Kaspersky ICS CERT

kaspersky

APT and financial attacks on industrial organizations in Q1 2025

19.06.2025

Version 1.0

This summary provides an overview of the reports of APT and financial attacks on industrial enterprises disclosed in Q1 2025, as well as the related activities of groups that have been 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 for industrial enterprises.

Executive summary

Although the findings of researchers are noticeably fewer in number than those of the previous quarter, there are many that deserve special attention – if only to ask ourselves again: "Is our organization reliably protected from this?"

Attackers continued to emphasize to Korean organizations the high risk of supply chain attacks involving locally developed products. This time, the attack target was a local developer of a VPN solution. At least one industrial company was affected – a manufacturer of semiconductor products.

Two cases highlighted the exploitation of zero-day vulnerabilities during attacks on industrial organizations – one involved the 7-Zip vulnerability in attacks discovered in Ukraine and the other involved the 0-click vulnerability in MS Windows. The developer refused to fix the latter vulnerability, even though it has been tracked in multiple malicious campaigns, the earliest of which occurred in 2017.

The technique of using polyglot files, which are constructed from data of different formats in such a way that they are interpreted by different legitimate interpreters, has suddenly become popular among attackers. Proofpoint researchers reported one such campaign involving PDF/HTA and PDF/ZIP polyglots, while Kaspersky experts reported another involving a PE/ZIP polyglot.

One of the stories describes sophisticated techniques used to steal authentication data for the lateral movement stages highlighting the need for industrial enterprises to continuously check their perimeter for the signs of potential compromise – such as making sure your login pages have not been modified with a malicious implant and that it is still only you who is in power of controlling you companies' DNS zone.

South-East Asia and Korean Peninsula

SalmonSlalom campaign

Kaspersky ICS CERT researchers reported on the SalmonSlalom campaign targeting organizations in the Asia-Pacific region via phishing emails deploying FatalRAT, a multifunctional Trojan capable of keystroke logging, memory manipulation, viewing browser data, downloading additional software such as AnyDesk and UltraViewer, performing file operations, starting a proxy server, scanning the network, and terminating processes. The campaign specifically targeted government and industrial organizations, particularly those in the manufacturing, construction, IT, telecom, healthcare, energy, and logistics and transportation sectors in Taiwan, Malaysia, China, Japan, Thailand, South Korea, Singapore, the Philippines, Vietnam, and Hong Kong. The lures used in the emails suggest that the phishing campaign targets Chinese-speaking users.

The attackers used a complex multi-stage payload delivery structure to evade detection and incorporated legitimate Chinese CDN myqcloud and Youdao Cloud Notes into the attack infrastructure. The starting point of the latest attack chain is a phishing email containing a ZIP archive with a file name in Chinese. When opened, the archive triggers a first-stage downloader that sends a request to Youdao Cloud Notes to retrieve the FatalRAT configurator and second-stage DLL loader. The configurator is a DLL that downloads the contents of another note from note.youdao[.]com, accessing the configuration information and opening a decoy file. The second-stage DLL downloader is responsible for downloading and installing the FatalRAT payload from the server ("myqcloud[.]com") specified in the configuration file, while simultaneously displaying a fake error message indicating a problem launching the application.

A significant distinguishing feature of the campaign is its use of DLL sideloading techniques to speed up the multi-stage infection sequence and download of the FatalRAT malware. FatalRAT performs 17 checks to determine if the malware is running in a virtual machine or sandbox environment. When examining the code of the malicious artifacts, the researchers noticed similarities with the workflows observed in previous campaigns organized by threat actors using Gh0st RAT, SimayRAT, Zegost, and FatalRAT. There is no clear consensus among researchers as to who is behind the attacks using FatalRAT.

VIP Keylogger attacks

Researchers from HP Wolf Security identified a malware campaign delivering VIP Keylogger that targeted engineering companies in the Asia-Pacific region in Q4

2024. The attackers sent malicious PDF files via email, posing as quotation requests, and tailored their messages to potential victim organizations based on the products they sold, such as automobile and industrial parts. When a user opens the PDF, they see a blurry image of a document with two messages. The first message informs the user that there is an update available for their PDF reader. The second message indicates that the document was compressed and that the user must click on the image to download the file to see the full version. Following these instructions triggers a web download of a ZIP archive. Opening the ZIP archive reveals a disk image (IMG) file. When opened, Windows mounts the disk image and shows its contents in a new File Explorer window. The mounted disk image only contains a single file – an executable made to look like a PDF document by changing the file's icon. Running the executable starts the final infection stage that installs the payload, VIP Keylogger, which shares similarities with Snake/404 Keylogger.

SideWinder attacks

In 2024, Kaspersky researchers published the article about SideWinder. It described the latest toolsets and a previously unknown advanced modular espionage tool named StealerBot. Following publication, researchers observed frenetic activity by this actor to update their toolset and create a large infrastructure to distribute and control compromised systems. The targeted sectors are consistent with those observed in the past. However, researchers noticed a significant increase in attacks against maritime infrastructure and logistics companies. During the first part of 2024, a spike in attacks against the aforementioned sectors, especially in Djibouti, was observed. Since then, the attackers have expanded their activity, attacking many different maritime infrastructures from South-East Asia to the Mediterranean Sea. Attacks against governments, military and diplomatic entities also continued. Moreover, researchers observed attacks indicating a particular interest in nuclear power plants and nuclear energy, with documents seemingly designed to target personnel in this sector.

Squid Werewolf/APT37 attacks

BI.ZONE researchers uncovered a phishing campaign carried out by Squid Werewolf (also known as APT37, Ricochet Chollima, ScarCruft, or Reaper Group). The attack begins with a phishing email, written in Russian, disguised as a job offer from a United Industrial Complex HR representative. The email includes a password-protected ZIP archive attachment. The attachment contains an LNK file that, when opened, executes a command that leads to the execution of an EXE file. The malware then runs a DLL, an obfuscated C#-based loader. This

loader disables autoruns from the startup folder by setting registry key parameters. It then downloads, decrypts and executes the malicious payload in memory. However, the payload was unavailable at the time of the research. The attack detected by BI.ZONE Threat Intelligence closely resembles one described by the Securonix team, who attribute it to the APT37 cluster. Previously, the attackers used a similar library in C#, but the payload was decrypted using the shift algorithm (Caesar cipher) and was obfuscated JavaScript code. This payload was another downloader that sent the computer name of the victim to the server, and downloaded and executed the next-stage code – a PowerShell script. This script was the VeilShell Trojan.

Chinese-speaking activity

PlushDaemon attacks

ESET researchers reported on the activities of a China-aligned APT group called PlushDaemon that has been active since at least 2019. The group is linked to a supply chain attack against South Korean VPN provider IPany. Trojanized software was found on the provider's official website. There was no targeting implemented on the site; all download requests resulted in delivery of the trojanized installer. ESET telemetry data revealed that several users attempted to run the trojanized installer from a Korean VPN developer within the networks of a semiconductor company and an unidentified software development organization in South Korea. The earliest known victims were in Japan and China in November and December of 2023, respectively.

PlushDaemon's main arsenal is the multifunctional backdoor SlowStepper, which supports a wide set of tools with 30 modules written in C++, Python, and Go. SlowStepper has been in development since January 2019, and the latest iteration was compiled in June 2024. All the SlowStepper tools, among other data collection capabilities, have capabilities for extensive data collection and audio and video recording for the purposes of spying. The tools were stored in a remote code repository hosted on the Chinese platform GitCode. The developers also implemented a custom shell in SlowStepper, or command line interface, on top of its communication protocol. ESET researchers have also observed the group gaining access via vulnerabilities in legitimate web servers.

J-magic attacks

Researchers at Black Lotus Labs of Lumen Technologies reported a malicious campaign targeting Juniper routers and VPN gateways. The campaign used

malware called J-magic, which is specifically designed for Junos OS. The name comes from the fact that the backdoor constantly monitors TCP traffic for a "magic packet" before launching a reverse shell. J-magic is a modified version of the publicly available cd00r backdoor, an experimental prototype that remains hidden and passively monitors network traffic for a magic packet before opening a communication channel with the attacker. The malware creates an eBPF filter on the specified interface and port as a command line argument when executed.

J-magic attacks targeted organizations in the semiconductor, energy, manufacturing, heavy machinery, construction, bioengineering, and IT industries. According to Black Lotus Labs, the J-magic campaign was active from mid-2023 to mid-2024 and employed a low-detection, long-term access format. Based on telemetry, researchers believe about half of the targeted devices were configured as VPN gateways for their organizations. They note that the campaign under study has technical similarities with SeaSpy malware, which is also based on the cd00r backdoor. However, some differences make it difficult to establish a connection between the two campaigns. Overall, the researchers assess with low confidence the correlation between J-magic and SeaSpy, the latter of which attacked Barracuda Email Security Gateways using CVE-2023-2868 as a zero-day in 2022-2023.

Shadowpad attacks

Trend Micro researchers discovered that Shadowpad, a malware family linked to various Chinese-speaking threat actors, is being used to deploy a previously undetected ransomware family. The attackers deploy the malware by exploiting weak passwords and bypassing multi-factor authentication mechanisms. According to the researchers, this malware family has targeted at least 21 companies in nine different industries across 15 countries in Europe, the Middle East, Asia, and South America. The manufacturing sector was the hardest hit. Other affected industries include transportation, publishing, energy, pharmacy, banking, mining, education and entertainment. The ransomware attack uses DLL side-loading to run a malicious payload. In two cases, researchers saw Shadowpad launching CQHashDumpv2.exe, part of the penetration testing toolkit CQTools that allows users to dump hashes from the system and change user passwords. Other post-exploitation tools include Impacket and an unidentified tool used to dump the Active Directory database (probably NTDSUtil). Researchers did not find strong enough evidence to link this activity to older operations or a known threat actor. However, they found two low-confidence indicators pointing toward the Teleboyi threat actor.

Winnti attacks

LAC's Cyber Emergency Center reported a new attack campaign called RevivalStone by the Winnti group. In March 2024, the campaign targeted Japanese companies in the manufacturing, material-based, and energy sectors, utilizing Winnti malware with enhanced capabilities and sophisticated evasion techniques. For initial intrusion, the attacker group exploited an SQL injection vulnerability in the ERP system running on the target organization's web server to place a WebShell. The attacker then used the WebShell to perform reconnaissance and collect credentials for lateral movement within the organization's network, and placed Winnti malware on the server to use as a foothold for future attacks. Winnti malware employs AES and ChaCha20 encryption algorithms to secure its payloads and communications. Unique identifiers, such as IP and MAC addresses, are used to generate decryption keys, which complicates analysis. The malware also installs a kernel-level rootkit to hide its communications. Code obfuscation and DLL hijacking techniques are used to bypass endpoint detection and response (EDR) systems.

Lotus Blossom attacks

Cisco Talos researchers revealed new campaigns by the Chinese-speaking Lotus Blossom APT group (also referred to as Spring Dragon, Billbug, or Thrip) targeting the government, manufacturing, telecom, and media sectors in the Philippines, Vietnam, Hong Kong, and Taiwan using updated versions of Sagerunex backdoor. Lotus Blossom has been known since 2009 and has been using Sagerunex since at least 2016. The Sagerunex backdoor is believed to be an updated variant of the previously known Billbug (Evora) malware.

The exact initial access vector in the latest intrusions is unknown. The observed activity is notable for two new malware variants that leverage cloud services such as Dropbox, Twitter, and Zimbra for C2. The Dropbox and Twitter/X versions of Sagerunex were used between 2018 and 2022, while the Zimbra version has been around since 2019. The latter is designed not only to collect information about the victim and send it to the Zimbra mailbox, but also to allow the attacker to use the contents of the Zimbra mailbox to send commands and control the victim's machine. If the mailbox contains legitimate command content, the backdoor downloads it and extracts the command. Otherwise, it deletes the content and waits for it to arrive. The results of the command execution are then packed as a RAR archive and attached to the draft email in "Trash" folders of the mailbox. Each Sagerunex variant implements various checks, such as time-based delays and system checks, to maintain persistence. The attacks also use other tools, including a Chrome browser credential stealer, the open-source proxy utility Venom, a privilege configuration program, custom

software for compressing and encrypting captured data, and the modified relay tool mtrain V1.01. The attackers were also observed running commands such as net, tasklist, ipconfig, and netstat to perform reconnaissance on the target environment, as well as probes to determine internet access. If internet access was restricted, the attackers used one of two strategies: they either used the target's proxy settings to establish a connection or relied on Venom to connect isolated machines to systems with internet access.

Earth Alux attacks

Trend Micro researchers uncovered a new Chinese-speaking threat actor called Earth Alux targeting various key sectors, including government, technology, logistics, manufacturing, telecom, IT, and retail in the Asia-Pacific region and Latin America. First observed in Asia in Q2 2023, Earth Alux has also been active in Latin America since mid-2024. The actor's primary targets are in countries such as Thailand, the Philippines, Malaysia, Taiwan, and Brazil. The infection chains begin with the exploitation of vulnerable services in web applications accessible via the internet. These services are used to inject a Godzilla shell to facilitate the deployment of additional payloads, including the VARGEIT and COBEACON (Cobalt Strike Beacon) backdoors.

VARGEIT downloads tools directly from its C2 server into a newly created Microsoft Paint process (mspaint.exe) for reconnaissance, collection and exfiltration. VARGEIT is also the primary method by which Earth Alux manages additional tools for various purposes and lateral movement. VARGEIT is used as a first-, second-, or later-stage backdoor, while COBEACON is used as a first-stage backdoor. COBEACON is loaded as an encrypted payload of the side-loaded DLL MASQLOADER, or as a shellcode using RSBINJECT, a Rust-based command-line downloader. Executing VARGEIT deploys more tools, including a component of the RAILLOAD downloader, which is executed using sideloading DLLs and is used to launch an encrypted payload in a different folder. The second payload is RAILSETTER, which modifies the timestamps associated with RAILLOAD artifacts on the compromised host and creates a scheduled task to run RAILLOAD. VARGEIT's most distinctive feature is its ability to support 10 different channels for communicating with the C2 over HTTP, TCP, UDP, ICMP, DNS, and Microsoft Outlook. The latter uses the Graph API to exchange commands in a pre-defined format via the drafts folder of the attacker-controlled mailbox.

Earth Alux performs several tests with RAILLOAD and RAILSETTER, including detections and attempts to find new hosts for sideloading DLLs. The group uses ZeroEye, an open-source tool that scans EXE import tables for imported DLLs

that can be used for sideloading. The group also uses VirTest, another widely used testing tool in the Chinese-speaking community.

Russian-speaking activity and targets in Russia

Sticky Werewolf attacks

In January, F6 researchers reported on the activities of the Sticky Werewolf group, which attacked Russian research and production enterprises. The attackers sent malicious emails containing instructions for placing orders from defense industry enterprises with penal institutions that involve the use of convict labor. The emails contained two attachments: a decoy cover document in the style of the Ministry of Industry and Trade, and a malicious password-protected RAR archive ("Filling form.rar"). The archive contained a document called "mailing list.docx" and a malicious executable file called "Form filling.pdf.exe" that, when launched, eventually delivered the Ozone RAT. Further investigation revealed a phishing email with a similar subject line dated December 23, 2024, containing two fake documents. The attackers targeted a research and production facility; however, the email did not contain an archive with the payload.

In March, F6 researchers also reported new attacks by the Sticky Werewolf group. This time, the group targeted an oil and gas equipment manufacturer. The detected mailing included emails with a password-protected 7z archive. Sticky Werewolf used a decoy document from the Ministry of Industry and Trade. As a result of executing the group's classic attack chain, which includes the NSIS dropper installer, BAT file and AutoIt script, the RegAsm.exe process is created and QuasarRAT is injected into it. One of the C2 domains (crostech[.]ru) has been used by the group since October 2024. The second domain (thelightpower[.]info) was registered later in December, and the earliest known attacks using it date back to March of this year.

Rezet/Rare Wolf attacks

F6 researchers reported attacks by the cyberespionage group Rezet (aka Rare Wolf), which has been active since October 2018 and involved in more than 500 cyberattacks on Russian, Belarusian and Ukrainian industrial enterprises. In January 2025, for example, malicious mailings were sent on behalf of a company that specializes in supporting contracts with enterprises performing state defense orders. The emails looked like invitations to managers and specialists for seminars on the standardization of defense products. The targets of the attack

were enterprises in the chemical, food, and pharmaceutical industries in Russia. The first mailing contained a malicious file inside a password-protected RAR archive, which contained a bait file in the form of a PDF document, as well as a payload. When launched, the PDF bait document opens to distract the user's attention while the system is infected in the background. The second and third mailings, which the attackers sent a few days later, contained an archive with two malicious files – a PDF document and a payload. Opening either of the files also resulted in system infection. The researchers did not specify what payload was used in the attacks.

Attacks on Ukrainian organizations using CVE-2025-0411

According to a Trend Micro report, a zero-day vulnerability in 7-Zip identified as CVE-2025-0411 was exploited to deploy the SmokeLoader malware in a cyberespionage campaign targeting Ukrainian organizations. The exploitation was identified in September 2024, and a patch was released on November 30, 2024. The vulnerability allows attackers to bypass Windows Mark-of-the-Web protections by double-archiving files, thereby evading essential security checks and enabling the execution of malicious content. Russian-speaking cybercrime groups actively exploited the vulnerability through spear-phishing campaigns involving compromised email accounts and spoofed document extensions to trick users and the Windows operating system into executing malicious files. Based on data uncovered by researchers, Ukrainian government entities and other organizations, including a ministry, an automobile, bus and truck manufacturer, a public transportation service, an appliance, electrical equipment and electronics manufacturer, a regional administration, an insurance company, a regional pharmacy, a water supply company, and a city council, may have been directly targeted and/or affected by this campaign.

Mythic Likho attacks

Kaspersky researchers reported attacks on Russian companies by the Mythic Likho group. The researchers initiated the study in January after analyzing an email addressed to the HR department of a machine factory. The authors – allegedly from another company's HR department – requested a character reference for a former employee. Mythic Likho is either a new group or one that has significantly improved its TTPs.

The phishing email attachment contains an archive with several components, including a secure decoy document and an LNK file that leads to infection. As a result of infection, the Merlin agent – an open-source post-exploitation tool compatible with the Mythic framework written in Go – is deployed on the host. Merlin can communicate with the server via HTTP/1.1, HTTP/2, and HTTP/3 (a

combination of HTTP/2 and the QUIC protocol). In addition to compatibility with the Mythic framework, researchers discovered a connection between Merlin and Loki backdoor attacks. For example, one of the Merlin instances with the mail.gkrzn[.]ru command center downloaded a new version of the Loki 2.0 sample with the pop3.gkrzn[.]ru command center to the victim's system. Like the first version, the second version of Loki sends various system and build data to the server, but this has been slightly expanded. Additionally, perhaps to complicate identification of the malware family, the malware authors decided to change the method of sending data to the command server from the POST request method to GET. As with the Loki backdoor, Merlin backdoor attacks have hit more than a dozen Russian companies from various industries, including telecommunications equipment suppliers and industrial enterprises.

ReaverBits attacks

F6 researchers reported new activity by the ReaverBits group. Active since late 2023, ReaverBits specializes in attacking Russian companies in the biotechnology, retail, agro-industrial, telecommunications and financial sectors. From September 2024 to January 2025, researchers observed three distinct infection chains involving updated tools – the publicly available Meduza Stealer and the new ReaverDoor malware. In September 2024, researchers detected phishing mailings purporting to be from the Investigative Committee of the Russian Federation. The emails contained a malicious PDF attachment. Once launched, the victim sees a notification about the need to update Adobe Font Package, and is given a link to download it. Clicking the link downloads an executable file with a name mimicking a legitimate Adobe Font Package update. The executable file is a downloader and contains code from the open-source project adbGUI, which downloads and launches the next stage Meduza Stealer.

In January, an email allegedly from the Russian Ministry of Internal Affairs was also detected. The email contained a link supposedly for downloading a document. When the recipient clicked the link, the server checked the browser's language settings. The downloaded executable file is based on .NET and classified as a downloader, similar to that in previous mailings. The file is based on the legitimate open-source NBTExplorer software, but with added malicious code. The downloaded final-stage malware was also Meduza Stealer.

Additionally, the researchers managed to find a previously undocumented backdoor named ReaverDoor on VirusTotal that was associated with a ReaverBits IP address. ReaverDoor is based on the legitimate open-source project Optimizer and contains malicious code that loads a .NET library. Various techniques are used to covertly execute the malicious code, including Process

Hollowing, as well as complex cryptographic encryption schemes such as a combination of AES-256, PBKDF2, XOR, and Base64.

Telemancon attackers

F6 researchers discovered a previously unknown state-sponsored group dubbed Telemancon. During their investigation of the group's infrastructure, the researchers found that the group's earliest activity dates back to February 2023. The identified attacks, based on the content of the phishing documents, targeted Russian organizations in the industrial sector, specifically the machinery industry. The group uses a custom-made dropper and PowerShell backdoor, named TMCDropper and TMCShell, respectively. The group employs a non-trivial method of concealing its command and control (C2) addresses, utilizing the legitimate telegra.ph service. While studying one of the samples, the researchers determined that TMCShell executed the following commands received from the control server on the victim's machine: net.exe user; net.exe user {username}; whoami.exe; whoami.exe /groups /fo csv; ipconfig.exe /all; and ARP.EXE -a.

According to Securonix researchers, this technique for storing C2 addresses was previously observed in the arsenal of the Shuckworm group (aka Gamaredon), but in a simpler form, without generating a URL path and verifying the signature. Overall, F6 researchers posit that the Core Werewolf group may be behind Telemancon's activity. However, there are not yet enough artifacts for confident attribution. Core Werewolf is also known as PseudoGamaredon because it often copies the TTPs of the Gamaredon group.

Head Mare attacks

In September 2024, Kaspersky researchers investigated several incidents in which indicators of compromise and TTPs related to the hacktivist group Head Mare were detected. The new attacks utilized well-known tools previously seen in Head Mare incidents, such as mimikatz, ngrok, LockBit 3.0, Babuk, etc., as well as new tools written in PowerShell. During their investigation, the researchers discovered that Head Mare uses tools such as the CobInt backdoor that were formerly used by another hacktivist group, Twelve (aka Shadows/Comet/Darkstar), to carry out attacks. The researchers also found C2s that, prior to investigating these incidents, were only used by the Twelve group. This may indicate that Head Mare is related to Twelve. Both groups targeted Russian companies in the manufacturing, government, and energy sectors.

Kaspersky researchers have detected a new wave of targeted attacks by the Head Mare group against Russian industrial companies using a new Python-

based backdoor called PhantomPyramid. According to Kaspersky telemetry, in March 2025, more than 800 employees of near 100 organizations received a mailing containing previously unknown malware. The infection chain included similar emails from a specific administrative body with the .zip attachment. The senders asked the recipients to confirm receipt of the information and to read the attached archived application. After opening the attachment, a decoy document is displayed with a request for equipment repair allegedly from a government ministry. The attackers sent a password-protected archive and used the polyglot technique for creating files containing both harmless components and malicious code. This time it was a zip archive appended to a malicious executable. The executable part of the polyglot file was the previously unknown backdoor PhantomPyramid. One of the downloadable components was MeshAgent software for remote device management with open-source code, included in the MeshCentral solution. The archive part contained an .lnk file disguised (via Windows Explorer) as a decoy PDF, but with a PowerShell script that opens the decoy documents (extracts the decoy PDF data, saves it to disk and opens it) and starts the backdoor binary.

Seashell Blizzard/Sandworm attacks

Microsoft published research detailing the BadPilot campaign, a multiyear, global cyberespionage operation conducted by the Seashell Blizzard subgroup (aka APT44, BlackEnergy, PHANTOM, UAC-0133, Blue Echidna and Sandworm). The campaign targeted organizations in various sectors, including government, energy, oil and gas, shipping, telecommunications, and manufacturing. The goal was to gain unauthorized access to sensitive systems and data. These access operations built upon previous efforts from 2021 to 2023 that primarily targeted Ukraine, Europe, and specific sectors in Central and South Asia, and the Middle East. Since early 2024, the subgroup has expanded its range to include targets in the United States and the United Kingdom by exploiting vulnerabilities. At least eight vulnerabilities have been exploited by this subgroup for initial access: ConnectWise ScreenConnect (CVE-2024-1709); Fortinet FortiClientEMS security software (CVE-2023-48788); Microsoft Exchange (CVE-2021-34473); Zimbra Collaboration (CVE-2022-41352); Openfire (CVE-2023-32315); JetBrains TeamCity (CVE-2023-42793); Microsoft Outlook (CVE-2023-23397); JBOSS (exact CVE is unknown).

Since late 2021, Seashell Blizzard has primarily used web shells to maintain footholds following successful exploitation. In early 2024, the group began using RMM suites, such as Atera Agent and Splashtop Remote Services, for persistence and command and control (C2). In some cases, Seashell Blizzard deployed OpenSSH with a unique public key, allowing them to access

compromised systems using an actor-controlled account and credentials. The group used a C2 method known as ShadowLink that facilitates persistent remote access by configuring a compromised system to register as a Tor hidden service. When Seashell Blizzard identified targets of likely strategic value, it often furthered its network compromise by deploying tunneling utilities, such as Chisel, Plink, and Rsockstun, to established dedicated conduits into affected network segments. Microsoft researchers have observed subsequent rogue JavaScript inserts to victims' sign-in pages, including those for Outlook Web Access (OWA), to steal credentials. They assess with moderate confidence that the group has been able to modify DNS A record configurations for selected targets, presumably to steal authentication data as well. The researchers conclude that these methods have likely provided the subgroup with the credentials necessary for lateral movement within several organizations.

Attacks with GoGo Exfiltration

At the end of August 2024, an unidentified threat actor launched a targeted operation against a manufacturing company in Russia that was discovered by Kaspersky Global Research & Analysis Team (GReAT) researchers. The investigation started with a previously unknown DLL file discovered in the svchost process memory and carrying a highly suspicious name – exfiltration.dll. During the campaign, the attackers likely exploited a one-day vulnerability in Microsoft Outlook and registered a domain that mimicked the victim's domain name. The attacks involved a constantly evolving custom module for the data exfiltration written in Go, which gave the malware its name. Some indicators led researchers to suspect that other malware types, such as a RAT or backdoor, remain undiscovered.

NGC4020 attacks

Solar researchers released a report on a new APT dubbed NGC4020, which they detected during an investigation of an incident involving a company in the industrial sector. While studying the attacked systems, the researchers found that the attackers exploited a vulnerability (CVE-2019-3980) in DameWare Mini Remote Control to download malware. The vulnerability allowed the attackers to load their own malicious driver into the kernel space from the LocalSystem account (CVE-2023-36802). This driver is designed to bypass protection tools and disable the self-defense components of antivirus software. The other malware discovered was Reverse Shell written in Java, system reconnaissance utilities and QuasarRAT. The attackers made a mistake when creating a task for QuasarRAT persistence, which prevented them from developing the attack. Upon examining the task parameters, it was found that the task should have

been launched using a domain system account, but the task had mistakenly specified the "Run only when user is logged on" parameter. A different parameter is required to perform tasks with system rights.

Middle East-related activity

Desert Dexter attacks

Researchers from Positive Technologies reported the discovery of a new attacker dubbed Desert Dexter, which has been targeting users in the Middle East and North Africa since September 2024 using a modified version of AsyncRAT. Check Point described a similar campaign in 2019, but some of the techniques used in the kill chain have evolved since then. Activity attributed to Desert Dexter was first detected in February 2025. Positive Technologies estimates that approximately 900 users fell victim to the campaign. Most of these users are located in Libya, Saudi Arabia, Egypt, Turkey, the United Arab Emirates, Qatar and Tunisia. For the most part, they are ordinary individuals, including employees of enterprises in the fields of oil production, construction, information technology, and agriculture.

The attackers create fake news groups on Facebook, mimicking Libya Press, Sky News, Almasar TV, The Libya Observer, and The Times of Israel, etc., to distribute malware and publish posts with advertisements and links to the Files.fm file sharing service or Telegram channel. The attack chain starts with a RAR archive containing either a batch script or a JavaScript file that launches a PowerShell script, which is responsible for executing the second stage of the attack. The script then establishes persistence on the system, collects and transmits system information to a Telegram bot, takes a screenshot, and ultimately launches the AsyncRAT payload by injecting it into the aspnet_compiler.exe executable. Analysis of messages sent to the Telegram bot revealed screenshots of the attacker's desktop, called DEXTERMSI, as well as a link to a Telegram channel called Dexterlyly. The ly substring in the channel name, according to the researchers, may indicate the channel owner's Libyan origin. This is corroborated by the geolocation in the data sent by the malware and the Arabic comments in the PowerShell script.

UNK_CraftyCamel attacks

Proofpoint researchers identified a highly targeted, email-based campaign attributed to a previously unknown actor tracked as UNK_CraftyCamel. This campaign targets entities in the UAE, with a specific interest in aviation and

satellite communications organizations, as well as critical transportation infrastructure. The campaign led to the discovery of a new Go backdoor dubbed Sosano that uses various techniques, including the use of polyglot files, which can be interpreted as multiple formats depending on how they are read (PDF/HTA and PDF/ZIP in this particular case), to obfuscate the malware and its payload. A notable aspect of the attack chain is the attacker's use of a compromised email account belonging to an Indian company, INDIC Electronics, to send phishing emails and deliver Sosano. The emails contained URLs pointing to a domain masquerading as an Indian company, which hosted a ZIP archive containing an XLS file and two PDF files. The XLS file was actually a Windows shortcut (LNK) that used a double extension, posing as a Microsoft Excel document. The two PDFs were polyglots: one was accompanied by an HTA file and the other by a ZIP archive. Depending on how they were parsed using programs such as file managers, command line tools and browsers, both PDFs could be interpreted as two different valid formats. The attack sequence involved using an LNK file to launch cmd.exe and then mshta.exe to launch a PDF/HTA polyglot file. This file would execute the HTA script, which contained instructions to unzip the contents of a ZIP archive contained in a second PDF file. One of the files in the second PDF is an internet shortcut file (URL), which downloads a binary file that implements the decoding and execution of the Sosano backdoor via an image file. Proofpoint researchers noted that UNK_CraftyCamel's activity does not overlap with other known attackers or groups, but is most likely related to Iran given the target sectors.

Other

MintsLoader attacks

Researchers at ESentire reported on an ongoing campaign first identified in early January 2025. The campaign leverages a malware loader called MintsLoader to distribute secondary payloads such as the StealC information stealer and the legitimate open-source network computing platform Berkeley Open Infrastructure for Network Computing (BOINC). MintsLoader is a PowerShell-based malware loader that has been delivered via spam emails containing a link to Kongtuke/ClickFix pages or a JScript file. It features a Domain Generation Algorithm (DGA) with a seed value based on the current day of the month and a constant, combined with anti-VM techniques to evade sandboxes and malware researchers. The campaign has targeted electricity, oil and gas, and the legal services sectors in the United States and Europe.

Attacks with ZDI-CAN-25373 vulnerability

Trend Micro researchers uncovered both state-sponsored and cybercriminal groups extensively exploiting ZDI-CAN-25373 (aka ZDI-25-148), a Windows .lnk file vulnerability that allows attackers to execute hidden malicious commands on a victim's machine by leveraging crafted shortcut files. The attacks use hidden command-line arguments in .lnk files to execute malicious payloads, complicating detection. This vulnerability has been exploited by APT groups based in various countries, including Water Asena (Evil Corp), Earth Kumiho (Kimsuky, APT43), Earth Imp (Konni), Earth Anansi (Bitter), Earth Manticore (APT37). Since at least 2017, organizations in the government, financial, telecommunications, military, and energy sectors in North America, Europe, Asia, South America, and Australia have been affected. In the analysis of the campaigns exploiting ZDI-CAN-25373 and their associated intrusion sets, researchers found that nearly 70% focus primarily on espionage and information theft, and over 20% pursue financial gain. Malware payloads in attack chains that exploit ZDI-CAN-25373 include Lumma Stealer, GuLoader, Remcos, and commodity malware payloads. According to the researchers, Microsoft declined to patch the vulnerability because it does "not meet the bar for servicing".

CISA alert on Ghost/Cring ransomware group

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a joint cybersecurity advisory regarding Ghost (Cring) ransomware and its IOCs and TTPs identified in an FBI investigation as recently as January 2025. The entities affected by the ransomware include critical infrastructure, schools and universities, healthcare, government networks, religious institutions, technology and manufacturing companies, and numerous small- and medium-sized businesses in more than 70 countries.

According to the advisory, Ghost first appeared in 2021. Located in China, the group rotated their ransomware executable payloads, switched file extensions for encrypted files, modified ransom note texts, and used numerous ransom email addresses. This led to variable attribution of the group. Over time, the group has been identified as Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada, and Rapture.

The FBI has observed Ghost actors gaining initial access to networks by exploiting vulnerabilities in Fortinet FortiOS appliances (CVE-2018-13379), servers running Adobe ColdFusion (CVE-2010-2861 and CVE-2009-3960), Microsoft SharePoint (CVE-2019-0604), and Microsoft Exchange (CVE-2021-

34473, CVE-2021-34523, and CVE-2021-31207 – commonly referred to as the ProxyShell attack chain). Ghost actors have also been observed uploading a web shell to a compromised server and leveraging Windows Command Prompt and/or PowerShell to download and execute Cobalt Strike Beacon malware that is then implanted on victim systems. Ghost actors sporadically create new local and domain accounts and change passwords of existing accounts. In 2024, they were observed deploying web shells on victim web servers to establish persistence. They used elevated access and Windows Management Instrumentation Command-Line (WMIC) to run PowerShell commands on additional systems on the victim network, often to initiate more Cobalt Strike Beacon infections. The group's actors use Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe, all of which are ransomware executables with similar functionality.

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