APT ACTIVITY REPORT T2 2022

AEROSPACE AND DEFENSE INDUSTRIES AMONG TARGETS

ESET Digital Security
Progress. Protected.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

CONTENTS

EXECUTIVE SUMMARY

Welcome to the inaugural 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 May until the end of August 2022 (T2 2022). Comprehensive descriptions of activities described in this document were initially provided exclusively to our premium customers, along with extensive lists of IoCs, MITRE ATT&CK techniques, YARA rules, CVEs and other information.

APT groups are usually operated by a nation-state or by state-sponsored actors. Their aim is to breach the security of governments, high-profile individuals, or strategic companies, and to evade detection in order to harvest highly confidential data. These groups possess advanced levels of expertise and substantial resources, among them techniques, tools, and exploits for zero-day vulnerabilities (vulnerabilities known to attackers and/or the affected vendors, but that have not yet been publicly disclosed or fixed).

In T2 2022, we saw no decline in APT activity of Russia-, China-, Iran-, and North Korea-aligned threat actors. Even more than seven months after the Russian invasion, Ukraine continues to be a prime target of Russia-aligned APT groups such as the infamous Sandworm, but also Gamaredon, InvisiMole, Callisto, and Turla. And speaking of defense, the aerospace and defense industries continue to be of high interest to North Korea-aligned groups, as do financial and cryptocurrency firms and exchanges. In the Middle East, organizations in or linked to the diamond industry were targeted by Agrius in what we believe was a supply-chain attack that abused an Israel-based software suite used in these verticals. On the other side of the world, we identified several campaigns by MirrorFace, a China-aligned group, with one possibly targeting the House of Councillors election in Japan.

ESET APT Activity Reports contain only a fraction of the cybersecurity intelligence data provided to our customers. ESET prepares in-depth technical reports and frequent activity updates detailing specific APT groups' activities in the form of ESET APT Reports PREMIUM. Delivering high-quality strategic, actionable, and tactical cybersecurity threat intelligence, these reports help organizations tasked with protecting citizens, critical national infrastructure, and high-value assets from criminal and nation-state-directed cyberattacks. More information about ESET APT Reports PREMIUM is available at the ***ESET Threat Intelligence offering website*** [1].

Malicious activities described in this report are detected by ESET products. Intelligence shared here is based mostly on proprietary ESET telemetry and has been verified by ESET Research.

Targeted countries and regions:

- Argentina
- Germany
- Hong Kong
- Iran
- Israel
- Japan
- Kyrgyzstan
- Netherlands
- Poland
- South Africa
- Ukraine
- United States
- Uzbekistan

- Asia
- Europe

Targeted business verticals:

- Aerospace
- Blockchain technology companies
- Branding and marketing
- Communications industry
- Cybersecurity
- Defense
- Diamond industry
- Education
- Embassies
- Engineering
- Financial services
- Information technology
- Insurance
- Law
- Manufacturing
- Media
- National and local governments
- Political entities
- Retail
- Social services
- Telecommunication

RU-ALIGNED ACTIVITY

Summary of Russia-aligned APT group activity seen by ESET Research in T2 2022

Russia-aligned APT groups were significantly active in T2 2022 and were particularly involved in operations targeting Ukraine. These groups include Sandworm, Gamaredon, InvisiMole, Callisto, and Turla.

Gamaredon

One of the most continuously active Russian APT groups, Gamaredon, continued its high level of activity targeting ***Ukrainian governmental entities*** in T1 throughout T2 2022. This group constantly modifies its tools to evade detection mechanisms. For instance, in order to evade domain-name-based blocklists, Gamaredon recently started to use a third-party service, `ip-api.com`, for resolving IP addresses of its C&C servers instead of regular DNS. In a similar manner, some Gamaredon tools use dedicated Telegram channels to get the IP addresses of their C&C servers. The group also increasingly relies on PowerShell to create its malicious toolset.

InvisiMole

Gamaredon's sporadic collaborator, InvisiMole, is also still active in targeting ***Ukrainian organizations,*** and ***diplomatic entities in Eastern Europe***. Among its common tools, such as its DNS downloader, in T2 InvisiMole started to use a new backdoor we have named PassiveMole. We also detected updated versions of Invisimole's TCP downloader tool and an updated RC2FM backdoor.

The Dukes

Government organizations in western countries were targeted by spearphishing campaigns deployed by The Dukes (aka APT29). The group continues to use HTML files to drop ISO disk images containing a LNK and other malicious files. To evade detection, the group has also started to use DLL side-loading. The final payload is Cobalt Strike, the commercial penetration testing tool, but the downloaders now fetch the final payload from cloud providers such as Slack and Google Drive instead of compromised websites. The advantage for the threat actor is that in a corporate environment these sites are less likely to be blocked or draw undue attention, compared to obscure, compromised WordPress websites or websites the malware operators set up themselves and that have little history or reputation.

Turla

Spearphishing waves, where each email had an Excel XLL add-in as an attachment, were detected in ***Poland*** where attackers sent emails about the topic of "decommunization" of Poland. We named the malicious XLL add-in SomoDrop. It drops a small JavaScript backdoor that uses compromised WordPress websites as its C&C servers. It should be noted that one of them was also used by Turla in a Kazuar sample from 2020, as reported by *McAfee/Trellix* [2]. As such, we assess with low confidence that SomoDrop is operated by Turla.

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 *ESET Threat Report T1 2022* [3]. As the war continues, so do the cyberattacks by Russia-aligned threat actors targeting various organizations.

Sandworm

In T2, Sandworm continued to be very active in this regard, using the ArguePatch loader. ArguePatch malware is a modified, legitimate binary that is used to load shellcode from an external file. A typical payload in this case would be CaddyWiper, a destructive data wiper, alongside Industroyer2. We observed Sandworm using a legitimate ESET executable as the host binary for ArguePatch's code, as described in our *Twitter thread* [4]. The ESET executable was stripped of its digital signature and some of the code overwritten. Together with CERT-UA, we identified three victims of these attacks; two of them were ***local governments in Ukraine***. In these two cases, ArguePatch was deployed via Active Directory Group Policy and ArguePatch is still being used to deploy CaddyWiper. We believe Sandworm is actively leaking information, via Telegram, stolen during CaddyWiper campaigns.

Callisto

Another group very active in T2, targeting ***Ukrainian officials and the defense industry*** with spear-phishing, was Callisto (aka ColdRiver or SEABORGIUM). It is a cyberespionage group specializing in webmail-account phishing. The group has phishing pages for common webmail services such as Gmail and Outlook, and for specific organization login pages. We believe that victims' stolen credentials are used to read confidential emails or to download files from cloud storage services.

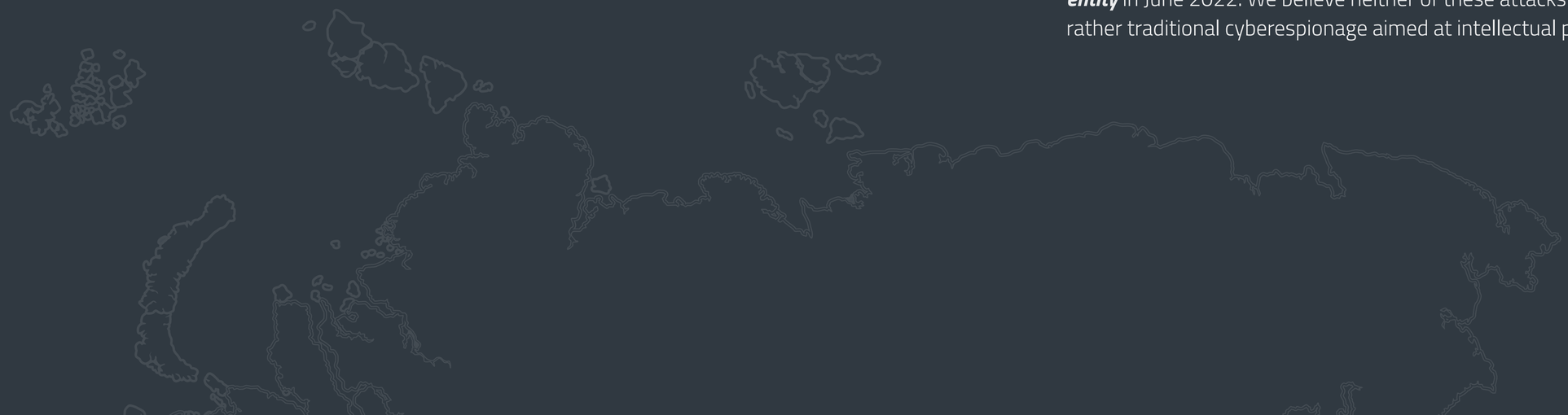
After entering authentication data, the victim is sometimes redirected to a decoy document – for instance, a PDF about cybersecurity stored on Google Drive, which is kind of ironic. It is available online on the *OODA website* [5].

Turla

As we described in the *Ransomware section* [3] of the ESET Threat Report T1 2022, the war saw a temporary influx of hacktivism attempts targeting Russia, using lock-screen variants containing, for instance, the Ukrainian national salute "Slava Ukraini!". Perhaps this was the reason why Turla decided to develop a fake DDoS Android application targeting the ***supporters of Ukraine***, first described by a researcher at *Google TAG* [6]. The malware was distributed on the attacker-controlled website `cyberazov[.]com`. As the Azov Regiment is a well-known Ukrainian military unit, it is likely that the Turla operators used this name for credibility. The app, which never was available on Google Play, claims to initiate a "DoS attack on the web servers of occupants". We also noticed that a Telegram channel named CyberAzov advertised the fake app in June; we believe it is also operated by Turla.

OTHER ACTIVITES IN UKRAINE

It is important to add that institutions in Ukraine are targeted not only by Russia-aligned threat actors. At an aerospace industry entity in Ukraine, we detected a new Mikroceen backdoor and a set of malicious tools. Previously, ESET researchers observed that same Mikroceen sample being used by a Chinese-speaking threat actor to target high-profile networks in *Central Asia* [7]. The malicious library is a new version of the Mikroceen backdoor disguised as a Windows Control Panel (CPL). Using this Mikroceen backdoor, attackers deployed the following set of tools: a file uploader, a proxy checker (DumpWeb), a fast reverse proxy tool (FRP), and a custom reverse proxy utility. Another example of a non-Russian APT group active in Ukraine is North Korea-aligned Lazarus. It targeted a ***governmental entity*** in June 2022. We believe neither of these attacks are directly linked to the current war, but rather traditional cyberespionage aimed at intellectual property theft.



CN-ALIGNED ACTIVITY

Summary of China-aligned APT group activity seen by ESET Research in T2 2022

During T2 2022, China-aligned APT groups remained very active. Among the most notable activities uncovered by our researchers are campaigns from MirrorFace, Websiic, Mustang Panda, and SparklingGoblin.

SparklingGoblin

In T2 we described further analysis of the Linux backdoor used against a ***Hong Kong university*** in February 2021, leading to the realization that it was a Linux version of SideWalk and hence that the SparklingGoblin APT group was responsible for that earlier attack. That same university was previously targeted by SparklingGoblin amidst student protests in May 2020. We found that a Linux backdoor named Specter RAT, a Linux backdoor first *documented by 360 Netlab* [8], targets IP cameras, NVR and DVR devices. In T2, we *discovered* [9] that Specter RAT is actually a Linux variant of the SideWalk backdoor. Further, we discovered a Linux userland rootkit sharing several code similarities with SideWalk. With high confidence, we believe this rootkit, which we named StealthyElf, is a part of the SparklingGoblin arsenal and most likely derived from the userland rootkit component of the Linux version of the Winnti malware *documented by Chronicle* [10]. SparklingGoblin also targeted a ***food manufacturing company in Germany***, leveraging a Confluence vulnerability (*CVE-2022-26134* [11]) and automating the initial compromise. We also think the same vulnerability helped the group get into a Confluence server of an ***engineering company based in the US***.

Activity targeting the US defense sector

A defense contractor in the US has suffered a compromise of a *Zoho ManageEngine ADSelfService Plus* [12] server, which is a web-based password management and single-sign-on product. We suspect the *CVE-2022-28810* [13] vulnerability was used in this incident. The attack was conducted only two days after the public disclosure of this vulnerability, which highlights the necessity of updating internet-facing software as soon as possible. In this compromise, the attackers relied almost exclusively on a Java webshell to conduct the intrusion. It is worth noting that the ADSelfService Plus software has been used as an initial access vector for months. The CISA advisory published in September 2021 (*AA21-259A* [14]) states that "[t]he exploitation of ManageEngine ADSelfService Plus poses a serious risk to critical infrastructure companies, U.S.-cleared defense contractors, academic institutions, and other entities that use the software". This case shows that outdated ADSelfService Plus versions are still used as an initial access vector to target high-profile targets, including US defense contractors. We found overlaps between this compromise and a group tracked by Microsoft as *DEV-0322* [15] and with an unnamed *group tracked by the FBI* [16]. However, we haven't yet found enough similarities to make a good attribution to a known group.

MirrorFace

MirrorFace continues to develop its LODEINFO backdoor and target ***organizations in Japan***. In June, we detected a new approach, where the group attempted to attack two unidentified entities in Japan utilizing a self-extracting archive that drops LODEINFO and a decoy Microsoft Word document. The threat actor sent spearphishing emails themed around job applications and the war in Ukraine. During the same month, we detected MirrorFace launching another campaign, this time targeting ***political and academic entities in Japan***. Based on the malicious attachment names and the content of the decoy documents used, we believe the campaign was carried out because of the House of Councillors election that was held on July 10, 2022.

Mustang Panda

Another group that has been very active during the monitored period is Mustang Panda. To target ***organizations in Europe and Asia in the government, education, and telecommunications sectors***, the group continues to use its *Hodur Korplug variant* [17] in combination with phishing lures connected to international events.

Websiic activity cluster

Between September and December 2021, we discovered a campaign targeting ***governmental entities in Uzbekistan and Kyrgyzstan***, which we were able to attribute in T2 to the *Websiic activity cluster* [18] (also known as ToddyCat). The campaign used a previously unreported backdoor that we have named MiniCSC. MiniCSC is a multipurpose backdoor capable of operating either in passive or active mode. Additionally, we discovered a connection between the Websiic activity cluster and an APT group named Speccom (also known as IndigoZebra): a downloader dropped from known Websiic malware had strong code similarities to malware samples associated with Speccom.

IR-ALIGNED ACTIVITY

Summary of Iran-aligned APT group activity seen by ESET Research in T2 2022

In T2, the growing number of Iran-aligned APT groups continued to target Israel and the Middle East, while also monitoring their own citizens.

POLONIUM

The cyberespionage group POLONIUM, which has been linked to Iran's Ministry of Intelligence and Security (MOIS) with an operational base in Lebanon in the past, targeted more than a dozen ***organizations in Israel***; ESET researchers *observed* [19] their activities between September 2021 and September 2022. This activity was also publicly *reported* [20] by Microsoft researchers. The numerous versions and changes POLONIUM introduced to their custom tools show a continuous and long-term effort to spy on its victims. Targeted verticals include ***engineering, information technology, law, communications, branding and marketing, media, insurance, and social services***. Some of the victims' *Fortinet VPN account credentials had leaked* [21] in September and were made available on an online forum. Since we started tracking this group, we have seen more than 10 different malicious modules. Our analysis shows that POLONIUM's toolset consists of many customized tools that abuse common cloud services and contain small components with limited functionality. We were also able to identify several backdoors that were previously undocumented – DeepCreep, MegaCreep, FlipCreep, TechnoCreep and PapaCreep.

APT35

We analyzed another campaign in Israel that targets various verticals including ***cosmetics retailing, cybersecurity holding companies, electronics manufacturing, and legal services***. This campaign, active since at least October 2021, used different versions of a backdoor we named SponsoredRunner based on the PDB path found in the samples. Interestingly, APT35 operators used a reverse tunnel during their intrusions that shares a lot of similarities to a reverse tunnel we had previously analyzed and linked to the MuddyWater APT group. This indicates there may be a connection or tool-use overlap between the two groups.

Agrius

Agrius targeted organizations in or linked to the ***diamond industry in South Africa, Hong Kong, and Israel***. We believe the group conducted a supply-chain attack abusing an Israeli-based software suite used in this vertical. This campaign deployed a wiper we have named Fantasy, which is built on the foundations of faux ransomware Apostle.

APT-C-50

We also *discovered* [22] a new version of the Android malware called FurBall that has been used in a Domestic Kitten campaign conducted by the APT-C-50 group. The Domestic Kitten campaign is known to conduct mobile surveillance operations against ***Iranian citizens*** and this new FurBall

version is no different in its targeting. The malware was distributed via a copycat of an Iranian website that provides articles, journals, and books translated from English to Persian. This malicious app was never available from the Google Play store and must be downloaded directly from the attacker's server, where the app has been available since at least June 2021. The samples we analyzed have only limited spying functionality enabled. They request only one intrusive permission – to access contacts – most likely to stay under the radar and to avoid attracting the suspicion of potential victims during the installation process. This might be the first stage of the attack, gathering information about compromised systems before deploying more capabilities if necessary. This falls in line with Iran-aligned groups, where some (TortoiseShell, SilentLibrarians, and APT-C-50) perform information gathering that is likely shared with other Iran-aligned groups.

OilRig

OilRig continues to use its SampleCheck5000 (SC5K) downloader (previously described in our private threat intelligence reporting), malware whose purpose is to download and execute additional OilRig tools using the Office Exchange Web Services API. ESET researchers analyzed a campaign against a ***governmental institution in Israel*** where a new version of this tool was deployed, along with other OilRig tools. SC5K logs into a remote Exchange server, iterates through email messages in the "Drafts" folder and extracts additional payloads from their attachments. The new version is now modular and depends on external modules to specify the Office 365 account used for malware distribution. This makes the retrieval and analysis of SC5K's malicious payloads harder. Furthermore, we discovered a previously unknown backdoor deployed against the same organization. The new backdoor, which we named OilBooster, is a C/C++ binary with statically linked OpenSSL and Boost libraries (hence the name), and is notable because it uses the Microsoft OneDrive API for C&C communications, which is in line with previous OilRig TTPs.

NK-ALIGNED ACTIVITY

Summary of North Korea-aligned APT group activity seen by ESET Research in T2 2022

North Korea-aligned APT groups remain very active: our research during T2 2022 shows these groups mainly focused on their usual targets such as the aerospace and defense industry, financial institutions, and cryptocurrency firms and exchanges.

Lazarus

A Lazarus campaign targeting an employee of an ***aerospace company in the Netherlands*** started with spearphishing emails containing malicious Amazon-themed documents. The employee was contacted via LinkedIn Messaging about a potential new job, resulting in an email with a document attachment being sent. The most notable tool delivered by the attackers was a user-mode module that gained the ability to read and write kernel memory due to the *CVE-2021-21551* [23] vulnerability in a legitimate Dell driver. This was the first ever recorded abuse of this vulnerability in-the-wild. The attackers then used their kernel memory write access to disable seven mechanisms in the Windows operating system, such as event tracing. This effectively blinds security solutions in a very generic and robust way. More technical details about this campaign were extracted from our private reporting and published in our *WeLiveSecurity blogpost* [24] and presented at the *Virus Bulletin conference* [25] in September.

In July, ESET researchers detected that Lazarus and its DangerousPassword campaign attempted to infiltrate the network of a ***blockchain technology company in Israel***. During the same month, the Lazarus campaign dubbed by ESET researchers as Operation In(ter)ception targeted a person from ***Argentina*** with malware disguised as a fake job offer at Coinbase, a company that operates a cryptocurrency exchange platform. This is the first time in our tracking that Operation In(ter)ception targeted a vertical other than ***aerospace and defense***. The attackers sent a macOS variant to the victim first, but that was a mistake since the victim's computer was a Windows system. The macOS payload was very similar to the one we *tweeted about* [26] in May.

Kimsuky

ESET researchers also detected that a ***financial services company based in Hong Kong*** was targeted by Kimsuky in June. It is most likely that the threat actor compromised the network via a vulnerable Microsoft Internet Information Services (IIS) server deployed on one of the machines. The attack was part of a long-running campaign belonging to the BabyShark cluster.

Konni

Konni continues to target the ***diplomatic vertical***, this time by using a trojanized version of Sumatra PDF viewer. This is not the first time we have seen North Korea-aligned groups use a trojanized version of this open-source PDF viewer; in fact Lazarus also has employed this technique in the past. A bogus PDF file is sent along with this PDF viewer. The target is then lured into launching the trojanized software, which will show a decoy document, but also install malware onto the system.

CONCLUSION

This report describes numerous campaigns and activities that are oftentimes directed at different governmental bodies and state-owned companies. However, entities and individuals working within other mentioned targeted profiles should also maintain a heightened state of awareness. Several cases in this report clearly show that acquired technology is not the only type of protection that should be deployed, but that organizations must also increase the overall cybersecurity awareness of their employees. A special area of focus here should be on spearphishing, as this is one of the most used initial compromise vectors seen in the described activities.

Many other campaigns are focused on credential stealing, where threat actors utilize phishing pages for common webmail services or even cloned login pages of specific organizations. If the targeted organizations had deployed multifactor authentication, they would have made it much harder for the attackers to infiltrate their network.

It is also important to remember that these APT groups largely conduct targeted operations. They don't focus only on the most used operating systems and applications; instead, they also actively develop and deploy malicious tools even for macOS and Linux devices if required. There is no "one solution for all cybersecurity risks" and each entity needs to take an individual approach, especially if the vertical within which it works is interesting enough to be targeted by these threat actors. Lastly, the case of the US defense contractor is a reminder of how fast organizations must act after the public disclosure of a vulnerability.

More actionable data on how to safeguard your organization and systems against threats described in this report is available in the ***ESET APT Reports PREMIUM*** [1] service that regularly delivers ongoing activity summaries and in-depth technical analyses, complete with extensive IoCs, to our ESET Threat Intelligence customers.

REFERENCES

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

[2] https://kcm.trellix.com/corporate/index?page=content&id=KB93391&locale=en_US

[3] https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

[4] https://twitter.com/ESETresearch/status/1527531726905409536

[5] https://www.oodaloop.com/archive/2021/06/14/cybersecurity-like-espionage-is-an-infinite-game/

[6] https://twitter.com/billyleonard/status/1545461166377508865

[7] https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/

[8] https://blog.netlab.360.com/ghost-in-action-the-specter-botnet/

[9] https://www.welivesecurity.com/2022/09/14/you-never-walk-alone-sidewalk-backdoor-linux-variant/

[10] https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

[12] https://www.manageengine.com/products/self-service-password/

[13] https://www.manageengine.com/products/self-service-password/advisory/CVE-2022-28810.html

[14] https://www.cisa.gov/uscert/ncas/alerts/aa21-259a

[15] https://www.microsoft.com/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/

[16] https://www.ic3.gov/Media/News/2021/211220.pdf

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

[18] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[19] https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/

[20] https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

[21] https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

[22] https://www.welivesecurity.com/2022/10/20/domestic-kitten-campaign-spying-iranian-citizens-furball-malware/

[23] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21551

[24] https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/

[25] https://www.virusbulletin.com/conference/vb2022/abstracts/lazarus-byovd-evil-windows-core/

[26] https://twitter.com/ESETresearch/status/1521735320852643840

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.