Kaspersky ICS CERT

kaspersky

APT and financial attacks on industrial organizations in Q2 2026

03.08.2026

Version 1.0

Contents

This summary provides an overview of reports on APT and financial attacks on industrial enterprises disclosed in Q2 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

The second quarter of 2026 was unprecedentedly dense with publications about targeted attacks on industrial control systems. The cyber-Armageddon genie mentioned in our overview for Q1 2026 began making increasingly frequent forays from its cozy bottle into various corners of a world transformed by its years of self-imposed confinement. Along the way, it built fewer castles and did it with diminishing enthusiasm, while its attempts to destroy cities grew bolder and more persistent.

The most notable of its recent achievements is an attack on an Israeli food processing facility, which resulted in the failure of a refrigeration unit and the release of refrigerant to the atmosphere. This incident certainly deserves special attention – the attackers unexpectedly demonstrated a considerable understanding of the design, operating principles, and functional safety vulnerabilities of modern industrial refrigeration systems. Another significant case is a campaign targeting CompactLogix and Micro850 PLCs by Rockwell Automation, exposed to the internet at critical infrastructure facilities in the USA. As a result, the attackers stole project files and spoofed data transmitted to HMIs and operator workstations. Finally, a large-scale campaign of scanning and fingerprinting internet-accessible Modbus devices, attempting to selectively DoS them, however the impact of these attacks was not assessed in the published research.

Despite their increasing frequency, many of the modern attempts to do something illegitimate with industrial automation systems appear either timid, lazy, or clumsy. A prime example of the latter is malware targeting desalination and water treatment plants in Israel. The fact that researchers obtained such a crude version of the malware, not battle-ready, likely speaks to the extreme carelessness and immaturity of its developers.

The unexpected discovery of the malware dubbed fast16, which appears to be a genuine cyberweapon, almost reaching the level of domain immersion of the infamous Stuxnet, was a stark contrast to the new technical and organizational standards of cyber-physical attacks. This finding turned out to be a time

capsule, taking us back over two decades. In 2005, the year this malware was created, the attackers' flight paths were much higher than those that now plague the digital sky. The malware's objective was to disrupt sophisticated mathematical packages used to model complex physical processes, such as detonation. The malware was targeting calculations that simulated the conditions for triggering an uncontrolled nuclear reaction (read: an atomic explosion) and was making subtle adjustments to the them, disrupting the simulation process. The malware appeared to have been used in practice — its developers iteratively refined it, adding support for other versions of targeted simulation software packages. One wonders how many more such discoveries of the cyber-archaeologists will delight us? The second important question is what impact these and other, as yet unknown, major developments of prehistoric hackers have had on the processes of technological, economic, and political development in different parts of the world? And the third question that is impossible to ignore is: are there other developments of this caliber that are still being quietly used today, hindering development in areas critically important to states and humanity as a whole?

Perhaps one of the most alarming developments in the evolving cyber-physical threat landscape was the publication on the use of ML agents and powerful cloud-based tools such as Claude and GPT-4.1 in attacks on Mexican government agencies and industrial enterprises. It describes a still extremely rare case of AI being used at most stages of the kill chain within the attacked network – reconnaissance, search for new targets and their prioritization, and lateral movement. In one case, the AI pointed the attackers to an interface to the OT-segment of the attacked organization's infrastructure and suggested a way to access it. While this first documented attempt by AI to reach OT was tentative and unsuccessful, we are seeing how ML tools, including large public models, are increasingly being used by industrial enterprises to solve an increasingly diverse range of OT-related tasks and, consequently, are accumulating ever-increasing domain knowledge that attackers will certainly exploit one day.

So, apparently, the day is not far off when ML/AI tools will be able to compensate for the difference between modern mass cyber-villains and the classic cyber-physical attackers of the past – and the everyday reality of industrial cybersecurity will take a sharp turn, for which it would be better for one to start preparing the day before yesterday.

Targets in Russia

Geo Likho attacks

APT

Spear phishing

Spyware

The Geo Likho group (also known as Batavia) has been orchestrating targeted attacks against organizations in the Russian Federation and Belarus since at least July 2024. Kaspersky researchers investigated the group's recent activity and found that the group uses spear-phishing as an initial access vector. When a user clicks a link that appears to be a path to an official document, a malicious VBE script is downloaded to the victim's machine, launching a three-stage infection. The attackers used the same toolset as in previous campaigns, including a VBE loader, a first-stage Delphi implant, and a second-stage malicious C++ file. The researchers discovered that the attackers have begun creating individual malware tools tailored to the victim's specific infrastructure. Reliable similarities were identified between the VBE loader code in previous and current campaigns, the code in the first-stage implant functions, as well as similarities in the decrypted payload strings. Kaspersky telemetry data indicated approximately 260 victims in the Russian Federation, roughly 20 victims in Belarus, and isolated cases in Germany, Serbia, and Hong Kong. The victims in the latter three countries appear to be random occurrences rather than part of a coordinated campaign. The attackers primarily target aviation and shipping companies. Other common targets include organizations in the mechanical engineering, education, and government agencies.

BO Team attacks

APT

Spear phishing

Linux malware

Backdoor

Kaspersky researchers continued to track the BO Team group's attacks on Russian organizations. During the investigation of BO Team's infrastructure, researchers identified several notable artifacts that ultimately led to the discovery of source code hosted in the group's private Git repository. Access to this codebase provided researchers with an opportunity to conduct an in-depth analysis of the group's main backdoor called ZeronetKit, enabling a comprehensive assessment of its architecture and embedded capabilities. Researchers also found active use of the Linux variant of the backdoor in recent attacks, indicating an expansion of the group's malware arsenal and adaptation to different types of target systems. In the first quarter of 2026, BO Team attacked 20 organizations. To gain initial access, the attackers continued to use spear phishing and a backdoor from the BrockenDoor family. In their latest attacks, the group used Windows Scheduler tasks to gain persistence, re-execute their payload and launch a ZeroSSH backdoor sample. The observed incidents revealed indicators suggesting a potential operational

linkage with another pro-Ukrainian threat actor, Head Mare. The BO Team campaigns studied targeted organizations in the Russian Federation across multiple economic sectors, including oil and gas, manufacturing, and telecommunications.

PhantomCore attacks

Cybercriminal

Spear phishing

RAT

On April 8, F6 researchers detected a spear-phishing attack by the PhantomCore group (aka Head Mare) targeting a Russian industrial company. The attackers sent phishing emails with the subject line "About the working visit of the DPRK delegation in April 2026" to various addresses within the target company. The emails contained a PDF bait file and a ZIP archive with malicious files. The ZIP file contained a malicious HTA file with hidden file attributes, as well as an LNK file whose primary purpose was to launch the HTA file. The HTA file had a script tag in its markup with a VB script that was executed after the file launched. Executing this VBS downloaded additional PowerShell scripts to the victim's device. The scripts were placed in a registry key for persistence and then launched. One of the downloaded PowerShell scripts was RAT malware dubbed KermitRAT. During the investigation, F6 researchers obtained a list of commands from the KermitRAT C2 server. One of these commands resulted in the download of MeshAgent, a remote monitoring and management (RMM) agent from the MeshCentral project.

Eagle Werewolf attacks

APT

New threat actor

Spear phishing

Telegram phishing

Backdoor

RAT

AI-generated code

In February 2026, BI.ZONE identified three clusters operating independently that distributed malware under the guise of Starlink device registration services and drone pilot training applications. Paper Werewolf (GOFFEE) deployed EchoGather, a C# RAT that uses XOR-plus-Base64 encoding, anti-VM checks, and a SHA-256-derived hardcoded key for HTTPS POST C2 communications. The group also conducted Telegram account credential harvesting through a fraudulent Starlink authorization portal. Versatile Werewolf (HeartlessSoul) staged a chain from MSI installer through AI-generated PowerShell and VBScript stagers to a .NET loader sideloading Sliver via a legitimate Windows binary, with a scheduled task masquerading as a Microsoft Edge update. Its generative-AI-developed JavaScript SoullessRAT that harvested Outlook data and screenshots.

In the article, BI.ZONE shared information about a third actor also involved in espionage activity associated with the Starlink device registration campaign. This activity was linked to an attack previously documented by Positive Technologies. Following the retrospective analysis, BI.ZONE experts decided to track the cluster as Eagle Werewolf. According to BI.ZONE, Eagle Werewolf has

been active since at least May 2023. Its primary targets are state organizations, industrial companies, and individuals engaged in drone manufacturing and engineering. The threat actor uses targeted phishing emails to gain initial access. Notably, in February 2026, it compromised a drone-focused Telegram channel to distribute malware. Eagle Werewolf leveraged the compromised channel to deliver a Rust dropper (Tauri framework, AES256-CBC, PBKDF2 key derivation) alongside a Go dropper that created a hidden local administrator account and configured SSH tunneling. The campaign also installed AquilaRAT (Rust, Blowfish-encrypted C2 server list, JSON task/subtask system, chunked file upload) and Go2Tunnel for a persistent SSH relay.

Cloud Atlas attacks

APT

Spear phishing

Compromised legitimate mailboxes

Compromised websites

Access brokers

Groups collaborating

Spyware

Probable APT/Criminal convergence

In late 2025, researchers at Positive Technologies detected a campaign by the Cloud Atlas group targeting Russian industrial and military-industrial organizations. The initial penetration was achieved through a spear-phishing email sent on behalf of a real counterparty through a compromised mailbox. A decoy DOC file was used as a downloader that, when opened, initiated a request to a remote RTF template, a link to which was embedded in the internal 1Table stream. Subsequent delivery of intermediate components and the payload was carried out via WebDAV resources published on compromised legitimate websites. The final payload was DeerStealer malware delivered by HijackLoader. Source code analysis of pages on these compromised legitimate websites revealed HTML and JavaScript injections that implemented redirects, tracking, and external content loading. The nature and logic of the injections do not correspond to typical Cloud Atlas TTPs. Analysis of the detected JavaScript injection revealed that its structure and operating logic are characteristic of Mustard Tempest (also known as TA569, DEV-0206, or Gold Prelude), the group and initial access broker (IAB) associated with the distribution of the SocGholish (FakeUpdates) JavaScript loader. This loader is injected into compromised websites and simulates a browser or software update. During the period that Mustard Tempest was distributing malware via the FakeUpdates scheme, Cloud Atlas malware was also being distributed from the same domains via separate URLs. This observation contrasts with previously described techniques and tactics for the Cloud Atlas group. In previous campaigns, the Cloud Atlas group typically used phishing documents, remote templates, and payloads hosted on servers controlled by the attackers themselves, rather than on compromised legitimate websites already used by other hacker groups. Given this, at least two hypotheses can be considered, according to PT researchers. The first is that Cloud Atlas partially adjusted its TTPs, compromised legitimate web resources on its own, and used them to deliver malware. The second hypothesis is that Cloud Atlas also adjusted its

TTPs but did not compromise web resources independently; rather it purchased access from Mustard Tempest. This significantly increases the complexity of analysis for researchers because it becomes more difficult to distinguish the roles of individual attack participants and correctly attribute activities to groups.

CapFix attacks

Cybercriminal

Spear phishing

Compromised websites

Backdoor

DLL sideloading

Code signing certificates

Positive Technologies researchers revealed attacks by the CapFix group targeting Russian organizations in the industrial and aviation sectors. Previously, the group targeted users with the ClickFix technique and used phishing files related to cryptocurrency and hotel bookings. At the end of December, the researchers noticed PDF documents containing links to download RAR archives. When clicked, users downloaded an archive from a compromised legitimate resource. This archive contained a CHM script that then downloaded an MSI file from a compromised legitimate domain and also opened a legitimate PDF document. The MSI file is signed by QILING Tech and disguises itself as the QILING Disk Master application. When launched, the file dropped several DLLs and the legitimate executable file MetadataConvert.exe, which was vulnerable to DLL sideloading, to the disk. Executing the legitimate file triggered the DLL sideloading chain, which loaded CapDoor as the payload. After analyzing various versions of the CapDoor backdoor and its supply chains, the researchers found that the malware is being actively developed and updated on a regular basis. In earlier versions, CapDoor was distributed as an executable file, while in newer attacks it is distributed as shellcode. The attackers previously used the GHOSTPULSE loader (also known as IDATLOADER or HIJACKLOADER) to load CapDoor. Later they used a sophisticated DLL sideloading technique. Early versions of CapDoor were not capable of taking screenshots, but this functionality was added in later versions. While researching CapDoor, Positive Technologies discovered early samples used by the group in their attacks that loaded SectopRAT or ArechClient2 as the final payloads.

Fluffy Wolf attacks

Cybercriminal

Spear phishing

GitHub links

Backdoor

Ransomware

BI.ZONE researchers detected a series of attacks by the Fluffy Wolf (aka VasyGrek) cluster from March to May, 2026. The group used spear-phishing attacks to target Russian organizations in various industries, including construction, consulting, manufacturing, engineering, retail, and e-commerce. Fluffy Wolf posed as employees of various specialized organizations in phishing emails, offering to pay off financial debts and providing links to documents supposedly attached to the email. Two types of phishing emails were identified:

one with an attachment containing malware in a RAR archive and another with a link to the attackers' GitHub repository, from which the RAR archive was downloaded. The attackers' GitHub profiles included multiple repositories containing RAR archives, executable files with .scr, .com, and .exe extensions, text files with payloads (reversed and Base64-encoded), and obfuscated batch and JS scripts. The RAR archives contained malicious downloaders and droppers designed to deliver the PureLogs stealer, PureRAT, and Pay2Key ransomware to the target system. The attackers also used various downloaders and droppers, including PureCrypter, a Rust downloader using the Donut shellcode, a Batch downloader, a JavaScript downloader, and a previously undocumented third-party downloader called PowerLoader that increased the effectiveness of penetration and bypassing security systems. As with PureCoder tools (PureCrypter, PureLogs, PureRAT), PowerLoader is distributed on shadow marketplaces via the malware-as-a-service (MaaS) model. Furthermore, researchers discovered a previously undisclosed PureRAT plugin called PluginRemoteDesktop that enables remote control of the desktop on a compromised system in attacks on Russian companies.

Attacks on Russian energy companies

Unknown threat actor

Spear phishing

RAT

Stealer

Kaspersky researchers uncovered the activity of a previously unknown group that has been targeting universities, financial companies, diplomatic services, and the energy sector in Russia since 2024. The Ravage pen testing framework was released on GitHub in September 2025, and attackers began using it by January 2026. Kaspersky discovered users of the framework among the attackers, who initially attracted little attention. This group, which used Ravage, was characterized by long periods of inactivity. It was later discovered that the group could be inactive for three to four months and then launch 10 attacks in a single month. In 2026, the attacks began with a phishing email with a ZIP archive containing an XLL file. It was disguised as a legitimate Microsoft Excel add-in. Double-clicking it launched the Excel application, which loaded an executable DLL into its process, executing the malicious code. The Microsoft Excel XLL add-in file type, combined with the familiar Excel logo, created the appearance of a legitimate document. In this case, the XLL file was compiled using the open-source Excel-DNA framework. The XLL file contained a module written in C# that downloaded and ran two executable files from embedded URLs. These URLs led to a compromised website where malicious files had previously been uploaded. The first URL downloaded a standard binder (a program that combines different types of files into one) for packing known backdoors and stealers. This file is a self-extracting CAB archive containing the AutoIt interpreter and its script, divided into several files, as well as a batch file. The AutoIt script contained the malicious payload in the form of an encrypted

executable file. The script decrypted the file, launched the RegAsm.exe process, and injected a malicious payload into this process. The decrypted payload was the PureRAT backdoor. The BatToExe utility was downloaded from the second URL. When executed, the utility creates one batch file and one PowerShell file, runs the batch file, which then runs a PowerShell script that is the Ravage framework loader. The researchers revealed that the group also used the Cobalt Strike tool and the RedLine stealer in attacks in 2024.

Unicorn attacks

Cybercriminal

Spear phishing

Spyware

On March 30, researchers from F6 detected a new attack by the Unicorn group. Since September 2024, the group has been targeting Russian companies with a recognizable style: spear-phishing emails, a long-lived C2, and minimal changes to the malware. The primary target of the new campaign is the aircraft manufacturing industry. The email contains a ZIP archive with an HTA file. When launched, the HTA file extracts eight identical scripts into two different directories. Based on their investigation, the researchers identified several changes compared to earlier activity. Specifically, there was a switch from VBScripts to JavaScript. For persistence, the JS scripts are added to startup via the registry (RunOnce) and the task scheduler. The capabilities of the JS scripts are similar to those previously implemented in Unicorn's VBS scripts: collecting files with specific extensions from user directories; collecting data from browsers, Telegram, and files from removable drives; interacting with the C2 to receive commands; and sending collected files. Another change identified is that the HTA file no longer has a final POST request. In previous attacks, the POST request was sent to Discord.

HeartlessSoul attacks

APT

Spear phishing

Malvertising

RAT

Malware distribution via legitimate platform

Fake installer

Kaspersky researchers reported on the activities of the HeartlessSoul (aka Versatile Werewolf) cyberespionage group, which targeted government agencies and commercial companies in the industrial and aviation systems sectors, as well as individual users. The main infection vector was phishing emails with archives containing LNK, XLL, or MSI files. Some of the discovered LNK files exploited the ZDI-CAN-25373 vulnerability. Additionally, the attackers used malicious advertising campaigns (malvertising) that mimicked websites offering software for aviation systems, from which victims downloaded infected installers. The group also distributed malicious installer using the legitimate SourceForge platform. The installer masqueraded as GearUP, a service for improving connections in online games. The initial infection involved executing PowerShell commands or scripts designed to download a JavaScript loader from C2 servers. This loader then downloaded and executed the main

JS-RAT and its modules, which included data collection and exfiltration tools, keyloggers, screen capture tools, UAC bypass tools, and other payloads, in memory. The group's ultimate goal appears to be collecting geospatial data and information from compromised systems. In their analysis, the researchers also identified overlaps in the attackers' infrastructure with the GOFFEE APT group.

Paper Werewolf attacks

APT

Spear phishing

RAT

Stealer

Fake installer

In March-April 2026, BI.ZONE uncovered a Paper Werewolf (aka GOFFEE) campaign targeting Russian industrial, financial, and transport organizations. The campaign used an expanded toolkit built around phishing PDFs, Inno Setup installers, loaders, downloaders, stealers, and custom implants. One attack chain used PDF lures that linked to ZIP archives delivering a fake Adobe Acrobat plug-in installer. This installer opened a decoy document while launching the EchoGather RAT for host profiling, C2 communication, file transfer, and command execution. BI.ZONE also identified PaperGrabber, a previously undocumented VB.NET stealer designed to collect documents from local, network, and removable drives, steal Telegram session data, and extract saved browser credentials. Other chains used JavaScript, C++, Python, and MSBuild-based downloaders to execute shellcode or load .NET assemblies in memory. One chain delivered a custom Mythic implant that performed an RSA-based encrypted key exchange before checking in with the C2 server and transmitting system information.

Coordinated cyberattacks by pro-Ukrainian groups

Hacktivist

Cybercriminal

Groups collaborating

Exploitation of public-facing applications

Backdoor

Ransomware

While investigating the activities of the 4BID pro-Ukrainian hacktivist group, Kaspersky researchers discovered a series of campaigns that appear to be led by several interconnected groups. The researchers revealed that the geography of the attacks studied is not limited to Russian and Belarusian organizations, but also includes companies from the government, medical, and aviation sectors in Kazakhstan, the UAE, Syria, and Egypt. This behavior correlates with a statement by a 4BID group member that attacks on the Russian Federation are no longer profitable. An analysis of the attacked infrastructures revealed that, in most cases, the attackers gained initial access by exploiting a ProxyShell vulnerability in Microsoft Exchange. After gaining access, the attackers used an ASP.NET web shell with a modular architecture that enables remote control, file transfer, and system data collection. Numerous indicators of activity by various pro-Ukrainian groups were identified in the infrastructure of the organization that served as the starting point for the research. Kaspersky researchers discovered several samples of BlackReaperRAT (attributed to the 4BID group), scripts for downloading

Panorama9 RMM, AnyDesk and Dev Tunnels, ClearWater ransomware, and Warp RAT (attributed to the GOFFEE group). The following utilities were also observed in the context of the described campaigns: Advanced IP Scanner, Nezha Monitoring Tactical RMM, Sliver, Havoc, Apollo Mythic, Adaptix, BlackSalt backdoor, and EDR-killers. The researchers also revealed that, in late January 2026, the 4BID group carried out a series of attacks on organizations in Russia using an updated version of Blackout Locker ransomware that was distributed using a dropper written in Rust.

Cyber groups targeting Russia

Cybercriminal

APT

Cloud services infrastructure

Spear phishing

Backdoor

LOTL

COM Hijacking

AI-generated code

Compromised websites

Positive Technologies researchers published an analysis of cyber group activities that targeted Russian organizations in the first quarter of 2026, along with updated TTPs, victimology, and toolsets. PT classified the activity as either cyberespionage or financially motivated. The groups targeted companies in the logistics, manufacturing, aviation, aerospace, defense, pharmaceuticals, agriculture, construction, chemicals, utilities and energy sectors, among others. The report details the activities of cyberespionage groups such as Rare Werewolf (Librarian Ghouls, Librarian Likho, Rezet), PhaseShifters (Angry Likho, Sticky Werewolf), PhantomCore (Head Mare), GOFFEE (Paper Werewolf), IAmTheKing (King Werewolf), Tolik (Fairy Werewolf), and BO Team (Lifting Zmiy). Financially motivated activity included that of Hive0117 and Fluffy Wolf (VasyGrek). The attack chains of all the groups began with phishing emails containing payloads such as Microsoft Word documents with macros, password-protected archives with LNK shortcuts, NSIS installers with a .pdf.exe double extension, HTA files, RTF documents exploiting OLE objects, Excel XLL files, SFX archives and BAT files. Windows Task Scheduler remained the most common persistence technique and was used by nearly all groups. The launching of payloads through trusted system binaries was used by all the described groups.

Rare Werewolf has switched from using the Blat utility for SMTP exfiltration to leaving comments on the GitHub Gist page. PhaseShifters stored the payload URL in a Bitbucket repository, updating the links via commits. Fluffy Wolf hosted an archive containing a dropper and intermediate .txt files with a Base64 payload in a GitHub repository, and also used Firebase Storage to store an image with a steganographic Base64 payload. PhantomCore stored stager malware on compromised legitimate websites. The GOFFEE group used modules with characteristics typical of LLM generation in attacks on Russian defense enterprises.

Operation Silent Rotor

Unknown threat actor

Spear phishing

Seqrite Labs described Operation Silent Rotor, a targeted spear-phishing campaign aimed at organizations and professionals in the Eurasian unmanned aviation (UAS/UAV) sector. The attackers timed the operation to coincide with the XIII Eurasian International Forum "Unmanned Aviation 2026" in Moscow and used aviation-themed lures, including fake order confirmations and technical documents, to deliver a malicious ZIP archive. The archive contains a 64-bit Rust-based executable disguised as a legitimate document from the Russian Aeronautical Information Center (CAI), along with decoy PDF, DOCX, and XLSX files to increase its credibility. Once executed, the malware performs host reconnaissance by collecting information such as the hostname, volume serial number, network adapter details, and environment variables before encrypting the collected data with a custom XOR routine and exfiltrating it over HTTPS to a C2 server. The first-stage loader subsequently downloads an encrypted second-stage payload, decrypts it using AES-256, and executes it in memory, enabling additional attacker-controlled functionality. According to Seqrite, the campaign targets aviation professionals and organizations in Russia, Tajikistan, Central Asia, the Middle East, and Europe. Researchers did not attribute the operation to any known threat actor.

Clubfoot Wolf attacks

Cybercriminal

Spear phishing

RAT

Cloud services infrastructure

BI.ZONE reported attacks by the Clubfoot Wolf group (aka NetMedved). Researchers discovered that the Clubfoot Wolf cluster carried out a large-scale campaign targeting Russian organizations in the manufacturing, retail, e-commerce, agriculture, IT, logistics, medicine, and science sectors in May and June of 2026. The primary targets were wholesale distributors of chemical products in Russia, but the attackers also targeted several organizations in Belarus. Clubfoot Wolf sent phishing emails containing legitimate NetSupport Manager remote administration software to target systems. In the emails, the attackers posed as employees of a company interested in purchasing products from the target organization. As in previously recorded campaigns, Clubfoot Wolf distributed archives with fake documents, imitating the activities of Russian organizations. The emails included a ZIP archive containing a set of decoy files in various formats (PDF, JPG, PNG, DOC, and DOCX) and a malicious LNK file. Clubfoot Wolf used the Yandex Mail email service to send the phishing emails. When the user ran the malicious LNK file, a Base64-encoded command was executed in the PowerShell interpreter, enabling in-memory execution of the next stage directly in the PowerShell process's memory. The final PowerShell script downloaded a ZIP archive containing NetSupport Manager remote administration software and a set of files filled with automatically

generated gibberish. These files were likely added to alter the archive's hash value and make it appear to be a legitimate software distribution. The PowerShell script also decodes and decrypts the PowerShell code that establishes NetSupport Manager's persistence in the OS registry.

Chinese-speaking activity

Silver Fox

APT

Spear phishing

RAT

Backdoor

In December 2025, Kaspersky researchers detected a wave of malicious mailings that imitated messages from the Indian tax service. A few weeks later, in January 2026, a similar campaign began targeting Russian organizations. Researchers linked this activity to the Silver Fox group (aka Monarch, SwimSnake, UTG-Q-1000 or Void Arachne). Both waves had an almost identical structure: phishing emails were formatted as official notices about tax audits or offered a download of an archive containing a "list of tax violations". Inside the archive was a modified Rust loader called RustSL, whose source code is publicly available on GitHub. The Silver Fox RustSL variant decrypts the malicious payload, and uses all available methods to detect virtual machines and sandboxes. It also checks whether the device is located in a given country. In later variants, only geolocation verification remained, but the list of countries in which work was allowed increased significantly. While the GitHub Rust loader variant only includes China in its list of countries to check, the modified version includes India, Indonesia, South Africa, Russia, Cambodia, and Japan was also later added to the list. RustSL downloaded and executed the known backdoor ValleyRAT. During the investigation it was also discovered that the attackers delivered a new plugin for ValleyRAT to victims' devices, which downloaded and executed a previously undocumented backdoor written in Python named ABCDoor. Retrospective research showed that ABCDoor had been in Silver Fox's arsenal since at least the end of 2024 and has been used in attacks from the first quarter of 2025 to the present. The campaign impacted organizations across the industrial, consulting, retail, and transportation sectors, with over 1600 malicious emails recorded between early January and early February. Researchers observed the highest number of attacks in India, Russia, and Indonesia, followed by South Africa and Japan.

Attacks with ShadowPad

APT

DLL sideloading

LOTL

Supply chain/trusted partner

Backdoor

F6 presented the results of their investigation into an attack on a Russian manufacturing company in late February 2026. For initial access, the attackers used a contractor's service account with access to the organization's internal network via Check Point VPN. Analysis of the TTPs revealed that the attackers used the ShadowPad backdoor, which is actively used by Chinese APT groups. The attackers used services created in the Windows operating system to execute the malware. Their persistence points were scheduled tasks, created services, and the malware's autorun via the RUN registry key. To move laterally, the attackers remotely created services on adjacent devices using the standard operating system utility, sc.exe. Based on the available data, the researchers could not definitively attribute this campaign to a specific APT group.

Shadow-Earth-053 attacks

APT

DLL sideloading

Exploitation of public-facing applications

Backdoor

Trend Micro shared details about a newly identified Chinese-speaking group that researchers track under the temporary intrusion set designation SHADOW-EARTH-053. The group's campaign primarily targeted government entities, mostly in Asia. Most of the observed targets were concentrated in South, East, and Southeast Asia, particularly Pakistan, Thailand, Malaysia, India, Myanmar, Sri Lanka and Taiwan. SHADOW-EARTH-053 also targeted the technology industry. A limited number of victims in the transportation industry in Southeast Asia were also identified.

The group exploits N-day vulnerabilities in internet-facing Microsoft Exchange and Internet Information Services (IIS) servers (e.g., ProxyLogon chain), then deploys web shells (GODZILLA) to gain persistent access and stages ShadowPad implants via DLL sideloading of legitimate signed executables. In one instance, ShadowPad samples were delivered via AnyDesk, a legitimate remote administration tool, suggesting the attackers either leveraged a prior compromise or obtained credentials through other means. The attackers deployed the legitimate Windows utility csvde.exe to export Active Directory objects to CSV format. They also used PowerView's Get-DomainUser cmdlet to enumerate user accounts and their associated email addresses from a domain controller. A custom binary named DomainMachines.exe was observed enumerating machines in the domain through LDAP, then connecting directly to ports related to SMB, web server and proxies, RDP, WinRM, MySQL, MS SQL, and Kerberos. However, this tool could not be retrieved for in-depth analysis. SHADOW-EARTH-053 used a legitimate Toshiba Bluetooth Stack executable to sideload a malicious DLL that employs a multistage evasion technique by retrieving its payload from the Windows Registry rather than embedding it

within the binary. Researchers observed the group leveraging the IOX proxy, GO Simple Tunnel, and Wstunnel.

SHADOW-EARTH-053 used WMIC for lateral movement, deployed a suspected custom RDP launcher and a C# implementation of SMBExec known as Sharp-SMBExec. In one environment, the group propagated web shells to additional internal Exchange servers by copying them over administrative shares. The group collects credentials that can be used to further its objectives, notably through the use of the Evil-CreateDump tool, which appears to be based on Microsoft's create-dump.exe utility, likely modified to target LSASS process memory for credential extraction. Mimikatz was executed directly via rundll32.exe with command-line arguments for credential extraction and local SAM database dumping. Additionally, the group dropped and executed a binary called newdcsync, which, based on the command line and filename, was likely used for DCSync attacks.

Attacks with DAEMON Tools

APT

Code signing certificates

Supply chain

Trojanized software

Backdoor

RAT

Kaspersky uncovered an ongoing DAEMON Tools supply-chain compromise in which legitimate, digitally signed installers from the official DAEMON Tools website were trojanized starting April 8, 2026. Compromised versions 12.5.0.2421 through 12.5.0.2434 activated a backdoor inside signed DAEMON Tools binaries, contacted the typosquatted C2 env-check.daemontools[.]cc, and could receive shell commands to download further payloads. Following deployment of the first trojanized version of DAEMON Tools on April 8, Kaspersky researchers observed thousands of attempted payload deployments using the compromised binaries. These deployments were observed on machines belonging to both individuals and organizations in more than 100 countries and territories, with the majority of victims located in Russia, Brazil, Turkey, Spain, Germany, France, Italy, and China. Analysis showed that 10% of the affected systems belonged to businesses and organizations. The attackers attempted to infect most of these machines with only the information collector payload. A minimalistic backdoor payload was observed on only a dozen machines belonging to government, scientific, manufacturing, and retail organizations in Russia, Belarus, and Thailand. In one case, a more complex implant dubbed QUIC RAT supporting multiple C2 protocols and process injection was deployed in an entity in the Russian education sector. Artifacts in the observed malicious implants suggest that the threat actor behind this attack is Chinese-speaking.

On May 6, Disc Soft Limited, the developer of DAEMON Tools Lite, confirmed that the software had been trojanized in a supply chain attack. The company released a new, malware-free version less than 12 hours after it received

notification. According to the company's statement, the issue was limited to the free version of DAEMON Tools Lite and did not affect any other products. The company identified unauthorized interference within its infrastructure. As a result, certain installation packages were impacted in the build environment and were released in a compromised state.

Attacks with TencShell malware

Unknown threat actor

APT

Backdoor

In April 2026, Cato CTRL identified and blocked an attempted intrusion against a customer of a global manufacturer with multiple regional sites. The attack specifically targeted the customer's site in India and involved TencShell, a previously undocumented Go-based implant derived from the open-source Rshell C2 framework. While the initial infection vector of the attack remained unknown, it was associated with a third-party user connected to the customer environment. The attack chain employed a first-stage dropper, Donut shellcode, a disguised .woff web font resource, memory injection, and web-like C2 communication. The TencShell malware deployed in the final stage includes capabilities commonly associated with mature post-exploitation frameworks. The recovered Go module names suggest the ability to perform several high-risk operator actions, including in-memory execution, BOF-style module execution, proxying and tunneling, WebSocket-based C2, and remote interaction. The implant also includes capabilities for remote shell and native OS command execution, file and process manipulation, persistence and defense evasion, UAC bypass, screen capture or remote interaction, browser artifact access, polling-based tasking, structured C2 reporting, and SOCKS5-based proxying for pivoting. Researchers assess the activity as being potentially associated with Chinese-speaking actors based on the apparent Rshell lineage, Tencent-themed API impersonation, and infrastructure patterns. However, they could not attribute it to any specific group.

FamousSparrow attacks

APT

DLL sideloading

Backdoor

Exploitation of public-facing applications

According to Bitdefender researchers, a group of hackers carried out a multi-stage attack on an Azerbaijani oil and gas company between late December 2025 and late February 2026. Bitdefender attributes the campaign with a high degree of confidence to the Chinese-speaking FamousSparrow (aka UAT-9244), which bears some tactical similarities to Earth Estries. The campaign was characterized by repeated exploitation of the same vulnerable Microsoft Exchange Server entry point despite multiple remediation attempts. It is believed the attackers exploited the ProxyNotShell vulnerability (CVE-2022-41040, CVE-2022-41082) to gain initial access. After initial access, attempts were made to deploy web shells to establish persistence and, ultimately, to

deploy the Deed RAT. This was done using an advanced DLL sideloading technique that exploited a legitimate LogMeIn Hamachi binary to download and execute a malicious DLL responsible for executing the main payload. Unlike standard DLL sideloading, which relies on simple file replacement, the observed method overrides two specific exported functions in the malicious library, creating a two-stage trigger.

The second wave occurred nearly a month after the initial intrusion, when the attacker unsuccessfully attempted to use a DLL sideloading technique with the legitimate Yandex executable "deskband_injector64.exe" to deploy the TernDoor backdoor using the Mofu Loader shellcode loader. The Azerbaijani company experienced a third attack in late February 2026 when the attackers attempted to deploy a modified version of Deed RAT using the same execution chain documented during the earlier stages of the intrusion. This suggests active efforts to refine and evolve their malware arsenal. The operation also involved RDP and SMB lateral movement, domain administrator credential abuse, Impacket-style execution, and redundant persistence, showing a sustained espionage operation focused on maintaining access to energy-sector infrastructure.

Mustang Panda attacks

APT

Spear phishing

DLL sideloading

Cloud services C2

Backdoor

Acronis reported two Mustang Panda espionage campaigns targeting India's hydropower sector and government entities in India that were involved in cooperation agreements with Taiwanese institutions. The campaigns used hydropower- and government-themed lure archives, hidden DLLs, and DLL sideloading through legitimate signed executables to deliver SHARDLOADER variants, which then deployed two newly identified implants: MINIRECON and ZOHOMURK. MINIRECON, derived from the Toneshell family, uses WebSocket-over-HTTPS C2 with proxy fallback, reverse shells, file transfer, remote command execution, and drop-and-execute capabilities. ZOHOMURK abuses Zoho WorkDrive for C2, victim registration, command retrieval, output upload, and data exfiltration, blending malicious traffic into a legitimate cloud service commonly used in the Indian government sector. Acronis attributed the activity to Mustang Panda with high confidence, citing tradecraft, malware overlaps, infrastructure patterns, and targeting aligned with the collection of intelligence around India's hydropower initiatives and defense cooperation with Taiwan.

CL-STA-1062 attacks

APT

Exploitation of public-facing applications

Backdoor

Unit 42 reported a CL-STA-1062 campaign targeting Southeast Asian government entities and critical infrastructure, especially state-owned organizations in the energy and government sectors. Active since at least 2022, the cluster is believed to overlap with UAT-7237. It compromised victims through exposed web applications, deployed ASPX web shells, conducted reconnaissance, staged tools, and exfiltrated database and web server source code data. The actors used a hybrid toolkit combining open-source utilities such as SoftEther VPN, VNT, Mimikatz, JuicyPotato, RAR, and tunneling tools with custom malware, including the newly documented TinyRCT .NET backdoor. TinyRCT fingerprints hosts, registers infected systems with the C2 server, executes commands, lists and exfiltrates files, captures screenshots, downloads payloads, and includes a self-destruct routine. Unit 42 assessed this activity as a persistent regional threat focused on strategic sectors in Southeast Asia and East Asia.

Middle East-related activity

CISA alert on cyber actors exploiting PLCs

APT

Attacks targeting ICS

The US Cybersecurity and Infrastructure Security Agency (CISA) published a joint cybersecurity advisory alongside federal intelligence and infrastructure agencies, warning organizations of ongoing attacks targeting programmable logic controllers (PLCs) in multiple US critical infrastructure sectors including Government Services and Facilities, Water and Wastewater Systems (WWS), and Energy, that have been identified since at least March 2026. The attacker is believed to be an Iran-affiliated advanced persistent threat (APT) exploiting Rockwell Automation/Allen-Bradley PLCs and possibly other PLC brands such as Siemens S7. The actors used leased, third-party hosted infrastructure with configuration software, such as Rockwell Automation's Studio 5000 Logix Designer software, to create an accepted connection to the victim's PLC. Targeted devices include CompactLogix and Micro850 PLC devices. The FBI identified that this activity resulted in the extraction of the device's project file and data manipulation on HMI and SCADA displays.

The advisory urges organizations to disconnect PLCs from the public internet and deploy secure gateways and firewalls; to query logs from within the attack time frame for indicators of compromise (IoCs), including suspicious traffic on ports 44818, 2222, 102, 22, and 502; and to place the physical mode switch on Rockwell Automation controllers to the run position. CISA strongly

recommends organizations check the full provided mitigation and hardening instructions as well as IoCs and attacker tactics, techniques, and procedures (TTPs). The advisory calls on manufacturers to create default settings that prevent internet exposure, to not charge for basic security features, and to support phishing-resistant MFA.

Nimbus Manticore attacks

APT

Spear phishing

DLL sideloading

Fake installer

Code signing certificates

AI-generated code

Backdoor

SEO poisoning

Check Point researchers reported new campaigns by the Iran-linked threat actor Nimbus Manticore (aka UNC1549) during the geopolitical conflict. The researchers tracked three waves of the threat actor's activity in February, March and April. In February 2026, Nimbus Manticore leveraged phishing lures to target employees in the software and aviation sectors with fake career opportunities. Targeted organizations in Saudi Arabia and Australia were directed to download a compressed ZIP archive stored on the OnlyOffice platform. In this campaign, the threat actor introduced a modified infection chain by abusing AppDomain hijacking for execution instead of relying on the usual DLL sideloading techniques – allowing malicious code to run inside trusted .NET applications – and deployed a new version of the MiniJunk backdoor.

In March campaign, in addition to career-themed phishing lures that masqueraded as communications from a US-based airline, the threat actor also sent false invitations to meetings with the trojanized Zoom installer. The malware abused a scheduled task created by Zoom installer as a persistence mechanism. Thus, the malicious activity imitated the usual legitimate one and reduced detection opportunities. The fake installer deploys a previously undocumented backdoor called MiniFast, which replaced the older MiniJunk malware family. Check Point assessed that the threat actor likely leveraged AI-assisted development techniques during malware creation.

In April, researchers observed Nimbus Manticore using SEO poisoning to distribute malware for the first time. They observed a new infection method: a fake website impersonating a download page for SQL Developer, a graphical tool used for working with databases. Users who attempted to download the software from the fake site instead received a weaponized installer that delivered the MiniFast backdoor.

Attacks with ZionSiphon

APT

Attacks targeting ICS

Cyber sabotage

Self-propagating malware

Darktrace researchers revealed ZionSiphon, new malware specifically designed for operational technology (OT) that targeted water treatment and desalination environments to sabotage their operations. Based on its IP targeting and political messages embedded in its strings, ZionSiphon appears to focus on targets based in Israel. Upon deployment, the malware checks that the host IP falls within Israeli ranges and that the system contains water/OT-related software or files, to confirm it is running in a water treatment or desalination system. Darktrace noted that the country verification logic is flawed due to an XOR mismatch, causing the targeting to fail and triggering the self-destruct mechanism instead of executing the payload. If ZionSiphon were to activate, it could cause significant damage by increasing chlorine levels and maximizing the flow and pressure. It does this via a function named "IncreaseChlorineLevel()," which checks a hardcoded list of configuration files associated with desalination, reverse osmosis, chlorine control, and water treatment OT/industrial control systems. As soon as it finds any one of these files present, it appends a fixed block of text to it and returns immediately. The malware scans the local subnet for the Modbus, DNP3, and S7comm communication protocols. Researchers have found only partially functional code for Modbus, and incomplete logic for two other protocols, indicating that the malware is still in an early development phase. ZionSiphon also has a USB propagation mechanism that copies itself to removable drives as a hidden 'svchost.exe' process and creates malicious shortcut files that execute the malware when clicked.

MuddyWater attacks

APT

Exploitation of public-facing applications

Credentials brute force

DLL sideloading

Backdoor

Oasis Security analyzed a multi-stage campaign attributed to the MuddyWater group targeting aviation organizations, energy and infrastructure companies, and public sector entities across the Middle East, including entities in Egypt, Israel, and the United Arab Emirates, as well as Portugal and India. The operation began in early February 2026 and involved large-scale automated reconnaissance, scanning more than 12,000 internet-exposed systems for five newly disclosed vulnerabilities (CVE-2025-54068, CVE-2025-52691, CVE-2025-68613, CVE-2025-9316, CVE-2025-34291) affecting web applications, email servers, IT management and monitoring systems, workflow and automation tools. Following this broad scanning phase, the actor shifted to selective, high-value targeting: brute-forcing Outlook Web Access credentials using custom tooling and multi-threaded frameworks such as Patator, with confirmed credential harvesting against organizations in Egypt, Israel, and the UAE. A modular, multi-protocol C2 infrastructure was used to manage

compromised hosts, leveraging TCP, UDP, and HTTP channels with AES-encrypted communications. These patterns are consistent with the ArenaC2 framework previously associated with MuddyWater. The campaign resulted in confirmed exfiltration of sensitive data from an Egyptian aviation organization, including passport and visa records, payroll data, credit card information, and internal corporate documents. Approximately 200 files were staged in attacker-controlled directories prior to exfiltration, indicating structured data collection.

Symantec reported a Seedworm (aka MuddyWater, Temp Zagros, Static Kitten) espionage campaign that affected at least nine organizations across nine countries in the first quarter of 2026, including a major South Korean electronics manufacturer, government agencies, an international airport, industrial manufacturers, a financial services provider, educational institutions, and professional services organizations. The attackers used DLL sideloading with legitimately signed Fortemedia and SentinelOne binaries to execute malicious DLLs while blending into normal software activity. The malicious DLLs contain ChromElevator, a publicly available post-exploitation tool capable of covertly stealing and exfiltrating data such as passwords, cookies, and payment card data from Chromium-based browsers. A Node.js-based loader was used that orchestrated PowerShell scripts for reconnaissance, screenshot capture, credential theft, SAM hive dumping, privilege escalation, and SOCKS5 reverse-proxy tunneling. In the South Korean electronics intrusion, Seedworm maintained access for about a week, staged tools from attacker infrastructure, established persistence through a Run key, repeatedly collected credentials, and exfiltrated data through the public file-transfer service sendit[.]sh. The campaign showed a disciplined operation focused on long-term access, intelligence collection, and stealthy data theft.

Cyber Isnaad Front attacks

Hacktivist

Attacks targeting ICS

Cyber sabotage

Wiper

Exploitation of public-facing applications

According to a Profero report, an Iranian state-directed persona, Cyber Isnaad Front, has been conducting destructive cyber operations against Israeli industry. The threat actor targeted the defense, telecom, fuel and transport logistics, food production sectors and demonstrated coordinated attacks against both IT and OT environments. Profero's incident responders discovered that the threat actor deployed the Go Remote Access Toolkit (GRAT) on IT networks, disguised as Microsoft updates, featuring both remote access and wiper capabilities in one executable. In parallel, the attacker performed deep physical sabotage in OT environments, such as reprogramming industrial CO2 refrigeration controllers of a food enterprise to destroy mechanical compressors.

In one case, the Cyber Isnaad Front actor manipulated industrial refrigeration controllers by changing the operating parameters, normal safety limits, while changing both the protection thresholds and alarm and alert limits, which together, if the organization's employees had not noticed the changes, would have led to product damage. In another case, the attacker went much deeper. They wiped the controller's entire configuration: changed the digital and analog inputs mapped to temperature sensors and pressure transmitters, the fault inputs, the digital outputs that start compressors, and the analog outputs that drive motorized valves and fans. Recovering the system required its complete configuration, which took several days.

Moreover, the Cyber Isnaad Front actor switched the valves of the gas cooler and receiver to manual mode and pinned permanently open, also opening the valves of consumers, which started the free circulation of the working fluid in the system and led to the ingress of liquid CO2 into the compressors and, consequently, to their destruction, as well as to the release of CO2 from the system to the atmosphere. The engineers had to replace the failed compressors with non-identical ones, significantly redo the entire system and pump a new portion of working gas into it, which took most of the week.

Finally, the attacker changed the central controller's credentials, depriving operators of access to management.

All this indicates that the attacker is well prepared to carry out the intention to achieve a cyber-physical effect. In addition to describing the cyber-physical part of the attack, the publication consists indicators of compromise of the IT part of the infrastructure, as well detection and hardening measures.

Asia-related activity

Andariel attacks

APT

RAT

Ransomware

In March 2026, ESET detected TigerRAT on a computer belonging to an engineering company based in South Korea. The company targeted by Andariel in this operation produces high-end industrial equipment used in various sensitive sectors. The last attack documented by ESET that presented typical Andariel TTPs occurred two years ago, also against a South Korean company, so this case likely represents a reemergence of Andariel. The attackers tried to compromise several of the company's network endpoints using variants of the Rook ransomware. The high sensitivity of Andariel's target likely suggests that the group was, at least partially, interested in stealing strategic technology. ESET researchers assess that the Rook ransomware may have been used to

distract defenders while also trying to opportunistically extract financial gain to fund the group's operations.

OceanLotus attacks

APT

Supply chain/trusted partner

DLL sideloading

Exploitation of public-facing applications

Backdoor

ESET researchers uncovered two OceanLotus campaigns conducted between 2024 and early 2026, both centered on the group's custom SPECTRALVIPER backdoor. One campaign involved the infiltration of a Vietnamese infrastructure and transport construction corporation that began as early as November 2024 and persisted until February 2026. Although the initial access vector was not directly observed, analysis of the victim's public-facing servers suggests that the attacker may have exploited remote code execution (RCE) vulnerabilities in a Microsoft SQL server to establish an initial foothold. The second campaign was a supply chain attack leveraging FireAnt Metakit, a software platform widely used by Vietnamese stock investors. On October 2, 2025, researchers detected the first malicious payload originating from FireAnt MetaKit's legitimate update URL. ESET found that only selected victims exposed through the FireAnt compromise ultimately received the SPECTRALVIPER payload, indicating highly targeted victim selection rather than broad malware distribution. In both campaigns, the SPECTRALVIPER backdoor was delivered by a DLL sideloading technique using the legitimate, signed executables Toolbox.exe and dtlupdate.exe. The researchers concluded that it is still unclear whether OceanLotus' domestic focus represents a temporary tactical adjustment or a long-term strategic evolution.

Russian-speaking activity

Sednit attacks

APT

Spear phishing

Backdoor

Cloud services C2

Trojanized software

In recent months, ESET has continued to observe Sednit (aka APT28, Fancy Bear, Sofacy) using a sophisticated toolchain to deploy two implants – Covenant and BeardShell – in Ukraine. The attacks usually begin with initial contact via Signal Desktop or WhatsApp Desktop, followed by the delivery of trojanized Word or Excel documents. ESET researchers previously documented this implant pair in a blogpost, highlighting their direct code lineage to the group's 2010-era implants. Targets primarily include Ukrainian military personnel, as well as Ukrainian drone manufacturers and Ukrainian organizations involved in drone research and development. In one attack, a trojanized Excel document was used to target a victim. When opened with macros disabled, the document displays only an image of a drone, which is intended to lure the recipient into enabling macros. Once macros are enabled, the document reveals text

containing technical information about the drone, but the execution chain ultimately leads to the deployment of the Covenant implant via a custom loader, KoalaLoader, which extracts payloads from steganographically encoded companion PNG files. From the deployed Covenant implant, Sednit can subsequently deploy BeardShell, which leverages a different cloud provider. This redundancy allows operators to quickly reestablish access if one implant's infrastructure is disrupted. As of February 2026, BeardShell no longer relies on the IceDrive cloud provider, but instead uses Drime. Although the coordinated use of Covenant and BeardShell appears primarily aimed at long-term monitoring of Ukrainian military personnel, both implants have also been used in broader campaigns. For instance, BeardShell was deployed in an opportunistic campaign in March 2025 via a trojanized Ukrainian drone application distributed on torrent sites. In January 2026, Covenant was used in a wave of spear-phishing emails exploiting CVE-2026-21509 that targeted Ukrainian governmental institutions, logistics companies in Turkey, and transportation companies in Poland.

Sandworm attacks

APT

Wiper

Ransomware

Tor network

According to ESET, from December 2025 to March 2026, Sandworm intensified its destructive operations against Ukraine, primarily using Active Directory Group Policy to deploy multiple strains of data-wiping malware. In January 2026, ESET researchers identified an attack disguised as ransomware targeting a grain company in Ukraine. The attackers used RansomTuga, which is open-source malware available on GitHub that can be configured to function either as a wiper or as ransomware. The attackers demanded a ransom payable in cryptocurrency, 600 units of Zcash. Along with the RansomTuga ransomware, researchers also detected deployment of Tor services in a similar manner to that of ShadowLink, which Microsoft Threat Intelligence originally described in a blog post about the BadPilot campaign. In that campaign, ShadowLink was used to configure the system so that it would be registered as a Tor hidden service by dropping a legitimate Tor service binary and a torrc configuration file. The configuration in that case included port forwarding of common services such as RDP and SSH. In the case observed by ESET, only the port forwarding of RDP was present. Microsoft Threat Intelligence attributed the BadPilot campaign to Seashell Blizzard (aka Sandworm).

In February 2026, Sandworm deployed its first data-wiping malware written in the Rust programming language, which was named ZeroRays. CERT-UA designated this malware as ZEROSETH. When executed without arguments, the malware recursively enumerates files across all logical drives excluding specific directories and file types, spawns subprocesses to wipe files by zeroing open

file handles via FSCTL_SET_ZERO_DATA, and ultimately forces an immediate system reboot. The malware was used in attacks against a local government institution, as well as heat energy and insurance companies in Ukraine. Researchers also identified further data-wiping malware uploaded to VirusTotal from Ukraine. This wiper is a slightly redesigned version of NikoWiper that uses the SDelete utility. In addition to SDelete, the MSI file contains a text file with ASCII art that reveals the malware's internal name – Occultus.

Other

Lotus Wiper

APT

Wiper

In light of the geopolitical tensions that occurred in the Caribbean region in late 2025 and early 2026, Kaspersky researchers identified a new file wiper dubbed Lotus Wiper that was uploaded to public multiscanner services along with other related artifacts. Initially, researchers suspected this malware was related to a new ransomware attack; however, it was not linked to any known ransomware group. Furthermore, no payment instructions associated with ransomware were found. Analysis of the metadata collected from the multiscanner showed that the emergence of the samples coincided with the public reporting of file wiper attacks targeting Venezuela's energy and utilities sector. Therefore, researchers believe the ultimate goal of this highly targeted attack was to completely destroy all the files and data on the device, rather than economic gain.

The researchers found two batch files that perform a sequence of actions and prepare the environment for the launch of Lotus Wiper. The second batch file executes a malicious binary that masquerades as a legitimate server task executable associated with HCL Domino (formerly Lotus Domino) on Windows. It supplies another malicious binary, named to resemble an HCL Domino component, as an argument, ultimately resulting in the retrieval and execution of the Lotus Wiper payload. This implies the attacker had prior access, as the executables would have needed to be staged on the victims' hosts beforehand, supporting earlier evidence of backdoor activity on the compromised hosts. Lotus Wiper enables all privileges in its current token to access administrative functions (relies on pre-existing elevated rights), deletes restore points, and wipes every physical drive by writing zeroes to its sectors. It then clears the update sequence numbers (USN) of the volumes' journals and, finally, scans all the volumes looking for files to delete.

CPU-Z/HWMonitor watering hole attack

Unknown threat actor

Compromised websites

Watering hole

Supply chain

DLL sideloading

RAT

Kaspersky researchers investigated a compromise of the website cpuid[.]com that hosts installers for popular system administration software CPU-Z, HWMonitor (and Pro), and PerfMonitor 2. The researchers discovered that from approximately April 9, 15:00 UTC, to April 10, 10:00 UTC, the legitimate download URLs for the software installers were replaced with URLs pointing to malicious websites distributing malware. The malware was distributed both as ZIP archives and as standalone installers. The files contain a legitimate signed executable file for the corresponding product and a malicious DLL, created using the DLL sideloading technique. The malicious DLL is responsible for connecting to the C2 and subsequently executing the payload. Before connecting, it also performs a series of sandbox checks. Notably, the attackers used the same C2 address and connection configuration that they used in the March 2026 campaign to host a fake FileZilla website that distributed malicious files. The downloader also contains a huge array of MAC addresses (represented as strings), which form the next-stage payload by converting the hexadecimal characters in the MAC addresses to their byte values. After a series of auxiliary loaders, the execution chain results in a sophisticated RAT. The attackers decided to reuse the STX RAT reported by eSentire as the final stage; it is fully detectable by the YARA rules provided by eSentire. The attackers tried to compromise a popular software site, but were unable to evade detection using known indicators of compromise. According to Kaspersky telemetry, over 150 victims have been identified, primarily individuals. However, organizations from various sectors, including retail, manufacturing, consulting, telecommunications and agriculture, have also been infected. Most of the infections occurred in Brazil, Russia, and China.

Fast16 malware

APT

Cyber sabotage

Self-propagating malware

Targeting physical modeling and engineering systems

Researchers at SentinelLabs uncovered a previously undocumented cyber-sabotage framework whose core components date back to 2005. They have tracked this framework as fast16. It predates Stuxnet by at least five years, and is the first known operation of its kind. The discovery was made when researchers traced the origins of a technique used by elite espionage malware families like Flame and Project Sauron. Those operations used a built-in scripting system called Lua, allowing attackers to update malware behavior on the spot. While searching older malware collections for early Lua use, the researchers found an obscure 2005 file named svcmgmt.exe. What appeared to be an ordinary Windows service program turned out to contain encrypted Lua code and references to a second component, fast16.sys. The name ‘fast16’ is referenced in the infamous Shadow Brokers’ leak of the NSA’s ‘Territorial

Dispute' components. According to researchers, fast16 appears to have been developed as a cyberweapon that spreads covertly through Windows networks before tampering with the output of advanced simulation software. Unlike Stuxnet, which directly targeted critical infrastructure machinery, fast16 was designed to interfere with the research and design process. The researchers said that the malware modifies calculations performed by high-precision engineering programs and simulation suites from the mid-2000s (LS-DYNA 970, PKPM, and the MOHID hydrodynamic modeling platform), introducing subtle errors into the code used for structural analysis, physics simulations, and other complex workloads. Tampering with these calculations could lead to flawed research, degraded systems, or costly design failures without any apparent signs of compromise.

Symantec released a report on the fast16 malware that expands on the findings of SentinelOne's researchers. Symantec researchers reviewed fast16's hook engine and confirmed LS-DYNA and AUTODYN as targeted applications. Symantec described in detail three unique mechanisms for interfering with the simulators' mathematical calculations. The malware infiltrates internal computer networks, spreads throughout the target infrastructure and then modifies the specific physical process being simulated. The algorithm is activated exclusively during explosion and compression simulations of materials with densities greater than 30 g/cm³, which corresponds to the density of uranium or weapons-grade plutonium when compressed before the implosion. When these values are reached, the malicious code intentionally reduces the output pressure values and disrupts the integrity of the calculations. As a result, engineers receive distorted data on uranium behavior, and supercritical state calculations are inaccurate. One of the program's mechanisms modifies Cauchy stress tensor calculations exclusively when using a specific equation of state for high explosives. Symantec research confirmed the unprecedented expertise of fast16's creators in nuclear physics, detonation processes, and nuclear explosion modeling.

Dragon Boss Solutions attacks

Cybercriminal

AV Killer

Code signing certificates

On March 22, Huntress researchers discovered a campaign in which digitally signed adware triggered alerts in multiple managed environments and deployed payloads that ran with SYSTEM privileges and disabled antivirus protection. The executables were signed by Dragon Boss Solutions LLC, a company claiming to conduct "search monetization research." The researchers observed 23,565 unique IP addresses in 124 countries trying to connect to the operator's infrastructure in a single day, with hundreds of infected endpoints present in high-value networks, including those in the educational, electric utility, power

cooperative, transport network, critical infrastructure provider, government, and healthcare sectors.

Huntress researchers discovered that the operation relied on the update mechanism of the commercial Advanced Installer tool to deploy MSI and PowerShell payloads. Analyzing the configuration file for the update process revealed several flags that rendered the operation completely silent and with no user interaction. The update process also installed the payloads with elevated SYSTEM privileges, prevented users from disabling automatic updates, and frequently checked for new updates. According to the researchers, the update process retrieves an MSI payload disguised as a GIF image. The MSI payload includes several legitimate DLLs that Advanced Installer uses for specific tasks, such as executing PowerShell scripts, searching for specific software on the system, or other custom actions defined in a separate file that contains instructions for the installer. Before deploying the main payload, the MSI installer conducts reconnaissance by checking the admin status, detecting virtual machines, verifying internet connectivity, and querying the registry for installed antivirus (AV) products from Malwarebytes, Kaspersky, McAfee, and ESET. The security products are disabled using a PowerShell script. Huntress researchers warned that, although the malicious tool currently uses an AV killer, a mechanism to introduce far more dangerous payloads to infected systems is in place and could be leveraged at any time to escalate the attacks.

Attacks on transportation and logistics

Cybercriminal

Code signing certificates

Cyber and traditional crime convergence

Spear phishing

RMM

In November 2025, Proofpoint described how threat actors gain access to companies in the shipping industry in order to steal cargo and siphon payments. The research continued, and in late February 2026, Proofpoint executed a malicious payload inside a controlled decoy environment that was delivered by email and targeted transportation organizations. After gaining access, the cybercriminals installed six separate remote access tools, including four ScreenConnect instances, Pulseway Remote Monitoring and Management (RMM), SimpleHelp RMM. The researchers believe this was an attempt to maintain remote control in case any of them were taken down. The fourth ScreenConnect instance used a PowerShell script that performed the core deployment using a third-party signing-as-a-service provider, which re-signed ScreenConnect installers and components with a valid code-signing certificate.

During the intrusion, Proofpoint observed the threat actor execute at least 13 PowerShell scripts, which collectively focused on determining whether the compromised host belonged to a financially valuable user. The scripts enumerated all local user accounts and browser profiles, extracted browsing

history, copied locked browser databases, identified hard-coded URLs associated with banking, payment, logistics, fleet service, and accounting platforms. The attackers scanned systems for cryptocurrency wallets and manually checked for PayPal credentials. A PowerShell script scanned the infected device for access points to financial institutions, money transfer services and online accounting platforms. According to researchers, the attackers intended to not only money, but also the cargo, because they searched for load management and freight brokerage platforms, as well as fuel card providers too.

Global campaign with targeted Modbus PLCs

Unknown threat actor

Attacks targeting ICS

Exploitation of public-facing applications

DDoS

Cato Networks researchers observed a global campaign involving suspicious Modbus/TCP activity against internet-exposed programmable logic controllers (PLCs), though the threat actors behind these activities remained unknown. Between September and November 2025, the researchers identified 14,426 unique targeted IPs in 70 countries, primarily in the United States. Over the three-month period, they saw thousands of requests from a broad and frequently low-reputation infrastructure set, as well as a small subset of higher-intent infrastructure of interest, including sources geolocated to China. The observed attack patterns fall into one of five categories, ranging from simple reconnaissance to critical manipulation attempts. A significant amount of the activity consisted of automated read operations. Hackers attempted to extract data from the holding registers to obtain information about the process state or configuration. Over 235,000 such requests were registered during the observation period. A second pattern involved so-called fingerprinting, in which the attackers used scripts to specifically query metadata, such as the vendor, product name, and version of the device. The fourth type of request was the expanded device identification, or higher-intent reconnaissance, which was rare and concentrated: 175 requests from six IPs. Most of these sources were geolocated in China and had strong reputation signals. In some cases, the researchers also observed high-frequency mass read operations, reminiscent of a denial-of-service (DoS) attack. The researchers were particularly concerned about the systematic write operations against writable holding-register regions. Over 3,000 write requests were identified, all originating from a single source IP. These writes followed a consistent structure, starting at 0x0BB8 and writing 27 to 122 registers. The top targeted sector was manufacturing, whose internet-exposed Modbus endpoints were targeted. It was followed by smaller shares across healthcare, construction, technology, transportation, finance, automotive and other sectors.

Attack on Mexican water utility

APT

AI-assisted breach

Between December 2025 and February 2026, an unidentified threat actor breached nine Mexican government entities using AI-assisted attacks, exfiltrating large amounts of data. According to a report from Gambit, Claude and GPT-4.1 APIs performed much of the technical work, including reconnaissance, exploit customization, privilege escalation, database architecture mapping, exfiltration infrastructure development, tunnel chain construction, and credential harvesting.

Dragos assisted Gambit's investigation, specifically focusing on an intrusion against a municipal water and drainage utility, the Servicios de Agua y Drenaje de Monterrey (SADM), and identified a significant compromise of the utility's enterprise IT environment had escalated into an attempt to breach an OT environment. The threat actor used a 17,000-line Python script written entirely by Claude as the central post-compromise framework. The script, which Claude named "BACKUPOSINT v9.0 APEX PREDATOR", featured 49 modules built upon publicly available offensive security techniques for network enumeration, credential harvesting, Active Directory interrogation, database access, privilege escalation, cloud metadata extraction, and lateral movement automation. Claude iteratively refined the framework throughout the intrusion, adding capabilities and addressing failures in response to operational feedback. Dragos discovered that the threat actor appeared to be looking for data to steal until becoming aware that the network at SADM contained an OT interface. Claude identified the utility's vNode industrial gateway as a high-value critical asset. The attacker instructed Claude to generate an attack, which turned out to be an unsuccessful password spraying attack. The failed attack indicates good password hygiene on the SADM system. Dragos observed no evidence of further activity against the vNode interface or of the adversary gaining visibility into any underlying OT environment during the intrusion. In its threat intelligence brief, Dragos wrote that AI can make OT systems more visible to adversaries already operating inside IT environments, and that further integration of AI into adversary operations reinforces the view that prevention-only security strategies are increasingly insufficient.

CISA alert on attacks targeting fuel tank monitoring systems

Attacks targeting ICS

Data manipulation

The US Cybersecurity and Infrastructure Security Agency (CISA), the FBI, the NSA, the Department of Energy, and other US government partners published a joint notice warning that hackers are targeting internet-exposed automatic tank gauge (ATG) systems used to monitor fuel and liquid storage tanks across various critical infrastructure sectors. ATG systems are widely used throughout

the energy, chemical, food and agriculture, and transportation sectors for automated and remote monitoring of storage tank parameters, including fuel and liquid levels, temperature, and leak detection. The government agencies urged ATG owners and operators to defend against this malicious activity by securing their ATG systems with strong passwords and removing them from the internet to reduce public exposure. The recent malicious activity observed by the authoring organizations and not yet attributed to threat actor group, involves cyberthreat actors compromising internet-exposed ATG systems and subsequently modifying them through command execution. According to the agencies, attackers are gaining access through authentication bypass vulnerabilities, hardcoded credentials, operating system command-execution flaws, SQL injection vulnerabilities, and privilege-escalation weaknesses. If the system is successfully compromised, the attackers can alter network settings, product identifiers, tank volumes, and pump controls. They could also disable system alerts and create conditions that prevent operators from properly monitoring tank fill levels, potentially increasing the risk of leaks or equipment failures. In May, CNN reported that Iranian hackers were behind a series of breaches involving ATG systems at gas stations in multiple states.

Attacks exploiting SmartOffice CRM

Unknown threat actor

APT

Stealer

Zero-day vulnerability

Backdoor

Exploitation of public-facing applications

In March 2026, ESET researchers noticed that unknown attackers had deployed a .NET-based browser-password stealer within the network of a defense company in the United Arab Emirates, prompting an investigation into the attack. The investigation revealed that this activity began on January 18, 2026, when the attackers compromised a server running the SmartOffice customer relationship management (CRM) platform by Zinnia and uploaded a web shell to the server. Since no publicly known remote code execution vulnerabilities were found in the product, the researchers concluded that attackers could have exploited a zero-day vulnerability. The attackers then conducted lateral movement within the compromised network and deployed several custom reverse proxy tools written in Rust. Besides the custom reverse proxy tools, the attackers deployed an OpenSSH client, validly signed by Microsoft.

On January 22, 2026, the attackers downloaded a custom hands-on-keyboard post-exploitation tool with the internal name “Koshka,” which means “female cat” in Russian. Preliminary analysis showed that it supports multiple capabilities. These include collecting information about the compromised system, such as available drives, loaded drivers, running processes, minifilter drivers, logon sessions, domain status, active TCP and UDP connections, and clipboard contents. The tool can also detect whether it is running inside a

hypervisor. In addition, it can exploit the CVE-2024-26229 vulnerability to gain SYSTEM privileges, create new user accounts, add users to existing groups, start a SOCKS proxy, dump NTLM hashes from the SAM database, and suspend the EventLog service. The tool can also load a Windows PE file, though doing so requires the payload to be encrypted with a hardcoded RC4 key.

Using telemetry, the researchers also found that the attackers attempted to deploy multiple samples of a custom reverse proxy tool written in the Rust programming language that uses the QUIC protocol over TLS to establish an encrypted tunnel. According to the debug PDB string, the project is internally named revsocks_rust. In addition to the custom reverse proxy tool, they discovered a binary whose source code is based on the open-source project portal-tunneler. By pivoting on the internal name revsocks_rust in VirusTotal, it was possible to identify multiple variants of the same malware uploaded from Yemen, that indicates potential targeting in this country.

INC attacks

Cybercriminal

Spear phishing

Linux malware

Exploitation of network devices and public-facing applications

LOTL

Ransomware

The Acronis Threat Research Unit (TRU) analyzed how INC ransomware evolved from a relatively new ransomware-as-a-service (RaaS) operation into one of the most active global ransomware groups by 2026. Since emerging in 2023, INC has claimed more than 800 victims and expanded its operations through an affiliate-based model that employs double extortion tactics. According to the report, organizations in the US account for more than 65% of the listed victims, with legal services, manufacturing, construction, technology and healthcare among the most targeted sectors. In their latest campaigns INC affiliates continued to gain initial access primarily by exploiting unpatched edge devices and public-facing applications, including vulnerabilities in Citrix NetScaler (CVE-2023-3519 and CitrixBleed 2 – CVE-2025-5777), Fortinet EMS (CVE-2023-48788), and SimpleHelp RMM (CVE-2024-57727), as well as through spear-phishing campaigns and credentials purchased from Initial Access Brokers. After compromising the system, the attackers perform network discovery, dump credentials from Veeam backup servers, and leverage a combination of living-off-the-land binaries, including RDP and PsExec, and commercial remote management (RMM) tools to move laterally and expand access across the victim environment. A key milestone in the group's evolution was the development of Linux/ESXi encryptors and the migration of both Windows and Linux payloads to Rust, which improved portability and operational resilience. The researchers also noted that the sale of INC's source code in 2024 contributed to the emergence of related ransomware families with significant code overlap, including Lynx and Sinobi.

This demonstrates the group's broader influence on the cybercriminal landscape.

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