

The various TA410 subgroups were defined in a WeLiveSecurity blogpost.

FlowingFrog

In mid 2023, we observed activity by the FlowingFrog TA410 subgroup on the server of a US hosting provider. We detected samples of the Tendyron backdoor that were deployed after the attacker unsuccessfully tried to deploy multiple Jakarta Server Pages (JSP) web backdoors. The Tendyron backdoor and multiple variations of the JSP web backdoor were transferred to the server in quick succession.

We believe initial access was achieved by exploiting a known vulnerability, since the affected server was running an out-of-date version of the Adobe ColdFusion application server.

LookingFrog

ESET researchers observed activity in our telemetry by the LookingFrog TA410 subgroup on a computer belonging to a governmental entity in Kuwait. We detected a sample of the group's custom LookBack implant, along with the Stegmap backdoor and a persistence tool; both of the latter two were previously attributed to Looking Frog in a blogpost by Symantec.

This version of LookBack is almost identical to those we described in our WeLiveSecurity blogpost, while the Stegmap sample downloads a image containing the encrypted next stage encoded in the image.

GREF

We recently published a WeLiveSecurity blogpost documenting two active campaigns targeting Android users, that we attribute to the GREF group.

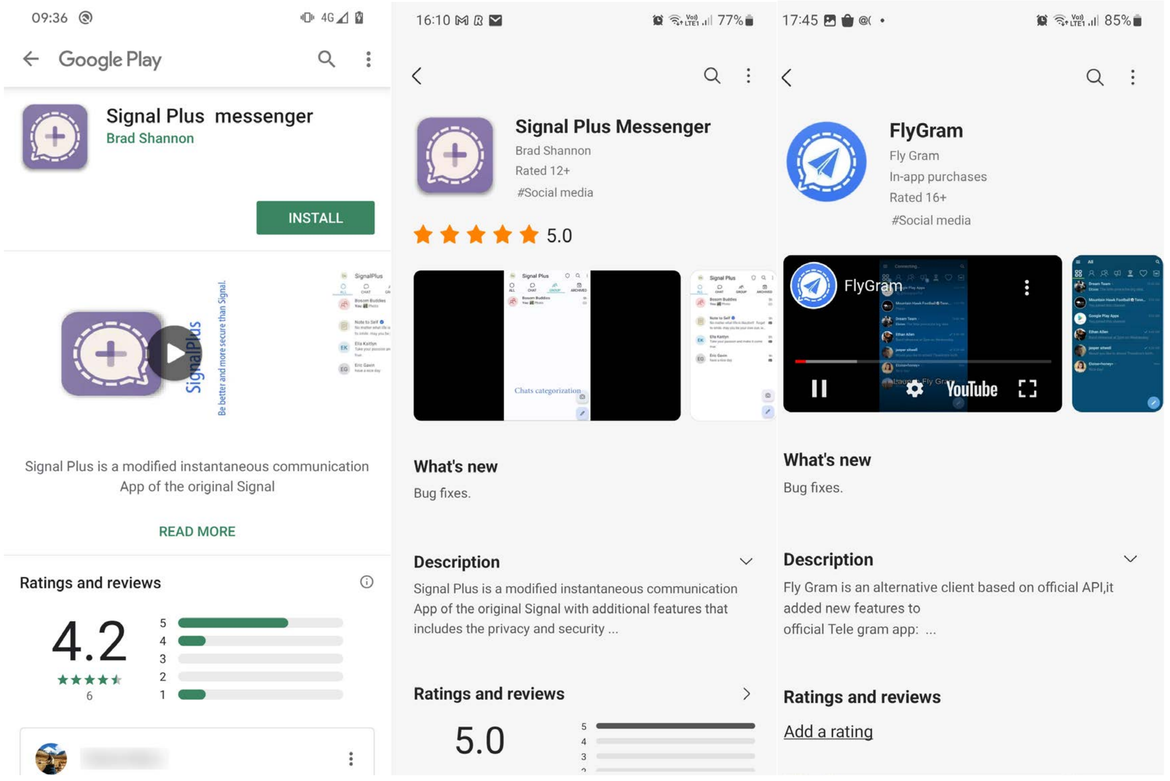

Figure 2. Signal Plus Messenger apps on Google Play (left; no longer available), Samsung Galaxy Store (center), and the FlyGram app on Galaxy Store (right)

The campaigns have distributed the Android BadBazaar espionage code through the Google Play store, Samsung Galaxy Store, and dedicated websites representing the malicious apps Signal Plus Messenger and FlyGram. The threat actors patched the open-source Signal and Telegram apps for Android with malicious code that we have identified as BadBazaar, which has previously been used to target Uyghurs and other Turkic ethnic minorities. Based on our research, potential victims were also lured to install the malicious FlyGram app from a Uyghur Telegram group focused on Android app sharing; see Figure 2.

The purpose of these trojanized apps is to exfiltrate user data and, specifically in Signal Plus Messenger, to spy on victims' Signal communication. After publishing our blogpost, Volexity published a report on three Android malware families – BadBazaar, BadSignal, and BadSolar – and attributed them to a group they call EvilBamboo. More specifically, the BadSignal malware family analyzed by Volexity is what ESET has described as trojanized Signal and Telegram applications, with the added malicious code that has the same functionality as earlier BadBazaar variants reported by Lookout. In order to avoid confusion: moving forward, we will adopt this naming convention to distinguish between the original BadBazaar, and its BadSignal variant, which is delivered via trojanized applications.

MirrorFace

MirrorFace continued with its campaigns targeting Japanese entities exclusively. In August 2023, we observed an interesting change in the attack vector: instead of compromising an entity via the victim opening a malicious attachment to a spearphishing email, MirrorFace compromised an IT company through a vulnerable server. Our analysis of the incident indicates that the server was most likely compromised through a vulnerable instance of **Proself**, an online storage service. Proself released an advisory in July 2023 stating that its products contained an authentication bypass and zero-day remote code execution vulnerability that had been confirmed to be already exploited.

A few days after the aforementioned incident, MirrorFace continued on the same trend and once again compromised a vulnerable server, but this time of a research institute. MirrorFace delivered its flagship backdoor LODEINFO alongside various publicly available exploitation tools such as **EfsPotato**, **DCOMPotato**, **FullPowers**, **Yasso**, the customized reverse proxy **frp**, and a previously undescribed backdoor. This shows that MirrorFace has enriched its toolset repertoire and, besides its in-house developed malware, MirrorFace has started using publicly available exploitation tools as well.

GALLIUM

During the last six months, ESET researchers have observed GALLIUM compromising telecommunications operators in Mali, Türkiye, and French Polynesia, and a government organization in Guatemala. We discovered these campaigns while monitoring implants known to have been used by GALLIUM in the past, including the recently documented toolset used during **Operation Tainted Love**.

Most of the compromised systems are Microsoft Exchange servers or Microsoft IIS servers, all with numerous webshells detected; it's likely that the attackers exploited one or more of the various remote code execution vulnerabilities discovered in the past few years on these platforms, or reused already deployed webshells in order to deploy their own implants.

On the compromised systems, GALLIUM deployed mim221, a custom credential theft implant based on Mimikatz.

DigitalRecyclers

ESET researchers uncovered the activity of a newly identified cyberespionage group, which we have named DigitalRecyclers, that repeatedly compromised a governmental organization in the European Union since 2018, using a toolset originally developed by threat actors from Pakistan in the 2010s.

In a recent incident, we were able to determine that the attackers dropped a first-stage downloader through a Microsoft Exchange web server accessible from the internet. Interestingly, attackers accessed the victim's server using a custom VPN service that is also used by **BackdoorDiplomacy**. The use of such custom anonymization networks is an ongoing trend among China-aligned threat actors.

We believe that DigitalRecyclers is loosely linked to BackdoorDiplomacy and the wider APT15 family.

TheWizards

TheWizards is a China-aligned APT group active since at least 2021, engaging in cyberespionage operations against Chinese-speaking individuals based in mainland China and abroad (e.g., the Philippines, the United Arab Emirates, and Hong Kong), and against gambling companies based outside mainland China. ESET researchers discovered this threat actor when a malicious update was downloaded by a popular, legitimate Chinese application.

TheWizards group has capabilities to conduct adversary-in-the-middle (AitM) attacks using a custom tool we discovered and have named Spellbinder. This tool uses **IPv6 SLAAC spoofing** to redirect traffic and deliver custom malware via software updates by legitimate applications. The tools developed by this group include two backdoors that we've named WizardNet and DarkNights.

Since gambling is **illegal under Chinese law** and Chinese citizens thus **turn to foreign online gambling companies**, this would explain why TheWizards group spies on such companies, most likely to identify Chinese citizens infringing the law. This is not the first time we have witnessed a China-aligned APT group targeting gambling companies: Operation ChattyGoblin, which we mentioned in **our previous APT activity report**, compromised a gambling company in the Philippines by targeting its support agents.

PerplexedGoblin

ESET researchers recently discovered a government organization in the European Union being targeted by an APT group we have named PerplexedGoblin. It uses a backdoor, TurboSlate, that we discovered and named in November 2022.

In our **T3 2022 APT Activity Report**, we mentioned the discovery of this new backdoor in a government organization in the European Union; it can

be deployed in various ways, including a DLL side-loading chain and a bring your own vulnerable software (BYOVS) chain. At that time, we attributed TurboSlate with medium confidence to Goblin Panda. However, after tracking the threat actor behind TurboSlate for months, we reevaluated our initial assessment: without a strong enough link between TurboSlate and a known group, we now track this activity cluster as PerplexedGoblin.

Worok

Worok is a China-aligned cyberespionage group, active since at least 2020, that targets high-profile companies and local governments mostly in Asia, which we first documented in a **WeLiveSecurity blogpost**.

ESET researchers discovered a previously undocumented Go backdoor that we have named GoFighting and that we attribute to Worok. GoFighting is a reimplementation of **Worok's PowHeartBeat backdoor** and the GoFighting commands are the same as the ones used by Worok's PowHeartBeat backdoor. A noticeable difference from PowHeartBeat is the presence in GoFighting of a network fallback mechanism based on GitHub.

India

Donot Team

Summary of India-aligned APT group activity seen by ESET Research in April 2023 – September 2023

During the last six months, we noticed most threat actors in the region moving away from malicious RTF (Rich Text Format) files and Equation Editor exploits, and trying to find new, reliable ways of distributing their malware. We detected attempts to use LNK (Windows shortcut) files, as well as CHM (Compiled HTML Help) and HTA (HTML Application) files, with varying degrees of success. The most prevalent compromise vector remains a spearphishing email with a macro-enabled Office document in the attachment.

Considering the prevalent use of the Zimbra collaboration suite in this region, it is no surprise to see that frequent phishing attempts targeting government organizations continue (we've documented similar attacks in this WeLiveSecurity blogpost) in Q2 and Q3 of 2023; most of them use free, dynamic DNS services, such as `servehttp.com` or `viewdns.net`, both owned by No-IP. We also have detected repeated phishing attempts imitating the Bangladesh Army Outlook Web Access portal; see Figure 3.

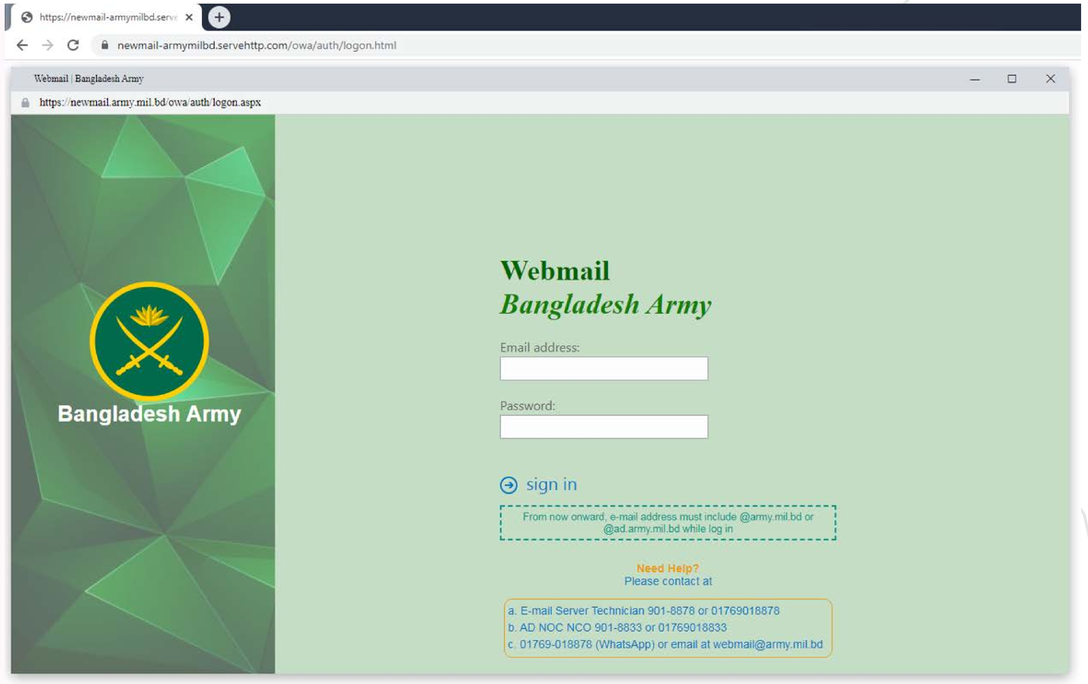

Figure 3. Phishing page imitating the Bangladesh Army webmail portal

Donot Team

In the mobile threat landscape, we saw threat actors increasing their efforts and a continuing evolution of threats. Donot Team reportedly managed to publish its Android trojan on the Google Play store for approximately two months; however, the number of victims is estimated to be only in the low hundreds. Speaking of Donot Team, in Q2 and Q3 of 2023 it continued its attacks on government organizations, mostly in Pakistan and Bangladesh. The group's yty framework is still being developed, with a steady stream of incremental updates.

Iran

MuddyWater OilRig

Summary of Iran-aligned APT group activity seen by ESET Research in April 2023 – September 2023

Over the course of Q2 and Q3 2023, ESET researchers continued tracking Iran-aligned threat groups targeting victims in Israel (OilRig) and Saudi Arabia (MuddyWater). The latter group continues to build and deploy PowerShell-based backdoors with a focus on initial access and data collection, possibly as an access development team for a more advanced group. Finally, OilRig has been observed developing and deploying C++ and C#/.NET backdoors that are generally full-featured backdoors. Initial access for OilRig still seems to be via spearphishing emails, particularly when targeting local governments in Israel – an effort on which OilRig has spent considerable time going back to 2021.

MuddyWater

In March 2023, prior to the attack on the Israel Institute of Technology (aka Technion) by **DarkBit** (a joint effort between MuddyWater and an unidentified group), ESET researchers were tracking the C&C infrastructure used by DarkBit as MuddyWater's. After that ransomware attack, MuddyWater continued well into April to use the same C&C servers to target an unidentified victim in Saudi Arabia. The initial vector of compromise is unknown, but post-compromise activities included the deployment of a batch script that downloaded a second payload from the C&C servers. The secondary payload, a PowerShell-based backdoor, can download and execute arbitrary payloads. It removes the first payload from disk, performs some information gathering on the compromised host, and begins beaconing to the C&C server every 10 seconds.

OilRig

In April, we observed OilRig deploying a new toolset to several victims in Israel. The backdoor, OilForceGTX (named after its filename, `gtx.exe`), is deployed in `C:\ProgramData\NVIDIA GTX\v10.1`, a path that mimics legitimate NVIDIA software. OilRig also deployed two helper DLLs, NotifyTrayLib and Nuget_Tools, to the same directory. These DLLs are meant to provide runtime support in the form of additional modules for OilForceGTX to evade detection. In conjunction with this discovery, we also uncovered a Microsoft Excel spreadsheet with a malicious macro that drops OilForceGTX, along with the original email used to deliver the spreadsheet. Both files were uploaded to VirusTotal by a user in Israel. Based on the upload location and content, we assess that OilRig was probably targeting a local government institution in Israel, which aligns closely with OilRig activity over the past two years.

In early July, we observed a new variant of OilRig's backdoor, **Mango**, that was uploaded to VirusTotal[1] by a user in the Netherlands. Five additional samples were submitted within the following week, mostly with the file path `%ALLUSERSPROFILE%\Office356\Menorah`. The sample is a C#/.NET first-stage backdoor and contains small updates to the first version of Mango that we discovered in early 2023. Both versions support the same capabilities, with only small changes in the implementation and constants. Some interesting changes are the changing of the filename and internal name of the assembly from Mango to Menorah and the modification of the symbol names throughout the code, probably using an obfuscator/name generator. The C&C server was updated, but the URL structure, encryption key, and C&C protocol remained the same.

[1] SHA-1: C9D18D01E1EC96BE952A9D7BD78F6BBB4DD2AA2A

Middle East

POLONIUM

Summary of Middle Eastern APT group activity seen by ESET Research in April 2023 – September 2023

POLONIUM

POLONIUM continues to field PowerShell-based backdoors, but also uses Python-based backdoors with a heavy focus on exploiting victims in Israel for espionage and data theft.

In April, we observed POLONIUM deploying a new backdoor, CreepyPie, to an unidentified organization in Israel. CreepyPie is a Python script that connects to a remote C&C server, receives and executes commands, and sends the output back to the C&C server. The attackers used a short VBScript to invoke CreepyPie, probably persisting in compromised systems by executing the VBScript from a scheduled task.

CreepyPie uses the WebSocket protocol to communicate with its C&C server. Operator command options include taking a screenshot (saved as `GameTools.png`) and any command accessible through `cmd.exe` (with output saved as a plain text file that is misleadingly named `GameTools.dll`).

POLONIUM continues to rely on the CreepySnail backdoor to target victims in Israel. We also saw the group utilize legitimate utilities such as `ntdsutil.exe` – a command line tool for managing Active Directory – to dump the Active Directory database. CreepySnail can then be used to extract such information from the compromised system.

North Korea

Andariel Lazarus ScarCruft Kimsuky Konni

Summary of North Korea-aligned APT group activity seen by ESET Research in April 2023 – September 2023

During the last six months, ESET researchers continued to track the development of several North Korea-aligned threat actors. Andariel and ScarCruft both targeted Japanese institutions, while most of the observed Lazarus activities were associated with the Operation DreamJob cluster. We also continued to investigate the use of the SimpleTea malware family: a common code base used by the Lazarus group to create malware for all major desktop OS platforms: Windows, Linux, and macOS. Finally, Kimsuky continued its targeting of international scholars and journalists specializing in North Korea, and Konni remained active in South Korea.

Andariel

In late May 2023, we observed an attack against an industrial network in Japan, conducted by the Andariel group. Various custom tools were deployed, such as an infostealer we have named Shoplifter, capable of logging keystrokes, stealing clipboard content, and exfiltrating the file system structure. Interestingly, the attackers also deployed AutoIt malware with very similar capabilities. Finally, we also observed a simple HTTP downloader capable of retrieving AES-128-encrypted payloads, and SpyXstealer, a custom tool used to steal browser data such as passwords and credit card information.

In general, the attackers' TTPs still include the easy-to-detect usage of native Windows command prompt tools in order to perform reconnaissance and lateral movement.

Lazarus

We saw activity mostly belonging to the Operation DreamJob cluster in this period. In April 2023, we **wrote** about new Linux malware, OdicLoader and SimplexTea, in connection with the infamous 3CX supply-chain attack. OdicLoader is an ELF downloader responsible for fetching and executing the SimplexTea Linux backdoor from the OpenDrive cloud service. At the time, we did not know that the code used to compile the SimplexTea Linux backdoor was in fact part of a common Lazarus code base used for all major desktop platforms: Windows, Linux, and macOS. After discovering this commonality, we decided to use the SimpleTea name for all malware derived from this common code base, even if there are slight variations in their functionalities.

In September, a user from Slovenia submitted a new variant of OdicLoader[2] to VirusTotal . While the variant discussed in our **blogpost** was disguised as an HSBC-themed job offer, this one has a MultiLayerSwap theme.

MultiLayerSwap appeared to be a cryptocurrency trading platform offering instant transfers across different blockchains. However, MultiLayerSwap did not appear very trustworthy and after a brief examination we concluded that it is a copycat of a legitimate **cBridge** project by **CelerNetworks**. This highlights Lazarus's ongoing targeting of cryptocurrency-related entities.

We also continued to observe Lazarus using macOS payloads against its targets. Samples of SimpleTea for macOS were uploaded to VirusTotal[3] from Hong Kong and China, and we also discovered a macOS WebbyTea downloader. Its associated Python loader has code to pick a payload according to the OS it is executed on: Windows, Linux, or Darwin (the core Unix system of macOS). This illustrates again the capability and willingness of the Lazarus group to attack all major operating systems.

ScarCruft

In this period, ScarCruft continued to target entities in South Korea, but also in Japan. It still relies on Ruby scripts in some of its campaigns, but also the RokRAT backdoor.

In September, a ZIP archive containing a malicious LNK file named `Korea National Intelligence Society 2023 Summer Academic`

[2] SHA-1: CB123A197A3BAA8865A3CA2CEE25022D0A578371
[3] SHA-1: 744A816A4D9FBC0B358500B25E6F5AFD7B52C718

`Conference and 5th National Strategy Colloquium (Final) - Korea's national security and intelligence in a period of great transition.lnk` was uploaded to VirusTotal[4] from South Korea.

Once executed, a decoy PDF is opened (see Figure 4) and shellcode is downloaded from OneDrive. At the time of analysis, the server responded with shellcode containing the RokRAT backdoor, illustrating the continuing usage of this backdoor by ScarCruft.

Kimsuky

Kimsuky adjusted its approaches and, like many other threat actors, started to utilize tools such as OneNote, Compiled HTML Help (CHM), and Windows shortcut (LNK) files in its campaigns. The group also rewrote some of its malware in Go to evade detections and to get the upper hand against security solutions.

Kimsuky's most notable activity is its continuation of a spearphishing campaign targeting analysts, academic scholars, researchers, and journalists who focus on North Korean matters. In this campaign, Kimsuky impersonates someone from a relevant community and distributes high-quality spearphishing emails, in the person's name, to other selected members of that community. This enables Kimsuky to gain the trust of its targets. Often, Kimsuky continues with the communication in a predefined way to establish

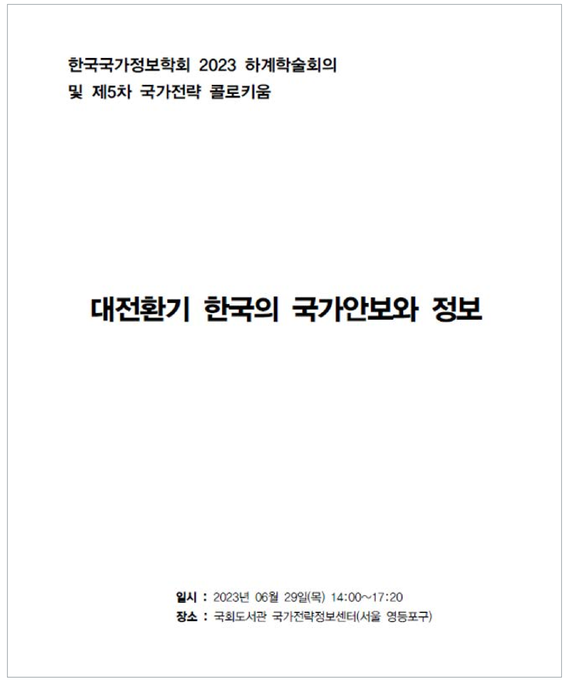

Figure 4. Decoy PDF document

rapport with the target. Once a certain point in the communication is reached, Kimsuky sends a malicious attachment or link to the target. The intention is either to compromise the target's machine or to harvest credentials through a fake website mimicking a known service. The ultimate goal of the campaigns is usually to gather strategic intelligence.

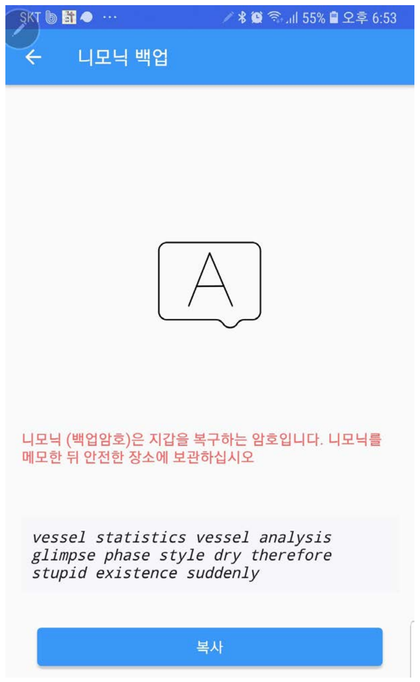

Figure 5. Decoy document screenshot of a Qbao cryptocurrency wallet PDF document

Konni

Konni ran several finance-themed campaigns targeting South Korea. The compromise chain consisted of spearphishing emails with a link to a ZIP file that contains a malicious LNK file. If the LNK file is executed, it runs PowerShell code that extracts both the decoy document and the actual payload from data appended to the LNK file. The payloads are commonly CAB or ZIP files containing BAT and VBS downloaders. Very similar compromise chains have also been reported to be used by the other North Korea-aligned APT groups **Kimsuky** (text in Chinese) and **ScarCruft**. The campaign's initial payload filenames mention taxes, salaries, or contracts, such as `국세청 종합소득세 해명자료 제출 안내.hwp.lnk` (machine translation: `Information on submitting comprehensive income tax explanation materials to the National Tax Service`) and `법인렌탈계약서.txt.lnk` (machine translation: `Corporate rental contract`).

Interestingly, we detected an attempt by Konni to abuse a recent WinRAR vulnerability: **CVE 2023-38831**. A crafted, misnamed ZIP file (`wallet_Screenshot_2023_09_06_Qbao_Network.rar`) containing a decoy HTML page as well as a malicious executable – a downloader – was uploaded to VirusTotal[5]. The decoy document contains screenshots of a Qbao cryptocurrency wallet; see Figure 5.

[4] SHA-1: 0105234C9FB904CC4BFD6EC0E1E78163B2F5825C
[5] SHA-1: E0795C874BD9BBDF71C10164C483357F759CB41E

Russia

Sandworm Gamaredon Turla Sednit

Summary of Russia-aligned APT group activity seen by ESET Research in April 2023 – September 2023

During the past six months, ESET researchers continued to observe activity of Russia-aligned APT groups mostly targeting Ukraine and EU countries. These groups include Sandworm, Gamaredon, Turla, and Sednit, with Gamaredon being the group most active in targeting Ukraine.

Sandworm

In April 2023, CERT-UA published a **notification** about a cyberattack conducted by Sandworm against a government institution in Ukraine. Attackers deployed a malicious BAT script (named RoarBat), which performs data wiping operations using a legitimate WinRAR application. The script uses `WinRAR.exe` in command line mode to move files into an archive, and then deletes the original files once they have been added to the archive.

In June 2023, we discovered another variant of RoarBat, deployed in a media organization in Ukraine, which is slightly different: specifically, it targets media files with extensions such as `.drawio`, `.jfif`, `.mkv`, `.avi`, `.mxf`, and `.MTS`, which are commonly found at media organizations.

In July 2023, we detected two data wiping attacks conducted by Sandworm using a new version of NikoWiper[6]. This wiper was deployed against a government organization and private companies. It abuses a legitimate command line utility for secure file deletion, **SDelete (Secure Delete)**. The functionality is like the older NikoWiper variant used in October 2022: at that time it was used against a company in the energy sector in Ukraine. In this variant of NikoWiper, the attackers left the PDB path `c:\Users\Mykyta\Desktop\prjs\Chelomey\Release\Chelomey.pdb`, which reveals that this malware project is probably named after **Vladimir Chelomey**, an engineer and designer in the missile program of the former Soviet Union. In addition, attackers left a false flag: they used the Ukrainian given name **Mykyta** rather than the same Russian name Nikita.

In August 2023, we detected a new wiper that we named SharpNikoWiper. SharpNikoWiper abuses the legitimate SDelete command line utility, as does NikoWiper, but unlike NikoWiper this variant is written in C#, hence the name SharpNikoWiper. In addition to data wiping using SDelete, this wiper attempts to rewrite with zeros the first 65,536 bytes of the first ten connected hard drives , if they exist, by writing directly to `\\.\PhysicalDrive<DRIVE_NUMBER>`.

During this period, we observed that Sandworm used a pro-Russian Telegram channel (@solntsepekZ) to promote information about cybersabotage operations it had conducted. This Telegram channel attempts groundlessly to blame CERT-UA and discredit its reputation.

Gamaredon

In the current reporting period, Gamaredon significantly improved its intelligence collecting capabilities. Specifically, it extended the functionality of existing tools and developed and deployed new tools to collect even more data from compromised computers.

In April, we discovered a new version of the PteroSteal credential stealer, which is now capable of stealing credentials, and other information related to email accounts, stored by the email clients Outlook and The Bat!.

In June, we discovered several new tools:

- PteroCookie, which is capable of stealing cookies from Opera, Firefox, Chrome, and Edge.
- PteroSig, which is designed to exfiltrate information stored by the Signal desktop application.
- PteroGram, which exfiltrates data from the Telegram Desktop application.

In August we discovered two new Gamaredon tools. First, PteroBleed is designed to exfiltrate **IndexedDB** data from Opera, Chrome, and Edge browsers. This tool specifically looks for data stored in this database by web

[6] SHA-1: BBB7D42ADB6C6F6D3FEE3F80BEBD8CBED7FC3A94

versions of Telegram and WhatsApp applications, and for data that might be used by various Ukrainian military web services. The second tool we discovered that month is PteroScout, which is used for reconnaissance. It gathers detailed information about the compromised system.

Turla

In July 2023, CERT-UA published a **technical analysis** of a new implant named CAPIBAR that it attributes to Turla. Using ESET telemetry, we were able to detect the deployment of CAPIBAR not only in Ukraine but also in Greece and Guyana. Most victims are governmental entities, a typical target of Turla.

We believe that the initial access vector used to deploy the server component, acting as a C&C server for other victims, is known RCE vulnerabilities in Microsoft Exchange such as ProxyLogon and ProxyShell.

Sednit

In June 2023, we discovered a set of spearphishing campaigns, which we named Operation RoundPress, exploiting an XSS vulnerability in Roundcube (**CVE-2020-35730**); see an example in Figure 6. Using this vulnerability, attackers are able to inject malicious JavaScript code into the victim's Roundcube webmail server. The injected code is able to steal emails, address books, and create forwarding rules to steal incoming emails. This campaign was also documented by **CERT-UA** and **Recorded Future**.

According to our telemetry, Operation RoundPress targets government staff in Armenia, Tajikistan, and Ukraine.

In August and September 2023, we detected an updated version of Operation RoundPress spearphishing, exploiting the same XSS vulnerability.

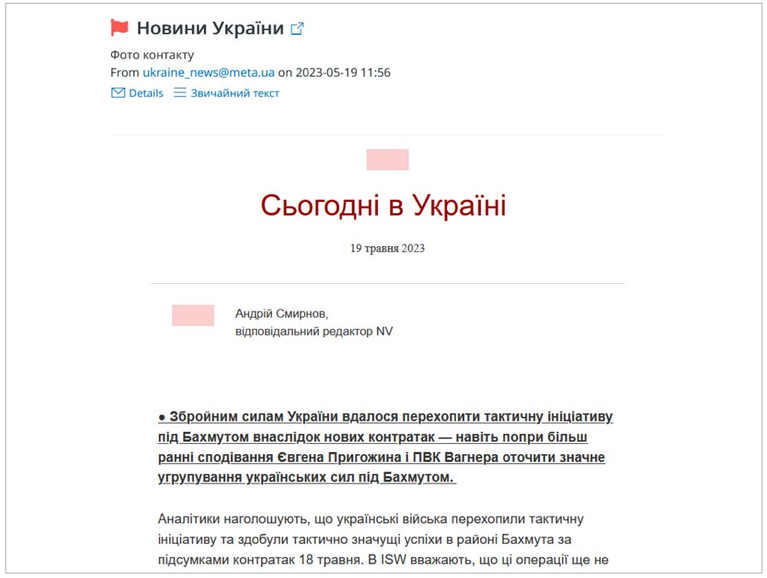

Figure 6. Spearphishing email used in Operation RoundPress

This campaign was targeting organizations in Serbia, Greece, Poland, and Ukraine.

In August 2023, we detected a Sednit spearphishing campaign targeting the **CVE-2023-38831** WinRAR vulnerability. This vulnerability allows attackers to execute arbitrary code with WinRAR versions prior to v6.23. According to **Group-IB**, it has been used in the wild since April 2023 by crimeware threat actors against traders. Sednit's emails used the agenda of the European parliament as a lure (see Figure 7) and targeted political entities in the EU and Ukraine.

In August 2023, we detected a new set of spearphishing emails used by Sednit that exploit the **CVE-2023-23397** vulnerability in Microsoft Outlook for Windows. This vulnerability allows attackers to trigger an NTLM authentication request to an attacker-controlled server by sending a specially crafted meeting invite. Initially, this was a zero-day vulnerability **disclosed** in March 2023. A newer campaign was targeting organizations in Ukraine, Poland, and Czechia.

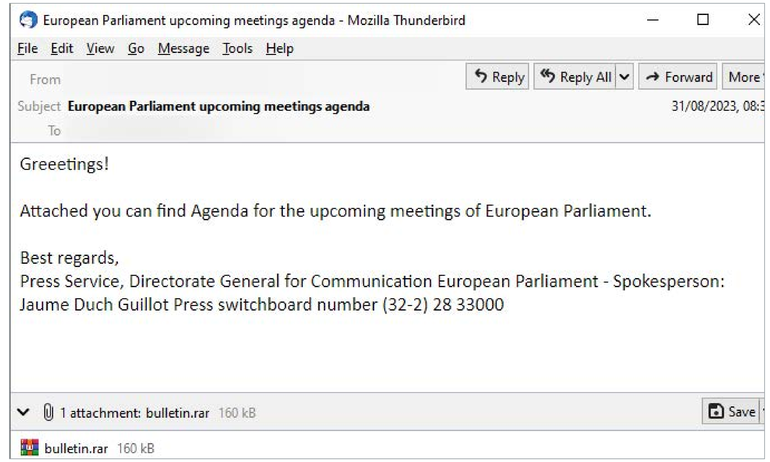

Figure 7. Targeted phishing using the European Parliament agenda as a lure

In September 2023, CERT-UA published a **notification** about a Sednit spearphishing campaign, whose execution chain relies on the user manually clicking on a link in the email, which opens an archive, and then executes a BAT script from that archive. To the best of our knowledge, this was a completely manual execution chain, relying on the lure to motivate the user to click on the malicious BAT script.

Other

SturgeonPhisher Winter Vivern

Other notable APT activities

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

SturgeonPhisher

SturgeonPhisher is a cyberespionage group that we first introduced in our previous APT activity report and that mainly targets governments in Central Asia. In that earlier report we mentioned that we observed a decline of SturgeonPhisher activity and we assessed that the group was busy retooling.

This actually happened in the following months and we observed new variants of the group's Telegram backdoor, now developed in PowerShell and Go, in addition to the usual Python variant based on pyTelegramBotAPI.

In late August 2023, SturgeonPhisher jumped on the WinRAR CVE-2023-38831 vulnerability bandwagon to target individuals in Tajikistan. A ZIP archive was sent as an attachment and attempts to exploit the CVE-2023-38831 vulnerability. If it succeeds, or if the user clicks on the `27885.pdf.cmd` file the archive contains, additional malware will be downloaded from `https://akn[.]tj/down/Winrar.rar`. Then it extracts and executes the next stage contained in this second archive: a .NET dropper and a custom Go backdoor we named GoBatDoor.

Winter Vivern

Winter Vivern is a cyberespionage group that we mentioned in our previous APT activity report. In particular, it exploited an XSS vulnerability, CVE-2022-27926, in the Zimbra portal to target at least two different governmental organizations in Europe.

In late August 2023, we detected a wave of spearphishing emails against a Ukrainian governmental entity. The email was intended to exploit an XSS vulnerability in Roundcube (CVE-2020-35730). Note that the same vulnerability is currently being exploited by Sednit in Operation RoundPress.

The email messages were probably sent from a compromised email address; their subject is `Important warning on maintenance`, and the body is the following:

```
Dear Colleagues,

Due to the planned technical work, the
Ministry's mail server https://<redacted>.
gov.ua/ may temporarily not respond to user
requests.

[WebResource:<script type=ext/
javascript">eval(atob('<base64-encoded
payload>'));</script>]:##str_replacement_0##

Best regards,

<redacted>
```

If the webmail server is vulnerable, JavaScript code will be executed in the context of the browser, leading to the display of a fake Roundcube login window that exfiltrates to its C&C server whatever credentials a victim might enter.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide. ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

WeLiveSecurity.com

@ESETresearch

ESET GitHub

ESET Threat Reports and APT Activity Reports