APT ACTIVITY REPORT T3 2022

SANDWORM DEPLOYING ITS ENHANCED WIPER ARSENAL

ESET Digital Security
Progress. Protected.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

CONTENTS

EXECUTIVE SUMMARY

Welcome to the T3 2022 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 September until the end of December (T3) 2022.

In the monitored timespan, Russia-aligned APT groups continued to be particularly involved in operations targeting Ukraine, deploying destructive wipers and ransomware. Among many other cases, we detected the infamous Sandworm group using a previously unknown wiper against an energy sector company in Ukraine. APT groups are usually operated by a nation-state or by state-sponsored actors; the described attack happened in October, in the same period as the Russian armed forces started launching missile strikes targeting energy infrastructure, and while we are not able to show these events were coordinated, it suggests that Sandworm and military forces of Russia have related objectives.

ESET researchers also detected a MirrorFace spearphishing campaign targeting political entities in Japan and noticed a gradual change in the targeting of some China-aligned groups – Goblin Panda started to duplicate Mustang Panda's interest in European countries. Iran-aligned groups continued to operate at a high volume – besides Israeli companies, POLONIUM also started targeting foreign subsidiaries of Israeli companies, and MuddyWater probably compromised a managed security provider. In various parts of the world, North Korea-aligned groups used old exploits to compromise cryptocurrency firms and exchanges; interestingly, Konni has expanded the repertoire of languages it uses in its decoy documents to include English, which means it might not be aiming at its usual Russian and Korean targets. Additionally, we discovered a cyberespionage group that targets high-profile government entities in Central Asia; we named it SturgeonPhisher.

ESET APT Activity Reports contain only a fraction of the cybersecurity intelligence data provided to ESET private APT reports customers. ESET prepares 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 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:

- Central Asia
- Egypt
- European Union
- Hong Kong
- Israel
- Japan
- Latvia
- Poland
- Saudi Arabia
- Serbia
- South Korea
- Tanzania
- Ukraine
- United States

Targeted business verticals:

- Blockchain-based solutions (Web3) developers
- Cryptocurrency firms and exchanges
- Defense
- Energy industry
- Engineering
- Financial services
- Gambling companies
- Logistics
- Managed security providers
- Manufacturing
- National and local governments
- Political entities
- Satellite communication companies

CN-ALIGNED ACTIVITY

Summary of China-aligned APT group activity seen by ESET Research in T3 2022

China-aligned APT groups remained very active in T3 2022.

Mustang Panda has continued to target European organizations, while Goblin Panda has been discovered targeting a government organization in the European Union. ESET researchers also uncovered a spearphishing campaign by MirrorFace targeting political entities in Japan. It seems likely that LuckyMouse compromised a gambling company in Hong Kong, by using a malicious update to legitimate software. We also found LuckyMouse samples signed with a valid code-signing certificate.

Mustang Panda

Mustang Panda continues to target European organizations. Last September, we detected a Korplug loader used by Mustang Panda at an organization in the energy and engineering sector in Switzerland. Even though we were unable to obtain the final payload, the loader is very similar to the ones used to load Hodur, which we also described in a *WeLiveSecurity blogpost* [2].

Goblin Panda

In November 2022, we discovered a new backdoor, which we named TurboSlate, in a government organization in the European Union. We attribute with medium confidence this malware to GoblinPanda. TurboSlate is deployed as a set of three files: a legitimate application from Gigabyte Technology that is vulnerable to DLL search-order hijacking, a TurboSlate loader, and encrypted shellcode containing a TurboSlate downloader (*T1574.002* [3]).

It's unusual for Goblin Panda to target European countries but this might be a change in the group's targeting, as observed with Mustang Panda in recent months.

MirrorFace

In September and October 2022, ESET researchers detected a new spearphishing campaign carried out by the APT group known as MirrorFace (*T1566.001* [4]). This campaign, which we also recently *documented on WeLiveSecurity* [5], targeted political entities in Japan with spearphishing emails containing a malicious attachment. Many of these entities had already been targeted in a previous MirrorFace campaign. The emails used specific content related to the House of Councillors election, which was *held in Japan in July 2022* [6].

The group sent targets a Virtual Hard Disk (VHD) file (*T1204.002* [7]) containing several files, including `R04-0920 人事案件_docx.exe` (machine translation: `R04-0920 Personnel matters`) and `K7AVScan.exe` (from K7 Computing Pvt Ltd), which is a legitimate binary that

MirrorFace has started using for DLL side-loading (*T1574.002* [3]). On at least two occasions, the attackers deployed a second-stage LODEINFO payload on the compromised machines. They also made use of previously undocumented malware, which we named MirrorStealer, to steal victims' credentials (*T1003* [8]).

LuckyMouse

In September 2022, a gambling company in Hong Kong was compromised via a malicious update pushed by the EsafeNet Cobra DocGuard Client (*T1195.002* [9]). This victim was compromised by LuckyMouse using the same technique in September 2021, making us believe that this new compromise is related to LuckyMouse as well. During this compromise, a new variant of the Korplug malware was discovered. It uses the magic header "ESET", which indicates that it may have been modified to try to bypass ESET products.

We also found new LuckyMouse samples on VirusTotal, including a new variant of the SysUpdate malware, a web browser password stealer (*T1555.003* [10]), and a Linux backdoor that uses DNS tunneling (*T1071.004* [11]). One of the uploaded DLLs and the browser password stealer were signed with a valid code-signing certificate from VMPSoft (*T1553.002* [12]), suggesting that LuckyMouse may have previously compromised the developer of the popular software packer VMProtect.

Pivoting on the digital certificate, we found another sample of the new SysUpdate variant on VirusTotal, signed and packed with VMProtect (*T1027.002* [13]). Therefore, it can be reasonably assumed that attackers also stole VMProtect builders when they stole the digital certificate.

IR-ALIGNED ACTIVITY

Summary of Iran-aligned APT group activity seen by ESET Research in T3 2022

Continuing with their high operational tempo, groups aligned with Iran and Iranian interests were fairly active in T3 2022.

A campaign that coincides with APT35 activity was discovered and documented to have been ongoing for several years. MuddyWater was actively targeting victims in the Middle East using compromised infrastructure and custom script-based tools. POLONIUM expanded its area of focus from Israel to Israeli companies abroad with its custom backoor, CreepyDrive. And WildPressure came back on to the scene with an update to its backdoor, Milum.

APT35

We are tracking a campaign overlapping with APT35 that began in late 2020 and has continued, on and off, since then. Initially documented by *Mandiant* [14], we recently discovered and analyzed samples packed using *ConfuserEx* [15] (*T1027* [16]), an open-source protector for .NET applications, to hide their backdoor, *NorthStarC2* [17]. This is an open-source C&C framework designed for red teams and penetration testing. The group also moved its C&C servers to new IPs.

MuddyWater

MuddyWater continues to be an active user of script-based backdoors and open-source tools. ESET researchers are tracking a new MuddyWater campaign targeting victims in Egypt and Saudi Arabia where MuddyWater is using the remote access tool *SimpleHelp* [18] and the SimpleHelp relays of a managed security provider (*T1584.006* [19]) to interactively access victims' systems. This indicates MuddyWater probably compromised a managed security provider at some point, likely to legitimize (in the eyes of defenders) their use of SimpleHelp.

Operators used SimpleHelp to drop *Ligolo* [20], a reverse tunnel long favored by MuddyWater, as well as *MiniDump* [21] (an LSASS dumper), *CredNinja* [22] (a credential dumper), and MKL64 (MuddyWater's custom credential collector (*T1555* [23])).

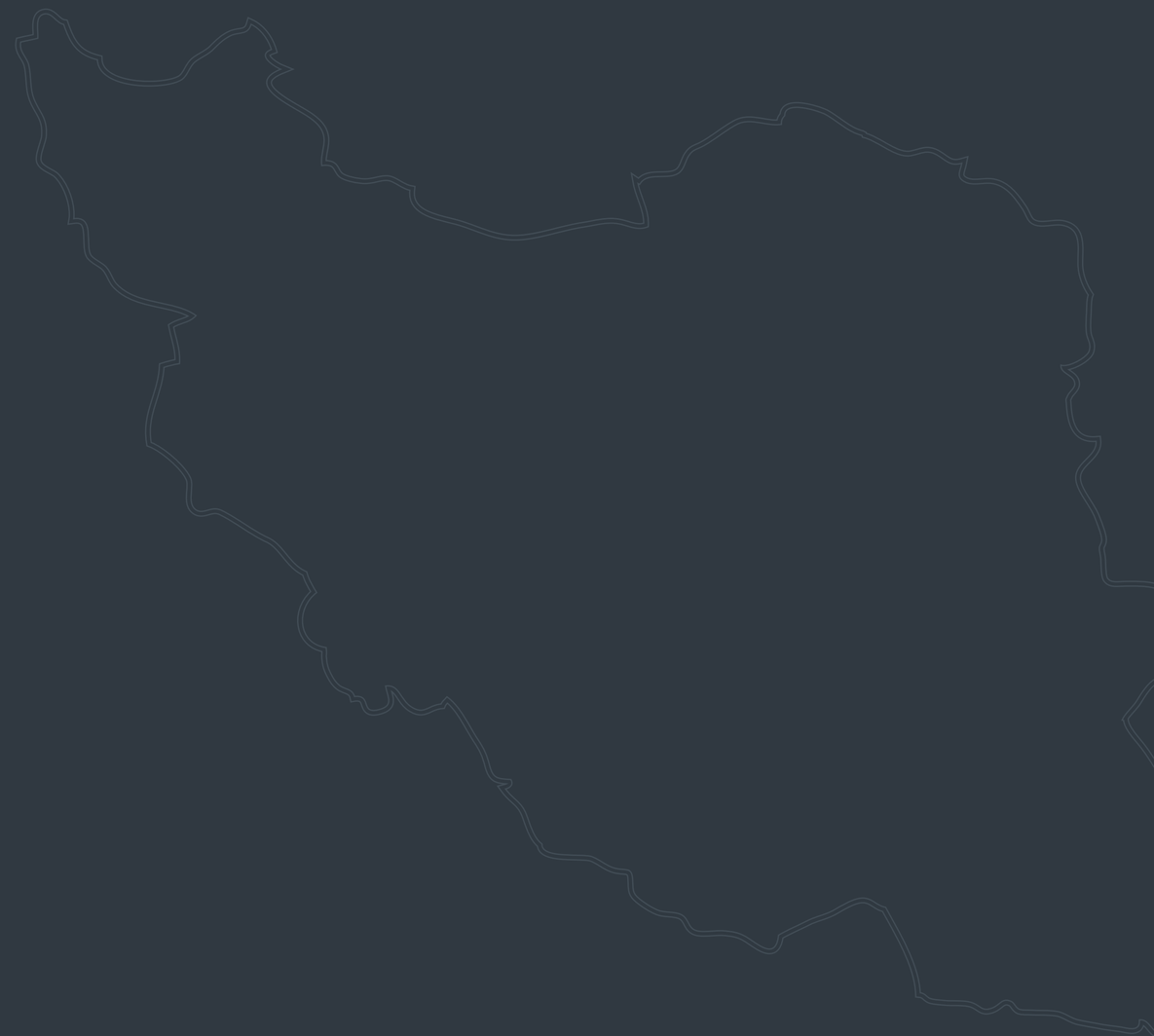
In a separate campaign, MuddyWater targeted an Israeli manufacturer with PowerShell information-gathering scripts and *Venom* [24], a multi-hop proxy for penetration testers (*T1090.003* [25]). MuddyWater operators also attempted to dump memory from LSASS using *ProcDump* [26] but was thwarted by ESET software.

POLONIUM

From mid-September through the end of November 2022, ESET researchers observed POLONIUM begin targeting an Israeli company in Serbia, a marked departure from strictly targeting victims in Israel. POLONIUM used a modified version of CreepyDrive, a custom backdoor, to execute reconnaissance commands on the victim's system and used Dropbox as a C&C (*T1567.002* [27]). POLONIUM used CreepyDrive to take screenshots every 5 seconds (*T1113* [28]), compress them into batches of 10 in a ZIP archive (*T1560.001* [29]), and upload them to Dropbox. Finally, POLONIUM used CreepyDrive to upload and execute, via PowerShell, a PuTTY binary that set up a remote tunnel to a secondary C&C server.

WildPressure

ESET researchers observed two new versions of the Milum backdoor, a custom WildPressure backdoor in use since *at least 2019* [30], deployed in the wild. The new versions maintain much of the same codebase of previous versions but, in a twist designed to evade detection, implement RC4 encryption of strings and API function calls (*T1027* [16]), as well as perform dynamic API resolution (*T1027.007* [31]). Victims were observed in Israel and align with previous WildPressure victimology.



NK-ALIGNED ACTIVITY

Summary of North Korea-aligned APT group activity seen by ESET Research in T3 2022

North Korean actors remained active in T3 2022, targeting crypto-currency firms and exchanges and continuing to use old exploits to first compromise their targets.

While the Kimsuky group continued its attacks without any significant change in its TTPs or targeting, ESET researchers saw both Lazarus and Konni use CHM files for the first time to deliver malware. CHM files are Microsoft Compiled HTML Help files (*T1218.001* [32]), consisting of HTML pages, JavaScript, images, and navigation tools.

Konni

We saw an unusual shift in Konni's targeting through the discovery of a decoy document about China's leader, written in English. Historically, Konni has mostly targeted Russians and Koreans, meaning that the decoy documents are usually in those languages. The malicious scripts used in this case have similarities with the *STIFF#BIZON campaign* [33] and were delivered through the use of CHM files, a first in our monitoring of Konni. Interestingly, the CHM file used in this campaign also contains two scanned images that comprise an invitation letter addressed to a Russian official. Considering that this letter is in Russian and that it is not displayed as part of the CHM's content, ESET researchers posit these images are remnants of an earlier campaign targeting Russian government organizations.

Lazarus

Lazarus continued employing similar tactics as were seen in Operation DreamJob, to target a financial organization in Tanzania and a Web3 developer in Latvia. The group used various VMProtect-ed payloads, including two new RATs that we decided to call BackbitingTea and SecondhandTea. The choice of names comes from the internal DLL names chosen by the developers of the RATS: `b_t_dll_x64.dll` leading to BackbitingTea and `SecondT_x64.dll` to SecondhandTea. We also saw them use webshells (*T1505.003* [34]) on compromised Java servers with interesting filenames: `wannaknow.jsp` and `wannago.jsp`. During analysis, these names stood out, reminding us of Lazarus's infamous Wannacry operation from 2017.

When we first reported on *Operation In(ter)ception back in 2020* [35], there was a clear distinction between this operation and Operation Dream Job. However, as we progress in time, this distinction becomes more and more blurred. We first noticed that there was network infrastructure overlap between the two and have now seen some cases where the malware toolset was also shared. The traditional targeting of defense and aerospace sectors for Operation In(ter)ception no longer holds as we have also seen their tools being used in campaigns with cryptocurrency platform *lures* [36].

Andariel

Finally, we covered a campaign by Andariel, using a recent RCE vulnerability (*T1190* [37]) against Confluence (*CVE-2022-26134* [38]) to compromise an organization based in South Korea. This campaign used Andariel's TigerRAT backdoor, but also a new backdoor written in Go that we named ApolonTroy, based on strings found in the malware body. We also noticed that this group uses a variety of SOCKS proxies (*T1090* [39]), including one using the publicly available *shadowsocks-go* [40] GitHub project.

RU-ALIGNED ACTIVITY

Summary of Russia-aligned APT group activity seen by ESET Research in T3 2022

Similar to T2 2022, Russia-aligned APT groups were significantly active in T3, and were involved particularly in operations targeting Ukraine. These groups include Sandworm, Callisto, Gamaredon, and the Dukes.

Callisto

Also known as COLDRIVER or SEABORGIUM, the group has been busy registering dozens of domains that are then used to conduct spearphishing attacks in order to steal webmail credentials. The size of their network infrastructure probably explains why the group recently received public attention including blogposts by *SEKOIA.IO* [41], *PwC* [42] and *Reuters* [43]. Some domains registered by the group suggest Callisto may have targeted the US satellite technology company Blue Sky Network (`blueskynetwork-shared[.]com`) and the Polish defense company UMO (`umopl-drive[.]com`).

Gamaredon

Gamaredon continues to be a prime threat to Ukrainian institutions. Typically its spearphishing campaigns, which *CERT-UA* [44] has reported on previously, use HTML smuggling (*T1027.006* [45]). When a target opens the HTML file attached to the email, it displays a dialog for downloading a RAR archive, but the archive is base64 encoded within the HTML attachment. The RAR archive contains a folder with a malicious LNK file that downloads the next stage from the C&C server and executes it using `mshta.exe`.

Interestingly, we observed email messages sent from legitimate email addresses in the format of `<number>@mail.gov.ua`. Such email accounts are normally obtained in order to contact Electronic Court in Ukraine by registering with a taxpayer ID, which is the `<number>` value in the address. More details about the process and restrictions that apply to these email addresses can be found on the following *official wiki page* [46]. Using legitimate email addresses like these for spearphishing possibly helps Gamaredon operators to bypass spam filters. Additionally, it might significantly increase their chances of tricking a victim into opening an email attachment.

During T3, the group mainly leveraged implants known as PteroCDrop, PteroLNK, and PteroPSDoor. We also found a new VBScript backdoor that we have named PteroVDoor. Interestingly, almost all PteroLNK payloads use Telegram channels to obtain the IP addresses of their C&C servers.

The Dukes

In our T2 report, we described spearphishing campaigns conducted by the Dukes (aka APT29) against government organizations in western countries. Surprisingly, the volume of these campaigns drastically dropped at the end of June 2022. It is likely that the attention they got in the past months reduced the effectiveness of those campaigns, so the Dukes decided to take a pause.

It was only in October that we found, on *VirusTotal* [47], a downloader very similar to what the group used a few months ago. The main difference is that it abused *Notion* [48], an in-the-cloud, note-taking software platform, for C&C communications (*T1102.002* [49]). We believe this downloader was aimed at fetching and executing Cobalt Strike.

Sandworm – activities related to the Russia-Ukraine war

Besides these activities, we also observed the continuation of various cyberattacks connected to the Russia-Ukraine war that we previously briefly described in the T1 and T2 ESET Threat Reports. ESET Research attributes those incidents to Sandworm.

In October, we detected a new version of CaddyWiper deployed in Ukraine. Unlike the previously used variants, this time CaddyWiper was compiled as an x64 Windows binary.

The same month we identified a new version of HermeticWiper that had been uploaded to VirusTotal[1]. The functionality of this HermeticWiper sample is the same as the previous version (see our analysis on *WeLiveSecurity* [50]), with a few minor changes (e.g., some strings are constructed on the stack instead of using their static form, some wiping functionality is done in a different order, etc.).

In addition to that, we identified a previously unknown wiper, which we named NikoWiper. This wiper was used against a company in the energy sector in Ukraine in October 2022. The NikoWiper is based on *SDelete* [51], a command line utility from Microsoft that is used for securely deleting files. This attack happened around the same period that the Russian armed forces targeted Ukrainian energy infrastructure with *missile strikes* [52]. Even if we were unable to demonstrate any coordination between those events, it suggests that both Sandworm and the Russian armed forces have the same objectives.

Besides straightforward data wiping malware, we detected Sandworm attacks using ransomware as a wiper. In those attacks, ransomware was used but the final objective was the same as for the wipers: data destruction. Contrary to traditional ransomware attacks, here the attackers do not aim to provide the key to decrypt the encrypted data.

In October 2022, we detected Prestige ransomware being deployed against logistics companies in Ukraine and Poland. This campaign was also reported by *Microsoft* [53].

In November 2022, we detected in Ukraine new ransomware written in .NET that we named RansomBoggs. The ransomware has multiple references to Monsters, Inc. We observed that malware operators used POWERGAP scripts to deploy this file coder. We publicly reported this campaign on *our Twitter account* [54].

In almost all the above-mentioned cases, Sandworm used Active Directory Group Policy (*T1484.001* [55]) to deploy its wipers and ransomware.

[1] SHA-256: A50EC84C9205116CE2515281909AB04BA6F9FD97BFFC62A4BCA366126DBCE323

OTHER NOTABLE APT ACTIVITY

SturgeonPhisher

SturgeonPhisher is a cyberespionage group that we discovered at the beginning of 2022. It mainly targets government entities in Central Asia using phishing websites mimicking official webmail portals. During T3, the group was very active with multiple phishing campaigns and a lot of a new phishing domains created. We believe that SturgeonPhisher is also the group behind a spearphishing campaign exposed by *Cyjax* [56] in 2021.

The group uses a crimeware-like toolkit including Warzone RAT, a reverse shell[2], a stealer named stink[3] available on *GitHub* [57], and a backdoor written in Rust that we named RustyRAT[4]. More recently, SturgeonPhisher started to distribute VHDX[5] disk images embedding malicious LNK files, even though *Microsoft has fixed* [58] the Mark of the Web bypass.

[2] SHA-256: 2BC366EB7759C0C7DEF2B74C2E16CEB399698250D2BE07B5317C5F4E33806E46
[3] SHA-256: DB9A6EFD5D64BA0BA1783C51B6D430873518FA032BF5265C6837C7674321E183
[4] SHA-256: 296599DF29F4FFA9BF753FF9440032D912969D0BAB6E3208AB88B350F9A83605
[5] SHA-256: B200B34F29EA4B9B6965D7B696D07AC7E72BCE49E19E3893817BBD9F15544FFE

REFERENCES

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

[2] https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[3] https://attack.mitre.org/versions/v12/techniques/T1574/002/

[4] https://attack.mitre.org/versions/v12/techniques/T1566/001/

[5] https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/

[6] https://en.wikipedia.org/wiki/2022_Japanese_House_of_Councillors_election

[7] https://attack.mitre.org/versions/v12/techniques/T1204/002/

[8] https://attack.mitre.org/versions/v12/techniques/T1003/

[9] https://attack.mitre.org/versions/v12/techniques/T1195/002/

[10] https://attack.mitre.org/versions/v12/techniques/T1555/003/

[11] https://attack.mitre.org/versions/v12/techniques/T1071/004/

[12] https://attack.mitre.org/versions/v12/techniques/T1553/002/

[13] https://attack.mitre.org/versions/v12/techniques/T1027/002/

[14] https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping

[15] https://yck1509.github.io/ConfuserEx/

[16] https://attack.mitre.org/versions/v12/techniques/T1027/

[17] https://github.com/EnginDemirbilek/NorthStarC2

[18] https://simple-help.com/

[19] https://attack.mitre.org/versions/v12/techniques/T1584/006/

[20] https://github.com/sysdream/ligolo

[21] https://github.com/cube0x0/MiniDump

[22] https://github.com/Raikia/CredNinja

[23] https://attack.mitre.org/versions/v12/techniques/T1555/

[24] https://github.com/r00t-3xp10it/venom

[25] https://attack.mitre.org/versions/v12/techniques/T1090/003/

[26] https://learn.microsoft.com/en-us/sysinternals/downloads/procdump

[27] https://attack.mitre.org/versions/v12/techniques/T1567/002/

[28] https://attack.mitre.org/versions/v12/techniques/T1113/

[29] https://attack.mitre.org/versions/v12/techniques/T1560/001/

[30] https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/

[31] https://attack.mitre.org/versions/v12/techniques/T1027/007/

[32] https://attack.mitre.org/versions/v12/techniques/T1218/001/

[33] https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

[34] https://attack.mitre.org/versions/v12/techniques/T1505/003/

[35] https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

[36] https://twitter.com/ESETresearch/status/1559553324998955010

[37] https://attack.mitre.org/versions/v12/techniques/T1190/

[38] https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

[39] https://attack.mitre.org/versions/v12/techniques/T1090/

[40] https://github.com/shadowsocks/shadowsocks-go

[41] https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/

[42] https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html

[43] https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/

[44] https://cert.gov.ua/article/971405

[45] https://attack.mitre.org/versions/v12/techniques/T1027/006/

[46] https://wiki-ccs.court.gov.ua/w/Категорія:Пошта_mail.gov.ua

[47] https://www.virustotal.com/gui/file/1CFFAF3BE725D1514C87C328CA578D5DF1A86EA3B488E9586F9DB89D992DA5C4

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

[49] https://attack.mitre.org/versions/v12/techniques/T1102/002/

[50] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[51] https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete

[52] https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities

[53] https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

[54] https://twitter.com/ESETresearch/status/1596181925663760386

[55] https://attack.mitre.org/techniques/T1484/001/

[56] https://www.cyjax.com/2021/09/16/emea-and-apac-governments-targeted-in-widespread-credential-harvesting-campaign/

[57] https://github.com/FallenAstaroth/stink

[58] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41091

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

ESET® Digital Security
Progress. Protected.