Kaspersky ICS CERT

kaspersky

APT and financial attacks on industrial organizations in Q4 2025

06.03.2026

Version 1.0

Contents

© 2026 AO KASPERSKY LAB

© 2026 AO KASPERSKY LAB

This summary provides an overview of reports on APT and financial attacks on industrial enterprises disclosed in Q4 2025, 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

In the last quarter of 2025, information security researchers published numerous interesting reports on attacks against industrial organizations.

Most of them highlight the persistence of long-standing problems: untimely installation of security updates, including on internet-accessible systems; insecure provision of remote access to internal systems; the difficulty of monitoring the security of trusted partners and suppliers; the inability to guarantee 100% protection for traditional operating systems with their inherent information security issues (DLL hijacking, BYOVD, and malware); and the lack of staff preparedness to resist basic social engineering techniques.

However, some deserve a special mention. In several cases, attackers managed to access OT systems and use them to control process units or facilities.

For example, in a joint bulletin released with the Royal Canadian Mounted Police, the Canadian Centre for Cyber Security (CCCS), describes three attacks in which hacktivists: (a) altered the pressure in a municipal water supply; (b) triggered false-positive alarms at an oil and gas company by tampering with an automated tank gauge (ATG) fuel-level monitoring system; and (c) manipulated the control systems of a grain-drying silo, setting incorrect temperature and humidity parameters – an extremely dangerous situation if not detected in time, as it threatens the spoilage of the grain and the development of toxic fungi.

According to another bulletin jointly released by the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI, hacktivists successfully accessed remote systems at US critical infrastructure facilities in the water and wastewater, food and agriculture, and energy sectors on a number of occasions via internet-accessible VNC. The most common result of these attacks was the temporary loss of remote control at the affected facilities.

Two stories describe how Chinese-speaking hackers successfully spoofed software updates from Chinese developers vulnerable to simple man-in-the-middle (MitM) techniques. The attackers compromised edge network devices

© 2026 AO KASPERSKY LAB

by installing an implant that redirected all DNS requests to their own servers. In at least one case, however, the attackers also demonstrated the ability to intercept and spoof traffic at the level of root internet routers. Most industrial organizations will find it very difficult to defend against this attack vector on their own.

An interesting tactic was observed in the arsenal of the Qilin ransomware group. They attacked Windows systems using Linux malware, after somehow enabling the Windows Subsystem for Linux (WSL) on them. This apparently reduced the likelihood of detection and blocking by security tools.

A curious piece of malware was discovered by Socket's Threat Research Team. Sharp7Extend is a malicious extension for the Sharp7 library, a C# implementation of an outdated version of the Siemens S7 PLC communication protocol. The malicious code terminates the parent process at every fifth attempt to access the PLC. The code likely acts as a filter, targeting the most irresponsible developers who have never heard of testing application functionality during development and before release. Users of the application developed by these irresponsible developers are in for a surprise. After 30–90 minutes of application execution, the malicious code begins returning an error code for four out of five attempts to write to the PLC. This is likely intended to cause failures in the application's logic. It seems that the purpose of the malware is to promote maturity and a better development culture among small developers of industrial automation systems.

The following studies were perhaps the most unexpected and unusual publications.

We all know that data obtained through cyberespionage can be used for financial, political, and geopolitical purposes, as well as for military intelligence, especially during military conflicts. This quarter, information about the probable traces of such cyberattacks has appeared in the public domain.

Amazon Threat Intelligence described scenarios in which cyberattacks were used to search for and select tracking and video surveillance systems on a ship that was hit by a missile strike several months later. Another scenario describes the compromise of street surveillance cameras in Jerusalem neighborhoods that were hit by missile attacks several days later.

The current pace of digitalization has made vessel systems vulnerable to attacks by not only intelligence agencies, but also ordinary cybercriminals. Cydome researchers reported the discovery of a new variant of the Mirai botnet dubbed Broadside. The botnet spreads by exploiting vulnerability CVE-2024-3721 in TBK Vision DVRs (digital video recorders) commonly used on ships. This poses a risk of infection for many ships and sends a clear message

© 2026 AO KASPERSKY LAB

to fleet owners, operators, shipbuilders and suppliers of ship system components about the urgent need to address cybersecurity issues seriously.

We've discussed and written extensively about the potential for cyber-physical attacks on transportation and logistics facilities. This quarter, Proofpoint researchers described a pattern of cyberattacks on transportation and logistics companies. The ultimate goal of these attacks was to hijack orders for cargo that interested the attackers. According to the researchers, the final stage – the physical theft of the cargo – was likely carried out in collaboration with ordinary (non-cyber) criminals. We believe that such criminal schemes no longer need to go beyond cyberspace – the final stages of delivering the stolen cargo can also be hacked or manipulated covertly. The development of online sales ecosystems and marketplaces allows for the fully automated delivery of stolen goods to arbitrary end customers.

Anthropic researchers reported a new level of AI technology exploitation discovered in the arsenal of the Chinese-speaking group GTG-1002. The attackers used Claude Code and AI agents at every stage of the attack, from targeting and exploiting vulnerabilities during initial penetration of the victim's infrastructure, to reconnaissance, lateral movement, and data exfiltration. This automates 80–90% of the entire process, leaving humans solely responsible for quality control and minor adjustments to the AI agents' actions during the attack. This research may publicly signal the start of the AI cyberweapons race.

Russian-speaking activity

Sandworm attacks

APT

Wiper

Groups collaboration

Exploitation of network devices and public-facing applications

Traffic interception

In an ESET APT activity report, researchers described Sandworm (also known as APT44, Seashell Blizzard, BlackEnergy, PHANTOM, Blue Echidna) attacks between April and September 2025. According to ESET, Sandworm is continuing its destructive campaigns in Ukraine, deploying a variety of data-wiping malware primarily through the exploitation of the Group Policy feature of Active Directory. In April, the threat actor launched two wipers, ZEROLOT and Sting, against a Ukrainian university. Notably, the Sting wiper was executed via a Windows scheduled task named DavaniGulyashaSdeshka, a phrase derived from Russian slang that translates roughly to "eat some goulash". In June and September, Sandworm deployed multiple variants of data-wiping malware against Ukrainian entities in the government, energy, logistics, and grain sectors. While all four sectors have been documented as targets of wiper attacks at some point since 2022, the grain sector stands out as a less frequent target. During this period, researchers observed and confirmed that the UAC-0099

© 2026 AO KASPERSKY LAB

Group conducted initial access operations and subsequently transferred validated targets to Sandworm for follow-up activity. Recent UAC-0099 activities were thoroughly documented by CERT-UA and Fortinet. Although some reports suggested a refocusing on espionage activities by Russian-speaking groups in late 2024, ESET researchers observed Sandworm regularly conducting wiper attacks against Ukrainian entities from the beginning of 2025.

Amazon's CISO reported with high confidence on a cluster of activity targeting Western energy companies linked to the Sandworm Group. He noted that up to 2024, the long-running campaign had exploited multiple vulnerabilities in WatchGuard (CVE-2022-26318), Confluence (CVE-2021-26084 and CVE-2023-22518), and Veeam (CVE-2023-27532) as the primary initial access vector, targeting misconfigured devices. In 2025, the threat actor relied less on vulnerabilities and more on targeting misconfigured customer network edge devices, such as enterprise routers, VPN gateways, network management appliances, collaboration platforms, and cloud-based project management solutions. Although Amazon did not directly observe the extraction mechanism, evidence in the form of delays between device compromise and credential abuse points to passive packet capture and traffic interception. Some of the compromised devices were customer-managed network appliances hosted on AWS EC2 instances. Amazon noted that the attacks did not exploit vulnerabilities in the AWS service itself, but rather leveraged misconfigured customer devices. Amazon believes that the Curly COMRades Group, first reported by Bitdefender, may have conducted post-compromise activity as part of a broader campaign involving multiple specialized subclusters because infrastructure overlap was observed between the two groups.

RomCom attacks

Groups collaboration

Compromised websites

Fake update

Backdoor

In September 2025, Arctic Wolf Labs identified a US engineering company that was targeted by the RomCom threat actor (also known as Void Rabisu, Storm-0978, Tropical Scorpius, or UNC2596) via SocGholish, operated by TA569. SocGholish is a long-running malware delivery framework first discovered in 2017. It consists of a downloader that is distributed via malicious JavaScript injected into compromised websites to facilitate the delivery of its payloads, which are collectively known as FAKEUPDATE. When the user manually clicks "Update", a malware payload is downloaded to their device. After execution, SocGholish exfiltrates data from infected systems via POST commands to the C2 infrastructure, enabling a multitude of malicious post-exploitation activities. In the case observed by Arctic Wolf researchers, the user unintentionally initiated the above attack chain by executing SocGholish's FAKEUPDATE payload, which allowed the operators to run commands on the system. Once

© 2026 AO KASPERSKY LAB

the reverse shell executed on the target's system, SocGholish operators performed digital reconnaissance, primarily through PowerShell commands. Three minutes prior to the delivery of RomCom's shellcode loader, a dynamichttp Mythic agent, the operator tested the connection to Mythic C2. This sample checks the domain that the system resides on, and if it matches the hardcoded value, it decrypts and executes the shellcode. According to the researchers, this was the first time a RomCom payload had been observed being distributed by SocGholish. A secondary payload, including VIPERTUNNEL – a custom Python backdoor – was also uploaded to the system and scheduled.

CISA alert on hacktivists attacks on critical infrastructure

Hacktivist

Exploitation of public-facing applications

DoS

Attacks targeting ICS

On December 18, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA) and several international partners put out a Cybersecurity Advisory highlighting known TTPs of Russian-speaking hacktivist groups targeting critical infrastructure. The authoring organizations assess that hacktivist groups are conducting less sophisticated attacks against critical infrastructure entities, compared to APT groups. These attacks use minimally secured, internet-facing VNC connections to infiltrate or gain access to OT control devices within critical infrastructure systems. The hacktivist groups Cyber Army of Russia Reborn (CARR), Z-Pentest, NoName057(16), Sector16, and affiliated groups are capitalizing on the widespread prevalence of accessible VNC devices to execute attacks against critical infrastructure entities, causing varying degrees of damage. Victim organizations reported that the most common operational impact is a temporary loss of view, necessitating manual intervention to manage processes. Targeted sectors include water and wastewater systems, food and agriculture, and energy. Hacktivist groups successfully targeted SCADA networks using basic methods, and in some cases, performed simultaneous DDoS attacks. The groups abuse popular internet-scraping tools, such as Nmap or OPENVAS, to search for visible VNC services and use brute-force password spraying tools to access devices via known default or otherwise weak credentials. Threat actors typically search for these services on the default port 5900 or other nearby ports (5901-5910). Their objective is to gain remote access to HMI devices connected to live control networks.

© 2026 AO KASPERSKY LAB

SHADOW-VOID-042 attacks

APT

Cybercriminal

Spear phishing

Browser exploitation

Security researchers at Trend Micro published a report detailing an active, highly targeted espionage campaign tracked as SHADOW-VOID-042. In October and November of 2025, SHADOW-VOID-042 campaigns targeted sectors such as energy, defense, pharmaceuticals, chemicals, logistics, manufacturing, food, retail, ICT, ISP, finance and cybersecurity. These campaigns began with personalized spear-phishing messages containing highly credible lures. Notably, these lures impersonated legitimate software updates (fake Trend Micro updates) or sensitive internal documents, such as HR harassment complaints. Other social engineering lures included invitations to join academic research or to fill out a work-related questionnaire. After clicking on the link, the target is redirected multiple times and ends up on an HTML page impersonating Cloudflare, where three different JavaScript files get loaded. One of the scripts contains code that exploits Chrome vulnerability CVE-2018-6065; the other two were not retrieved. If the vulnerability exploitation fails, the target is redirected to a decoy website crafted to mimic Trend Micro's corporate branding. The JS file contains a hardcoded 64-bit shellcode that sends a request to the C2 server and retrieves an encrypted binary. The binary is then decrypted and written to a hardcoded file path. The final payload was not retrieved in these campaigns. According to researchers, this operation shows technical overlap with the Void Rabisu Group (also known as RomCom, Tropical Scorpius, or Storm-0978). Void Rabisu conducts both financial cybercrime and intelligence collection via cyberespionage.

Targets in Russia

Attacks with GoRed Backdoor

Hacktivist

Supply chain

Backdoor

Exploitation of public-facing application

Trojanized software

Groups collaboration

The GoRed backdoor, also known as the Bulldog backdoor, is sophisticated cyberespionage malware that targets Russian organizations. It is linked to ExCobalt and Shedding Zmiy, according to public research (Kaspersky researchers track this activity as Red Likho). First discovered in 2023, recent Kaspersky research uncovered a new infection vector, a complex malware delivery method and other TTPs of the GoRed operators. The GoRed backdoor targets organizations in various industries, including IT, manufacturing, automotive, energy, and software development. Recent campaigns have shown a significant focus on the software development industry, suggesting a strategic effort to conduct supply chain attacks.

© 2026 AO KASPERSKY LAB

In one incident, attackers compromised a public web portal and, by exploiting configuration errors in PostgreSQL, were able to remotely execute commands that downloaded the GoRed backdoor. This infection vector had not been encountered before in attacks involving GoRed. In addition to compromising the victim's web portal, the attackers gained initial access by exploiting a chain of ProxyShell vulnerabilities affecting Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207). After gaining elevated privileges, the attackers uploaded a malicious web shell (.aspx) to the root directory of the Exchange server. They performed initial reconnaissance using this web shell and then downloaded the GoRed backdoor through it by executing the obfuscated command.

In GoRed attacks, researchers observed trojanized samples similar to those used by the BO Team Group. One of Red Likho's victims was mentioned among BO Team's victims on their Telegram channel. Based on these facts, researchers suspect that the two groups may have conducted joint operations. Given that BO Team is known to collaborate with other hacktivists targeting Russia, such as the Ukrainian Cyber Alliance, it is likely that the group is sharing knowledge and tools with Red Likho, or they could be conducting a joint, coordinated operation.

Coordinated cyberattacks by pro-Ukrainian groups

Cybercriminal

Hacktivist

Backdoor

Ransomware

Trojanized software

Groups collaboration

Kaspersky researchers reported a series of coordinated cyberattacks carried out by several pro-Ukrainian hacktivist groups. The campaigns targeted organizations in Russia across various sectors, including manufacturing, healthcare, and government. One notable aspect of these incidents is that two to three distinct groups were simultaneously involved in targeting a single victim. This overlapping activity significantly complicates attribution because it becomes challenging to distinguish the TTPs of each group.

Researchers examined a series of campaigns publicly attributed to the pro-Ukrainian group 4BID. The group emerged in early 2025 via a Telegram channel that became its primary communication outlet. Initially focused on smaller regional enterprises, 4BID has expanded its scope to larger, high-profile targets. Researchers found evidence of activity linked to two other known threat groups, BO Team and Red Likho, in the organizations affected by these 4BID campaigns. Specifically, the infrastructure attacked by 4BID was also infected with GoRed, a backdoor associated with Red Likho, and ZeronetKit, a backdoor linked to BO Team.

Analysis revealed a diverse toolkit that included 4BID's ransomware, dubbed Blackout Locker. Notable artifacts also included custom scripts for checking

© 2026 AO KASPERSKY LAB

computers on the network for AnyDesk or Kaspersky solutions, as well as for installing AnyDesk. There was also a patched Process Explorer sample that downloaded Tuoni or Cobalt Strike. This combination of tools suggests that the groups are working together or in parallel with overlapping goals, such as disruption, data exfiltration, and persistent access to critical systems.

Cloud Atlas attacks

APT

Spear phishing

DLL sideloading

Backdoor

F6 researchers reported attacks by the Cloud Atlas Group on Russian companies in the agro-industrial and defense industries. In mid-October 2025, F6 recorded a Cloud Atlas attack targeting a Russian agro-industrial company. The bait document downloaded an RTF file via a template. The RTF file contained an exploit for the CVE-2017-11882 vulnerability, resulting in the download of the VBShower dropper. In a similar attack on enterprises from the agro-industrial complex in September, the payload was also the VBShower backdoor.

While investigating the October attack, F6 detected two additional files associated with the .live domain used by the attackers that were uploaded to the VirusTotal platform. The names and contents of the files were related to procurement and the collection of data from employees at enterprises, indicating potential attack targets among Russian defense industry companies. Further analysis of the network infrastructure and file characteristics revealed also .fr domain. The payload was unavailable at the time of analysis. Researchers noted that the group rarely uses domains outside the preferred zones: com, net, org and info. This behavior was also observed in November 2023 and October 2024 when the group used the domains .online and .cfd in attacks on Russia and Belarus.

In July 2025, two similar LNK files were uploaded to VirusTotal, matching LNK files uploaded in late 2024. They contained a bait PDF file and PowerShell commands for making a request to a server and processing the server's response. In both cases, the payload was unavailable, but infrastructure analysis led to the conclusion that the Cloud Atlas APT Group was, with a high degree of certainty, behind the attack using these LNK files.

In 2025, Kaspersky researchers described the infection chain and tools used by the Cloud Atlas Group, including previously undescribed implants. The observed implants included PowerShower PS script, the VBShower and VBCloud VBS files, and the CloudAtlas backdoor. The CloudAtlas backdoor is installed using VBShower from the downloaded archive via a DLL hijacking attack, where the legitimate VLC application acts as a loader, accompanied by a malicious library that reads the encrypted payload from the file and transfers

© 2026 AO KASPERSKY LAB

control to it. The CloudAtlas backdoor retrieves various payloads from the C2 server, including FileGrabber, PasswordStealer, and InfoCollector. The Cloud Atlas Group uses a custom Python script to extract saved credentials from browsers on infected systems. The identified targets of the malicious activities were located in Russia and Belarus, with activity observed dating back to the beginning of 2025. Targeted industries included organizations in the telecommunications sector, construction, government, and manufacturing.

Cyber groups targeting Russia

Cybercriminal

APT

Hacktivist

Phishing websites

ClickFix

Spear phishing

Backdoor

In the third quarter of 2025, Positive Technologies researchers published an analysis of activity by cyber groups targeting Russian organizations, along with updated TTPs, victimology, and toolsets. PT classified the groups' activities as either cyberespionage, financial motivated, or hacktivism. The groups' attacks targeted companies in logistics, manufacturing, and energy companies, among others.

Cyberespionage activities included those of the Telemancon Group, which targeted Russian industrial organizations and previously used a custom-written TMCDropper with separate encrypted code segments. However, the attackers have switched to VM-based obfuscation with multi-layered encryption in the current version of TMCDropper, making it significantly more difficult to analyze their programs. Another of the group's tools, the TMCShell backdoor, can now detect whether the attack was launched in a sandbox. The report also details the activities of other cyberespionage groups such as PseudoGamaredon, TA Tolik, XDSpy, Rare Werewolf, Goffee, and IAmTheKing. The attack chains of these groups began with phishing emails. The PhantomCore group used phishing pages with fake CAPTCHAs that prompted the execution of a PowerShell script.

Financially motivated activity included DarkGaboon, DarkWatchman, and Fluffy Wolf, all of which used phishing emails with malicious archives. The hacktivist group Black Owl continued to attack companies in the transportation and logistics sector with business-related spear-phishing emails. To increase their chances of successfully launching malware, attackers increasingly included several identical samples in one archive, differing only in the decoy documents. Using legitimate tools for tracking email opening, the attackers assessed recipient engagement and prioritized further actions for contacts most likely to open the attachment.

© 2026 AO KASPERSKY LAB

Attacks on the aerospace industry in Russia

Hacktivist

Spear phishing

Phishing websites

Compromised legitimate mailboxes

Backdoor

Intrinsec analyzed multiple intrusion campaigns targeting Russian aerospace companies and organizations linked to electronic warfare, military supply, and the energy sector. The activity appears to have originated from several hacktivist groups aligned with Ukrainian interests, using both credential-phishing pages and malware-based operations. The attackers sent spear-phishing emails that impersonated Russian government bodies and linked to fake login pages hosted on services like IPFS, Vercel, Contabo S3, and Cloudflare buckets. More advanced intrusion sets, such as Head Mare and Hive0117, used weaponized emails and custom malware delivered from compromised Russian email servers.

Arcane Werewolf attacks

APT

Spear phishing

C2 mimicking industrial companies

Backdoor

Bi.ZONE researchers reported malicious activity from the Arcane Werewolf (Mythic Likho) cluster, targeting Russian industrial companies in October and November of 2025. As in previous cases, the attackers likely used phishing emails as their initial access vector, although the emails were not retrieved. The emails allegedly contained a link to download a malware archive from a hacker-controlled resource masquerading as a Russian industrial company. The downloaded archive contained a malicious LNK file, as well as a "Photos" ("Фото") directory with a collection of JPG images. After launching the LNK file and executing the command via PowerShell, an executable file was downloaded and launched via conhost.exe. The downloaded icon2.png file is a PE32+ executable and malware dropper implemented in Go. It contained two Base64-encoded payloads: a PE32+ executable file that acts as a malicious downloader and a decoy PDF document containing information about defective batches of electronic goods. The dropper decodes and saves the payload to the %TEMP% directory, then executes commands to deliver Loki 2.0.

Further activity from the Arcane Werewolf cluster was detected in November, but unfortunately, the entire attack chain could not be reconstructed. A malicious network resource was mimicking the website of a Russian industrial company. The decoy PDF document contained information about an internal investigation into the package. A new C++ dropper and an updated Loki 2.1, compatible with Mythic and Havoc, were detected in this attack.

© 2026 AO KASPERSKY LAB

Paper Werewolf attacks

APT

Spear phishing

AI-generated decoy documents

Backdoor

Researchers from Intezer identified Paper Werewolf (aka GOFFEE) as the group that launched a new campaign targeting Russian military personnel and defense-industry organizations. The campaign emerged in October and used a malicious XLL file uploaded to VirusTotal, first from Ukraine and later from Russia. The files, titled "Плановые цели противника.xll" (“enemy’s planned targets”) and "Плановые цели противника НЕ ЗАПУСКАТЬ.xll" ("DO NOT LAUNCH enemy planned targets"), were designed to automatically execute malicious code when opened in Excel. When launched, the files downloaded an undocumented backdoor dubbed EchoGather, which allowed the attackers to collect system information, execute commands, and transfer files. The stolen data was sent to a C2 server disguised as a food delivery website.

The GOFFEE Group phishing lures also included a fake invitation to a concert for senior military officers. The document showed clear signs of being generated artificially, such as linguistic errors and a distorted imitation of Russia’s double-headed eagle emblem. Another lure impersonated a letter from a deputy in Russia’s Ministry of Industry and Trade, requesting pricing justification documents related to state defense contracts. The letter was addressed to major defense and high-tech enterprises, which Intezer said were likely the intended targets. Both lures were also associated with the EchoGather backdoor.

Operation FrostBeacon

Cybercriminal

Spear phishing

Seqrite Labs uncovered a financially motivated cyber campaign targeting Russian B2B enterprises, particularly those in the logistics, industrial production, construction, and technical supply sectors. The threat actors' ecosystem includes multiple infection chains and decoys designed to target the finance and legal departments of Russian organizations. Dubbed Operation FrostBeacon, the campaign employs a multi-layered infection chain to deliver Cobalt Strike beacons. The threat actors utilize two distinct clusters for initial access. The first cluster uses phishing emails with malicious archive files, which contain LNK and HTA loaders. The second cluster exploits legacy vulnerabilities CVE-2017-0199 and CVE-2017-11882 via weaponized DOCX files. In this case, the phishing emails claim to be legal demands for debt repayment. Both clusters ultimately lead to the execution of an obfuscated PowerShell loader that decrypts and runs shellcode in memory to deploy Cobalt Strike. The campaign's infrastructure includes multiple RU zone domains configured as C2 endpoints with a customized Cobalt Strike malleable profile to evade detection. Researchers observed an overlap of TTPs and targeting with those of the Cobalt Group, which has targeted financial institutions around the world.

© 2026 AO KASPERSKY LAB

However, they haven't seen any specific malware families used by the attackers in Operation FrostBeacon.

VasyGrek attacks

Cybercriminal

Spear phishing

GitHub links

Backdoor

Ransomware

F6 researchers reported on new activities by VasyGrek related to phishing emails targeting Russian organizations for cyberespionage purposes. VasyGrek (also known as Fluffy Wolf) is a Russian-speaking threat actor that targets Russian companies in various sectors and has been active since at least 2016. The new F6 report detailed VasyGrek's tools and attacks from August to November 2025. During this period, VasyGrek attacked Russian companies in the following sectors: manufacturing, construction, energy, agriculture, security, trade, finance, information technology, media, and entertainment.

After publishing research in July 2024, including on the collaboration with the malware vendor Mr. Burns, VasyGrek stopped using BurnsRAT. However, the attacker's infection chains remained largely unchanged from then until October 2025. The attackers continued to send accounting-related phishing emails containing malicious files delivered to potential victims either as an attachment, or via links to GitHub repositories or domains registered by VasyGrek. The malicious file was either an archive containing an executable file or a PureCrypter executable, which could deliver subsequent next-stage malware to the victim's system and inject payloads into the desired processes. The stages could be downloaded from external resources or stored locally in encrypted form. VasyGrek used software from the PureCoder developer (PureCrypter, PureHVNC/PureRAT, PureLogs Stealer) as well as Pay2Key, a ransomware service distributed as ransomware as a service (RaaS) built on the well-known Mimic ransomware.

Some changes in infection chains were observed in November: instead of archives containing executable files, email attachments were now being used with archives containing BAT and VBS files. In the chain containing the VBS file, the final payload was the PureHVNC malware, but a different downloader – the PowerShell stego downloader – was used to deliver it instead of the usual PureCrypter. This downloader has been used by various attackers, and repeatedly observed in the arsenal of the Sticky Werewolf Group.

© 2026 AO KASPERSKY LAB

Korean Peninsula

Lazarus attacks

APT

RAT

Trojanized software

DLL sideloading

DLL proxying

Compromised websites

Spear phishing

Backdoor

ESET researchers uncovered a new wave of Operation DreamJob by the Lazarus Group, targeting European aerospace and defense companies, particularly those developing unmanned aerial vehicle (UAV) technology. The primary goal of the attackers was likely to steal proprietary information and manufacturing know-how. Initial access was most probably achieved via social engineering. The target received a decoy document containing a job description and trojanized software to open it. The campaign used trojanized open-source software such as modified Notepad++, WinMerge, TightVNC Viewer and MuPDF projects to deliver the ScoringMathTea remote access Trojan (RAT). This malware employed DLL sideloading, reflective code loading, and AES/ChaCha20 encryption for stealth, enabling remote control, file manipulation, and data exfiltration. To evade detection, the attackers embedded their malicious loaders within legitimate projects and used multi-stage droppers and loaders before deploying the RAT in memory. Analysis shows that Lazarus continues to refine its DreamJob operations with new libraries for DLL proxying, modular loaders, and improved obfuscation techniques to maintain a consistent and effective strategy for targeting the technology and defense sectors.

ENKI researchers uncovered a new Lazarus Comebacker variant delivered through fake aerospace- and defense-themed Word documents, indicating a targeted espionage operation. The lure files carried malicious macros that decrypted multiple stages of the malware, eventually loading the final Comebacker backdoor directly in memory. The actor used a refined infection chain with custom decryption, ChaCha20-protected loaders, and AES-encrypted C2 traffic, highlighting a clear upgrade from earlier Comebacker versions. Infrastructure research revealed additional command-and-control domain and samples dating back to March 2025, indicating an ongoing, long-running campaign. The decoys impersonated organizations such as Edge Group, IIT Kanpur, and Airbus, suggesting deliberate targeting. The campaign's goal appears to be intelligence gathering and long-term access within sensitive industries.

© 2026 AO KASPERSKY LAB

Middle East-related activity

MuddyWater attacks

APT

Spear phishing

Access brokers

Backdoor

ESET Research disclosed a refined cyberespionage campaign by MuddyWater targeting entities in Israel and Egypt, including those in the government, manufacturing, transportation, utilities, engineering and technology sectors. Initial access is typically achieved through spear-phishing emails, often containing PDF attachments that link to installers for RMM software hosted on free file-sharing platforms such as OneHub, Egnyte, or Mega. These links lead to the download of RMM tools including Atera, Level, PDQ, and SimpleHelp. Also among the tools deployed by MuddyWater operators is the VAX-One backdoor, named after the legitimate software it impersonates: Veeam, AnyDesk, Xerox, and the OneDrive updater service. The operation also introduced previously undocumented custom tooling, including the Fooder in-memory loader and MuddyViper, a C/C++ backdoor designed for stealthy persistence, credential theft, and remote control. Fooder evades detection using game-inspired delay logic and reflective loading, while MuddyViper supports extensive command execution, data exfiltration, and multiple persistence mechanisms. The campaign also deploys credential and browser data stealers (CE-Notes, LP-Notes, and Blub) and go-socks5 reverse tunnels for covert C2 routing. Compared to earlier MuddyWater campaigns, ESET observed reduced hands-on-keyboard activity and increased operational discipline. Notably, the activity shows operational overlap with the Lyceum (OilRig) subgroup, suggesting cooperation or access-broker behavior. Overall, the campaign reflects a clear maturation in MuddyWater's tooling and tradecraft while retaining a predictable espionage-focused playbook.

GalaxyGato attacks

APT

DLL sideloading

Backdoor

ESET researchers reported that the Iran-aligned threat group GalaxyGato started targeting victims in Greece's shipping industry, much like MuddyWater and some China-aligned groups. Since July 2025, GalaxyGato has used its C5 backdoor (another name for the group) and iteratively improved on it. During the campaign targeting Greece, GalaxyGato used PowerShell scripts to gather information on compromised systems and list installed programs (likely in an effort to evade cybersecurity software). Using PowerShell, particularly in this manner, is practical and offers a low probability of being detected by SOC analysts. According to the researchers, this was not the first time this particular C5 version had been discovered in the wild. In July 2025, GalaxyGato debuted this version in a campaign targeting an organization in Israel. Again, GalaxyGato

© 2026 AO KASPERSKY LAB

used PowerShell, but this time to deliver C5 from the C2 server. It is heavily obfuscated with the ConfuserEx protector. An interesting twist in this campaign is a DLL search order hijack in which GalaxyGato pushed a malicious DLL to the Windows Defender directory (C:\Program Files\Windows Defender). Windows Defender calls a DLL with the same name – Version.dll – but the malicious DLL loads first (based on its location on disk). The malicious DLL calls another malicious DLL nested one directory lower (C:\Program Files\ Windows Defender\Offline\MMpLics.dll) that GalaxyGato also pushed to the victim's system. This second DLL – MMpLics.dll – is called by LSASS whenever a user enters credentials, at which point MMpLics.dll writes those credentials to another file in the Windows Defender directory (C:\Program Files\ Windows Defender\en-US\MsMpCon.dll.mui). GalaxyGato can then exfiltrate the credentials for lateral movement and privilege escalation.

UNC1549 attacks

APT

Spear phishing

Backdoor

C2 proxied via Azure

DLL sideloading

Code signing certificates

Supply chain/trusted partner

Linux malware

Mandiant researchers uncovered ongoing espionage operations by UNC1549 (also known as Smoke Sandstorm, TA455, Yellow Liderc, Tortoiseshell, and Imperial Kitten) targeting organizations in the aerospace, aviation, and defense industries, primarily in the Middle East. The group gains initial access through two methods: highly tailored phishing emails and compromising trusted third-party suppliers to enter networks through legitimate connections. Once inside, they use creative lateral movement, such as breaking out of Citrix/VMware sessions, abusing internal ticketing systems, and stealing data to craft more convincing phishing emails. UNC1549 deploys multiple custom backdoors (TWOSTROKE, DEEPROOT, MINIBIKE and GHOSTLINE), often using DLL hijacking and Azure-hosted infrastructure to remain hidden. One of the malware programs used is DEEPROOT, a Linux backdoor written in Golang. The attackers also rely heavily on reverse SSH tunnels and long-dormant backdoors designed to survive detection and reappear later. They use credential theft, screen capture, and fake login prompts to escalate privileges and gather sensitive data. UNC1549 uses DCSYNCER.SLICK, a modified version of the open-source tool DCSyncer, to perform Active Directory DCSync operations and extract password hashes. The threat group was observed signing some of their backdoor binaries with legitimate code signing certificates to weaponize malware samples, including variants for GHOSTLINE, POLLBLEND, and TWOSTROKE. In September, Check Point and Prodaft also reported on UNC1549 attacks, describing some of these features.

Amazon Threat Intelligence uncovered a new trend they call cyber-enabled kinetic targeting, where nation-state groups use cyber intrusions to directly support physical military attacks. In one case, Imperial Kitten hacked maritime

© 2026 AO KASPERSKY LAB

tracking systems and even shipboard CCTV months before a missile strike on the same vessel. In another case, MuddyWater accessed live CCTV cameras in Jerusalem days before Iran's missile attacks, providing visual intelligence for targeting purposes. Amazon notes that this marks a shift from cyber operations being separate from warfare to becoming a core part of battlefield targeting.

Chinese-speaking activity

PassiveNeuron attacks

APT

SQL server compromise

GitHub DDR

CloudFront C2

Kaspersky researchers identified a new wave of Windows Server infections linked to the PassiveNeuron campaign, which was previously described in 2024. These infections were observed in government, financial, and industrial organizations in Asia, Africa, and Latin America. Analysis of these incidents provided additional insights into the campaign. Specifically, the initial infection vector was identified as an SQL Server compromise, suspected to have been carried out using the SQLMap tool. Following the compromise, the attackers attempted to deploy web shells. They also used the Neursite (a custom C++ modular backdoor), NeuralExecutor (a custom .NET implant used for running additional .NET payloads), and Cobalt Strike implants to conduct further malicious activity on the infected machines. It was noted that the NeuralExecutor implant had been updated to use GitHub as a dead drop resolver to obtain a C2 server. Additionally, researchers were able to attribute the PassiveNeuron campaign to a Chinese-speaking actor with a low degree of confidence. A PDB string in one of the analyzed DLLs pointed to the APT41 Group mentioned in a Cisco Talos report.

PlushDaemon attacks

APT

AitM

Backdoor

Supply chain

Exploitation of public-facing applications

ESET researchers uncovered a Chinese-speaking espionage operation called PlushDaemon that uses a network implant named EdgeStepper to hijack software updates through adversary-in-the-middle attacks. The attackers first compromise routers or other network devices and redirect all DNS traffic to their own servers, tricking update mechanisms into downloading malicious files. PlushDaemon was observed hijacking updates to the Sogou Pinyin Method input editor, but researchers also observed other popular Chinese software updates being hijacked in the same way. The downloads deliver LittleDaemon and DaemonicLogistics, which in turn install the group's SlowStepper backdoor. The group also uses web-server exploits and supply-chain attacks to create additional entry points. This long-running campaign targets both individuals and

© 2026 AO KASPERSKY LAB

organizations. PlushDaemon has compromised individuals and organizations in the following regions: the USA, Taiwan, and China (including a university and a Taiwanese electronics manufacturer), Hong Kong, New Zealand, and Cambodia (including a company in the automotive sector and a branch of a Japanese company in the manufacturing sector).

SinisterEye attacks

APT

AitM

Backdoor

According to ESET researchers, the Chinese-speaking group SinisterEye (also known as LuoYu or CASCADE PANDA) conducted cyberespionage operations in China against domestic and foreign entities. With probable access to internet backbone infrastructure, the group's main initial access technique is to hijack updates in order to deliver its flagship backdoors: WinDealer for Windows and SpyDealer for Android. From May, the group constantly targeted a Taiwanese defense aviation company's offices in China. This company is also involved in the semiconductor industry. In August, SinisterEye began targeting representatives of a US trade organization based in China, and the offices of a Greek governmental entity in China. In the former case, researchers believe this targeting relates to the ongoing commercial tug-of-war between the USA and China because the targeted organization was reportedly involved in lobbying efforts meant to ease some US tariffs on several Asian countries. In September, researchers also detected WinDealer samples on machines of an Ecuadorian government entity. While SinisterEye's hijacking mechanism appears to be focused mostly on outdated update protocols of Chinese software, such as Sogou Pinyin Method, 360 Total Security, Taobao, and Youdao, researchers have observed cases in which executable files appear to have been replaced in transit. This suggests that SinisterEye's capabilities are not limited to a fixed set of supported updates.

APT24 attacks

APT

Spear phishing

Compromised websites

DLL sideloading

Supply chain

Backdoor

Researchers from Google Threat Intelligence Group reported the discovery of BadAudio, previously undocumented malware deployed by the Chinese-speaking APT24 Group during a three-year espionage campaign featuring highly sophisticated attack variants. The malware was delivered to victims through various methods, including phishing, supply chain hacking, and watering hole attacks. From November 2022 to September 2025, APT24 compromised more than 20 legitimate websites, ranging from regional industrial concerns to recreational goods. This indicated an opportunistic approach to initial access, with selective targeting executed against visitors identified via fingerprinting. The legitimate websites were weaponized by injecting a malicious JavaScript payload. The script collected fingerprints that met the attack criteria and

© 2026 AO KASPERSKY LAB

displayed a fake software update pop-up window that mimicked Chrome and prompted the user to download BadAudio. Starting in August 2024, the group launched phishing attacks, distributing the BadAudio malware via emails purportedly from an animal rescue organization as bait. In some variants of these attacks, APT24 used legitimate cloud services like Google Drive and OneDrive to deliver the malware instead of its own servers.

The BadAudio malware is heavily obfuscated. It leverages DLL search order hijacking for execution via legitimate applications. BadAudio collects system information (hostname, username, and architecture), encrypts it with a hardcoded AES key, and sends it to a hardcoded C2 address. It then downloads the AES-encrypted payload from the C2, decrypts it, and executes it in memory via a DLL loader. Google researchers observed the deployment of Cobalt Strike Beacon via BadAudio in one case, but could not confirm the beacon's presence in all incidents.

WARP PANDA attacks

New threat actor

Exploitation of network devices and public-facing applications

Cloud services C2

Linux malware

Backdoor

CrowdStrike researchers disclosed a previously unidentified Chinese-speaking intrusion set dubbed WARP PANDA that is responsible for long-term, covert intrusions targeting VMware vCenter and ESXi environments at legal, technology, and manufacturing entities based in the USA. Active since at least 2022, the group demonstrates advanced operational security (OPSEC) and cloud expertise, primarily focusing on data theft. WARP PANDA deployed a unique malware stack that includes BRICKSTORM, a Golang-based backdoor that leverages WebSockets, DNS-over-HTTPS (DoH), and cloud services for stealthy command and control. The group also introduced two previously unknown ESXi-focused implants, Junction and GuestConduit, that enable traffic tunneling via VSOCK. Initial access was typically gained by exploiting internet-facing edge devices and vCenter vulnerabilities, followed by lateral movement using SSH and the highly privileged vpxuser account. The adversary staged and exfiltrated data from live virtual machine snapshots, cloned domain controller VMs, and abused cloud access to harvest Microsoft 365 data. Overall, the activity reflects a highly resourced espionage actor that specializes in virtualization- and cloud-centric tradecraft.

Speccom attacks

APT

Spear phishing

Backdoor

According to ESET researchers, Chinese-speaking group Speccom targeted the energy sector in Central Asia in July via a spear-phishing email with an attached document that contained a malicious macro. The spear-phishing email was sent from an apparently compromised government organization, also located in Central Asia. After compromise, Speccom operators deployed a

© 2026 AO KASPERSKY LAB

first-stage backdoor named CalaRat. They used it to deploy a variant of the BLOODALCHEMY backdoor, which has been publicly analyzed by Elastic Security and ITOCHU Cyber & Intelligence, and appears to be a tool shared among China-aligned threat actors. The group also deployed another backdoor that researchers named kidsRAT due to its use of the DWORD 0x6B696473 (the word "kids" in ASCII) in its communication protocol. They also deployed a backdoor written in Rust named RustVoralix.

Cybercriminal and others

Attacks with PhantomVAI Loader

Cybercriminal
Spear phishing
RAT
Infostealer
Steganography

Researchers at Unit 42 uncovered global phishing campaigns that deploy a loader dubbed PhantomVAI. This evolved .NET-based malware loader delivers multiple infostealers, including Katz Stealer, AsyncRAT, XWorm, FormBook, and DCRat. These attacks use multi-stage chains that begin with phishing emails containing obfuscated JavaScript or VBS files, followed by PowerShell loaders employing steganography to conceal DLL payloads within GIF images. Once executed, PhantomVAI performs VM detection, establishes persistence through scheduled tasks or Run keys, and uses process hollowing (typically into MSBuild.exe) to inject the final payloads. PhantomVAI is originally linked to the malware-as-a-service (MaaS) Katz Stealer, gathering credentials, crypto wallets, Telegram data, and system information while avoiding execution on systems in the CIS region. Threat actors deploy PhantomVAI Loader in attacks worldwide, targeting organizations in a wide range of sectors, including manufacturing, education, utilities, technology, healthcare, the information industry, and government.

Qilin attacks

Cybercriminal
Ransomware
BYOVD
Linux malware
Phishing websites
ClickFix

Trend Micro researchers identified the Agenda ransomware group, also known as Qilin, deploying a Linux-based ransomware binary on Windows hosts by abusing legitimate remote management and file transfer tools. Agenda has affected more than 700 victims in 62 countries since January 2025, primarily targeting organizations in developed markets and high-value industries. Most of the victims were in the USA, France, Canada, and the UK, with manufacturing, technology, financial services, and healthcare among the hardest hit.

Researchers assess that the threat actors likely initiated their attack campaign with a sophisticated social engineering scheme involving fake CAPTCHA pages. Analysis of the embedded obfuscated JavaScript within these fake CAPTCHA

© 2026 AO KASPERSKY LAB

pages revealed a multi-stage payload delivery system. The pages appear to have delivered information stealers to compromised endpoints, which then harvested authentication tokens, browser cookies, and stored credentials from the infected systems.

The attack chain demonstrated advanced techniques, including the use of Bring Your Own Vulnerable Driver (eskle.sys driver likely belongs to a game-related package) to evade defenses. The threat actors established a C2 infrastructure by deploying multiple SOCKS proxy instances, identified as the COROXY backdoor. The attackers abused legitimate tools, specifically installing AnyDesk through ATERA Networks' remote monitoring and management (RMM) platform and using ScreenConnect for command execution. Agenda used Splashtop Remote's management service (SRManager.exe) to execute the Linux ransomware binary directly on Windows systems, most probably to evade detection. To execute the Linux binary on Windows systems, the attackers likely enabled Windows Subsystem for Linux (WSL). The Agenda Group specifically targeted Veeam backup infrastructure to harvest credentials, recognizing that backup systems often store credentials for accessing multiple enterprise systems. Multiple PuTTY SSH clients were systematically deployed on compromised systems to facilitate lateral movement to Linux systems within the environment.

CCCS alert on internet-accessible ICS

Hacktivist

Internet-accessible ICS

The Canadian Centre for Cyber Security (CCCS) and the Royal Canadian Mounted Police issued a warning about reports of incidents involving internet-accessible industrial control systems (ICS). The alert described three recent incidents in which hacktivists tampered with critical systems. In one case, intruders altered the water pressure at a local utility, disrupting services for residents. In another case, they tampered with an automated tank gauge at an oil and gas company, setting off false alarms. A third incident involved a grain drying silo on a Canadian farm, where temperature and humidity levels were manipulated, something that could have resulted in unsafe conditions if not caught in time. The Canadian authorities believe these attacks may have been opportunistic, aimed at garnering media attention, undermining trust in the country's authorities, and harming its reputation, rather than being planned and sophisticated. In response to the elevated hacktivist activity, the Canadian authorities recommended inventorying and assessing all internet-accessible ICS devices, removing direct internet exposure where possible, using VPNs with two-factor authentication, IPS, vulnerability management, and conducting penetration testing.

© 2026 AO KASPERSKY LAB

Attacks on transportation and logistics in North America

Unknown threat actor

Cybercriminal

Cyber and traditional crime convergence

Spear phishing

Compromised legitimate mailboxes

RMM

According to researchers at Proofpoint, unnamed attackers are compromising trucking and freight companies using RMM (remote monitoring and management) tools to bid on cargo shipments before stealing them. The hackers then ship the cargo overseas or sell it online, collaborating with organized crime groups the entire time. Since at least June 2025, threat actors have employed three tactics to deliver RMM tools to these companies. They either compromise an account for a broker load board facilitating load bookings for trucking companies. The threat actors then publish a fake listing for a load and reply with phishing links to the freight carriers that respond. Once the attackers successfully phish a transportation company, they install remote access tools, bid on real loads to transport using a compromised carrier account, and subsequently intercept the cargo from those real orders. Another tactic involves injecting malicious content and URLs into existing conversations in compromised email accounts. The third tactic involves direct email campaigns against larger entities, including asset-based carriers, freight brokerage firms, and integrated supply chain providers.

The threat actors use RMM tools, including ScreenConnect, SimpleHelp, PDQ Connect, Fleetdeck, N-able, and LogMeIn Resolve. The campaigns described in the report are similar to activity that Proofpoint researchers detailed in September 2024. However, researchers cannot assess with high confidence whether the historic and current campaigns are conducted by the same or multiple groups. Although the campaigns that Proofpoint discusses in the report relate to North American cargo theft, the problem is global. According to Munich RE, global cargo theft hotspots include Brazil, Mexico, India, the USA, Germany, Chile, and South Africa, while the most targeted commodities are food and beverages.

CISA alert on Akira ransomware group

Cybercriminal

Exploitation of public-facing applications

Linux malware

LOTL

Ransomware

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), the Department of Defense Cyber Crime Center (DC3), and several international partners published a Cybersecurity Advisory highlighting known Akira ransomware IOCs and TTPs identified through FBI investigations and trusted third-party reporting as recently as November 2025. In a June 2025 incident, Akira threat actors encrypted Nutanix AHV VM disk files for the first time, expanding their capabilities beyond VMware ESXi and Hyper-V by exploiting CVE-2024-40766, a SonicWall vulnerability, for initial access. Nutanix's AHV platform is a Linux-based virtualization solution that runs and manages virtual machines on Nutanix's infrastructure. To breach corporate

© 2026 AO KASPERSKY LAB

networks, Akira affiliates also commonly use stolen or brute-forced VPN and SSH credentials on exposed routers. Then they exploit the CVE-2023-27532 or CVE-2024-40711 vulnerabilities on unpatched Veeam Backup and Replication servers to access and delete backups.

Within a network, Akira members have been observed using utilities such as nltest, AnyDesk, LogMeIn, Impacket's wmiexec.py, and VB scripts to perform reconnaissance, spread laterally to other systems, and establish persistence. The threat actors also commonly remove endpoint detection tools and create new administrative accounts for persistence. In one incident, the attackers powered down a domain controller VM, copied its VMDK files, attached them to a new VM, and extracted the NTDS.dit file and SYSTEM hive to obtain a domain administrator account. The advisory notes that the "Megazord" tool previously associated with Akira operations appears to have been abandoned in 2024.

The Akira ransomware threat actors are associated with the Storm-1567, Howling Scorpius, Punk Spider, and Gold Sahara groups, and may have connections to the now-defunct Conti ransomware group. Akira threat actors primarily target small- and medium-sized businesses, but have also impacted larger organizations across various sectors. They have a particular interest in educational institutions and organizations in critical manufacturing, information technology, healthcare and public health, financial services, and food and agriculture.

Beamglea campaign

Unknown threat actor

Cybercriminal

Phishing websites

Trusted infrastructure

Socket's Threat Research Team uncovered 175 malicious npm packages (26,000+ downloads) serving as infrastructure for a widespread phishing campaign targeting over 135 industrial, technology, and energy companies worldwide. The campaign uses npm's public registry and unpkg.com's CDN to host scripts that redirect victims to credential harvesting pages designed to look like business or Microsoft login pages. The attackers automated their workflow through Python scripts that generated randomized package names, injected victim-specific details, and published them to npm, with unpkg.com automatically serving each package as a trusted HTTPS resource. HTML lures disguised as purchase orders, project specs, and technical documents loaded these scripts directly from unpkg.com. This enabled the campaign to scale quickly without hosting costs or SSL management.

© 2026 AO KASPERSKY LAB

Attacks with NuGet packages

Malicious packages

Supply chain

DoS

Extension method hijacking

Code signing certificates

Socket's Threat Research Team discovered malicious NuGet packages downloaded in 2023 and 2024 that were designed to execute malicious code after specific dates in 2027 and 2028. They are capable of causing a DoS attack on databases and ICS systems. The set includes nine malicious NuGet packages, authored by a user named shanhai666. These include: MyDbRepository, MCDbRepository, Sharp7Extend, SqlDbRepository, SqlRepository, SqlUnicornCoreTest, SqlUnicornCore, SqlUnicorn.Core, and SqlLiteRepository. The packages were downloaded a total of 9488 times. The attacker published a total of 12 packages; the remaining three working as intended without any malicious functionality. All of them have now been removed from NuGet. The malicious packages support RDBMS that commonly uses in .NET applications (SQL Server, PostgreSQL, and SQLite), as well as industrial control systems through the Sharp7Extend package.

Sharp7Extend uses dual sabotage mechanisms: immediate random process termination and silent write failures that begin 30–90 minutes after installation. The package targets users of the legitimate Sharp7 library, a .NET implementation for interacting with Siemens S7 PLCs. The malware exploits C# extension methods to transparently inject malicious logic into every database and PLC operation. Extension methods allow developers to add new methods to existing types without modifying the original code – a powerful C# feature that the threat actor weaponizes for interception. The malicious packages add an Exec() extension method to database command types and a .BeginTran() method to S7Client objects. Each time an application executes a database query or PLC operation, these extension methods automatically execute, checking the current date against trigger dates.

In the case of Sharp7Extend, the malicious logic is activated immediately upon installation and remains active until June 6, 2028. After that date, the termination mechanism automatically stops. Eight packages target database systems and have a 20% probability of terminating the database process after the trigger date. Certain SQL Server, PostgreSQL, and SQLite implementations, bundled with other packages, are scheduled to launch on August 8, 2027 and November 29, 2028. Although the perpetrators behind the NuGet supply chain attack remain unknown, Socket Security researchers believe that source code analysis and the choice of the name "shanhai666" indicate activity associated with a Chinese-speaking user.

© 2026 AO KASPERSKY LAB

GTG-1002 attacks

AI-orchestrated attack

Anthropic researchers detailed the disruption of what they believe to be the first documented case of a cyberespionage campaign orchestrated and executed almost entirely by artificial intelligence. The operation is attributed to the allegedly Chinese-speaking group GTG-1002, which targeted approximately 30 major organizations, including technology corporations, financial institutions, chemical manufacturing companies, and government agencies in multiple countries. Experts emphasize the AI's special role in the new era of cyberwarfare, where autonomous AI agents are gradually becoming weapons in cyberspace. The report claims that the attackers used Claude Code and AI agents at all stages of the attack process, from reconnaissance to the exfiltration of sensitive data. According to the researchers, AI agents performed up to 80–90% of tactical operations autonomously, acting like a single team of professional penetration testers at superhuman speeds. Initially, the attackers used "social engineering," convincing Claude LLM that it was participating in a legitimate penetration test. The AI model demonstrated its ability to autonomously detect vulnerabilities, create payloads, and successfully deploy them in real-world operations, although some shortcomings also emerged. The AI's hallucinations became a serious obstacle for the attackers because the model periodically fabricated data and exaggerated results. To investigate the attack, Anthropic actively used its own AI models, emphasizing AI's dual role in cybersecurity.

Broadside botnet attacks

Exploitation of network devices

DDoS

Spyware

Cydome researchers reported the discovery of a new variant of the Mirai botnet named Broadside that is actively targeting the maritime logistics sector. The botnet exploits a critical command injection vulnerability (CVE-2024-3721) in TBK Vision DVR devices commonly found on vessels. The vulnerability affects TBK DVRs and rebranded models from manufacturers such as CeNova, Night Owl, and QSee. The Broadside botnet employs a custom C2 protocol over TCP port 1026, with fallback communications over TCP 6969, and with packets that are marked by a unique four-byte "Magic Header" (0x36694201). It utilizes Netlink kernel sockets and payload polymorphism to avoid detection. Broadside also contains a "Judge, Jury, and Executioner" module, a self-protection routine that dynamically kills competing malware or unwanted processes. It maintains in-memory allowlists and blocklists to ensure only Broadside-controlled operations persist. In addition to launching UDP-based distributed denial-of-service (DDoS) attacks, Broadside also steals sensitive credential files like /etc/passwd and /etc/shadow, facilitating privilege escalation and lateral movement within a compromised network. Researchers have observed the

© 2026 AO KASPERSKY LAB

botnet's fluctuating infrastructure over several months, suggesting ongoing updates. Cydome emphasizes the risk to marine vessels because DDoS attacks can flood a vessel's network and satellite communications, potentially impacting the connectivity of other, mission-critical systems.

GOLD SALEM attacks

Cybercrime

Exploitation of public-facing applications

BYOVD

DLL sideloading

Cloud services C2

Ransomware

Sophos Counter Threat Unit analyzed six months of intrusion activity attributed to the GOLD SALEM cybercrime group and assessed with high confidence that these operations were intended to deploy Warlock ransomware. The investigation of 11 incidents at organizations in the agriculture, government, energy, automotive, engineering, retail, and other sectors showed a consistent tradecraft pattern that includes exploitation of on-premises SharePoint vulnerabilities (including the ToolShell exploit chain), creation of persistent administrator accounts, credential theft via LSASS access and Mimikatz, and extensive use of legitimate tools such as Velociraptor, VS Code (tunnel mode), and Cloudflare for command-and-control and lateral movement. Defense evasion relied on BYOVD techniques using drivers from Chinese security vendors to disable AV/EDR, occasional DLL side-loading, and staged tool delivery via Cloudflare Workers domains. While Warlock was the primary payload, some intrusions also involved LockBit and Babuk variants, indicating operational flexibility rather than strict reliance on a single ransomware family. Overall, the activity reflects a financially motivated group with above-average technical capability, opportunistic victim selection, and evolving tooling, rather than clear evidence of state-directed espionage.

© 2026 AO KASPERSKY LAB

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

© 2026 AO KASPERSKY LAB