Kaspersky ICS CERT

kaspersky

APT and financial attacks on industrial organizations in Q1 2026

21.05.2026

Version 1.0

Contents

Quarterly summary 3
Targets in Russia 4
Head Mare attacks 4
Stan Ghouls attacks 6
Vortex Werewolf attacks 6
Toy Ghouls attacks 7
Librarian Ghouls attacks 8
PseudoSticky attacks 9
Cyber groups targeting Russia 10
Russian-speaking activity 11
Attacks on Polish energy grid 11
APT28 attacks 13
Asia-related activity 14
SloppyLemming attacks 14
TGR-STA-1030 attacks 15
Chinese-speaking activity 16
UAT-8837 attacks 16
Middle East-related activity 16
MuddyWater attacks 16
Void Manticore attacks 18
Password-spraying campaign targeting cloud environments 19
Cybercriminal and others 20
LockBit 5.0 attacks 20
C77L attacks 21
Diesel Vortex attacks 21
Warlock attacks 22
Operation CamelClone 23
Hydra Saiga attacks 24

This summary provides an overview of reports on APT and financial attacks on industrial enterprises disclosed in Q1 2026, as well as the related activities of groups observed attacking industrial organizations. For each topic, we summarize the key facts, findings and conclusions of researchers that we believe may be useful to professionals addressing practical issues of cybersecurity in industrial enterprises.

Quarterly summary

After analyzing technical papers relating to attacks on industrial enterprises published in Q1 2026 by cybersecurity research teams, it can be assumed that some of the alarming discoveries from the previous quarter – Q4 2025 – may signify new trends in the evolution of the threat landscape.

One such new trend is cyberattacks on transportation and logistics companies aimed at physically stealing goods. The previously unknown Armenian-speaking group Diesel Vortex has chosen this cyber-physical method to monetize attacks on freight operators and logistics organizations in the USA and Europe. Another alarming trend that appears to be becoming part of everyday reality is the use of cyberattacks to gather information for planning and evaluating the effectiveness of military strikes. This appears to be evidenced by a Check Point Research publication. Some trends in the evolving threat landscape are driven by technical factors, such as the retooling of industrial enterprises and the latest technological advances that promise increased efficiency. For example, the growing popularity of Linux platforms is leading to an increased diversity of malicious tools designed for these platforms. In line with current technological advances, the number of cases involving the use of artificial intelligence in malware development and other stages of attacks targeting industrial enterprises is inevitably increasing.

It has been almost 16 years since the first publications about Operation Olympic Games, better known as Stuxnet, which ushered in the era of cyber-physical attacks. It became clear then that the genie could not be put back in the bottle. Everyone expected new operations of this kind, perhaps even more technically complex, large-scale, and daring. However, there was no significant continuation that lived up to this expectation. Publications about new attacks were rare, and the malicious campaigns themselves were increasingly straightforward, with less sophisticated tools. The number of such campaigns was likely limited by factors of interstate relations, and the rejection of complex tools appears to have been largely dictated by rational and technical considerations. It has become apparent that industrial automation systems are much more vulnerable to attack than was believed just 10 years ago. Currently,

most incidents involving cyberattacks on key production assets are caused by trivial information security issues within the affected organizations – as described by CERT Polska. However, as international political instability grows, the number of such incidents is increasing, the geographic scope of operations is expanding, and new players, sometimes associated with unexpected countries, are entering the arena.

Targets in Russia

Head Mare attacks

Cybercriminal

Spear phishing

Compromised legitimate mailboxes

Exploitation of public-facing applications

Backdoor

Replacement of legitimate applications

F6 researchers discovered a wave of malicious emails from the PhantomCore group (aka Head Mare), which they detected on January 19 and 21, 2026. The attackers used legitimate email addresses for their mailings, which suggests that these addresses may have been compromised. The campaign targeted Russian organizations in the housing utilities, finance, e-commerce, B2C, municipal services, aerospace, chemical, construction, manufacturing, and marketplace industries. The emails had the subject "ТЗ на согласование" ("Specifications for Approval") and included an attachment called "ТЗ на согласование сб 54 от 19.01.26.zip" ("Specifications for Approval Sat 54 from 01/19/26.zip") containing DOC and LNK files. The .doc file in the ZIP archive was a RAR archive containing a directory with the same name that contained files related to the actual document. After launching the LNK file, a cmd command was executed, initiating the download and execution of a PowerShell script. This script downloaded and displayed the decoy document, loaded the next-stage PowerShell script into memory, and established persistence for the next-stage script in Windows Task Scheduler. This next-stage PowerShell script was virtually identical to PhantomCore.PollDL (PhantomRemote).

At the end of 2025, Kaspersky analysts identified a new malicious campaign targeting organizations in Russia in government, construction, and manufacturing sectors that they attributed to the Head Mare threat group. The campaign continued into early 2026. As part of this activity, the group once again expanded its toolset by introducing a new PowerShell-base backdoor named PhantomHeart. Initially distributed as a DLL, it was later reworked into a PowerShell script. PhantomHeart implements a remote access channel that combines HTTP communication with the C2 and the ability to deploy an SSH tunnel upon request. Its persistence mechanism is activated by launching via the task scheduler under the guise of a legitimate update script located in the LiteManager directory. The researchers also discovered that the group repurposed the previously known PhantomProxyLite tool and implemented it

as a PowerShell script. The intrusion chain included the exploitation of the BDU:2025-10114 TrueConf vulnerability. In some cases, the group still used phishing emails.

Kaspersky researchers also discovered a large-scale phishing campaign by the Head Mare group, this time using a new version of the PhantomCore (PhantomDL) backdoor. This new Head Mare campaign affected several hundred users from Russian organizations, including in the public sector and companies from the logistics, financial, and industrial sectors. Recipients received emails purporting to be from a research organization offering contracts. The attachments contained encrypted archives with a series of LNK files that automatically launched the process of downloading and installing a backdoor. When any of the shortcuts was launched, a command was executed to download an intermediate script written in PowerShell located on the attackers' server. This script downloaded a new variant of PhantomCore written in C++ from a remote server, then downloaded and opened a decoy document, ensuring persistence in the system and enabling autorun. Persistence was achieved using the PSFactoryBuffer COM hijacking technique. The primary function of the new PhantomCore variant is to provide the attackers with a remote command prompt on the infected system. Once launched, the backdoor sends two POST requests to the C2 containing JSON data. In response, the attackers transmit a sequence of commands for the backdoor, including the command to download and unpack an archive. The archive contains a module for running ssh.exe, written in Golang. The module's persistence is achieved in the system using a scheduler task.

In March, Kaspersky researchers reported a new malware campaign by the Head Mare group targeting educational and scientific institutions, as well as energy sector organizations in Russia. The activity was detected in February 2026, but the campaign itself had been active since at least December 2025. Victims received a link inviting them to join a video conference. After clicking it, they were prompted to install a service to connect to the video call. During the installation process, the system was infected when a previously unknown backdoor named PhantomPxPigeon was installed on the victims' machines. At the time of the report's publication, the researchers also observed a new wave of similar activity, specifically a number of compromised TrueConf servers at various organizations in the transportation sector, as well as at scientific and educational institutions. The TrueConf client application distributions downloaded from these servers were replaced with malicious ones. The attack vector that led to the client application being replaced was unclear, but the attackers presumably exploited vulnerability BDU:2025-10116, identified by researchers and patched by the vendor in August 2025. The malicious distributions detected by Kaspersky did not have a valid digital signature.

Stan Ghouls attacks

Cybercriminal

Spear phishing

RAT

Backdoor

Linux malware

The Stan Ghouls group (also known as Bloody Wolf) has been orchestrating targeted attacks against organizations within the Russian Federation, Kyrgyzstan, Kazakhstan, and Uzbekistan since at least 2023. This group is known for its well-prepared attacks tailored to specific victims, primarily from the manufacturing, finance, and IT sectors, specialized Java-based malicious downloaders, and substantial infrastructure with dedicated resources allocated for specific campaigns. Kaspersky researchers revealed that the group initiated new campaigns against more than 50 victims in Uzbekistan and a limited number of victims in the Russian Federation, Kazakhstan, Turkey, Serbia and Belarus, though the latter three were likely collateral damage. Researchers analyzed the group's latest campaign and observed changes to the attackers' infrastructure, including newly identified domains. The group used phishing emails containing malicious PDF attachments. Previously, Stan Ghouls utilized the malicious remote access Trojan (RAT) STRRAT (Strigoi Master) as its primary payload. However, last year the group shifted its focus and began employing legitimate software – NetSupport – as its tool of choice. Indicators suggesting that this group has incorporated Mirai IoT malware into its arsenal were also identified.

Vortex Werewolf attacks

New threat actor

APT

Spear phishing

Telegram phishing

Phishing websites

Cloud services infrastructure

Tor network

In December 2025 and January 2026, BI.ZONE researchers detected malicious activity from a new Vortex Werewolf (aka SkyCloak) cluster targeting Russian organizations in the public administration and defense industries. Cyble and Seqrite reported that Vortex Werewolf had previously targeted Belarusian government and defense structures as well. According to network infrastructure research, Vortex Werewolf has been active since at least December 2024. The attackers use Cloudflare in their network infrastructure. The initial access method could not be determined, but it is believed that the attackers delivered malware via phishing emails and directly through the Telegram messenger. Victims were sent a link disguised as a Telegram address to download a document – an archive containing a malicious LNK file and an additional archive containing a set of files, including a PowerShell script. The phishing page simulated the process of downloading a file and initiated a procedure to restore access to the Telegram account. Users were asked to confirm their country code and enter their phone number, after which a confirmation code was sent to their Telegram app. If two-factor authentication was enabled for the account, the victim was also asked to enter their cloud password. This allowed Vortex Werewolf to obtain an active session of the user's Telegram account. To increase the credibility of the attack, in some

cases, the attackers placed a decoy document on the phishing page with intentionally blurred content.

The Vortex Werewolf group uses GitHub Pages to host static JavaScript and CSS resources, with a separate repository containing those resources created for each phishing domain. After successfully verifying the entered code and password with two-factor authentication enabled, a link is generated. Clicking the link initiates the download of a ZIP archive hosted on Dropbox that contains an LNK file. Following a successful compromise, Tor and OpenSSH are installed on the system, using obfs4 bridges rather than public Tor entry nodes to communicate with the control infrastructure. Remote access is also configured through the Tor network using RDP, SMB, SFTP, and SSH. The malware persists in the Windows Task Scheduler by creating tasks. Researchers note that Vortex Werewolf resembles the Core Werewolf group (aka Awaken Likho). The clusters have similar targets and attack regions, and use SSH to establish remote access to compromised systems, as well as military-related decoy documents. However, BI.ZONE did not have sufficient data to definitively attribute Vortex Werewolf to Core Werewolf, so this activity is considered a separate threat cluster.

Toy Ghouls attacks

Cybercriminal

Ransomware

Linux malware

Exploitation of public facing applications

Trusted relationship

Toy Ghouls (also known as Bearlyfy or laboo.boo) is a financially motivated group active since at least January 2025. The group exclusively targets Russian organizations with ransomware from the LockBit and RedAlert families for Windows systems, and Babuk for Linux and ESXI. The main industries targeted by the attackers are manufacturing, construction, automotive, and telecommunications. There are also indications of possible connections to the Head Mare group, based on the use of the same tools and network infrastructure. Kaspersky researchers analyzed their techniques and procedures using a unified kill chain methodology. A common initial access vector involves third-party contractors, where the attackers leverage stolen user certificates to authenticate to a customer's VPN. After establishing VPN access, they use RDP to connect to internal systems and traverse the victim's environment further. The Toy Ghouls group often exploits vulnerable 1C servers by uploading 1C-Shells via separate .epf files. To discover the internal network, the attackers use SoftPerfect Network Scanner and fscan, which can search for and exploit vulnerabilities. Toy Ghouls uses scheduled tasks to execute its activities on compromised hosts, PowerShell to execute malicious scripts, and the Windows command shell and Bash to execute commands on *nix systems.

F6 researchers also tracked the latest activity of the Bearlyfy/Toy Ghouls group, which has carried out over 70 attacks on Russian companies since its

emergence. Bearlyfy initially used LockBit 3 Black for Windows and its own modified version of the Babuk ransomware to encrypt data on Linux systems. Since May 2025, several attacks have used a slightly modified version of the PolyVice ransomware from the well-known RaaS Vice Society. According to F6, since March 2026, Bearlyfy began using its own ransomware program for Windows called GenieLocker. Its cryptographic scheme and approaches are clearly borrowed from the Venus/Trinity families of ransomware. F6 believes the malware authors focused too much on demonstrating their knowledge of cryptography and anti-analysis techniques and trying to outperform LockBit 3 with their creation. F6 also observed Bearlyfy collaborating with other, more experienced pro-Ukrainian groups, such as Head Mare. However, Bearlyfy has maintained its own distinct style from the very beginning. Perhaps the group's decision to re-equip itself with its own ransomware is motivated by a desire to stand out from other groups.

Librarian Ghouls attacks

APT

Spear phishing

RAT

Kaspersky researchers reported Librarian Likho (Librarian Ghouls) activity that was detected in November 2025. The new wave of attacks targeted a wide range of Russian organizations from various sectors, including the public sector, construction, and manufacturing. The attacks began with phishing; the actor sent over a thousand emails containing malicious attachments that were virtually identical in functionality and context, indicating an automated attack. In this new campaign, victims received a phishing email with a malicious executable file disguised as a collaboration offer or a completed contract form. The attachment is an installer created using Smart Install Maker. Once launched, it drops two .cab archives containing a decoy Office document, a text file with C2 addresses, an executable file, and scripts. The malicious attachment then launches a CMD file from the archive that parses the C2 addresses from the text file. During execution, it creates a virtual environment and variables for specific addresses from which payloads are downloaded. The script downloads two RAR archives from the C2 server, as well as a custom version of WinRAR. It then unpacks the downloaded files using the archiver and a hardcoded password. The RAR archives contain an AnyDesk remote host management executable, a utility for disabling Windows Defender, a utility for exfiltrating data via SMTP, a utility for hiding windows of running processes, a utility for recovering passwords from email clients, and a script for password exfiltration and bypassing information security tools. The last script's main purpose is to provide the operator with connection data and prepare the node for further post-exploitation activities. Ultimately, the malicious attachment launches this script.

PseudoSticky attacks

New threat actor

APT

Spear phishing

RAT

AI-generated code

In November 2025, F6 researchers discovered a malware campaign in which a new group of attackers used PureCrypter and DarkTrack RAT malware. One of the malicious components – the HTA file that initiated the DarkTrack RAT download – was likely created using LLM. This assumption is supported by the simplicity of the code, its formatting, and good documentation with no grammatical errors. Further examination revealed various connections between the new group and the Sticky Werewolf group, primarily in terms of TTPs and tools used, as well as direct references by the actors (in one case, the group used the "StickyWerewolf" string as a password for a malicious archive), thus the new group was dubbed PseudoSticky. Upon closer analysis, differences in infrastructure, malware implementation, and individual tactical elements became apparent, suggesting deliberate mimicry. Since December 2025, PseudoSticky attacks have targeted businesses in various sectors, including retailers, construction and developers, research organizations and instrument-making companies.

PseudoSticky uses spear-phishing emails with malicious archive attachments. The main types of lures are files with names related to the military industry, from aircraft missiles to drones, as well as files disguised as software licenses and other documentation. The final payloads were DarkTrack RAT and Remcos RAT. In one infection chain, a custom loader was used. The loader downloaded a list of C2 addresses from a Bitbucket resource. Requests to these C2 addresses resulted in the download of another payload that the researchers didn't retrieve. However, on the payload's web page on the public online sandbox, there was a comment stating that the payload was a Remcos RAT, as well as markings identifying it as belonging to the StickyWerewolf group. Moreover, a config of this sample, corresponding to Remcos RAT, was found on another public online sandbox.

Cyber groups targeting Russia

Cybercriminal

APT

Spear phishing

RAT

Exploitation of public-facing applications

DLL sideloading

Linux malware

Positive Technologies researchers published an analysis of the activity of cyber groups targeting Russian organizations in the fourth quarter of 2025, along with TTPs and victimology. PT classified the groups as either cyberespionage or financially motivated. These groups targeted companies in the aerospace, logistics, manufacturing, energy sectors, among others.

Cyberespionage activities include those of the ExCobalt group (Shedding Zmiy, Red Likho, Cobalt Werewolf), which compromises contractors and gains access through published RDP services, and uses the Cobint backdoor for remote control and post-exploitation. To encrypt the infrastructure, the group uses Babuk for Linux hosts and VMware ESXi hypervisors, and LockBit for Windows nodes. ExCobalt compromises Telegram accounts by stealing the tdata directory on victims' devices. One method of gaining a foothold in the attacked infrastructure, previously unseen in ExCobalt's arsenal, is to place shells as separate .epf files that implement external processing mechanisms in 1C software products. ExCobalt uses the PUMAKIT kernel-level rootkit in Linux systems to provide long-term resilience and stealth. Another cyberespionage group, QuietCrabs (Subtle Werewolf, UTA0178, UNC5221, Red Dev 61), was observed exploiting vulnerable services (CVE-2025-4427, CVE-2025-4428, and CVE-2025-53770) and downloading KrustyLoader malware and the Sliver cross-platform implant. The report also mentions the activities of cyberespionage groups such as APT31 (Zirconium, Fair Werewolf, Violet Typhoon, Bronze Vinewood, Judgment Panda, Sheathminer), Rare Werewolf (aka Librarian Ghouls, Librarian Likho, Rezet), and PseudoGamaredon (Awaken Likho, Core Werewolf, and GamaCopy) that use phishing emails as the initial attack vector.

Financially motivated activity includes Werewolves (aka Lone Wolf, Moonshine Trickster), NetMedved (aka Clubfoot Wolf), Silver Fox (aka Void Arachne), Hive0117 (aka Watch Wolf, Ratopak Spider, UAC-0008), all of which use phishing emails with malicious archives. The Werewolves group deploys Cobalt Strike Beacon in the final stage; the NetMedved group deploys NetSupport Manager (NetSupportRAT); the Silver Fox group deploys ValleyRAT; and the Hive0117 group deploys PowerShell keylogger and a malicious JavaScript script.

Russian-speaking activity

Attacks on Polish energy grid

APT

Wiper

Exploitation of network and ICS devices

Attacks targeting ICS

On January 13, Poland's energy minister announced at a press conference that there had been attempted attacks on the Polish energy sector at the end of 2025. According to a January 15 statement on the Polish government website, the targeted systems included combined heat and power plants as well as a system that manages power derived from renewable energy resources, such as wind turbines and photovoltaic farms. The attacks did not result in any negative consequences, such as destabilization of the national energy system or a blackout.

On January 23, researchers at ESET published a blog post describing the attack on Poland's power grid. The researchers mentioned a wiper dubbed DynoWiper that was used in the attack and attributed it to the Sandworm APT with medium confidence due to a strong overlap with numerous previously analyzed Sandworm wiper activities. On January 30, ESET researchers published more technical details about the incident involving DynoWiper that affected a company in Poland's energy sector. According to the post, the discovered DynoWiper samples focus solely on the IT environment, with no observed functionality targeting the industrial components of operational technology.

On January 30, CERT Polska published an Energy Sector Incident Report on the December 29 cyberattacks. According to the report, the attacks affected at least 30 wind and solar farms, a private manufacturing company, and a combined heat and power (CHP) plant supplying heat to nearly half a million customers in Poland. The report described the attack vectors and initial access used by the threat actors, and provided a list of indicators of compromise (IoC).

In each affected facility, a FortiGate device served as both a VPN concentrator and a firewall. In every case, the VPN interface was exposed to the internet and allowed authentication to accounts defined in the configuration without multifactor authentication. Some of those devices were found to have been vulnerable in the past, including to remote code execution vulnerabilities. In the case of a manufacturing organization, after gaining access to the device, the attacker made changes intended to maintain persistent access, even if user passwords were changed.

At the time of the attack, the threat actor had administrative privileges on the device. These privileges were likely used to obtain credentials for a VPN account with access to all subnets. The attacker used the credentials obtained from the on-premises environment in attempts to gain access to cloud

services. After identifying accounts in the M365 service that corresponded to the credentials, the attacker downloaded selected data from services such as Exchange, Teams, and SharePoint. The attacker was particularly interested in files and email messages related to OT network modernization, SCADA systems, and technical work carried out within the organizations. The attacker also attempted to expand their privileges by exploiting misconfigured permissions. The attacks involved DynoWiper and LazyWiper. DynoWiper malware was used in the incident involving renewable energy farms and was executed directly on the HMI machine. In contrast, at the CHP plant (DynoWiper) and the manufacturing sector company (LazyWiper), the malware was distributed within the Active Directory domain via a PowerShell script executed on a domain controller.

CERT Polska's report identified three ICS vendors whose products were targeted in the attack: Hitachi Energy, Moxa, and Mikronika. In the case of Hitachi, targeted devices included RTU560 remote terminal units (RTUs), which threat actors accessed using default credentials. This allowed the attackers to upload malicious firmware. Researchers found that a security feature intended to prevent malicious firmware updates had not been enabled, but even if it had been, the devices were affected by CVE-2024-2617, a known vulnerability allowing unsigned firmware updates. According to CERT Polska, the threat actors also targeted Hitachi Relion protection and control relays. They gained access to these devices because of the failure to disable a default FTP account and the use of default credentials. The attackers also targeted RTUs and human-machine interfaces (HMIs) made by Mikronika. Both types of ICS devices were protected with default credentials. Moxa NPort serial device servers were also targeted. These devices had the web interface enabled and were configured with default login credentials. Analysis of the attack infrastructure showed a high degree of overlap with that used by the activity cluster publicly known as Static Tundra (Cisco), Berserk Bear (CrowdStrike), Ghost Blizzard (Microsoft), and Dragonfly (Symantec).

APT28 attacks

APT

Spear phishing

Backdoor

Cloud services infrastructure

Compromised legitimate mailbox

DLL sideloading

Zero-day vulnerability

Wiper

At the beginning of February, CERT-UA and Zscaler reported that the UAC-0001 (aka APT28, Fancy Bear) group had launched attacks exploiting the CVE-2026-21509 vulnerability against Ukrainian government agencies and public sector organizations in Slovakia and Romania. CVE-2026-21509 allows an unauthorized local attacker to bypass Object Linking and Embedding (OLE) mitigations when a targeted user opens a malicious Office file because of the reliance on untrusted inputs in a security decision. Social engineering lures were crafted in both English and localized languages (Romanian, Slovak and Ukrainian). The threat actor employed server-side evasion techniques, responding with the malicious DLL only when requests originated from the targeted geographic region and included the correct User-Agent HTTP header. Zscaler researchers discovered two variants of a dropper that led to the deployment of MiniDoor, an Outlook macro-based email stealer, and PixyNetLoader that led to deployment of a Covenant Grunt implant.

In a report released on February 4, Trellix researchers noted broader APT28 activity targeting maritime, transportation, and diplomatic entities in countries including Poland, Slovenia, Turkey, Greece and the United Arab Emirates. According to the report, the attacks were part of a concentrated 72-hour spear-phishing campaign that sent at least 29 distinct emails across nine Eastern European countries. The hackers exploited the newly disclosed CVE-2026-21509 vulnerability within 24 hours of the company's January 26 emergency security advisory that addressed the flaw. The phishing messages were sent from compromised government email accounts in several countries, including Romania, Bolivia and Ukraine. The attackers used geopolitically themed lures such as transnational weapons-smuggling alerts, military training program invitations, NATO and European Union diplomatic invitations, and meteorological emergency bulletins. The attached documents were designed to resemble legitimate government correspondence and may have been based on previously stolen material. Once opened, the files deployed a series of tools, including MiniDoor and PixyNetLoader, which ultimately installed a Covenant backdoor on infected systems. The campaign also made extensive use of legitimate cloud services to obscure malicious activity. According to researchers, APT28 used the cloud storage platform Filen.io as a C2 channel, enabling the malware to blend in with normal internet traffic.

Trend Micro identified a campaign by the Pawn Storm APT group (aka APT28, Fancy Bear, UAC-0001, and Forest Blizzard) that deployed a malware suite called PRISMEX against Ukraine's defense supply chain and its NATO allies. Active since at least September 2025, the campaign significantly escalated in January 2026. It exploited two Microsoft vulnerabilities: CVE-2026-21509 and

CVE-2026-21513, a protection mechanism failure in the MSHTML framework that was exploited as a zero-day at least 11 days before Microsoft's patch. Infrastructure preparations for CVE-2026-21509 began two weeks before public disclosure, indicating advance knowledge. PRISMEX consists of four components: PrismexSheet, a macro-enabled Excel dropper that uses steganography to conceal payloads within the file itself; PrismexDrop, a native dropper that establishes persistence via COM hijacking; PrismexLoader, a proxy DLL that reconstructs payloads from steganographic PNG images using a custom "Bit Plane Round Robin" algorithm unique to Pawn Storm; and PrismexStager, a Covenant Grunt implant that abuses the Filen.io cloud storage service for encrypted C2 communications. Post-exploitation activity included both data collection and a destructive wiper command that deleted files under the user profile directory, indicating the intent to engage in both espionage and sabotage. The campaign was corroborated by CERT-UA, Zscaler ThreatLabz, Synaptic Systems, and Akamai.

Asia-related activity

SloppyLemming attacks

APT

Spear phishing

Backdoor

Cloud services infrastructure

DLL sideloading

Between January 2025 and January 2026, Arctic Wolf tracked an extensive cyberespionage campaign targeting government entities and critical infrastructure operators in Pakistan and Bangladesh that researchers believed was conducted by SloppyLemming (aka Outrider Tiger, or Fishing Elephant). The group has evolved from using off-the-shelf red teaming tools, like Cobalt Strike and Havoc C2, to developing its own custom tools written in the Rust programming language. The group also expanded its command-and-control infrastructure, which is based on Cloudflare's Workers service, to at least 112 domains, up from 13 a year ago. The campaign employed two distinct attack chains. The primary vector delivered PDF lure documents that redirected victims to ClickOnce application manifests, which deployed a DLL sideloading package consisting of a legitimate Microsoft .NET runtime executable (NGenTask.exe) and a malicious loader (mscorsvc.dll). This loader decrypted and executed a custom x64 shellcode implant named BurrowShell by Arctic Wolf. The second attack vector used a malicious Excel spreadsheet containing a VBA macro that executed when the document was opened. The macro then downloaded two files: a legitimate Microsoft binary (phoneactivate.exe) used for DLL sideloading, and a malicious loader (sppc.dll), which is a Rust-based keylogger with extended reconnaissance capabilities, including port scanning and network enumeration. Based on the content of multiple lure documents, C2 domain naming conventions, VirusTotal submission metadata, and

infrastructure analysis, the researchers assessed that this threat actor had targeted the nuclear, defense, telecommunications, and government sectors in Pakistan, the energy, financial, and media sectors in Bangladesh, and the defense sector in Sri Lanka.

TGR-STA-1030 attacks

APT

New threat actor

Spear phishing

Backdoor

Rootkit

Linux malware

Exploitation of network devices and public-facing applications

According to a report by Palo Alto Networks' Unit 42, a state-sponsored cyberespionage group based in Asia, tracked as TGR-STA-1030 (aka UNC6619), breached the systems of at least 70 government and critical infrastructure entities in 37 countries over the past year and conducted reconnaissance in 155 countries between November and December 2025. The group has been active since at least January 2024. Unit 42 assessed that, in addition to government organizations, the threat group compromised entities that included Brazil's Ministry of Mines and Energy, a Bolivian entity associated with mining, the Venezolana de Industria Tecnológica facility, an Indonesian airline, a major Taiwanese power equipment supplier, as well as critical infrastructure entities in the Democratic Republic of the Congo, Djibouti, Ethiopia, Namibia, Niger, Nigeria, and Zambia. By closely monitoring the timing of the group's operations, researchers have drawn correlations between several of its campaigns and real-world events. Early operations relied on highly tailored phishing emails sent to government officials. The emails contained links to malicious archives with localized names hosted on the Mega[.]nz storage service. The compressed files contained a malware loader called Diaoyu and a zero-byte PNG file. After certain prerequisites were met, the Diaoyu loader fetched Cobalt Strike payloads and the Go-based C2 VShell framework.

The TGR-STA-1030/UNC6619 toolkit also included web shells such as Behinder, Godzilla, and Neo-reGeorg, as well as network tunneling tools like GO Simple Tunnel (GOST), Fast Reverse Proxy Server (FRPS), and IOX. Unit 42 researchers also discovered a custom Linux kernel eBPF rootkit called ShadowGuard that they believe is unique to the TGR-STA-1030/UNC6619 threat actor. Apart from phishing, TGR-STA-1030/UNC6619 also exploited at least 15 known vulnerabilities to achieve initial access, including those in SAP Solution Manager, Microsoft Exchange Server, D-Link, Ruijieyi Networks, Eyou Email System and Microsoft Windows. The researchers noticed the use of C2 domains that would appear familiar to the target: in attacks on French-speaking countries, the attackers used the gouvn[.]me domain, and in attacks on European countries, the dog3rj[.]tech domain.

Chinese-speaking activity

UAT-8837 attacks

APT

Exploitation of public-facing applications

Zero-day vulnerability

Backdoor

Cisco Talos tracked UAT-8837, a threat actor assessed with medium confidence to be a Chinese-speaking APT based on overlapping tactics, techniques, and procedures with other known Chinese-speaking threat actors. According to Cisco Talos, the group has focused on critical infrastructure sectors in North America since at least 2025. Their TTPs and post-compromise activity indicate that they are primarily tasked with obtaining initial access to high-value organizations. UAT-8837 gains initial access either through successful exploitation of vulnerable servers, including a recently exploited ViewState Deserialization zero-day vulnerability (CVE-2025-53690) in SiteCore products, or by using compromised credentials. After obtaining access, the threat actor primarily deploys open-source tools to harvest sensitive information such as credentials, security configurations, and Active Directory information to create multiple channels of access. Their toolkit includes Earthworm for network tunneling, SharpHound for AD reconnaissance, DWAgent for remote administration, Certipy for AD discovery and abuse, GoExec for remote command execution, Rubeus for Kerberos abuse, and Impacket-based binaries. The actor cycles through different tool variants to evade detection and creates backdoored user accounts for persistent access. In one case, the actor exfiltrated DLL-based shared libraries related to the victim's products, raising the possibility of future supply-chain compromises or reverse engineering to find vulnerabilities.

Middle East-related activity

MuddyWater attacks

APT

Spear phishing

RAT

Backdoor

Telegram C2

AI-generated code

CloudSEK researchers identified a spear-phishing campaign attributed to the MuddyWater APT group (aka Earth Vetala, MERCURY, Mango Sandstorm, Static Kitten, and TA450) targeting multiple sectors across the Middle East, including diplomatic, maritime, financial, and telecom entities. Spear-phishing emails masquerading as cybersecurity guidelines were sent with a Microsoft Word document containing a malicious VBA macro responsible for deploying the Rust implant binary dubbed RustyWater. Also referred to as Archer RAT and RUSTRIC, RustyWater gathers information about the victim machine, detects installed security software, sets up persistence through a Windows Registry key, and establishes contact with a C2 server to facilitate file

operations and command execution. The macro code extracted from the phishing document exhibits striking similarities to previously documented MuddyWater campaigns, specifically the WriteHexToFile and love_me_ function patterns, including the distinctive use of hex encoded payload embedding within UserForm controls. Upon further investigation, CloudSEK researchers found many similar lures targeting the UAE and the Middle East. The campaign analyzed in the CloudSEK report overlaps significantly with the Seqrite Labs report. The use of RUSTRIC was flagged by Seqrite Labs in December 2025 as part of a campaign targeting IT, MSPs, human resources, and software development companies in Israel. The cybersecurity company tracks this activity under the names UNG0801 and Operation IconCat.

The Group-IB Threat Intelligence Team reported a new MuddyWater campaign, dubbed Operation Olalampo, targeting a number of organizations and individuals primarily located in the MENA region. The new activity was first observed on January 26, 2026. The campaign starts with spear-phishing emails containing a Microsoft Office document with a malicious macro and concludes with the deployment of a new second-stage downloader or backdoor. Specifically, GhostFetch, the HTTP_VIP downloader, a Rust backdoor called CHAR and an advanced GhostBackDoor implant were spotted.

The first observed chain was a malicious Microsoft Excel document mimicking an energy and marine services company in the Middle East. The targets of this variant were likely contractors associated with the organization or the company itself. This variant led to the deployment of the CHAR backdoor. The second chain adopted the same theme for the same energy and marine services company, but the document led to the deployment of the GhostFetch downloader, which subsequently downloaded GhostBackDoor. The third variant was a Microsoft Word document with multiple themes such as flight tickets and reports. This variant resulted in the deployment of the HTTP_VIP downloader, which then deployed Anydesk RMM.

GhostFetch is a first-stage downloader that profiles the system, monitors mouse movements and screen resolution, checks for debuggers, virtual machine artifacts, and antivirus software, and loads and executes secondary payloads directly in memory. GhostBackDoor is a second-stage backdoor implemented by GhostFetch that supports an interactive shell, file reading/writing, and re-launching GhostFetch. HTTP_VIP is a downloader that performs system reconnaissance, connects to an external server for authentication, and deploys AnyDesk from the C2 server. CHAR is a Rust backdoor that is controlled by a Telegram bot (named Olalampo and with the username stager_51_bot) that allows directory hopping and execution of cmd.exe or PowerShell commands. Executing PowerShell commands involved

launching a SOCKS5 reverse proxy or another backdoor called Kalim, exfiltrating data from browsers, and launching unknown executables that could not be retrieved. An analysis of CHAR's source code revealed signs of AI-assisted development, including the presence of emojis in debug strings.

Palo Alto Networks' Unit 42 provided a comprehensive threat assessment of Boggy Serpens' (aka MuddyWater) activities over the last year. Social engineering and phishing emails remained its defining traits. The group conducted a targeted campaign against a national marine and energy company in the Middle East. Researchers identified four distinct waves of attack against this single entity from August 2025 through February 2026, demonstrating the group's attempts to infiltrate regional maritime infrastructure. The first campaign targeted project engineers using industry-specific terminology for subsea pipelines. The lure document contained an embedded macro. The second attack deployed an Excel file that mimicked the target's internal financial records. This lure was designed to look like a spreadsheet containing payment and cash flow projections. The group launched a parallel spear-phishing effort targeting an individual associated with the company. The attackers created a Word document with a personalized Air Arabia flight reservation that deployed malware named GhostBackDoor, previously reported by Group-IB. A fourth attack utilized an Excel file that delivered an entirely new payload family known as Nuso (named HTTP_VIP by Group-IB).

Over the last year, Boggy Serpens systematically hijacked official government and corporate accounts to bypass standard email filtering. In recent campaigns, the group used several tools designed for persistence and evasion: the UDPGangster backdoor, the BlackBeard Rust-based backdoor, and LampoRAT (aka CHAR or Olalampo), which is written in Rust and leverages the Telegram Bot API C2. The latter RAT masqueraded as a Kaspersky Anti-Virus software executable file (avp.exe) and embedded the string "Kaspersky" in the file's metadata. Additionally, a distinct stylistic artifact was found within the binary file strings, strongly suggesting the threat actor used generative AI to accelerate development.

Void Manticore attacks

Hacktivist

Wiper

AI-generated code

Researchers from Check Point Research published a technical profile of Void Manticore (aka Storm-0842, Red Sandstorm, and Banished Kitten), describing the actor as conducting destructive "hack-and-leak" operations. The threat actor operates several online personas, including Handala Hack, and has been responsible for multiple intrusions in Israel. Recently, it has expanded its targeting to US-based enterprises, such as the medical devices and equipment manufacturer Stryker.

Over the last few months, Check Point identified hundreds of logon and brute-force attempts against organizational VPN infrastructure linked to Handala-associated infrastructure. This activity typically originated from commercial VPN nodes. In a recent intrusion attributed to Handala, it is believed that initial access was established well before the destructive phase, with network access dating back several months. To reach hosts that were not directly accessible from outside the network, the group was observed manually deploying NetBird. During the destructive phase of the attack, researchers observed the group deploying four distinct wiping techniques in parallel.

The first one involved the deployment of a custom wiper, referred to as Handala Wiper capable of both rewriting file data and whipping out MBR. The wiper was distributed across the network as a scheduled task using Group Policy logon scripts that executed a batch file.

Alternatively, the attackers deployed an additional, custom, PowerShell-based wiper that was also distributed through Group Policy logon scripts. Based on the code structure and detailed comments, it is likely that this PowerShell script was developed with the help of AI.

In addition to the custom wiping tools, the attackers attempted to leverage VeraCrypt, a legitimate and widely used disk encryption utility. In this case, they connected to the compromised host via RDP and used the system's default web browser to download the software directly from the official website.

In some cases, Handala Hack operators manually deleted virtual machines directly from the virtualization platform or files from compromised machines. This straightforward process involved logging in via RDP, selecting all the files, and deleting them.

RDP connections used by the attackers were initialized from default hostnames in the format DESKTOP-XXXXXX or WIN-XXXXXX.

Password-spraying campaign targeting cloud environments

APT

Exploitation of public-facing applications

Suspected cyber-kinetic targeting

Researchers from Check Point Research reported the discovery of a large-scale password-spraying campaign targeting Microsoft 365 accounts belonging to public and private organizations, which began in early March. The attacks primarily targeted Israeli organizations, but organizations in the UAE, Saudi Arabia, Europe, the United States and the United Kingdom were also targeted. The scanning was conducted from Tor exit nodes that were frequently changed to avoid blocking. The scan used a user agent that masqueraded as Internet Explorer 10 (IE10): Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0). When the attackers found valid credentials, they

conducted the full login process from VPN IP addresses (Windscribe IP range 185.191.204.X or NordVPN IP range 169.150.227.X) geolocated in Israel to evade geographic restrictions. While similar campaigns are common, this one caught the researchers' attention because they observed a correlation between the campaign's targets and cities targeted by Iranian missile strikes in March, suggesting support for kinetic operations and damage assessment activities following the bombings. Check Point Research assessed with moderate confidence that the actor behind the M365 password-spray activity originates from Iran. This assessment is based on the activity profile aligning with Iranian interests, such as targeting Israeli local government entities and organizations in the satellite, aviation, energy, and maritime sectors. Analysis of M365 logs suggests similarities to Gray Sandstorm, including the use of red-team tools to conduct attacks via Tor exit nodes. The threat actor used commercial VPN nodes hosted at AS35758 (Rachamim Aviel Twito), aligning with recent activity tied to Iran-nexus operations in the Middle East.

Cybercriminal and others

LockBit 5.0 attacks

Cybercriminal

Ransomware

Linux malware

Double extortion

In September 2025, a new version of LockBit ransomware was released that was compatible with Windows, Linux and ESXi systems. According to the threat actors, the new version has improved defense evasion and faster encryption. The threat actors claimed the ransomware was capable of working on all versions of Proxmox, an open-source virtualization platform being adopted by enterprises as an alternative to commercial hypervisors. This makes Proxmox another prime target of ransomware attacks. The Acronis Threat Research Unit (TRU) analyzed version 5.0 of the LockBit ransomware and its victims based on a data leak site. According to the affiliate program page on the data leak site, LockBit permits affiliates to target any organization, including critical infrastructure and medical facilities. However, LockBit prohibits attacks on countries in the post-Soviet region. After analyzing the latest victims from data leak sites, the researchers noted that private businesses were the primary target of LockBit. Other victims included medical facilities, financial and manufacturing companies, and government and educational agencies. Most victims were in the US, as well as in Italy, Brazil, Spain and Mexico. LockBit 5.0 employs the same encryption scheme as its predecessor: XChaCha20 for symmetric and Curve25519 for asymmetric encryption. The new version also introduced a mutex option to ensure that only one instance runs in an environment at a time, as well as a wiper component and a feature that allows it to delay execution prior to encryption.

C77L attacks

Cybercriminal

Ransomware

Exploitation of public facing applications

F6 researchers highlighted ransomware group that has attacked more than 40 Russian and Belarusian companies in less than a year. The C77L ransomware-as-a-service (RaaS) emerged in March 2025 and has targeted Russian and Belarusian small and medium-sized businesses, primarily in the trade, manufacturing, and service sectors. State-owned companies were also among the victims. By the end of 2025, C77L ranked sixth in the number of ransomware attacks. Researchers believe that C77L was created as a separate affiliate program by Proton threat actor participants. The C77L ransomware shares similarities with families such as Proton, Proxima, and LokiLocker. Developed in the C++ programming language, C77L is characterized by its high file encryption speed. In nine months, the developers released five versions of the ransomware. C77L attacks are short-lived, with attackers not aiming to exfiltrate victims' data, focusing entirely on encrypting information as a key means of obtaining quick and stable financial gain. According to F6, C77L's primary initial attack vector is brute-force attacks on publicly accessible remote access service accounts (RDP and VPN). The attackers typically penetrate the victim's infrastructure at night. These attacks only target Windows systems. C77L attackers employ the techniques with no sophisticated or innovative methods. The attackers do not require advanced skills; they follow standard instructions and use ready-made scripts to automate most actions. Nevertheless, most of the attacks on Russian and Belarusian enterprises were successful.

Diesel Vortex attacks

Cybercriminal

New threat actor

Spear phishing

Cyber and traditional crime convergence

In February 2026, researchers at the domain protection platform Have I Been Squatted, in collaboration with Ctrl-Alt-Intel, discovered a financially motivated threat group dubbed Diesel Vortex. The group stole credentials from freight and logistics operators in the USA and Europe through phishing attacks using 52 domains. In a campaign that had been running since September 2025, the threat actor had stolen 1649 unique credentials from critical freight industry platforms and service providers. The researchers uncovered the campaign after finding an exposed .git directory containing an SQL database from a phishing project that the threat actor called GlobalProfit and marketed to other cybercriminals under the name MC Profit Always. The repository also included a file with Telegram webhook logs that revealed communications between the phishing service operators. Based on the language used, the researchers believe Diesel Vortex is an Armenian-speaking actor.

The Diesel Vortex group built dedicated phishing infrastructure for platforms used daily by freight brokers, trucking companies, and supply chain operators.

This included load boards, fleet management portals, fuel card systems, and freight exchanges. The attacks involved sending phishing emails to targets via a phishing kit's mailer using Zoho SMTP and Zeptomail, and combining Cyrilic homoglyph tricks in the sender and subject fields to evade security filters. Voice phishing and infiltration into Telegram channels frequented by trucking and logistics personnel were also used in the attacks. When a victim clicked on a phishing link, they were directed to a minimal HTML page on a '.com' domain with a full-screen iframe that loaded the phishing content, followed by a nine-stage cloaking process on the system domain (.top/.icu). The phishing pages were pixel-level clones of the targeted logistics platforms. Depending on the target, the pages captured credentials, permit data, MC/DOT numbers, RMIS login details, PINs, two-factor authentication codes, security tokens, payment amounts, payee names, and check numbers. The phishing operator used Telegram bots to decide when to approve steps and activate the next phases. Possible actions included requesting passwords for Google, Microsoft Office 365, and Yahoo, use of 2FA methods, redirecting the victim, or even blocking them mid-session.

According to the researchers, the Diesel Vortex operation, including panel and phishing domains and GitLab repositories, was disrupted following coordinated action involving GitLab, Cloudflare, Google Threat Intelligence, CrowdStrike, and the Microsoft Threat Intelligence Center. Based on the evidence that was uncovered, the researchers determined that Diesel Vortex stole credentials and coordinated activities related to freight impersonation, mailbox compromise, and double brokering or cargo diversion. Double brokering involves the use of stolen carrier identities to book loads and then reassigning or diverting freight cargo. This allows the goods to be sent to fraudulent pickup points so they can be stolen.

Warlock attacks

Cybercriminal

Ransomware

Exploitation of public-facing applications

BYOVD

DLL sideloading

Trend Micro researchers have identified new tactics, techniques, and procedures (TTPs) used by the Warlock ransomware group. The group has added new techniques to enhance its persistence, lateral movement, and defense evasion. These new observations include the use of the TightVNC remote access tool to maintain persistent control, abuse of new open-source tools to conduct C2 communications, and a persistent Bring Your Own Vulnerable Driver (BYOVD) technique that leverages a vulnerability in the NSec driver to continuously terminate security processes. Warlock's method of gaining initial access to victim networks has remained consistent and includes exploiting unpatched Microsoft SharePoint servers. According to Trend Micro telemetry, the SharePoint worker process (w3wp.exe) was observed spawning

the Cobalt Strike beacon agent. This agent utilizes the DLL-sideloading technique with the legitimate Microsoft Edge browser binary MsMpSrv.exe, the EndProcess.exe utility, which was likely used to terminate security products or other processes, and msiexec.exe, which was used to silently download and install the legitimate Velociraptor tool disguised as "v4.msi" and hosted on Supabase cloud storage. The W3wp.exe process was also observed writing the web shell cproxy.aspx to disk, confirming post-exploitation persistence within the IIS/SharePoint environment. The attackers were also found to be using Yuze, a new and lightweight open-source tunneling tool. This purely C-based tool is designed for intranet penetration and supports forward and reverse SOCKS5 proxy tunneling. The threat actors weaponized Active Directory Group Policy for the mass distribution of ransomware components that are placed in SYSVOL and NETLOGON shares. Based on the group's leak site from the second half of 2025, the technology, manufacturing, government and education sectors were among the most targeted industries. The most targeted countries were the USA, UK, Germany, and Russia.

Operation CamelClone

APT

Spear phishing

Cloud services
C2

The Seqrite Labs APT Team identified a campaign dubbed Operation CamelClone targeting multiple countries. The affected entities included government agencies, defense and military organizations, foreign affairs and international cooperation departments, policy and diplomatic institutions, and energy and strategic resource sectors in Algeria, Mongolia, Ukraine and Kuwait. The attackers used spear-phishing emails with ZIP attachments. One of the attachments contained an LNK file and a lure image with the logo of MonAtom LLC, a state-owned Mongolian company responsible for uranium exploration and nuclear energy development. The LNK file contained a malicious PowerShell command that connected to an anonymous file-sharing website to download a JavaScript loader tracked as HOPPINGANT by researchers. HOPPINGANT downloaded a lure document and another archive containing an executable file, which was a legitimate version (v1.70.3) of the Rclone software. This executable file was used to collect and upload files from the victim's system. The campaign relied on publicly accessible services to host and deliver malicious payloads. The threat actor abused MEGA[.]nz, a publicly available cloud storage service, as the remote endpoint for stolen data. The researchers have not yet attributed this campaign to any known threat actor.

Hydra Saiga attacks

APT

Spear phishing

Telegram C2

Backdoor

LOTL

Exploitation of public-facing applications

Attacks targeting ICS

According to analysis conducted by VMRay, the Hydra Saiga group (aka Yorotrooper or Tomiris) compromised at least 34 organizations in eight countries and scanned over 200 additional targets worldwide, including critical water and energy infrastructure in Central Asia. More specifically, between September 2024 and March 2025, Hydra Saiga conducted an extensive campaign targeting critical water infrastructure, research institutions, and government ministries. The group focused on infrastructure linked to two major regional rivers: the Syr Darya and Amu Darya. The campaign led to compromises in hydroelectric power plants and the water resource service in Kyrgyzstan, as well as a regional administration, a research institute, and the Ministry of Water Resources in Uzbekistan, and the Ministry of Energy and Water Resources in Tajikistan.

According to researchers, on April 29, 2024, the Hydra Saiga threat actor also attempted to access several exposed SCADA endpoints and the systems of industrial equipment manufacturers in multiple countries, including Argentina, Brazil, India, the Netherlands, and Czechia. While these intrusion attempts appeared to have been unsuccessful, the following day, the actor attempted to gain access to the gas distribution system of a Russian region bordering Kazakhstan. Researchers assume that the Hydra Saiga group was testing their capabilities and experimenting with SCADA endpoints in preparation for the intrusion attempt against Russia because the targets did not align with their usual victims.

The researchers discovered two December 2024 spear-phishing campaigns by the group with password-protected RAR or ISO archive attachments. A defining characteristic of the group is the use of the Telegram Bot API for C2 communication. Post-exploitation tactics include manual, keyboard-driven command streams, living-off-the-land (LOTL) techniques, and a new browser-data stealer that bypasses Chrome's app-bound encryption – the proprietary technology of safeguarding user application data. The actor also employs a combination of custom implants written in Rust, Go, and Python. Specifically, the researchers discovered the JLORAT samples, a backdoor written in Rust that was initially described by Kaspersky in April 2023 and that is associated with the Tomiris threat actor.

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