APT ACTIVITY REPORT

Q4 2022–Q1 2023

LAZARUS EXTENDS TARGETING TO ALL MAJOR DESKTOP OSes

ESET Digital Security
Progress. Protected.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

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 October 2022 until the end of March 2023. Attentive readers will notice that a small portion of this report also mentions some events previously covered in APT Activity Report T3 2022. This stems from our decision to release this report on a semi-annual basis, with the current issue encompassing Q4 2022 and Q1 2023, while the forthcoming edition will cover Q2 and Q3 2023.

In the monitored timeframe, several China-aligned threat actors focused on European organizations, employing tactics such as the deployment of a new Ketrican variant by Ke3chang, and Mustang Panda's utilization of two new backdoors. MirrorFace targeted Japan and implemented new malware delivery approaches, while Operation ChattyGoblin compromised a gambling company in the Philippines by targeting its support agents. India-aligned groups SideWinder and Donot Team continued to target governmental institutions in South Asia with the former targeting the education sector in China, and the latter continued to develop its infamous yty framework, but also deployed the commercially available Remcos RAT. Also in South Asia, we detected a high number of Zimbra webmail phishing attempts.

In the Middle East, Iran-aligned group MuddyWater stopped using SimpleHelp during this period to distribute its tools to its victims and shifted to PowerShell scripts. In Israel, OilRig deployed a new custom backdoor we've named Mango and the SC5k downloader, while POLONIUM used a modified CreepySnail.

North Korea-aligned groups such as ScarCruft, Andariel, and Kimsuky continued to focus on South Korean and South Korea-related entities using their usual toolsets. In addition to targeting the employees of a defense contractor in Poland with a fake Boeing-themed job offer, Lazarus also shifted its focus from its usual target verticals to a data management company in India, utilizing an Accenture-themed lure. Additionally, we also identified Linux malware being leveraged in one of their campaigns. Russia-aligned APT groups were especially active in Ukraine and EU countries, with Sandworm deploying wipers (including a new one we call SwiftSlicer), and Gamaredon, Sednit, and the Dukes utilizing spearphishing emails that, in the case of the Dukes, led to the execution of a red team implant known as Brute Ratel. Finally, we detected that the previously mentioned Zimbra email platform was also exploited by Winter Vivern, a group particularly active in Europe, and we noted a significant drop in the activity of SturgeonPhisher, a group targeting government staff of Central Asian countries with spearphishing emails, leading to our belief that the group is currently retooling.

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 updates 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 that deliver high-quality strategic, actionable, and tactical cybersecurity threat intelligence is available at the ***ESET Threat Intelligence*** [1] 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 regions:

- Australia
- Bangladesh
- Bulgaria
- Central Asia
- China
- Egypt
- Europe
- Hong Kong
- India
- Israel
- Japan
- Namibia
- Nepal
- Pakistan
- The Philippines
- Poland
- Saudi Arabia
- South Korea
- Southwest Asia
- Sri Lanka
- Sudan
- Taiwan
- Ukraine
- The United Kingdom
- The United States

Targeted business verticals:

- Data management companies
- Defense contractors
- Diplomats
- Educational institutions
- Energy sector
- Financial services
- Gambling companies
- Governmental organizations
- Healthcare
- Hospitality
- Media
- Research institutes

CN-ALIGNED ACTIVITY

Summary of China-aligned APT group activity seen by ESET Research in Q4 2022–Q1 2023.

In the last half year, Mustang Panda has continued to target European organizations with new implants, while Ke3chang targeted a high-profile governmental organization in the European Union with a new Ketrican variant and loader. MirrorFace has continued to target Japan with updated loading schemes. We also discovered a new compromise at a gambling company in the Philippines carried out by one of the clusters of activity behind Operation ChattyGoblin.

Mustang Panda

We recently published a ***blogpost*** [2] documenting a Mustang Panda campaign targeting Bulgaria, Australia and Taiwan, which uses a new backdoor we have named MQsTTang. While monitoring the network infrastructure used in this campaign, we came across another new backdoor.

This new backdoor is written in Go and shares some similarity with MQsTTang. Like the latter, it functions as a barebones remote shell. It uses PowerShell to download a `Robots.txt` file from the C&C server and to run its content as a PowerShell script. The downloaded script is an HTTP reverse shell.

When executed from inside a ZIP file, the backdoor will communicate with its C&C server, sending it, over HTTP, XOR-ed information about the current user and connected interface. The server response contains a base64-encoded command to be executed by the backdoor using the `os/exec.Command` function from the Go standard library.

Ke3chang

In January, we detected the compromise of a high-profile governmental organization in a European Union country. In two instances, a new variant of Ke3chang's signature backdoor, Ketrican, was deployed using a new loader that we named KetriADS because it is designed to read, decrypt, and execute its payload from the alternate data stream (ADS) of one of its modules. Several code similarities were observed with known Ke3chang tools and the new Ketrican variant. At the same organization, Ke3chang's Okrum backdoor was also deployed.

In January, Palo Alto Networks Unit 42 ***published a report about BackdoorDiplomacy*** [3], a China-aligned APT group active ***since at least 2012*** [4]. While Unit42's report is focused on the group's network infrastructure and updated tools, it also asserts that the group is equivalent to Ke3chang. To the best of our knowledge, a solid link between BackdoorDiplomacy and Ke3chang has never been established, although we noted their shared use of a specific form of DLL search-order hijacking ***in our 2021 blogpost*** [5]. During this investigation, we also discovered a backdoor linked to ***BackdoorDiplomacy*** [5] and the group's custom version of Merlin

(an open-source backdoor written in Go) on several machines that, within a few months of each other, were compromised by both Ketrican and KetriADS. This allows us to corroborate the hypothesis from the Unit 42 blogpost: with low confidence, Ke3chang is linked to BackdoorDiplomacy. Further information is required to establish the nature of this link.

MirrorFace

MirrorFace continues reworking its approach to malware delivery with updated loading schemes. In March, a ZIP archive[1] containing a malicious Microsoft Word document[2] and a decoy Word document belonging to MirrorFace was uploaded to VirusTotal from Japan. The malicious document contains a VBA macro responsible for running shellcode that acts as a downloader with the final payload probably being a LODEINFO loader (loaded using DLL side-loading) and its encrypted LODEINFO payload.

A few days later, we detected an attack against an organization in Japan. Based on the detections in our telemetry, we believe with medium confidence that the organization is in the hospitality sector. In this attack, MirrorFace utilized the new malware delivery approach described above, making use of a new DLL side-loading host named `Elze.exe` (developed by Digital Arts Inc) to load a `frau.dll` LODEINFO loader.

Operation ChattyGoblin

Operation ChattyGoblin is ESET's name for a series of attacks against Southeast Asian gambling companies by China-aligned groups and happening since October 2021. These attacks use a specific tactic: targeting the victim companies' support agents via chat applications – in particular, the Comm100 (first ***documented by CrowdStrike*** [6]) and LiveHelp100 apps.

Last March, the support agents from a gambling company in the Philippines were targeted by one of the clusters of activity related to Operation ChattyGoblin.

Written in C#, the initial dropper deployed by the attackers is named `agentupdate_plugins.exe` and was downloaded by the LiveHelp100 chat application. The dropper deploys a second C# executable based on the ***SharpUnhooker tool*** [7]. The purpose of that executable is to download the second stage of the attack, which resides within a password-protected ZIP archive.

The final payload is a Cobalt Strike beacon using `duckducklive[.]top` as its C&C server.

[1] SHA-1: `53579094BD9BB9DF2E140DE6FC7C739278EC4F83`
[2] SHA-1: `C08BF05DB87896A15AC1913AC96BD47A35220225`

IN-ALIGNED ACTIVITY

Summary of India-aligned APT group activity seen by ESET Research in Q4 2022-Q1 2023.

In the last half year, Donot Team continued to target governmental institutions in Pakistan and Bangladesh with its yty framework. We also detected attacks using Remcos RAT, which we attribute to Donot Team with medium confidence. SideWinder relied on RTF documents as well as LNK and HTA files to target governmental organizations in South Asia. There was also an uptick in Zimbra webmail phishing attempts targeting webmail users in the Southwest Asia region.

Donot Team

We reported on several spearphishing campaigns performed by Donot Team. According to our telemetry, this group is actively targeting government institutions in Pakistan and Bangladesh, and to a lesser extent, Sri Lanka and Nepal. We observed frequent spearphishing attacks using malicious Office documents, as well as less common attacks via malicious InPage documents. Not only did Donot Team continue to develop its infamous yty framework, but we also detected several attacks using the commercially available Remcos RAT.

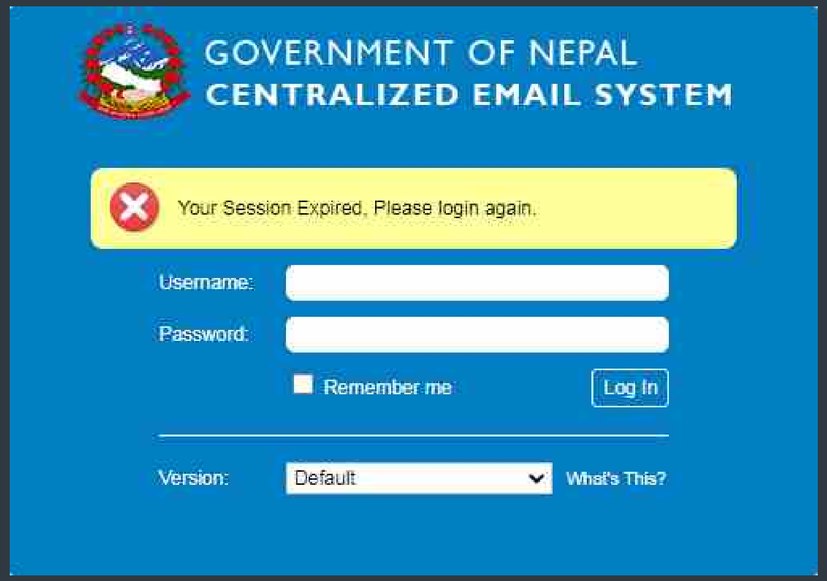
NewsPenguin

In February, fellow researchers from BlackBerry *described* [8] a new India-aligned APT group they named NewsPenguin. In addition to the modules described in the article, we also found a USB worm module that would allow NewsPenguin to spread inside the affected organization. However, we haven't seen any new activity after the initial campaign.

Other notable activities

The activity of other India-aligned groups was less noticeable during this period. We detected continued attacks by the APT group SideWinder, most of them using malicious RTF documents, as well as LNK and HTA files. Targeted government organizations were in Sri Lanka, Pakistan, and Bangladesh, as well as educational institutions in China. We also saw limited activity from the APT group Confucius using its Ragnatela RAT (also known as BADNEWS RAT).

In Southwest Asia, we also detected a significant number of phishing attempts targeting Zimbra webmail users. These phishing pages are designed to mimic websites of government or military institutions and frequently use subdomains of `netlify.app` or `rf.gd`. Even though these phishing operations seem to be unsophisticated, they appear to be quite effective and prevalent within this region.



Phishing page impersonating Government of Nepal hosted on `email1-centralized-system.rf[.]gd`

IR-ALIGNED ACTIVITY

Summary of Iran-aligned APT group activity seen by ESET Research in Q4 2022–Q1 2023.

In the last half year, Iran-aligned groups continued to target organizations based in the Middle East. We saw a shift in MuddyWater's TTPs, where the group stopped using the SimpleHelp tool, and saw new malware being used by OilRig and POLONIUM.

MuddyWater

In January 2023, MuddyWater continued to use the SimpleHelp remote access tool as an initial implant to distribute other tools to victims. On this occasion, MuddyWater used SimpleHelp to push Venom to a victim's system in Sudan. Later in January 2023, MuddyWater used SimpleHelp to target an Israeli victim in the hospitality industry. Separately, MuddyWater used SimpleHelp to drop ProcDump, FRP (Fast Reverse Proxy), and Ligolo on a victim's system in Saudi Arabia. Lastly, MuddyWater deployed SimpleHelp to a victim's system in Egypt. We previously reported on MuddyWater's use of SimpleHelp in T3 2022.

Towards the end of January 2023, MuddyWater shifted tactics and stopped using SimpleHelp. A new victim in Saudi Arabia received a PowerShell script that downloads and executes Fast Reverse Proxy (FRP), Chisel, Tight VNC, Ligolo, Mimikatz, ProcDump, and a Go-compiled version of Palo Alto's Global Protect agent. The PowerShell script is written with a cascading if-then structure, attempting to establish a reverse tunnel for MuddyWater operatives to interactively connect to the victim's system. The script also attempted to dump LSASS with ProcDump and parse it with Mimikatz.

OilRig

In December 2022, we detected OilRig deploying a new custom backdoor, Mango, to a victim in the Israeli healthcare vertical. In addition to Mango, OilRig also deployed its newest version of SC5k, a downloader that uses the Microsoft Office 365 (O365) API to log in to a pre-established account and download and execute payloads stored as attachments to emails in the O365 account. This victim was previously targeted by OilRig in June 2021 and August 2021 using the Shark backdoor and a custom keylogger.

POLONIUM

In January 2023, POLONIUM deployed a modified version of CreepySnail to a victim in Israel. This modified version only executes PowerShell commands and does not upload or download files. This victim also received *Plink* [9] to setup a reverse tunnel where POLONIUM used interactive commands to dump Active Directory and LSASS.

In mid February 2023, POLONIUM deployed a small reverse shell written in Lua. It is executed by a combination of PowerShell and Visual Basic scripts. POLONIUM used this tool to target several organizations in Israel.

NK-ALIGNED ACTIVITY

Summary of North Korea-aligned APT group activity seen by ESET Research in Q4 2022–Q1 2023.

In the last half year, ScarCruft continued to target South Korean organizations with ROKRAT and malicious CHM files. Kimsuky also used malicious CHM files in its campaigns, but also relied on AnyDesk, a remote desktop application. Finally, the Lazarus group continued to target defense contractors, but also data management companies.

ScarCruft

The group is still using ROKRAT, its flagship backdoor, as evidenced by a recent upload to VirusTotal[3] from South Korea. Other files uploaded to VirusTotal from the same country[4] exhibit a similar initial execution method as described recently in an AhnLab *report* [10]. This RAR archive contains a password-protected document alongside a CHM (Microsoft Compiled HTML Help) file named `password.chm`. When the user is lured into opening the CHM file to obtain the document password, it downloads and executes an HTA payload.

Andariel

Andariel was still active during this period as we saw it target a hospital in South Korea. In January 2023, the group used various payloads such as a *Nirsoft tool* [11] for collecting browser passwords; a *Nirsoft tool* [12] for recovering network passwords; a spying tool that logs keystrokes, the clipboard, and the titles of opened windows; a SOCKS tunnelling TCP client; and a custom TCP backdoor.

Kimsuky

In January 2023, we detected an attack against a US-based expert on Korea. In the attack, Kimsuky used malware typical of the BabyShark cluster, but connecting to previously unseen C&C servers. Similar activity continued in February 2023, when Kimsuky launched an attack attempt against a Hong Kong company that focuses on financial services. This cluster of activity is still very active, and we saw instances of it in most regions of the world.

Kimsuky continues to use CHM file in its malicious campaigns. In one such case, we detected a spearphishing email sent to a staff member of a research institute in Japan where the CHM file posed as a questionnaire (in Korean) from KBS News Line.

The overall TTPs generally remain unchanged; just tiny tweaks in their tooling were registered.

[3] SHA-1: `8A50A4EE479D9BA2F5525FA899420B30296E3ED8`
[4] SHA-1: `12103BC077F677AFB2BA7FAC6445DF3DD2F6DF00`

Lazarus

In January 2023, a company in India focused on data management was attacked with an Accenture-themed lure. The goal of the attackers was to monetize their presence in the company's network, most likely through business email compromise. This attack was unusual because the targeted company was not in the aerospace/defense or cryptocurrency/financial institutions verticals. Similar payloads using IBM- and Airbus-themed lures appeared on VirusTotal from the Netherlands, Portugal, and Germany in late 2022.

In February 2023, Lazarus attackers targeted a defense contractor in Poland by sending fake job offers, apparently from Boeing, to the company's employees. The attack involved a trojanized PDF reader based on SumatraPDF. The attack also included a RAT called ScoringMathTea and a complex downloader that we have codenamed ImprudentCook.

Lazarus continues to distribute its malware through ISO images. We investigated cases where such ISO images were used to distribute mini-BlindingCan as well as TightVNC Viewer GUI. We also noticed an interesting archive containing a .NET application importing *DevExpress PDF Viewer* [13] and showing a lure document capitalizing on *the FBI indictment* [14] of the Bitzlato founder.

In March 2023, we discovered that Lazarus is now targeting Linux desktop users with malware that has been tailored to this particular platform. This malware was used as part of Operation DreamJob, a social engineering scheme aimed at tricking unsuspecting victims into opening job offers containing malware. Upon further investigation, we *uncovered* [15] striking similarities in the code and network infrastructure between this campaign and the recent 3CX supply-chain attack, strengthening the belief that Lazarus is responsible for that compromise too.

RU-ALIGNED ACTIVITY

Summary of Russia-aligned APT group activity seen by ESET Research in Q4 2022–Q1 2023.

In the last half year, Russia-aligned APT groups were active, mostly targeting Ukraine and EU countries. These groups include Gamaredon, Sandworm, Sednit, the Dukes, and SaintBear. These independent attacks used tools such as wipers, spearphishing emails and Brute Ratel to accomplish their goals.

Gamaredon

Gamaredon continues to be one of most active APT groups targeting Ukraine, aiming at stealing confidential information. In addition to that, we noticed a spearphishing campaign targeting governmental institutions in several EU countries. The observed campaign relies on known Gamaredon tactics: emails with an attached malicious HTML document which, upon opening, offered to save an archive containing a malicious LNK file. The LNK file would subsequently download the next stage from its C&C server and execute it via `mshta.exe`.

The group continued adjusting the obfuscation of its tools to evade detection. Specifically, in this period we observed an increased number of attempts to store code parts of the Gamaredon toolset in the Windows registry to make detection harder. In addition to that, we noticed that this group is experimenting with various methods to evade network-based detections. For example, besides Telegram channels, some Gamaredon tools started to use the *Telegra.ph* [16] service to store the IP address of its C&C server.

Sandworm

Sandworm continues targeting various verticals in Ukraine, including government, the energy sector, and media.

In January 2023, we detected Sandworm's deployment of a new wiper in Ukraine, which we named SwiftSlicer. It was deployed using Active Directory Group Policy. This wiper is written in the Go programming language. Upon execution, it deletes shadow copies by executing the command `wmic shadowcopy delete`, then recursively overwrites files located in specific directories. We published an alert about this activity in our *Twitter account* [17].

In January 2023, CERT-UA published a *notification* [18] about a cyberattack conducted by Sandworm against the National News Agency of Ukraine (Ukrinform). This attack involved several wipers, depending on the attacked platform – AwfulShred and BidSwipe on Unix-based systems, and for Windows: CaddyWiper, SDelete, ZeroWipe, and batch files.

Sednit

In Q1 2023, we observed Sednit spearphishing using a fake warning disguised as service messages from Google and Yahoo. In addition to that, we discovered a new version of the CredoMap malware, publicly described by *CERT-UA* [19] and by *MalwareBytes* [20] in June 2022. To deploy this malware, Sednit operators sent an email with a self-extracting RAR archive in its attachment. This archive contains CredoMap malware and a decoy document in Ukrainian about a ring laser gyroscope.

Interestingly, that discovered version of CredoMap doesn't use the IMAP protocol for data exfiltration anymore. Instead, it leverages free legitimate services such as `free.keep.sh` and `tiny.cc`.

АРСЕНАЛ
Казенне підприємство спеціального приладобудування

ЛАЗЕРНІ ГІРОСКОПИ
ДЛЯ НАВІГАЦІЙНИХ СИСТЕМ

ПРИЗНАЧЕННЯ: вимірювач проекції вектора кутової швидкості основи на вісь чутливості ЛГ.

ОСОБЛИВОСТІ:

Лазерні гіроскопи з 3-ма довжинами периметру. Моноблочна конструкція, кільцевий лазер на віброопідставці в електромагнітному екрані.

СФЕРА ЗАСТОСУВАННЯ:

ЛГ використовуються у складі безплатформних інерціальних навігаційних систем.

ТЕХНІЧНІ ХАРАКТЕРИСТИКИ:

Модель (довжина периметру, см):	RL-28 (периметр - 28 см)	RL-16 (периметр - 16 см)	RL-08 (периметр - 8 см)
Зміщення нуля, град./год.	0.005...0.01	0.02...0.05	0.3...0.7
Випадковий відхід в куті, град./√год.	0.001...0.003	0.006...0.02	0.03...0.08
Нестабільність масшт. коефіцієнта	10 ppm	20 ppm	100 ppm
Диапазон кутових швидкостей, град./с	± 400	± 600	± 1000
Температурний діапазон, °С	-40 ... +65	-40 ... +65	-40 ... +65

Decoy document about a ring laser gyroscope

The Dukes

In Q1 2023, we detected a spearphishing campaign targeting diplomats in an EU country. The spearphishing emails impersonate the ministry of foreign affairs of the Czech Republic and contain a link to an HTML page that offers to download a ZIP archive. The ZIP archive is encoded in the body of the HTML page; this technique is known as *HTML smuggling* [21].

The ZIP archive contains an executable vulnerable to DLL search order hijacking, and a side-loaded DLL. This DLL is a downloader that uses *Notion* [22] as its C&C server. We observed that this chain leads to in-memory execution of a red team implant known as Brute Ratel.

[redacted]: "Assistant to the Ambassador" <[redacted]@seznam.cz>
[redacted]
[redacted]: Meeting request - Ambassador of the Czech Republic

Dear Colleague,

The Ambassador of the Czech Republic, would be delighted to have the opportunity to pay a courtesy call to H.E. the Ambassador [redacted]

I would be most grateful for your advice as to when it may be possible to schedule such a meeting. You can find the Ambassador`s convinient date/time here.

Kind regards,
Zdenek Holych
Assistant to the Ambassador
email: zdenek.holych@mav.cz | web: www.mzv.cz

Ministry of Foreign Affairs
of the Czech Republic

#StandWithUkraine

The Dukes' spearphishing email

SaintBear

In Q1 2023, we detected a new build of of the Elephant framework V2 (both ElephantDownloader and ElephantClientImplant). This build was deployed together with various tools, such as Cobalt Strike, HardBit ransomware, SDelete, ADExplorer, and BgInfo, against a company in the healthcare vertical in the United Kingdom.

Additionally, we discovered a simple, new, SaintBear backdoor, which we named ElephantLauncher. This backdoor was distributed via larger campaigns utilizing a trojanized TeamViewer installer. As with other SaintBear tools, ElephantLauncher is written in Go and it is capable of fingerprinting a compromised computer, and downloading then executing additional tools.

OTHER NOTABLE APT ACTIVITY

Summary of APT group activity of unclear regional affiliation seen by ESET Research in Q4 2022–Q1 2023.

This section covers APT groups for which we do not have enough information to determine their alignment with a particular entity.

SturgeonPhisher

SturgeonPhisher is a cyberespionage group that we first introduced in our T3 2022 *APT Activity Report* [23] and that strongly overlaps with what Talos researchers track under the name *YoroTrooper* [24]. Following that blogpost, we noticed a big drop in activity; we believe that the group is currently retooling.

Before that, the group was sending regular waves of spearphishing emails to government staff of Central Asian countries. SturgeonPhisher operators have been experimenting with new compromise chains including the use of LNK files that point to HTA files that, in turn, download a reverse shell. We also noted a change in their network TTPs: the group started using compromised websites to deliver payloads. In particular, in March 2023, SturgeonPhisher compromised the website of the chamber of commerce and industry of a Central Asian country.

Winter Vivern

Winter Vivern is a cyberespionage group that was first introduced by *DomainTools* [25] in 2021. In recent months the group has been particularly active in Europe; in February, it targeted Ukrainian and Polish officials, as reported by the *State Cyber Protection Centre* [26] of Ukraine.

Their usual modus operandi is to send spearphishing emails to entice targets to click a link leading to a website where they can download a fake antivirus, which then installs a custom PowerShell backdoor.

Other waves of spearphishing aim to steal mailbox credentials. For example, in February 2023, Winter Vivern exploited an XSS vulnerability, *CVE-2022-27926* [27], in the Zimbra portal to target at least two different governmental organizations in Europe. This was used to load a remote JavaScript file that would show the target a fake login page on top of the webmail. If victims enter their credentials, those credentials will be exfiltrated to a remote server and the victims will again be shown the normal webmail page.

- Часті збої додатків
- Незвичайні повідомлення про помилки
- Браузер часто зависає
- Комп'ютер перестає відповідати на запити
- Система перезапускається сама
- Доступ до файлів і програм заблоковано

Поради: як діяти

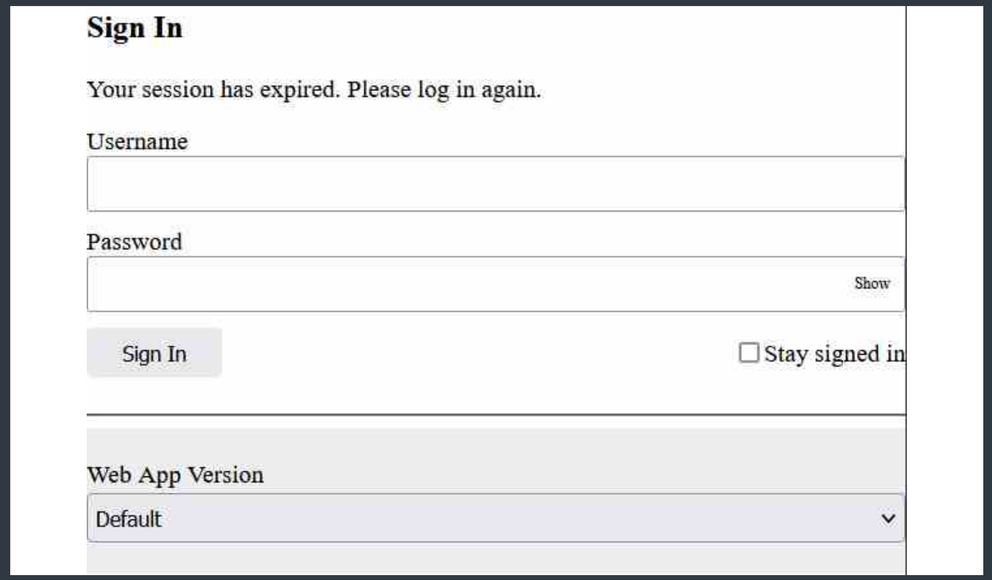
- **Скачайте наше програмне забезпечення!**

Завантажити

- Запустити програму **(Оскільки розроблена програма не є загальнодоступним продуктом, може знадобитися підтвердження дій користувача при запуску).**
- Отримайте результат (додаток просканує необхідні каталоги і покаже результат сканування).
- **При визначенні незаконного програмного забезпечення програма сканування відобразить місце розташування вірусів, вам необхідно їх видалити!**

Слава Україні!

Fake antivirus download page



Fake Zimbra login page

REFERENCES

[1] https://www.eset.com/int/business/services/threat-intelligence/

[2] https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/

[3] https://unit42.paloaltonetworks.com/playful-taurus/

[4] https://securelist.com/a-targeted-attack-against-the-syrian-ministry-of-foreign-affairs/34742/

[5] https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

[6] https://www.crowdstrike.com/blog/new-supply-chain-attack-leverages-comm100-chat-installer/

[7] https://github.com/GetRektBoy724/SharpUnhooker

[8] https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool

[9] https://the.earth.li/~sgtatham/putty/0.78/htmldoc/Chapter7.html#plink

[10] https://asec.ahnlab.com/en/49089/

[11] https://www.nirsoft.net/utils/web_browser_password.html

[12] https://www.nirsoft.net/utils/network_password_recovery.html

[13] https://docs.devexpress.com/WindowsForms/15216/controls-and-libraries/pdf-viewer

[14] https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money

[15] https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

[16] https://telegra.ph/

[17] https://twitter.com/ESETresearch/status/1618960022150729728

[18] https://cert.gov.ua/article/3718487

[19] https://cert.gov.ua/article/341128

[20] https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine

[21] https://attack.mitre.org/techniques/T1027/006/

[22] https://www.notion.so/

[23] https://www.welivesecurity.com/wp-content/uploads/2023/01/eset_apt_activity_report_t32022.pdf

[24] https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/

[25] https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/

[26] https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1lj/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1lj.pdf

[27] https://nvd.nist.gov/vuln/detail/CVE-2022-27926

About ESET

For more than 30 years, *ESET®* has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit *www.eset.com* or follow us on *LinkedIn*, *Facebook*, and *Twitter*.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.