Kaspersky ICS CERT

kaspersky

APT and financial attacks on industrial organizations in Q2 2025

04.09.2025

Version 1.0

Contents

This summary provides an overview of reports on APT and financial attacks on industrial enterprises disclosed in Q2 2025, as well as the related activities of groups observed attacking industrial organizations and critical infrastructure facilities. For each topic, we summarize the key facts, findings and conclusions of researchers that we believe may be of use to professionals addressing practical issues of cybersecurity in industrial enterprises.

Executive summary

Some sophisticated tactics and techniques were reported this quarter in attacks targeting industrial organizations. Nobody is surprised to see 0-day vulnerability exploits being used by APTs in the wild: Lazarus used 0-days in South Korean software in their local campaigns, Stealth Falcon attempted to use a 0-day vulnerability in a legitimate tool by Microsoft against a major defense company in Turkey, and Sednit sent spear-phishing emails exploiting a 0-day XSS vulnerability in MDaemon Email Server to their targets among defense companies. No doubt the most sophisticated case was reported by Kaspersky, where the actors were caught targeting Russian high-profile organizations through update files for the ViPNet cybersecurity solution.

Besides exploiting 0-day vulnerabilities, sophisticated actors also used other non-trivial techniques, such as spreading from a compromised organization to its peers with hijacked emails (BEC attack), including what Cloud Atlas reported to be doing when targeting high profile organizations in Russia.

But this level of sophistication isn't needed to make it in the OT environment (as the regular statistical report by our team shows). This fact was illustrated by a pro-Iranian group that by initiating their attacks with stolen credentials for SSL VPN systems, or hosting web shells on publicly accessible servers, managed to get a foothold in the restricted network segment hosting OT-related systems of at least one of its critical national infrastructure victims in the Middle East.

The need for industrial enterprises to always take care of basic cybersecurity measures was further emphasized by a few other cases.

At least 65 organizations from the governmental, IT, industrial, and logistics sectors fell victim to attacks that injected malicious code into their Microsoft Exchange Servers, thus showcasing that four years is still not enough for patching server-side vulnerabilities such as ProxyShell.

Some high-profile organizations, including governments, universities, and even some major global corporations showcased that ignoring cybersecurity basics

such as keeping track of discontinued corporate resources inevitably leads to cybersecurity incidents.

Many actors, including the ones who attacked global and Middle Eastern targets in multiple sectors (transportation, utilities, energy, finance and government) with ClickFix phishing campaigns, reminds industrial organizations that teaching personal cybersecurity hygiene is a must-have corporate budget item.

To wrap up our summary, we must admit that the report released by Kaspersky researchers on activities by Cyber Partisans that switched to finding new targets in Russia has become an unintended forecast for major future incidents.

Targets in Russia

GOFFEE attacks

Kaspersky researchers reported on GOFFEE (aka Paper Werewolf), a threat actor that appeared in early 2022. Since then, it has continued its malicious activities targeting exclusively entities in Russia, leveraging spear-phishing emails containing a malicious attachment. Starting in May 2022 and up until summer of 2023, GOFFEE deployed a modified Owowa (malicious IIS module) aimed at stealing credentials and enabling remote command execution from OWA.

Kaspersky first documented Owowa in late 2021. Since 2020, it had been deployed primarily in Asia. At that time, researchers showed that Owowa may have been developed by a Chinese-speaking individual. Later, it was discovered that starting in May 2022, an updated variant was uniquely used against targets in Russia. Kaspersky researchers were later able to link the deployment of Owowa with an email-based intrusion chain that mimicked known Cloud Atlas activity.

As of 2024, GOFFEE started to deploy patched malicious instances of explorer.exe via spear phishing. During the second half of 2024, GOFFEE continued to launch targeted attacks against organizations in Russia, utilizing PowerTaskel, a non-public modification of the Mythic agent, and introducing a new implant dubbed PowerModul. The targeted sectors included media and telecommunications, construction, government entities, and energy companies.

Cloud Atlas attacks

Positive Technologies researchers reported new Cloud Atlas group attacks targeting Russian military-industrial complex companies with updated network infrastructure, which were identified during an investigation of an incident at one

of the enterprises in November 2024. The malicious files associated with the new infrastructure used in cyberattacks appeared in early January 2025, while the servers, domain names, TLS certificates and necessary DNS records were registered and appeared on the network in late October to early November 2024.

The malicious Microsoft Office documents contained a C2 server in the 1Table stream of the document, which is a characteristic Cloud Atlas technique. PT researchers previously described that opening these documents leads to the execution of malicious VB scripts written in alternate data streams that interact with the Google Sheets API to transmit information about the infected system and download the PowerShower backdoor, followed by the exfiltration of stolen data to cloud storage. The malicious documents observed in the new wave of attacks spanned topics including an invitation to advanced training courses, documents related to anti-corruption checks and mobilization activities, certificates regarding employees, and CVs of CNC machine operators. The phishing documents were most likely stolen by the group from the networks of previously infected enterprises. Researchers revealed the use of compromised emails of previously infected Russian defense industry enterprises to send malicious documents to counterparties in so-called BEC attacks.

FakeTicketer attacks/Operation HollowQuill

Seqrite Labs researchers reported the discovery of a cyber-espionage campaign dubbed Operation HollowQuill targeting Russian industrial enterprises. The threat entity delivers a malicious RAR file containing a .NET malware dropper, which further drops another Golang-based shellcode loader along with the legitimate OneDrive application and a decoy-based PDF with a final Cobalt Strike payload. The lure document relates to the Ministry of Science and Higher Education of Russia, specifically concerning Baltic State Technical University "VOENMEKH" named after D.F. Ustinov. The document appears to be an official communication addressed to multiple organizations, potentially discussing state-assigned research projects or defense-related academic collaborations. The observed targets included academic and research institutions, and military and defense industry, aerospace and missile technology, and government-oriented research entities.

F6 researchers identified unique artifacts that link the HollowQuill campaign to the already known FakeTicketer group. The activity described by Seqrite Labs researchers was first detected by Positive Technologies researchers at the end of 2024, and additional analysis allowed F6 to establish intersections with the activities of the FakeTicketer group. According to F6, the attackers have been active since at least June 2024, their main motivation presumably being

espionage, with industrial organizations, government agencies, and sports functionaries among the targets. Analysis of the malware and attacker infrastructure revealed that the HollowQuill campaign and FakeTicketer have overlapping dropper code and domain naming. Both droppers, LazyOneLoader (from Operation HollowQuill) and Zagrebator.Dropper (from earlier operations), are written in C#, use the same icon names (faylyk), and have similar file and class naming, store dropper files, and the icon in resources. In both cases, the OneDrive*.exe and OneDrive*.lnk files are used to hide activity, and the droppers' code for creating shortcuts is almost identical.

Attacks impersonating a ViPNet update

In April 2025, Kaspersky researchers identified a sophisticated APT campaign by an unknown actor. Over the course of the campaign, attackers had been infecting machines of high-profile organizations in Russia through update files for ViPNet software. These updates include a loader executable msinfo32.exe designed to read the encrypted payload file. The loader processes the contents of the file to load the backdoor into memory. This backdoor is versatile: it can connect to a C2 server via TCP, allowing the attacker to steal files from infected computers and launch additional malicious components, among other things. On April 18, ViPNet solution developer confirmed an incident involving a sophisticated targeted attack on a number of clients and released product updates and recommendations.

Sapphire Werewolf attacks

BI.ZONE researchers reported new activity of Sapphire Werewolf using an updated version of Amethyst Stealer. The attackers continue to deliver malware via phishing emails, this time targeting fuel and energy companies in Russia. Sapphire Werewolf disguises a malicious attachment as a memo and sends it to the victim on behalf of the HR department. The email contains an archive named Memo.rar, which contains an executable file of the same name with a PDF document icon. The malicious file is a .NET downloader written in C# and protected by .NET Reactor. It contains a Base64 encoded payload, Amethyst Stealer, which is also protected by .NET Reactor. The functions of Amethyst Stealer include exfiltration of authentication data from Telegram, Chrome, Opera, Yandex, Brave, Orbitum, Atom, Kometa, Edge Chromium, FileZilla and SSH configuration files, the exfiltration of various configuration files of remote desktops and VPN clients, and the exfiltration of various types of documents (including from external media).

Librarian Ghouls attacks

Kaspersky researchers reported on activities of the Librarian Ghouls group. Librarian Ghouls (aka Rare Werewolf, Rezet) is an APT actor focused on conducting targeted cyber-espionage attacks against organizations located in Russia and Central Asia. It uses spear phishing as the primary infection vector, with the discovered phishing emails containing malicious password-protected archives. A malicious implant from an archive is disguised as a payment order. This sample is a self-extracting installer created using the Smart Install Maker utility for Windows. When launched, it deploys legitimate utilities, such as AnyDesk and Blat that are further used by attackers to exfiltrate sensitive data. Apart from these utilities, attackers also deploy the XMRig cryptocurrency miner to infected machines. Kaspersky researchers also believe, with a low level of confidence, that the Librarian Ghouls actor uses phishing webpages for credential theft. These webpages have been found to impersonate the mail.ru email provider. According to Kaspersky telemetry, infection attempts conducted by Librarian Ghouls have been observed in more than a hundred industrial and academic organizations in Russia. Several attempted infections in organizations in Belarus and Kazakhstan were also observed.

Silent Werewolf attacks

BI.ZONE researchers discovered new campaigns from the Silent Werewolf cluster targeting organizations in Russia and Moldova. BI.ZONE detected two waves of attacks: the first was aimed exclusively at Russian organizations in the energy (nuclear industry), tool making, aircraft manufacturing, and mechanical engineering sectors. The attackers used phishing emails disguised as a pre-trial claim and a residential construction project that contained a link to download a ZIP archive. The ZIP archive contained two files: LNK and another ZIP archive with a legitimate EXE file, a malicious library (C# loader), and a distracting PDF document. The loader is a DLL file launched using the legitimate executable file H5GDXM70NJ.exe (DeviceMetadataWizard.exe) using the DLL sideloading technique. The loader is designed to download a malicious payload from the attacker's server, attach it to the host in the system startup, and open the distracting PDF document. The payload was unavailable at the time of the study, but a retrospective analysis of similar Silent Werewolf attacks shows that XDigo was most likely used as the payload.

The second wave of attacks mainly targeted Moldovan companies, with possible expansion to Russian ones. The new version of the loader was distributed under the guise of a schedule for service pass exchange and recommendations for protecting the company's information infrastructure from ransomware attacks.

As in the previous campaign, the attack was presumably carried out using phishing emails with a link to download an archive.

PhantomCore attacks

F6 researchers reported new attacks of the PhantomCore group (aka Head Mare) in May 2025, as well as previously unknown group activity dating back to 2022. According to researchers, the tools and targets of attacks have changed over time: at first it was data theft and damage and destruction of data, then by 2024 the focus shifted to encrypting victim infrastructures for ransom.

Researchers were able to find unique intersections in domain registration data when studying the PhantomCore infrastructure, which made it possible to identify additional domains and related samples dating back to 2022. According to F6, in 2022, PhantomCore distributed the VALIDATOR.msi dropper with StatRAT malware and a decoy executable file that mimicked the legitimate software Validator 1.0, which performs network verification for compliance with a specific federal law. In addition to processing various commands from the C2 server, the StatRAT malware has a stealer module and wiping features.

In 2025, PhantomCore continued to refine its tools and rewrite them using various programming languages. On May 5, F6 detected and blocked malicious mailings that were attributed to PhantomCore. Among the recipients were industrial organizations and energy and utility companies. The emails contained an attached executable file in the form of an archive with the name "Документы_на_рассмотрение.zip" ("Documents_for_consideration.zip"). The file "Сопроводительное_письмо.pdf" ("Cover_letter.pdf") was used as PDF bait, which was a contract for the supply of materials and equipment between two commercial companies. The malicious executable file was an updated version of the PhantomCore group's backdoor called PhantomeCore.GreqBackdoor v.2 written in Golang without obfuscation.

Fairy Wolf attacks

BI.ZONE researchers discovered a Fairy Wolf (aka Unicorn) campaign using a new distribution vector through the Telegram messenger. The attackers did not pose as a CEO or accountant, as they had done before. Instead, they offered financial assistance for participating in a corrupt scheme. The attackers sent a document with detailed instructions named “Условия работы.rar” ("Working conditions.rar") containing an HTML Application file "Document.hta", which was a Unicorn stealer dropper. The Unicorn stealer collected files under 100 MB with various extensions. The stealer also extracted the contents of the %APPDATA%\Telegram Desktop\tdata folder and credentials from browsers.

According to BI.ZONE, Fairy Wolf performed more than 10 attacks involving the distribution of the Unicorn stealer in May, targeting Russian energy companies, as well as organizations in heavy industry and the military-industrial complex. The attackers used a variety of disguises to distribute malware, pretending to be specialist resumes, reports, contracts, documents with working conditions, and more.

Vengeful Wolf/room155 attacks

F6 researchers reported the activities of the room155 group (aka DarkGaboon or Vengeful Wolf), which was first reported in January 2025 by Positive Technologies researchers. The attackers were implementing attacks on Russian companies and sending phishing emails with a malicious archive as an attachment. In known incidents, either Revenge RAT or XWorm was distributed through email. During their research, F6 also identified other malware samples in the attackers' arsenal: Stealerium, DarkTrack, DCRat, AveMaria RAT, and VenomRAT. Samples of different malware families were found on the same devices and used the same domains as C2.

The attackers sign malware with fake X.509 certificates and use homoglyphs in the names of executable files, email subjects, and attachment names. The group also recently started using double extensions for executable files (.pdf.scr, .pdf.exe, .xsl.scr, .xlsx.scr) and continue to use different icons for them (MS Office and PDF). During the recent campaign, the attackers alternately used the Themida and .NET Reactor protectors. In addition, an obfuscated .NET megadropper was used, which extracts 4 saved packed resources from itself, each corresponding to a separate payload. Throughout their activity, the attackers used Dynamic DNS domains, which formed two non-overlapping clusters: the first from December 2022 to mid-2023, and the second from mid-2023 to present. An analysis of room155 victimology helped researchers identify the main targets: financial organizations (51%). Further down the list are companies in the transport sector (16%), retail (10%), industry and logistics (7% each), construction and housing and communal services (3%), medicine, tourism and IT (2% each). The ultimate goal of the attackers is to encrypt the victim's systems using LockBit 3.0 and then demand a ransom for decryption. The group does not have its own DLS website.

Werewolves attacks

F6 researchers discovered a new wave of malicious mailings initiated by the Werewolves group and mimicking fake pre-trial claims with malicious attachments on behalf of a special equipment plant, recreation center, and electrical equipment manufacturer. Werewolves is a ransomware group that has

been active since 2023 and uses Anydesk, Netscan, CobaltStrike, Meterpreter, and Lockbit. The group employs a traditional double extortion technique.

In spring 2025, F6 researchers detected a malicious mailing to companies in various sectors, including banks, industrial enterprises, and retail and logistics companies. Then in June, the attackers again sent out emails, this time to industrial, financial, energy organizations and retailers. To deliver malware, the attackers send legal and financial-related emails. The group continued to use the same tools as in previous attacks. The following topics were used as subjects in the June mailings: "Pre-trial claim", "Pre-trial", and "Notification (pre-trial)". The attachment contained an archive with an LNK file with a double .pdf.lnk extension, and a Microsoft Office document for exploiting the CVE-2017-11882 vulnerability. The attackers continue to use the same domain to send emails as in previous mailings: kzst45[.]ru, mimicking the website of a Russian manufacturer of special equipment. Recent attacks used a new domain, mysterykamchatka[.]ru, which mimics a legitimate .com website. The attackers continued to use spoofing in their mailings: in one of the emails, the group replaced the sender's address to send an email on behalf of the chief accountant of a Russian airport. The final payload was Cobalt Strike's Beacon.

BO Team attacks

Kaspersky researchers analyzed the activities of pro-Ukrainian hacktivist group BO Team (aka Black Owl, Lifting Zmiy and Hoody Hyena), which targets Russian companies. In addition to causing damage to the victims, the group aims to obtain financial gain. The BO Team group first made itself known in early 2024 through a Telegram channel where it outlined its position regarding the Russia-Ukraine conflict. The attackers use phishing emails with malicious attachments that implement an infection chain with a payload in the form of backdoors: DarkGate, BrockenDoor and Remcos. The group impersonated a real company that specializes in the automation of technological processes, thereby creating a plausible context for contacting potential victims in the government, technology and energy sectors. To disguise the sender, fake domains are used mimicking the domains of legitimate companies. After gaining initial access to target systems, the BO Team attackers use the Living-off-the-Land (LoTL) technique using PowerShell and WMI. To ensure constant access to the compromised infrastructure, BO Team uses a number of persistence techniques, one of which is the creation of scheduled tasks in the Windows operating system. The attackers use previously compromised accounts belonging to the organization's full-time employees to escalate privileges. In some cases, access was achieved using remote connection protocols and tools (RDP, SSH or VPN). After compromising the target systems, BO Team methodically destroys backup

copies of files and the company's virtual infrastructure, and deletes data from the hosts using the SDelete utility. In some cases, the attackers additionally use the Babuk ransomware for Windows, subsequently making ransom demands.

Russian-speaking activity

Void Blizzard attacks

Microsoft Threat Intelligence Center identified a global cluster of cloud abuse activity attributed to the Void Blizzard (also known as LAUNDRY BEAR) threat actor. Void Blizzard's cyber-espionage operations are highly targeted, focusing on specific organizations in various sectors, including government, defense industrial base, transportation, media, non-governmental organizations (NGOs), and healthcare, primarily in Europe and North America. The threat actor typically uses stolen credentials, likely obtained from commodity infostealer ecosystems, to collect a large volume of emails and files from compromised organizations. In a recent evolution, Microsoft Threat Intelligence observed Void Blizzard adopting more direct tactics to steal passwords starting in April 2025, such as sending phishing emails designed to trick users into divulging their login credentials. In a small number of Void Blizzard compromises, Microsoft Threat Intelligence also observed the threat actor accessing Microsoft Teams conversations and messages via the Microsoft Teams web client application.

PathWiper attacks

Researchers from Cisco's Talos Intelligence detected previously unknown wiper malware dubbed PathWiper that was used to conduct an attack against a Ukrainian critical infrastructure entity, destroying data on targeted systems. The attack was instrumented via a legitimate endpoint administration framework (indicating that the attackers likely had access to the administrative console) that was then used to issue malicious commands and deploy PathWiper across connected endpoints. Throughout the course of the attack, the filenames and actions used were intended to mimic those deployed by the administrative utility's console, indicating that the attackers had prior knowledge of the console and possibly its functionality within the victim enterprise's environment.

PathWiper bears similarities to HermeticWiper, a destructive tool deployed against Ukrainian targets. HermeticWiper, also known as FoxBlade, was attributed to the Sandworm group in third-party reporting with medium to high confidence. Unlike HermeticWiper, which blindly scans for and destroys data

across all drives, PathWiper operates more selectively, identifying and validating drives before executing the data-wiping process.

Sandworm attacks

In October 2024, ESET researchers detected Sandworm activity at several energy companies in Ukraine. In at least one case, ESET observed that Sandworm used a remote monitoring and management (RMM) tool, specifically Atera Agent, in the early stages of the compromise. Sandworm has intensified its operations involving data-wiping malware over the past six months. In December 2024, and again in February and March 2025, Sandworm deployed a new wiper named ZEROLOT against different organizations in Ukraine. In all cases, the attackers used Active Directory Group Policy to deploy the wiper to computers in the affected organizations. Once executed, ZEROLOT wipes all files in the C:\Users\ subdirectory and from the root on all logical drives except C:, skipping files with .dll, .exe, and .sys extensions. It uses fsutil.exe to overwrite file data and then deletes the files. Additionally, it deletes physical drive layouts using the DeviceIoControl Windows API.

Sednit attacks

According to ESET researchers, Sednit's (aka APT28, Fancy Bear and Sofacy) Operation RoundPress campaign has broadened its scope to include several other webmail services such as Horde, MDaemon, and Zimbra, in addition to Roundcube. The attackers behind Operation RoundPress have been sending spear-phishing emails containing XSS exploits, typically targeting vulnerabilities that have already been addressed by the vendor. The exploits lead to the execution of malicious JavaScript code within the context of the webmail client web page running in a browser window. Researchers identified several JavaScript payloads, such as SpyPress.HORDE, SpyPress.MDAEMON, SpyPress.ROUNDCUBE, and SpyPress.ZIMBRA. Most of these SpyPress payloads collect email messages and contact information from the victim's mailbox when a malicious email is received or viewed in a vulnerable webmail client. The data is then exfiltrated to a C&C server.

ESET detected several Sednit campaigns against defense companies in Bulgaria and Ukraine. For example, in November 2024, the researcher detected a spear-phishing email targeting a Bulgarian company. The email was sent from a compromised email address with the subject Путин се стреми Тръмп да приеме руските условия вдвустранните отношения (machine translation: Putin seeks Trump's acceptance of Russian conditions in bilateral relations). The message body contained excerpts (in Bulgarian) and links to articles from News.bg, a legitimate Bulgarian newspaper. On November 1, 2024, ESET

detected spear phishing emails targeting Ukrainian companies. These emails exploited a zero-day XSS vulnerability in MDaemon Email Server, specifically in the rendering of untrusted HTML code in email messages. ESET reported the vulnerability to the developers on November 1, 2024, and it was patched in version 25.4.1, which was released on November 14, 2024. Researchers issued CVE-2024-11182 for this vulnerability.

East Asia

Operation SyncHole

Kaspersky researchers have been tracking the campaign by the Lazarus group since last November. It targets organizations in South Korea with a sophisticated combination of a watering hole strategy and vulnerability exploitation within South Korean software Cross Ex and Innorix Agent. The campaign, dubbed Operation SyncHole, has impacted at least six organizations in South Korea's software, IT, financial, semiconductor manufacturing, and telecommunications industries.

In the earliest attack case, the actor leveraged a variant of ThreatNeedle, a variant of Agamemnon Downloader, and a variant of wAgent. The execution chains in the subsequent cases were fully updated, utilizing the SIGNBT and COPPERHEDGE malware instead. The SIGNBT has been recognized as the updated 1.2 version, with key improvements focused on the loader's capability to load additional malware. COPPERHEDGE, a malware named by CISA in 2020 and historically associated with the DeathNote cluster, also demonstrated enhanced features in some of its commands.

During further investigation, a number of commands were executed by the actor through the COPPERHEDGE backdoor to conduct reconnaissance on the victim organization. The actor primarily executed native Windows commands through the cmd.exe process, and at times also mistakenly entered certain commands. This indicates that the actor is still performing reconnaissance manually to identify targets. Based on their activities observed throughout the campaign, Kaspersky researchers were able to track their operational hours. Most of the activities suggest that the actor is in the GMT+9 time zone in regards to typical business hours.

Swan Vector attacks

Seqrite Labs APT-Team uncovered a campaign dubbed Swan Vector active since December 2024 and targeting Taiwan and Japan. The campaign is aimed at

educational institutes and the mechanical engineering industry. Intrusions commenced with the distribution of spear-phishing emails delivering fake resumes of candidates acting as a decoy. They also contain a malicious ZIP file containing an LNK file, which downloads an executable that triggers the Pterois DLL implant. After leveraging dynamic API resolution and covertly loading the appropriate library functions, Pterois then uses Google Drive as a C2 server and authenticates using OAuth credentials for further payload retrieval before proceeding with self-deletion. Further DLL sideloading then enables the execution of the Isurus implant that performs API resolution and encrypted Cobalt Strike shellcode execution before deploying the Cobalt Strike beacon. Swan Vector was also noted by researchers to employ tactics similar to the APT10, Lazarus, and Winnti threat operations.

Chinese-speaking activity

Billbug/Lotus Panda attacks

Symantec researchers reported a new campaign by the Chinese-speaking Billbug group (aka Lotus Blossom, Lotus Panda, Bronze Elgin) that targeted a number of companies in an unnamed Southeast Asian country between August 2024 and February 2025. The targets included a ministry, air traffic control organization, telecom operator, and construction company. One of the targets was a news agency located in another Southeast Asian country, and an air freight organization located in another neighboring country. The threat cluster is a continuation of a campaign that the researchers reported back in December 2024 as a large-scale attack cluster in Southeast Asia that had been ongoing since at least October 2023. The group has been active since 2009, but first came into the spotlight in June 2015, when Palo Alto attributed it to a spear-phishing campaign that exploited a Microsoft Office vulnerability (CVE-2012-0158) to distribute the Elise (Trensil) backdoor, designed to execute commands and manipulate files.

In February, Cisco Talos linked Lotus Panda to attacks targeting government, manufacturing, telecommunications, and media sectors in the Philippines, Vietnam, Hong Kong, and Taiwan using a backdoor known as Sagerunex. In the latest wave of attacks observed by Symantec, the attackers used legitimate Trend Micro (tmdbglog.exe) and Bitdefender (bds.exe) executables to sideload malicious DLLs, which were used as loaders to decrypt and launch a next-stage payload embedded in a locally stored file. The Bitdefender binary was also used to sideload another DLL, which was not retrieved. The attackers used an updated version of Sagerunex, a tool used exclusively by Lotus Panda. It has the

ability to collect information about the target host, encrypt it, and transmit it to an external server of the attacker. The attacks also involved a reverse SSH tool and two stealers, ChromeKatz and CredentialKatz, which are capable of intercepting passwords and cookies stored in Google Chrome. The attackers deployed the publicly available Zrok tool, using the tool's sharing feature to provide remote access to services that were exposed inside. They also used another legitimate tool called datechanger.exe, which is capable of changing file timestamps.

Earth Lamia attacks

Trend Micro researchers described the activities of the Earth Lamia threat actor, which has been targeting multiple industries in Brazil, India, and Southeast Asia since at least 2023. Initially, the group focused on the financial services sector, but has since shifted its attention to logistics and online retail, and most recently has been targeting IT companies, universities, and government organizations. Earth Lamia's operations have previously been mentioned in various research reports: REF0657, STAC6451 and CL-STA-0048.

They primarily exploit various known SQL injection vulnerabilities in web applications, including Apache Struts2, GitLab, WordPress File Upload, JetBrains TeamCity, CyberPanel, SAP NetWeaver Visual Composer, and Craft CMS, using sqlmap to gain access to the servers of target organizations. To evade detection, Earth Lamia developed and customized its own hacking tools, including the previously undocumented modular .NET backdoor PULSEPACK and the BypassBoss privilege escalation tool. The lateral movement phase involves certutil.exe or powershell.exe to download additional tools. GodPotato and JuicyPotato are used to escalate privileges, Fscan and Kscan to scan the network, rakshasa and Stowaway to create proxy tunnels, and schtasks.exe is used for persistence in backdoor execution. Earth Lamia deploys web shells in web applications, collects domain controller information and credentials with "nltest.exe" and "net.exe", adds the "helpdesk" user account to the local administrators' group, and executes backdoors generated from command-and-control frameworks such as Vshell, Cobalt Strike, and Brute Ratel.

Earth Ammit attacks

Trend Micro researchers analyzed two waves of campaigns conducted by the Earth Ammit threat actor between 2023 and 2024. The first wave, known as VENOM, primarily targeted software service providers, while the second wave, TIDRONE, focused on military and satellite industries. Trend Micro first disclosed TIDRONE in September 2024, detailing attacks on drone manufacturers in Taiwan. During the TIDRONE campaign, Earth Ammit abused ERP and remote

desktop access to deploy the CXCLNT and CLNTEND backdoors. Subsequent post-exploitation activities included privilege escalation, persistence, disabling antivirus software, and information gathering.

During the VENOM campaign, Earth Ammit infiltrated the upstream segment of the drone supply chain, relying heavily on open-source tools. The VENOM campaign is characterized by exploiting web server vulnerabilities to deploy web shells, gain access to install RATs, and gain persistent access to compromised hosts, as well as using the REVSOCK and Sliver open-source tools. The attackers then use the stolen credentials of victims to launch attacks on downstream clients. Earth Ammit also used customized tools such as SCREENCAP (a screen capture tool) and VENFRPC (a fast reverse proxy) in the VENOM campaign, both adapted from utilities available on GitHub.

The victims of these campaigns were mainly located in Taiwan and South Korea, spanning multiple industries, including military, satellite, heavy industry, media, technology, software services, and healthcare. The connection between VENOM and TIDRONE campaigns is linked to their common victimology and C2 infrastructure. Trend Micro noted that the group's TTPs resemble those used by another Chinese-speaking APT group, Dalbit (m00nlight), indicating a common toolset.

UNC5221 attacks

EclecticIQ observed the active exploitation of Ivanti EPMM vulnerabilities CVE-2025-44277 and CVE-2025-44288, which allow unauthenticated remote code execution on exposed systems. Interestingly, the first vulnerability exploitations were tracked to the day of the vulnerability disclosure by the vendor (May 15, 2025). With high confidence, this campaign is attributed to UNC5221, a chinese-speaking espionage group. The group has targeted critical sectors, including healthcare, telecommunications, aviation, municipal government, finance, and defense, across Europe, North America, and the Asia-Pacific region. The affected organizations include a German manufacturer specializing in industrial rotary technology, a U.S. medical device manufacturer, a Japanese automotive parts supplier, and a U.S.-based firearms manufacturer. The threat actors used reflective Java payloads for command execution, and deployed KrustyLoader to load encrypted Sliver implants. They also leveraged hardcoded MySQL database credentials to extract sensitive data, such as LDAP details and Office 365 tokens. Additionally, the attackers utilized tools like FRP (Fast Reverse Proxy) and the Auto-Color Linux backdoor to enable internal reconnaissance and maintain persistent access to compromised systems.

PurpleHaze/ShadowPad attacks

In April, SentinelLabs researchers revealed preparations for an attack on SentinelOne itself, discovered in October 2024. The cluster they investigated was named PurpleHaze and attributed to the activities of the APT15 and UNC5174 groups. In June, the researchers reported an attack on their IT equipment supplier as part of a large-scale campaign using the ShadowPad modular malware platform. SentinelLabs claims that the goals of these attacks overlap with those of PurpleHaze. Between June 2024 and March 2025, more than 70 organizations around the world were compromised by ShadowPad samples obfuscated with ScatterBrain. The affected organizations belong to the government, manufacturing, financial, telecommunications, and research sectors.

SentinelLabs researchers suspect that the most common initial access vector of the global ShadowPad operation involved the exploitation of Check Point gateway devices, consistent with previous research on this topic. Communication to ShadowPad C2 servers originating from Fortinet Fortigate, Microsoft IIS, SonicWall, and CrushFTP servers was also observed, suggesting potential exploitation of these systems as well.

When analyzing a ShadowPad intrusion into a South Asian government entity in June 2024, it was revealed that the malware was delivered to the target via PowerShell. The attackers also deployed an open source Nimbo-C2 remote access framework and PowerShell-based exfiltration script that performs a recursive search for confidential user documents, archives them in a password-protected 7-Zip archive, and then extracts them. ScatterBrain-obfuscated ShadowPad activity is attributed by Google Threat Intelligence Group to the Chinese-speaking APT41 actor.

Middle East-related activity

Lemon Sandstorm attacks

The FortiGuard Incident Response (FGIR) team reported a long-term campaign by an Iranian state-sponsored threat group targeting critical national infrastructure (CNI) in the Middle East. The activity lasted from at least May 2023 to February 2025, with traces of compromise going as far back as May 2021. Fortinet researchers attributed the attack to the Lemon Sandstorm (formerly Rubidium) group, which is also tracked as Parisite, Pioneer Kitten, and UNC757. The attack observed against CNI by Fortinet was carried out in four stages, using an ever-changing arsenal of tools as the victim implemented

countermeasures. The group gained a foothold using stolen credentials to access the victim's SSL VPN system, hosted web shells on publicly accessible servers, and deployed Havoc, HanifNet, and HXLibrary backdoors to ensure long-term access. Lemon Sandstorm deployed additional web shells and the NeoExpressRAT backdoor using plink and Ngrok tools to penetrate deeper into the network, perform targeted exfiltration of the victim's emails, and move laterally within the virtualization infrastructure. In late 2024, the group deployed new web shells and two additional backdoors, MeshCentral Agent and SystemBC, in response to the ongoing containment efforts by the victim. Since then, Lemon Sandstorm attempted re-entry into the network using the Biotime vulnerabilities (CVE-2023-38950, CVE-2023-38951, and CVE-2023-38952) and spear-phishing attacks on 11 employees to harvest Microsoft 365 credentials.

Other malware families and open-source tools used in the attack include: HanifNet, HXLibrary, CredInterceptor, RemoteInjector, RecShell, NeoExpressRAT, DropShell, and DarkLoadLibrary. Fortinet researchers believe that the primary target of the attack was the victim's limited Operational Technology (OT) network based on the nature of the threat actor's reconnaissance activity. FGIR identified evidence of an adversary foothold within the restricted network segment hosting OT related systems. However, there was no evidence that the adversary had penetrated the OT network. Much of the malicious activity involved manual operations performed by different operators (based on the group's spelling errors and regular work schedule). During the intrusion, the attacker used a chain of proxies and custom implants to bypass network segmentation and move within the environment. In later stages, the attackers sequentially combined four different proxy tools to access internal network segments, demonstrating a sophisticated approach to maintaining persistence and evading detection.

Stealth Falcon attacks

Check Point Research identified an attempted cyberattack against a major defense company in Turkey conducted by the Stealth Falcon APT group (also known as FruityArmor). Stealth Falcon is a notorious APT group that has been active since at least 2012 and is known for conducting sophisticated cyber-espionage operations. Over the years, the group has been observed acquiring zero-day exploits and utilizing custom-built payloads to target entities across the Middle East. In the described campaign, the threat actors employed a previously undisclosed technique to execute files hosted on a WebDAV server under their control. This was achieved by changing the working directory of iediagcmd.exe, a legitimate built-in Windows tool, to a URL pointing to a malicious WebDav server. The tool then runs the malware payload instead of the

legitimate route.exe located in the system32 folder. Following responsible disclosure, Microsoft assigned the vulnerability the designation CVE-2025-33053 and released a patch on June 10, 2025. The WebDAV-based exploitation of CVE-2025-33053 was used to deliver the Horus Agent, a custom implant built on the Mythic C2 open-source framework. The Horus Agent represents an evolution of the group's customized Apollo implant used previously.

MuddyWater attacks

ESET researchers observed MuddyWater campaigns in January and February 2025 notable due to what appears to be cooperation and overlap between a MuddyWater compromise followed in rapid succession with Lyceum (an OilRig subgroup) gaining access to a system in the manufacturing vertical in Israel. MuddyWater created the initial compromise via a spear-phishing email with a link to an RMM installer (Syncro). Subsequently, MuddyWater installed an additional RMM (PDQ, the recent RMM of choice for MuddyWater). A MuddyWater operator then engaged in a hands-on session of Windows shell commands, creating a lot of noise and achieving very few operational objectives. Finally, MuddyWater deployed Mimikatz via a custom loader and injector. The same day, probably using credentials harvested using Mimikatz, Lyceum took control of adversarial activities within the organization. ESET researchers previously noted that MuddyWater may be acting as an access broker for other Iran-aligned groups. In another detected campaign, MuddyWater used an injector that reflectively loads a backdoor into memory and attempts to circumvent security software. The campaign lasted two months (September through October 2024) and targeted victims in Israel in the engineering and government verticals.

Cybercriminal and others

Attacks with ClickFix

Proofpoint researchers discovered state-sponsored actors in multiple campaigns using the ClickFix social engineering technique, which uses dialogue boxes with instructions to copy, paste, and run malicious commands on the target's machine for the first time. From late 2024 through the beginning of 2025, threat actors, including TA427, TA450, UNK_RemoteRogue, and TA422 (aka Sofacy, APT28 and Fancy Bear), were seen using the ClickFix technique in their routine activity.

Proofpoint researchers observed TA450 actor sending an English-language phish to targets in at least 39 organizations on November 13-14, 2024. The email

masqueraded as a security update from Microsoft with the subject line: “Urgent Security Update Required – Immediate Action Needed” to convince individuals to execute a series of steps to address a security vulnerability. The attackers deployed the ClickFix technique by persuading the target to first run PowerShell with administrator privileges, then copy and run a command contained in the email body. The command was responsible for installing Level remote management and monitoring (RMM) software. TA450 targeted the Middle East with an emphasis on the UAE and Saudi Arabia, but also global targets. The targets spanned multiple sectors, including transportation, utilities, energy, and the most popular targets: finance and government organizations.

Proofpoint researchers also observed a targeted campaign that used compromised infrastructure to send 10 emails to individuals in two organizations associated with a major arms manufacturer in the defense industry. The campaign was carried out by a suspected Russian group tracked as UNK_RemoteRogue. The emails contained a malicious link that spoofed Microsoft Office with the title “RSVP Office - Створюйте, редагуйте документи та діліться ними в Інтернеті”. If the target visited the link, it displayed HTML that spoofed a Microsoft Word document with ClickFix-style instructions in Russian to copy code from the browser into their terminal. The webpage included a link to a YouTube video tutorial on how to run PowerShell. The commands pasted in the terminal ran malicious JavaScript that then executed PowerShell code linked to the Empire C2 framework.

CrazyHunter attacks

Trend Micro researchers provided analysis of attacks by an emerging ransomware group, CrazyHunter, targeting critical sectors in Taiwan, including healthcare, education, and industry. The ransomware operator utilizes various open-sourced tools from GitHub to facilitate operations, including ZammoCide to terminate AV/EDR processes, SharpGPOAbuse for privilege escalation and lateral movement, and the opensource, Go-based Prince ransomware to encrypt victims’ files. Prince ransomware uses ChaCha20 and ECIES encryption to securely encrypt files. The attackers customized it by adding the ".Hunter" extension to encrypted files. The ransomware drops a ransom note called "Decryption Instructions.txt", changes the victim's desktop wallpaper, and demands payment.

CISA alert on cyberattacks targeting oil and gas sector

The Cybersecurity and Infrastructure Security Agency (CISA) released a cybersecurity advisory warning about cyber actor(s) targeting ICS/SCADA systems within U.S. critical infrastructure sectors (Oil and Natural Gas),

particularly in energy and transportation systems. According to the advisory, these activities often include basic and elementary intrusion techniques. Poor cyber hygiene and exposed assets can escalate these threats, leading to significant consequences such as defacement, configuration changes, operational disruptions and, in severe cases, physical damage. CISA, the Federal Bureau of Investigation (FBI), the Environmental Protection Agency, and the Department of Energy (DOE) also published primary mitigations to reduce the risk of potential intrusions. The detailed guidance urges organizations to take basic measures like removing operational technology from the internet, changing default passwords, securing tools used to remotely access networks, and segmenting operational networks from business IT networks. A CISA spokesperson declined to provide Recorded Future with details about which actors were being referred to and what incidents prompted the advisory.

Attacks with NetBird deployment

Trellix reported a highly targeted spear-phishing campaign by an unknown threat actor targeting CFOs and finance executives at banks, energy companies, insurers, and investment firms across Europe, Africa, Canada, the Middle East, and South Asia. The attack began with email purporting to be from a Rothschild & Co recruiter, offering a "strategic opportunity" with the firm. The email contained a link to a Firebase-hosted page disguised as a brochure protected by a custom math-quiz CAPTCHA. After solving the CAPTCHA, the victim was prompted to download a ZIP file containing a VBS script. Running the script led to the silent installation of two legitimate MSI packages, NetBird and OpenSSH, as well as the creation of a hidden local-admin account and the enabling of RDP, providing the attacker with an encrypted channel for remote access. NetBird promptly took action to block the malicious actors and terminated their access to prevent further exploitation of their platform.

Hazy Hawk attacks

Researchers at Infoblox investigated campaigns conducted by a threat actor known as Hazy Hawk. Hazy Hawk hijacks abandoned cloud resources, such as S3 buckets and Azure endpoints belonging to high-profile organizations, including governments, universities, and major corporations, such as Honeywell and Unilever. These hijacks rely on misconfigured DNS records, specifically exploiting dangling CNAME records to gain control over subdomains from trusted domains. The attackers register a new cloud resource with the same name as the abandoned CNAME, causing the original domain's subdomain to resolve to the attacker's new cloud-hosted site. Once in control, the group uses these subdomains to distribute scams, malicious content, and push notifications

through complex layered redirect chains and traffic distribution systems. Infoblox researchers noted that such sites are used to scam tech support, fake antivirus alerts, and promote fake streaming and porn sites.

Attacks via Microsoft Exchange Server

Positive Technologies researchers observed a series of attacks involving the injection of malicious code into the login page of compromised Microsoft Exchange Servers, similar to those conducted in May 2024, with no modifications made to the original keylogger code. The researchers discovered malicious code samples, which were categorized into two types: those that save collected data to a local file accessible from the outside, and those that immediately send the collected data to an external server. During the investigation, approximately 65 victims were identified across 26 countries, with the majority of compromised servers found in government organizations, as well as in IT, industrial, and logistics companies.

Anubis attacks

Trend Micro reported a new emerging Ransomware-as-a-Service (RaaS) operation called Anubis that combines file encryption with file destruction. Anubis joined X in December 2024. At the time of this report, the group's leak site listed seven victims. The group has targeted a range of industries, including healthcare, engineering, and construction, across multiple regions, such as Australia, Canada, Peru, and the United States. The latest Anubis samples analyzed by researchers contained a wiper, which in their opinion, helps increase pressure on victims and force them to pay faster. When activated, the wiper erases all the contents of files, reducing their size to 0 KB, while keeping the names and file structure intact. The victim will still see all the files in the directories, but their contents will be irreversibly destroyed, making recovery impossible. The attacks begin with phishing with malicious links or attachments. Trend Micro analysis showed that Anubis supports several commands at startup, including privilege escalation, directory exclusion, and target paths for encryption. Critical system and program directories are excluded by default. The ransomware deletes volume shadow copies and terminates processes and services that could interfere with the encryption process. The encryption scheme uses ECIES (Elliptic Curve Integrated Cryptography), which has some tactical similarities in terms of implementation with EvilByte and Prince. The encrypted files are appended with the .anubis extension, and an HTML ransom note is placed in the affected directories. Anubis ransomware also attempts to change the desktop wallpaper.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com