APT and financial attacks on industrial organizations in Q3 2025 | Kaspersky ICS CERT EN

By Kaspersky ICS CERT Team

Published: 2025-12-01 · Archived: 2026-04-05 15:26:25 UTC

This summary provides an overview of reports on APT and financial attacks on industrial enterprises disclosed in Q3 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

The third quarter of 2025 saw a wealth of technical details related to attacks that affected industrial organizations worldwide. This article contains more stories than last quarter’s summary and significantly more than the Q3 2024 article.

Numerous conclusions can be drawn from the reports and technical papers by various researchers on attacks on industrial organizations published this quarter. Some of these conclusions are trivial and expected; they indicate trends in the evolving threat landscape for industrial enterprises that had already been noted, or are part of broader processes affecting cybersecurity in general. Others may seem unexpected and paradoxical. Some highlight security issues that ought to be familiar by now, but have proven difficult to get accustomed to – perhaps due to a sense of fairness.

Artificial intelligence serving the attackers

As expected, artificial intelligence is useful not only to analysts, engineers, traders, journalists, business executives, government officials, and ordinary people, but also to attackers. This quarter, we learned more about how it’s being used in attacks on industrial enterprises.

- The first and most obvious use is the concept of AI itself. Attackers have long taken advantage of their potential victims' interest in new technologies by disguising their malicious code as a seemingly harmless AI tools. For example, in attacks on Middle Eastern organizations, a downloader was used to deliver the PipeMagic backdoor under the guise of the ChatGPT client.
- The second obvious use of AI is to leverage its capabilities. For instance, the operators of the GLOBAL GROUP ransomware platform built an automated ransom negotiation system with AI-powered chatbots to spare their members the trouble of learning English.
- And, of course, it's possible to combine different AI approaches, as the attackers nicknamed EvilAI did. They disguised their malware as AI-powered productivity tools and partially developed it using an LLM, making the malicious code appear more legitimate.

Exploiting generic and long-standing security issues in traditional operating systems and other IT systems

As we and others have repeatedly stated, cybersecurity experts will not achieve a definitive victory in the fight against threat actors as long as IT systems and technologies that were not developed with cybersecurity as a high priority are widely used. This includes most general-purpose operating systems, even the most modern ones. Generic security issues in these systems, including architectural ones, increase the attack surface and facilitate the development of malicious activity by complicating automatic detection and blocking.

DLL hijacking/sideloading

This is one of the most frequently exploited architectural flaws in Windows operating systems by attackers because it allows developers (including Microsoft itself) to create insecure applications. Attackers can load malicious code into these applications by replacing legitimate dynamic libraries with their own malicious ones. This approach can significantly complicate the detection and blocking of malicious activity. Security solutions cannot analyze the behavior of all running processes equally deeply for performance reasons, so they are forced to reduce the depth of analysis for many operating system key processes and trusted applications.

- DLL sideloading was used in attacks on telecommunications and manufacturing organizations in Central and South Asia using the PlugX malware, and in Charon ransomware attacks on Middle Eastern organizations for the shellcode deployment.
- The MiniBike malware components used in attacks on European telecommunications, aerospace, and defense companies are compiled specifically for the victim and executed via DLL sideloading. Attackers utilize a specific method of modifying the export tables of legitimate DLLs to seamlessly integrate the malicious code.
- Researchers also described a couple of other interesting DLL hijacking techniques. The first was demonstrated by the aforementioned attackers who targeted organizations using PipeMagic. In one of its loader variants, the dynamic link library for a Google Chrome update executable contained malicious code in the DllMain function. The second technique was employed by the Nimbus Manticore group in attacks on defense, telecommunications, and aviation companies in Western Europe using the MiniJunk backdoor. During the backdoor's execution, DLL sideloading is used twice. The first time is rather unusual: the DllPath parameter of the RTL_USER_PROCESS_PARAMETERS structure used in undocumented low-

level NT API is manipulated. This parameter determines the search path for the DLL if it is not found in the application directory. Thus, the malware was loaded from the directory to which it was copied from an archive into the memory of a Windows Defender process running from a different directory entirely.

BYOVD (Bring Your Own Vulnerable Driver)

In addition to loading malicious code from the context of trusted applications, which makes it more difficult to detect and block, attackers can perform malicious actions using legitimate code at the OS kernel level by installing new or using existing legitimate vulnerable drivers. These drivers enable attackers to sometimes completely disable or render security solutions ineffective (e.g., by disabling their ability to intercept system operations, such as process launches, file openings, etc.). The OS itself is the only reliable protection against all such scenarios. However, modern general-purpose operating systems (such as Windows and Linux) do not offer this level of protection, meaning security solution developers must devise their own strategies to minimize this risk.

- This quarter, researchers published two stories about attacks on industrial organizations in which the attackers used these tactics. Notably, both stories describe ransomware operations (Crypto24 and The Gentlemen) rather than APTs, further demonstrating that some ransomware actors have become “advanced” in many ways.

Zero-day vulnerabilities

Although extending the OS kernel functionality by installing an additional driver is a convenient architectural approach for third-party developers of hardware components, peripherals and performance-intensive applications, it’s a cybersecurity nightmare, as discussed above. **Unfortunately, vulnerabilities exist not only in drivers from third-party vendors but also in drivers developed and maintained by general-purpose OS developers.** These vulnerabilities are also exploited in attacks, including those against industrial organizations.

- This quarter, our colleagues at Kaspersky reported one such case. CVE-2025-29824 is a privilege escalation vulnerability in the Common Log File System (CLFS) driver that allows read and write access to kernel memory. Surprisingly, this is the 33rd vulnerability discovered in this particular driver, and the fourth to be exploited by attackers. Researchers have suggested that the security issues in the driver likely stem from two sources. The first is related to the architecture of the storage system for the logs it processes, specifically their format. They explicitly store kernel data structures, including pointers to kernel memory. The second originates in the architecture of the driver itself: to protect the OS from “screens of death” when the driver crashes, the developers layered its code with exception handlers. This masks errors in the code, making them difficult to detect via fuzzing techniques. It is also noteworthy that this zero-day vulnerability was first discovered in attacks by a ransomware group, not an APT.

Zero-day vulnerabilities in popular applications may not be as dangerous as vulnerabilities in OS kernel code, but they can still provide attackers with significant advantages at various stages of an attack, especially during the initial access and persistence phases.

- This quarter, researchers reported two cases of attacks on industrial organizations exploiting the zero-day vulnerability CVE-2025-8088 in WinRAR, which allowed attackers to trick victims and bypass security

solutions. Interestingly, the RomCom cybercriminal group used the exploit for this vulnerability in attacks by before it was used in the Paper Werewolf/GOFFEE APT operations.

Incomplete patches and 'Won't Fix'

Another of the most serious problems with the current widespread approach to securing IT and OT systems, including their key components such as the OS, is that vendors tend to give this task a relatively low priority. As a result, we often see carelessness when developing and releasing security patches, or even a complete reluctance to release them. This quarter, security researchers publicly shared two stories that confirm this.

- The first concerns a chain of ToolShell vulnerabilities used in attacks on SharePoint servers running on organizational networks in many countries, including those of industrial enterprises. The patches initially released by Microsoft (CVE-2025-49704 and CVE-2025-49706) proved insufficient. According to the researchers, changing just one byte in the exploit code was enough to bypass the patches. Microsoft was forced to release new patches (CVE-2025-53770 and CVE-2025-53771) to address the vulnerabilities.
- The second describes attacks by access brokers on ASP.NET applications, including those on publicly accessible resources of industrial enterprises. The attackers stole "machine keys" and used them to inject malicious modules into the memory of Internet Information Services (IIS), a web server developed by Microsoft. This technique, known since 2014 as "Viewstate Deserialization," was exploited in attacks on various ASP.NET services that use this serialization technology. Microsoft has labeled this security issues as a "Won't Fix".

UAC bypass

Another systemic security problem in modern IT and OT environments is that developers of key components, such as the OS, do not always ensure the effectiveness of their security enhancements. The developers' creation and implementation of other functional system components and their new features can often allow attackers to bypass previously implemented security measures. This is the case, for example, with the User Account Control (UAC) mechanism, which requires additional confirmation from the user when a process attempts to perform a privileged action. Since some system processes are among those requiring privileged access, this mechanism has numerous exceptions, allowing attackers to bypass it. There are currently several dozen known UAC bypass techniques, many of which are frequently used in attacks, including against industrial enterprises.

- One such case is described in the aforementioned Crypto24 ransomware campaign, in which the attackers bypassed UAC using one of the most common methods: exploiting the CMSTPLUA COM interface.

Exploiting trust

It's common knowledge that, in addition to the technical issues described above, attackers routinely exploit their potential victims' organizational weaknesses, employing psychological tactics to develop social engineering methods that exploit trust. However, trusting relationships between people and organizations often have a technical aspect beyond psychological and communicative ones. This can include additional communication channels that bypass the security perimeter or are less secure, or a lack of technical capability on one side to fully verify the information security status of technological components and digital artifacts provided by the other party.

- One of the most interesting technical stories published this quarter described attacks by Chinese-speaking APT groups targeting organizations in the telecommunications, government, transportation, military, and housing sectors in various countries. The attackers primarily targeted the network cores of major telecommunications providers, as well as the edge routers of providers and their client organizations. They then used compromised devices and trusted relationships to compromise the networks of new victims.

Legitimate (including stolen) digital signature certificates

The most common method of automating trust relationships in IT and OT is based on cryptographic signature mechanisms. For example, a mail server signs outgoing email messages with a DKIM key enabling the receiving server to verify the email's origin, even if it passes through multiple relays. The sender signs the email using SMIME or PGP so that the recipient can identify the sender and verify that the email's contents were not altered during delivery. The operating system verifies the digital signature of an executable file before launching it to ensure it was created by a legitimate developer and has not been modified. A specialized security solution also verifies this digital signature to determine the level of analysis required for the application's behavior, as discussed above in the section on DLL hijacking. Unfortunately, attackers who obtain a valid private signature key can use it to bypass trust mechanisms. They can do this by stealing the key from the legitimate owner or by deceiving the certification authority. For example, they can create a fake organization or temporarily seize the domain zone of a legitimate organization. Two such cases were included in stories published this quarter about attacks on industrial organizations.

- Subtle Snail has been using digital signatures for its malware in attacks on European telecommunications, aerospace, and defense companies since at least May 2025. All malicious binaries used in the group's attacks are signed with a valid digital certificate issued by SSL.com to Dutch company Insight Digital B.V.
- GhostRedirector, which compromised at least 65 Windows servers belonging to educational, healthcare, insurance, transportation, retail, and IT organizations in several countries, signed some of its malware with a certificate issued by TrustAsia RSA Code Signing CA G3 to the developer Shenzhen Diyuan Technology Co., Ltd.

In both cases, it is unclear from the published articles how the attackers obtained the certificates.

Exploiting compromised email accounts

The final method of exploiting trust relationships highlighted in this quarter's technical articles on attacks on industrial organizations involves exploiting the trust between people. This reduces the likelihood that malicious activity will be detected by automated security tools. When you receive an email from a known ("trusted") counterparty, especially if it's part of an ongoing conversation, you're likely to open the attachment, click the link, or perform some other reckless action prompted by the email's content – after all, the corporate spam and phishing filter has automatically checked it and didn't flag it as suspicious. Therefore, many attackers are keen to gain access to legitimate email accounts, which they then use in subsequent attacks. In one of our articles, we uncovered an entire ecosystem of attackers operating primarily using this method.

- In the aforementioned malicious campaign, Paper Werewolf/GOFFEE posed as a major research institute and sent emails to Russian and Uzbek organizations. They used a compromised email address belonging to

a furniture supplier.

- In a large-scale cyberespionage campaign against Russian organizations, including industrial enterprises, the Head Mare/PhantomCore APT group gained initial access to victim networks through phishing emails. The attackers used compromised email accounts belonging to legitimate Russian companies.
- The Tomiris APT group specifically sent phishing emails to Russian government agencies, as well as energy, mining, and manufacturing companies. The senders purported to be Kyrgyz government officials. One of the emails used an address that was listed on the website of the Kyrgyz Republic's regulator. This address had apparently been compromised for use in previous attacks.
- ComicForm specifically targets Russian companies in the industrial, financial, tourism, biotechnology, research, and trade sectors, as well as organizations in Belarus and Kazakhstan. The attackers send phishing emails and distribute malware from email addresses registered in the .ru, .by, and .kz top-level domains. Some of these addresses were presumably compromised.
- The UNK_FistBump group sent phishing emails to recruiters and HR staff at organizations involved in the design, production, and supply of semiconductor products. The emails were sent from compromised National Taiwan University email accounts, with the senders posing as university graduates seeking employment.

Indifference and carelessness

Finally, and perhaps the most glaring problem of all, is the lack of attention to industrial enterprise information security by responsible employees. This quarter, researchers published two papers that highlight the issue's relevance.

- Cisco Talos, in collaboration with the Federal Bureau of Investigation, issued a warning about an APT group exploiting the seven-year-old CVE-2018-0171 vulnerability against border routers of organizations in the critical infrastructure sector.
- Palo Alto Networks researchers reported attacks exploiting the critical (CVSS 10.0) CVE-2025-32433 vulnerability in the SSH server implementation of the Open Telecom Platform. This vulnerability was discovered and patched in April 2025. It is worth noting that approximately 70% of more than 3000 exploitation attempts occurred on specialized industrial firewalls accessible from the internet. These firewalls are designed to separate communications between IT and technological networks and are most likely not equipped to counter the wide variety of threats that can reach them from the internet.

Russian-speaking activity

RomCom attacks

Cybercriminal | Spear phishing | Zero-day vulnerability | Backdoor

ESET researchers discovered an unknown vulnerability in WinRAR that is currently being exploited in the wild by the RomCom (also known as Storm-0978, Tropical Scorpius, or UNC2596) threat actor. This is at least the third time RomCom has been caught exploiting a significant zero-day vulnerability in the wild. The path traversal vulnerability, assigned CVE-2025-8088, is made possible by the use of alternate data streams. After immediate notification, WinRAR released a patched version on July 30, 2025. The vulnerability enables attackers to hide

malicious files in an archive, which are silently deployed during extraction. Successful exploitation attempts delivered various backdoors used by the RomCom group, specifically a SnipBot variant, RustyClaw, and the Mythic agent. The campaign targeted financial, manufacturing, defense, and logistics companies in Europe and Canada.

Static Tundra attacks

APT | Exploitation of network devices | Firmware implant

Both Cisco Talos and the Federal Bureau of Investigation (FBI) warned that a state-sponsored cyber-espionage group was exploiting a seven-year-old vulnerability in the Smart Install feature of Cisco IOS software. CVE-2018-0171 is an improper input validation issue in the discontinued Smart Install feature of Cisco IOS and Cisco IOS XE software. Cisco Talos named the group Static Tundra. It is likely a sub-cluster of the Energetic Bear APT group (also known as Crouching Yeti, Berserk Bear, and Dragonfly), based on an overlap in tactics, techniques and procedures (TTPs), as well as victimology. The attackers target end-of-life devices that have not been patched in the telecommunications, higher education, and manufacturing sectors around the world. Users unable to apply the patch have been urged to disable Smart Install. According to Cisco Talos, the attackers' goal is to steal configuration data and gain persistent access to vulnerable systems. Static Tundra employs sophisticated persistence techniques, including the historic SYNful Knock firmware implant (first reported in 2015), as well as bespoke SNMP tooling, to maintain undetected access for years.

Curly COMrades attacks

New threat actor | Backdoor | Compromised websites

Bitdefender researchers detailed a cluster of malicious activity that they've been tracking since mid-2024, which revealed a new threat actor group named Curly COMrades. The group has targeted critical organizations in post-Soviet countries, launching focused attacks against judicial and government bodies in Georgia and an energy distribution company in Moldova. The group's primary objective is to gain long-term access to target networks and steal valid credentials. Curly COMrades uses proxy tools such as Resocks, SSH, and Stunnel to establish multiple entry points into internal networks. The group frequently executes remote commands through these established proxy relays, often using tools like Atexec. As the last stage tool, the attackers deployed a new backdoor dubbed MucorAgent. To maintain persistent access, they involve using a sophisticated technique that hijacks of Windows Tasks responsible for periodical or occasional (such as on .NET Framework updates) running of NGEN (Native Image Generator) – a performance optimizer precompiling .NET intermediate code into native machine code. They also strategically use compromised but legitimate websites as traffic relays. Curly COMrades repeatedly attempted to extract the NTDS database from domain controllers. The database is the primary repository for user password hashes and authentication data in a Windows network. Additionally, they attempted to dump LSASS memory from specific systems to recover active user credentials.

Targets in Russia

UNG0901 attacks/Operation CargoTalon

Unknown threat actor | Spear phishing | Backdoor

Seqrite Labs researchers uncovered a cyber-espionage campaign called Operation CargoTalon that targeted Russian companies using the EAGLET backdoor. The malicious activity was attributed to a threat cluster tracked as UNG0901 (Unknown Group 901). The targets were employees of an aircraft production association, as suggested by a malicious email file uploaded to VirusTotal. The attacks involved phishing emails with bait related to cargo delivery, titled “Транспортная_накладная_ТТН_№391-44_от_26.06.2025.zip” (Transport_Consignment_Note_TTN_No.391-44_from_26.06.2025.zip). The ZIP archive contains an LNK file that uses PowerShell to display a decoy XLS document and execute the EAGLET DLL file via rundll32.exe. EAGLET collects system information, establishes connections to a hardcoded remote server, and executes commands on the compromised Windows machine. The implant supports shell access and file upload/download capabilities. However, the exact nature of the next-stage payloads being delivered is unknown because the C2 server was offline at the time of the study.

Seqrite researchers discovered a similar campaign targeting the Russian military-industrial complex with the decoy “Договор_РН83_изменения.zip” (Contract_RN83_Changes.zip) using EAGLET. Unlike previous campaigns, in the second similar campaign, the EAGLET implant didn’t contain a decoy file in its overlay section. The researchers observed multiple overlaps between these campaigns, including similar target interests and implant code, and the threat entity known as Head Mare, which has been targeting Russian-speaking entities, and was initially discovered by researchers at Kaspersky. In particular, the researchers noted functional parallels between EAGLET and PhantomDL, a Go-based backdoor with a shell and file upload/download capabilities, as well as similarities in the naming algorithm applied to attachments in phishing emails.

Attacks with Batavia stealer

New threat actor | Spear phishing | Spyware

Kaspersky researchers reported on new, previously unknown spyware dubbed Batavia that is involved in attacks on Russian industrial enterprises. Batavia consists of the following malicious components: a VBS script and two executable files. The targeted attacks began in July 2024 with the sending of emails containing malicious links under the pretext of signing a contract. After clicking on the link, an archive containing a VBS script is downloaded. The script is encrypted with a proprietary Microsoft algorithm. The observed script names were “договор-2025-5.vbe” (contract-2025-5.vbe), “приложение.vbe” (application.vbe), and “dogovor.vbe”. The script initiates a three-stage infection of the machine that involves two more executable files. The first executable file, written in Delphi, collects files of several categories, including various system logs and office documents on computers and removable media. In addition, it periodically takes screenshots and sends them to the C2. The second executable file, written in C++, has similar spyware functionality, but with additional file extensions added to the list of collected files. The second malicious file also contained two commands: one to change the C2 server and another to download and run additional files.

Paper Werewolf/GOFFEE attacks

APT | Spear phishing | Zero-day vulnerability

According to the BI.ZONE team, the Paper Werewolf/GOFFEE threat actor attacked Russian and Uzbek organizations in July and early August. One of the targets was a Russian manufacturer of specialized equipment.

The attackers sent an email that appeared to be from a large research institute, but was actually from a compromised email address belonging to a furniture manufacturer. The RAR archive attached to the email contained decoy documents purporting to be from a ministry and a modified XPS Viewer executable with embedded malicious shellcode (a reverse shell) that connects to the C2 server. This provided the attackers with remote access to the cmd.exe shell on the victim's computer. In this attack, the attackers exploited the known vulnerability CVE-2025-6218 in WinRAR. Subsequent attacks targeting companies in Russia and Uzbekistan exploited a new zero-day vulnerability, CVE-2025-8088, that hadn't yet been described and affected WinRAR versions up to and including 7.12. This vulnerability was also used by the RomCom threat actor. ESET researchers noted that Paper Werewolf began exploiting CVE-2025-8088 a few days after RomCom started doing so. The phishing emails targeting Russian organizations included an archive disguised as a document from the Ministry of Industry and Trade. The phishing emails targeting Uzbek organizations included an archive named "DON_AVIA_TRANS_RU.rar" that impersonated a travel agency. The attachments contained a malicious file that exploited a directory traversal vulnerability to write files outside the target directory. Notably, shortly before these attacks occurred, an apparently functioning WinRAR exploit, presumably for this vulnerability, appeared on a darknet forum. The dropped malicious files were .NET applications written in C# that downloaded a .NET assembly payload from a server and ran it in memory.

PhantomCore attacks

APT & Cybercriminal | Spear phishing | Compromised legitimate mailboxes | Phishing websites | ClickFix | Polyglot files | Backdoor

Positive Technologies researchers published a report on the PhantomCore APT (also known as Head Mare). Over the past year and a half, the group has significantly expanded its offensive arsenal and carried out cyberattacks on Russia's critical infrastructure. In early May, researchers detected a new large-scale cyber-espionage campaign targeting Russia. According to PT researchers, at the time of publication, the PhantomCore group had gained access to 181 infected hosts as part of its campaign. The first infection occurred on May 12, 2025. The cyberattack peaked in late June, when 56% of all infections occurred on June 30. The group's average stay in a compromised network is 24 days, with a maximum of 78 days. As of publication, 49 hosts remained under the group's control. The group initially gains access by delivering backdoors in phishing emails in the form of polyglot files, using hacked email addresses of legitimate Russian companies, among other things. The group uses the following tools: PhantomRAT, PhantomRShell C++ backdoor, PhantomTaskShell PowerShell backdoor, PhantomStealer written in Go, PhantomProxyLite SSH-tunnel, XenArmor All-In-One Password Recovery Pro, the RClone and RSocx open-source utilities, and MeshAgent. Researchers discovered that the group registered its phishing website in April, just before the cyber-espionage campaign was discovered, using the real identity of a Russian citizen. It uses the original HTML layout of the official Moscow City Compulsory Medical Insurance Fund website and entices visitors to paste and run the contents of the clipboard in the Windows command prompt under the pretext of completing a fake CAPTCHA, implying a ClickFix technique. Furthermore, researchers discovered a branch of the group that is separate from the main group and composed of low-skilled specialists. It operates another reverse shell with some similarities to PhatomRAT and PhantomRShell. It is written in Go and was called PhantomGoShell by the researchers. The identified group was probably organized as a cybercriminal startup by a core member of PhantomCore who had access to the source code of custom tools and recruited Russian-speaking amateur hackers from gaming Discord communities.

Cavalry Werewolf attacks

APT | Spear phishing | RAT | Telegram C2 | Compromised legitimate mailbox

From May to August 2025, BI.ZONE Threat Intelligence recorded activity from the Cavalry Werewolf threat actor (also known as YoroTrooper, SturgeonPhisher, Silent Lynx, Comrade Saiga, Tomiris, and ShadowSilk). The group conducted targeted phishing campaigns against Russian state agencies and enterprises in the energy, mining, and manufacturing sectors, using spoofed email addresses of Kyrgyz state agency employees. In one phishing email, the attackers used a real email address found on the website of a Kyrgyz regulatory agency. It appears the attackers had previously compromised this address for use in attacks.

The phishing emails contain RAR files with FoalShell or StallionRAT malware, both of which are controlled via Telegram. FoalShell, written in Go, C++, and C#, is a simple reverse shell used by Cavalry Werewolf to execute arbitrary commands in the cmd.exe command-line interpreter on a compromised host. StallionRAT is a remote access Trojan written in various variants in Go, PowerShell, and Python. It allows attackers to execute commands, download files, and exfiltrate data.

The group's attacks were not limited to Russia and other CIS countries; they also targeted countries in the Middle East, as evidenced by the presence of files named in Arabic. The investigation revealed more information related to Cavalry Werewolf's preparations for attacks and testing of malicious programs. This includes potential targeting of Tajikistan and the use of other tools such as AsyncRAT.

Hive0117 attacks

Cybercriminal | Spear phishing | Backdoor

Researchers at F6 detected a new wave of malicious emails from Hive0117, a financially motivated group that has been conducting attacks using the DarkWatchman RAT since February 2022. The emails were distributed on a massive scale. The attackers masquerade as legitimate organizations by registering infrastructure for email campaigns and control domains, often reusing domains. On September 24, after several months of silence, F6 detected new activity from the DarkWatchman RAT Trojan. Previously, it was distributed under the guise of an archive supposedly from the Ministry of Defense and fake subpoenas. This time, the attackers impersonated the Federal Bailiff Service to target companies using emails. Similar email campaigns were also detected in June and July. Instead of legitimately looking domain names these mailings used the domains 4ad74aab[.]cfd and 4ad74aab[.]xyz. A recipient analysis showed that the HIVE0117 group targeted companies in Russia and Kazakhstan. The list of 51 recipients includes banks, marketplaces, telecom operators, logistics companies, auto dealerships, manufacturing companies, construction companies, grocery retailers, lottery operators, insurers, investment companies, fuel and energy companies, pharmaceutical companies, research institutes, technology parks, waste management operators, travel services, fitness centers, and IT companies.

ComicForm attacks

Spear phishing | Spyware

F6 researchers released a report analyzing phishing attacks by the new ComicForm group. The group targeted Russian companies in the industrial, financial, tourism, biotechnology, research, and trade sectors, as well as companies in Belarus and Kazakhstan. The ComicForm group has been active since at least April 2025. The attackers use phishing emails to distribute FormBook, a data-stealing malware. F6 observed a phishing campaign targeting Russian organizations that took place between May and June 2025. The emails contained the following subject lines: “Re: proforma invoice”, “Re: Bank Reconciliation report”, “Re: invoice and shipping documents”, “INvoice for Payment”, and others. The attached file contained a hidden downloader that delivered the stealer to the victim’s computer. A distinctive feature of the phishing emails was hidden links to animated GIF images of superheroes in the attachment code that were not used in the attack. For this reason, F6 assigned the name ComicForm to the attackers. ComicForm uses email addresses registered on the top-level domains .ru, .by, and .kz for their phishing emails; some senders may have been compromised. Another distinctive feature of the group was the use of the “rivet_kz@” email address, which was registered with a publicly accessible Russian email service and used as a reply-to address. In addition to malicious attachments, the attackers also used phishing pages of document storage services. After clicking the link in the email, victims were redirected to phishing login forms. Their data was then transferred to the attackers’ remote servers.

Clusters of cyberthreats targeting Russia and Belarus

Cybercriminal | Hacktivist | APT

The study by Kaspersky examined the cyberthreat posed by pro-Ukrainian groups and focuses on their activities targeting the Russian Federation and Belarus. To provide a comprehensive understanding of these threats, Kaspersky researchers have compiled a study that clusters pro-Ukrainian groups, describes their tactics, techniques, and procedures (TTPs), and investigates their motivations and interconnections. The study describes three clusters. Cluster One consists of hacktivist and financially motivated groups using similar TTPs. It includes thefollowing groups: Twelve, BlackJack, Crypt Ghouls, Head Mare, and C.A.S. Cluster II included pro-Ukrainian APT groups whose TTPs differ from those of hacktivists: Awaken Likho,Angry Likho, Mythic Likho, Librarian Likho, Cloud Atlas, GOFFEE, and XDSpy. Cluster III included hacktivist groups that showed no signs of active collaboration with the other groupsdescribed above: Bo Team and Cyberpartisans.

South Asia

APT36/Transparent Tribe attacks

APT | Linux malware | Phishing websites | Backdoor

Hunt.io researchers investigated recent campaigns conducted by the APT36 threat actor (also known as Transparent Tribe). What began as military-focused campaigns expanded to encompass broader targets, including Indian railway systems, oil and gas infrastructure, and the Ministry of External Affairs. These campaigns use advanced phishing techniques, novel payload strategies, and persistent backdoors. When targeting Linux systems, the attackers use .desktop files disguised as PDF documents to execute scripts that download malware and establish persistence via cron jobs. Two attack variants were identified. One variant uses a single C2 server, while the other variant includes redundant servers for resiliency. The Poseidon backdoor, which is built on the Mythic framework and written in Go, is used to maintain access and support lateral movement. More than 100 phishing

domains were discovered, many of which impersonated Indian government organizations and were hosted by AlexHost. The first phishing domains in this campaign were registered in early July 2025, with live infrastructure observed as of mid-July. This suggests ongoing and active targeting.

UNC1549 attacks

APT | Spear phishing | Backdoor | C2 proxied via Azure | DLL sideloading | Code signing certificates

Prodaft researchers have been tracking cyberattacks by the Subtle Snail threat actor (also known as UNC1549, Smoke Sandstorm, TA455, or Imperial Kitten), which is part of the Eclipsed Wasp (Charming Kitten) network. Active since at least June 2022, the group has recently shifted its focus to European telecommunications, aerospace, and defense organizations. In their latest campaign, Subtle Snail infected 34 distinct devices belonging to 11 organizations through targeted operations leveraging fake recruitment processes on LinkedIn. The group poses as HR representatives from legitimate entities to engage employees and compromises them by deploying a Minibike backdoor variant that communicates with C2 infrastructure proxied through Azure cloud services to bypass detection.

MiniBike's primary purpose is to load additional components in the form of DLLs. The threat actor deployed additional DLL modules: a keylogger, a browser stealer, and an Outlook/Winlogon credential stealer. Since at least May 2025, Subtle Snail has been digitally signing their malware. According to Prodaft, all malicious binaries used in Subtle Snail attacks are signed with a valid digital certificate issued by by SSL.com to the Dutch company Insight Digital B.V. Malicious DLLs developed by the threat actor – each implementing a dedicated malicious function and tailored to specific victims – are being run via DLL sideloading. To facilitate seamless execution, the actor modifies legitimate DLLs manipulating their export tables, thus the resultant files appear as legitimate though carrying out malicious activities. The group creates email accounts to support their phishing operations. To manage their Azure proxy servers and support their phishing campaigns, the threat actor also creates cloud accounts using these email accounts. They purchase these accounts in line with the domains they will use for their phishing attacks. Depending on their target, they create a fake PDF job ad that is made to look like it came from Telespazio. To increase their success rate, they purchase deceptive domains like telespazio-careers.com. Similarly, they purchased the safrangroup-careers.com domain to impersonate Safran Group, the French multinational aerospace, defense and security corporation. The attackers consistently choose domains that follow the same *-careers.com or *careers.com patterns.

Researchers at Check Point also tracked a long-running campaign by the Nimbus Manticore actor that overlaps with UNC1549, Smoke Sandstorm, and the "Iranian Dream Job" operations. According to the researchers, the ongoing campaign targets defense manufacturing, telecommunications, and aviation. Recent activity by Nimbus Manticore indicates a heightened focus on Western Europe, specifically Denmark, Sweden, and Portugal. The threat actor impersonates local and global organizations in the aerospace, defense manufacturing, and telecommunications industries. The threat actor uses tailored spear-phishing from alleged HR recruiters to direct victims to fake career portals. The campaign relies on a highly obfuscated backdoor called MiniJunk and a lightweight stealer with separate versions for stealing credentials from Chrome and Edge browsers called MiniBrowse. Check Point's analysis of MiniJunk showed that it was a much-improved version of Minibike. The malware's new capabilities include method of loading malicious DLLs into a Windows Defender and other vulnerable binaries by Microsoft via manipulating DllPath parameter of the

RTL_USER_PROCESS_PARAMETERS structure used in the undocumented low-level NT API. The parameter defines the search path for the dll if it's not found in the process directory. Nimbus Manticore actors have been digitally signing their malware using certificates from the SSL.com service since at least May 2025. Based on the signing dates and an analysis of samples signed by this certificate, the researchers determined that they were generated by the threat actor, masquerading as legitimate IT organizations in Europe.

Chinese-speaking activity

Attacks against the Taiwanese semiconductor industry

APT | Spear phishing | AitM | Backdoor | Compromised legitimate mailboxes

From March to June 2025, Proofpoint researchers observed three Chinese-speaking threat actors conducting targeted phishing campaigns against Taiwan's semiconductor industry. In all cases, the motive was most likely espionage. The targets of these campaigns ranged from organizations involved in the manufacturing, design, and testing of semiconductors and integrated circuits to entities within the wider equipment and services supply chain of this sector, as well as financial investment analysts who specialize in the Taiwanese semiconductor market. The UNK_FistBump threat actor launched employment-themed phishing campaigns targeting semiconductor design, manufacturing, and supply chain organizations, resulting in the delivery of Cobalt Strike or the custom Voldemort backdoor. Posing as a graduate student seeking employment, the actor used compromised Taiwanese university email addresses to send phishing emails to recruitment and HR personnel. The UNK_DropPitch threat actor conducted targeted phishing campaigns against multiple large investment banks. This activity focused specifically on individuals specializing in financial investment analysis of the Taiwanese semiconductor and technology sectors. The phishing emails were sent from attacker-owned email addresses purporting to be from a fictitious financial investment firm seeking to collaborate with the individuals. The campaign delivered a custom backdoor. Using a custom adversary-in-the-middle (AitM) phishing kit, UNK_SparkyCarp conducted a credential phishing campaign targeting a Taiwanese semiconductor industry company that the group had previously targeted in November 2024. The phishing emails masqueraded as account login security warnings and contained a link to the actor-controlled credential phishing domain.

UNC3886 attacks

APT | Zero-day vulnerabilities | Linux malware | LOTL | Backdoor

On July 18, Singapore's Coordinating Minister for National Security revealed that the country was under attack by a highly sophisticated threat actor targeting critical infrastructure – UNC3886. First reported in 2022, this threat group has been targeting essential services in Singapore, posing a severe risk to the country's national security. Trend Micro researchers provided analysis of previously recorded UNC3886 attacks. The group's known targets also include entities in the US and Europe. It has historically targeted critical infrastructure, including telecommunications, government, technology, and defense. The group is known for rapidly exploiting zero-day and high-impact vulnerabilities in network and virtualization devices, such as VMware vCenter/ESXi, Fortinet FortiOS, and Juniper Junos OS. UNC3886 deploys custom toolsets, including TinyShell, a covert remote access tool, Reptile, a stealthy Linux rootkit, as well as Medusa, leveraging layered persistence and advanced defense

evasion methods, such as rootkit deployment, living-off-the-land tactics, and replacement or backdooring of core system binaries.

Salt Typhoon joint advisory

APT | Exploitation of network devices and public-facing applications | Trusted relationship

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA) and other US and foreign organizations from 13 countries have published a joint Cybersecurity Advisory. It provides technical details about Chinese-speaking APT actors. The advisory is published jointly by agencies from the US, Australia, Canada, New Zealand, the UK, Czechia, Finland, Germany, Italy, Japan, the Netherlands, Poland, and Spain. The malicious activity outlined in the advisory partially overlaps with cybersecurity industry reporting on threat actors referred to by names such as Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor, among others. This cluster of cyberthreat activity has been observed in the United States, Australia, Canada, New Zealand, the United Kingdom, and other regions worldwide. These activities have been linked by the advisory authors to multiple China-based entities, that are said to be providing cyber products and services to China's authorities. The advisory notes that the threat actors are targeting networks worldwide, including, but not limited to, those in the telecommunications, government, transportation, lodging, and military infrastructure networks. While these actors focus on large backbone routers of major telecommunications providers, as well as provider edge (PE) and customer edge (CE) routers, they also leverage compromised devices and trusted connections to pivot to other networks. These actors often modify routers to maintain persistent, long-term access to networks. The document provides technical details about the group's initial access, persistence, lateral movement, lateral data collection, and exfiltration. It also includes a case study, threat hunting guidance, indicators of compromise, suggested mitigations, and other resources.

GhostRedirector attacks

New threat actor | Exploitation of public-facing application | Backdoor | Code signing certificates

ESET researchers identified a previously unknown Chinese-speaking threat actor dubbed GhostRedirector. This actor compromised at least 65 Windows servers across multiple regions, including Brazil, Thailand, and Vietnam. GhostRedirector doesn't appear to be interested in a specific industry or sector. Researchers have seen victims in sectors such as education, healthcare, insurance, transportation, technology, and retail. The attackers exploited public-facing applications, likely through SQL injection, to gain initial access. They then deployed a variety of malicious tools, including a passive C++ backdoor called Rungan for remote command execution, and Gamshen, a malicious Internet Information Services (IIS) module designed to manipulate Google search results for SEO fraud benefiting gambling websites. The toolkit also included custom privilege escalation utilities based on BadPotato and EfsPotato, a multi-purpose DLL called Comdai, and a tool called Zunput that dropped multiple web shells. GhostRedirector abused code-signing certificates, created rogue administrator accounts, and used tools like GoToHTTP to maintain persistent access.

RedNovember/TAG-100 attacks

APT | Exploitation of network devices and public-facing applications | Backdoor

Insikt Group reported on the activity of the TAG-100 group, tracked under the name RedNovember. Between June 2024 and July 2025, RedNovember targeted the perimeter appliances of high-profile organizations around the world. The group used the Go-based Pantegana backdoor and Cobalt Strike to carry out these intrusions. The group expanded its targeting to include government and private sector organizations, such as defense and aerospace companies, space agencies, and law firms. RedNovember has been observed performing reconnaissance and compromising edge devices, including SonicWall, Cisco ASA, F5 BIG-IP, Fortinet FortiGate instances, as well as Outlook Web Access and Ivanti Connect Secure VPN appliances. The group's activity demonstrates the ability to combine weaponized proof-of-concept exploits with open-source post-exploitation frameworks, lowering the entry barrier for less-capable threat actors. Insikt Group identified several new likely victims, including a Central Asian ministry of foreign affairs, an African state security organization, a European government directorate, and a Southeast Asian government. RedNovember also targeted at least two US defense contractors, two US oil and gas companies, a European engine manufacturer, and a trade-focused intergovernmental organization in Southeast Asia. RedNovember's targeting efforts have also been observed in close proximity to geopolitical and military events that are of key strategic interest to China.

Naikon attacks

APT | Backdoor | DLL sideloading

Cisco Talos discovered a campaign active since 2022 that targets the telecommunications and manufacturing sectors in Central and South Asia. The campaign delivers a new variant of the PlugX malware. This new variant exhibits similarities to the RainyDay and Turian backdoors, such as the use of the same legitimate applications for DLL sideloading and the XOR-RC4-RtlDecompressBuffer algorithm to encrypt and decrypt payloads. The new variant's configuration differs from the standard PlugX configuration format, but resembles the structure used by RainyDay, leading Talos to assess with medium confidence that this campaign can be attributed to Naikon, a Chinese-speaking threat actor. Analysis of the victimology and technical malware implementation suggests a potential connection between Naikon and the BackdoorDiplomacy threat actor. This raises the possibility that they are the same group or are sourcing their tools from the same vendor.

Cybercriminal and others

Scattered Spider/UNC3944 attacks

Cybercriminal | Phone calls | Ransomware

Google Threat Intelligence Group (GTIG) reported on a sophisticated campaign conducted by the financially motivated threat group UNC3944 (also known as 0ktapus, Octo Tempest, and Scattered Spider) that targeted multiple sectors, including the retail, aviation and insurance industries. The group was suspected of turning its ransomware and extortion operations to the US retail sector, according to GTIG. The campaign soon expanded to include airline and transportation organizations in North America. The group's core tactics have remained consistent, and do not rely on software exploits. Instead, they use a proven playbook that centers on phone calls to an IT help desk by someone impersonating a regular employee. After compromising one or more user accounts using social engineering, they manipulate trusted administrative systems and use their control of Active Directory

as a launchpad to pivot to the VMware vSphere environment. This provides an avenue to exfiltrate data and deploy ransomware directly from the hypervisor.

The GTIG publication was followed by a Palo Alto Networks report and a Cybersecurity and Infrastructure Security Agency (CISA) advisory on the Scattered Spider actor, describing its TTPs and providing recommendations for hardening defenses. The report and advisory indicated that Scattered Spider had deployed DragonForce ransomware in recent campaigns.

Attacks with Gunra ransomware

Cybercriminal | Linux malware | Ransomware

Trend Micro researchers analyzed the Linux variant of Gunra ransomware, which has notable features, including the ability to run up to 100 encryption threads in parallel and support partial encryption. It also allows attackers to control how much of each file gets encrypted and provides the option to store RSA-encrypted keys in separate keystore files. Gunra ransomware was first observed in April 2025 in a campaign targeting Windows systems with techniques inspired by the infamous Conti ransomware. The Gunra ransomware's leak site claims it has successfully targeted enterprises in Brazil, Japan, Canada, Turkey, and the United States. Its leak site also lists victims from various industries, including manufacturing, legal and consulting services, healthcare, IT, and agriculture. Trend Micro's threat intelligence data detected activity from Gunra ransomware in enterprises in Turkey, Taiwan, the United States, and South Korea. Trend Micro data showed that the ransomware group targeted government organizations, as well as enterprises in the healthcare, manufacturing, and transportation industries.

TGR-CRI-0045/Gold Melody attacks

Cybercriminal | Access brokers | Exploitation of Machine Keys | ASP.NET View State deserialization

Unit 42 researchers uncovered a campaign by an initial access broker (IAB) that exploited leaked machine keys – cryptographic keys used on ASP.NET sites – to gain access to targeted organizations. IABs breach organizations and then sell access to other threat actors. The IAB used these leaked keys to sign malicious payloads that provide unauthorized access to targeted servers. The technique has been known since 2014 as "Viewstate Deserialization" and has been exploited in attacks against various ASP.NET services that use serialization technology, a security issue for which Microsoft has labeled "Won't Fix." This minimized their on-disk presence and left few forensic artifacts, making detection more challenging. The group's tooling appears to be under active development. The earliest evidence of exploitation and tool deployment occurred in October 2024, followed by a significant increase in activity between late January and March 2025. This surge included the deployment of post-exploitation tools, such as open-source port scanners and custom-built utilities for persistence and privilege escalation. Unit 42 tracks this actor as the temporary group TGR-CRI-0045 and, with medium confidence, attributes it to Gold Melody (also known as UNC961 or Prophet Spider). This group appears to follow an opportunistic approach and has attacked organizations in Europe and the United States in the following industries: financial services, manufacturing, wholesale and retail, high technology, and transportation and logistics.

GLOBAL GROUP attacks

Cybercriminal | RaaS | AI chatbots | Exploitation of public-facing applications | Ransomware

EclecticIQ researchers reported a new ransomware-as-a-service (RaaS) called GLOBAL GROUP that is leveraging advanced AI technologies to carry out campaigns targeting a wide range of companies. As of July 14, 2025, the group claimed 17 victims in the United States, United Kingdom, Australia, and Brazil in the healthcare, oil and gas equipment manufacturing, industrial machinery and precision engineering, automotive repair, and business process outsourcing industries. The group actively uses initial access brokers (IAB) to distribute ransomware and leverages access to vulnerable VPN appliances such as Cisco, Fortinet, and Palo Alto Networks peripherals. They also use brute-force tools to crack passwords for Microsoft Outlook and RDWeb portals. The RaaS platform includes a negotiation portal and a partner panel that allows cybercriminals to manage victims, create ransomware malware for VMware ESXi, NAS, BSD, and Windows, and monitor operations. GLOBAL GROUP uses an automated system powered by AI chatbots to conduct ransom negotiations, enabling non-English-speaking operators to engage more effectively with victims. EclecticIQ assesses with medium confidence that GLOBAL GROUP was likely a rebranding of the BlackLock RaaS operation. Analysis of the GLOBAL ransomware sample confirms that the group uses a customized variant of Mamona ransomware. Unlike Mamona, GLOBAL includes added functionality for automated, domain-wide installation of ransomware. It uses SMB connections and malicious Windows service creation to enable more scalable deployment. EclecticIQ analysts observed that the now-defunct Mamona RIP ransomware operation and GLOBAL GROUP operation used the same Russian VPS provider, IpServer.

Charon ransomware attacks

Cybercriminal | DLL sideloading | Ransomware

Trend Micro researchers identified a new ransomware family called Charon, which was deployed in a targeted attack on the public sector and aviation industry in the Middle East. The threat actor employed a DLL sideloading technique similar to tactics previously documented in the Earth Baxia campaigns, which have historically targeted government sectors. The attack chain leveraged a legitimate browser-related file, Edge.exe (originally named cookie_exporter.exe), to sideload a malicious msedge.dll (SWORDLDR), which then deployed the Charon ransomware payload. Although the researchers observed technical overlap, particularly in the usage of the same binary to load a malicious DLL that deploys encrypted shellcode, they could not definitively attribute this attack to Earth Baxia. The techniques could indicate either direct involvement, deliberate imitation, or the independent development of similar tactics. The ransomware's custom ransom note specifically references the victim organization by name, confirming that this was a targeted operation rather than an opportunistic campaign. This case exemplifies a concerning trend of ransomware operators adopting APT-level techniques, including DLL sideloading, process injection, and anti-EDR capabilities.

CISA alert on Interlock ransomware group

Cybercriminal | Compromised websites | Drive-by download | ClickFix | Linux malware | RAT

On July 22, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) published a Cybersecurity Advisory highlighting known Interlock ransomware indicators of compromise, as well as tactics, techniques, and procedures identified through recent FBI investigations. Interlock ransomware first gained visibility in late September 2024, targeting various businesses,

critical infrastructure, and other organizations in North America and Europe. The FBI stated that these actors target their victims based on opportunity, and their motive is purely financial. Interlock ransomware encryptors were created for Windows and Linux operating systems. These encryptors have been encrypting virtual machines (VMs) on both operating systems. The FBI observed attackers obtaining initial access via a drive-by download from compromised legitimate websites, which is an uncommon method among ransomware groups. Interlock actors use fake Google Chrome or Microsoft Edge browser updates or common security software to trick users into executing a RAT on the targeted system. The attackers also used the ClickFix social engineering technique for initial access. After accomplishing this, the attackers then use various methods for discovery, credential access, and lateral movement to spread to other systems on the network.

Warlock ransomware attacks

Cybercriminal | Exploitation of public-facing applications | LOTL | Ransomware

Trend Micro researchers discovered an attack by the Warlock ransomware group that exploited internet-exposed, unpatched on-premises Microsoft SharePoint servers, abusing newly discovered vulnerabilities to gain initial access to their target's system. Warlock ransomware operators exploited vulnerable Microsoft SharePoint servers by sending targeted HTTP POST requests to upload web shells, which enabled reconnaissance and credential theft. According to earlier reports, Warlock's list of victims included organizations spanning industries from the technological sector to critical infrastructure in North America, Europe, Asia, and Africa. Just a few days after its first public statement, the group had claimed responsibility for at least 16 successful attacks, roughly half of which targeted government agencies in countries such as Portugal, Croatia, and Turkey. Other victims included organizations from the financial services and manufacturing sectors. The attacks escalated through Group Policy abuse, credential theft, and lateral movement using built-in Windows tools and custom malware, culminating in the deployment of ransomware. Encrypted files had the .x2anylock extension, and data was exfiltrated via RClone.

Crypto24 ransomware attacks

Cybercriminal | Google Drive | LOTL | BYOVD | Ransomware

Trend Micro researchers identified Crypto24, a ransomware group targeting organizations in Asia, Europe, and the United States. The group focuses on sectors such as financial services, manufacturing, entertainment, and technology. Crypto24 uses legitimate tools such as PSExec and AnyDesk alongside custom malware, including a keylogger that exfiltrates data via Google Drive and a customized RealBlindingEDR tool that disables security solutions, potentially exploiting new or unknown vulnerable drivers. The attackers maintain persistence by creating privileged accounts and scheduling tasks that integrate malicious activities with normal operations. Crypto24 ransomware achieves privilege escalation by exploiting the CMSTPLUA COM interface to bypass User Account Control (UAC) restrictions. This technique has been observed in other sophisticated ransomware families, including BlackCat and LockBit. It enables execution with elevated privileges without triggering UAC prompts. Analysis revealed that the threat actor operates with a high level of coordination, frequently launching attacks during off-peak hours to evade detection and maximize impact.

The Gentlemen ransomware attacks

New threat actor | Ransomware | Double extortion | BYOVD

Researchers at Trend Micro analyzed a new ransomware campaign launched by The Gentlemen, a previously undocumented threat group that demonstrated advanced capabilities in compromising enterprise environments. The campaign leveraged a combination of legitimate driver abuse, Group Policy manipulation, custom anti-AV tools, privileged account compromise, and encrypted exfiltration channels to bypass enterprise endpoint protections. The group has targeted multiple industries and regions, including manufacturing, construction, healthcare, and insurance, with attacks spanning at least 17 countries. The group also engineered ransomware deployment via privileged domain accounts and created evasion methods to persist against security controls.

The DireWolf ransomware attacks

Cybercriminal | Ransomware | Double extortion | Anti-recovery technique

AhnLab researchers detailed the activities of the DireWolf ransomware group, which emerged in May 2025 and has since launched attacks against companies worldwide, targeting various industries, including manufacturing, IT, construction, and finance. The group uses a double extortion technique, encrypting data and threatening to leak it, and has already compromised 16 organizations in 16 regions. DireWolf's ransomware relies on command-line arguments to control its operations and uses a combination of Curve25519-based Diffie-Hellman key exchange and ChaCha20 stream encryption to encrypt files. The encryption process generates a random session key for each file, which is then used to derive the encryption key. The affected files are given the .direwolf extension, and the encryption design effectively blocks all known decryption methods. DireWolf also employs anti-recovery and anti-analysis techniques, including terminating backup and restoration processes, deleting event logs, and disabling recovery environments. Once encryption is complete, the malware attempts to force a reboot and removes the malicious executable file, reducing the likelihood of forensic analysis and malware recovery.

Attacks with ToolShell vulnerability

Unknown threat actors | Exploitation of public-facing applications

On July 19-20, 2025, various security companies and national CERTs published alerts about the active exploitation of on-premises SharePoint servers. According to the reports, the observed attacks did not require authentication and allowed the attackers to gain full control over the infected servers. The attacks were performed using an exploit chain of two vulnerabilities: CVE-2025-49704 and CVE-2025-49706, publicly named ToolShell. On the same dates, Microsoft also released out-of-band security patches for the vulnerabilities CVE-2025-53770 and CVE-2025-53771, intended to address the security bypasses in previously issued fixes for CVE-2025-49704 and CVE-2025-49706. According to the researchers changing just one byte in the exploit code would be enough to bypass the initial fixes by Microsoft. The release of the new, "proper" updates caused confusion about which vulnerabilities the attackers were exploiting and whether they were using zero-day exploits. Kaspersky products proactively detected and blocked malicious activity linked to these attacks. This allowed us to gather statistics about the timeframe and spread of the campaign.

The Kaspersky report examined the internal workings of the exploitation mechanism of ToolShell vulnerabilities. The researchers demonstrated how the payload can be injected without proper authentication, highlighting the bypass mechanism that enables effective exploitation. According to Kaspersky statistics, widespread exploitation

started on July 18, 2025. The attackers targeted servers in Egypt, Jordan, Russia, Vietnam, and Zambia. Entities in multiple sectors were affected, including those in government, finance, manufacturing, forestry, and agriculture.

Attacks targeting CVE-2025-32433

Unknown threat actors | Exploitation of public-facing applications

On August 11, researchers from Palo Alto Networks published a post detailing their observations of attacks exploiting a maximum-severity flaw discovered and patched in April 2025. The flaw affected the Erlang programming language's Open Telecom Platform (OTP) libraries prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. CVE-2025-32433 has a CVSS score of 10.0 and allows malicious actors to gain unauthorized access to a system and execute arbitrary commands without valid credentials by exploiting the secure shell (SSH) daemon's improper state enforcement. The researchers noted that OT and 5G environments use Erlang/OTP because of its fault-tolerance and scalability for high availability systems with minimal downtime. Remote commands are often executed through the native SSH implementation.

Palo Alto Networks provided an analysis of the payloads, vulnerable attack surface, and distribution of exploitation attempts by geography, timing, industry, and correlation with OT firewalls, noting that a significant number of OT firewalls are both vulnerable and exposed to the internet. Overall, nearly 70% of all the exploitation attempts came from the internet-facing OT firewalls.

Researchers found that the education industry was hit hardest and that OT firewalls in the healthcare, agriculture, media and entertainment, and high technology sectors were disproportionately affected -over 85% of all attacks targeting these sectors were detected on their OT firewalls.

The manufacturing, wholesale and retail, and financial services industries experienced more balanced detection across both IT and OT, necessitating integrated defenses.

Although the utilities, energy, mining, aerospace and defense sectors did not return detections in OT networks, Palo Alto Networks viewed this as potential evidence of weak detection or delayed targeting.

The researchers recommended applying current security patches, updating signatures in intrusion prevention systems, and closely monitoring environments, possibly also disabling the SSH server or restricting access with firewall rules if patching is not immediately possible.

Attacks with PipeMagic backdoor

Ransomware | Backdoor | Zero-day vulnerability

In April 2025, Microsoft patched 121 vulnerabilities in its products. According to the company, only one of them was being used in real-world attacks when the patch was released: CVE-2025-29824. The exploit for this vulnerability was executed by the PipeMagic malware, which Kaspersky researchers first identified in December 2022 in a RansomExx ransomware campaign. The victims were industrial companies in Southeast Asia. The backdoor's loader was a trojanized version of Rufus, a utility for formatting USB drives. In September 2024, Kaspersky researchers encountered it again in attacks on organizations in the Middle East. This time, rather than exploiting vulnerabilities for initial penetration, the attackers used a fake ChatGPT client application as bait. The

fake app was written in Rust using two frameworks: Tauri for rendering graphical applications, and Tokio for executing asynchronous tasks. The fake app had no user functionality – when launched, it simply displayed a blank screen. Notably, it was the same version of PipeMagic used in 2022. Most recently, in 2025, Kaspersky solutions prevented PipeMagic infections at organizations in Brazil and the Middle East. In a joint investigation with BI.ZONE, researchers traced the evolution of PipeMagic – from its initial detection in 2022 to new incidents in 2025 – and identified key changes in the tactics of its operators. They also provided an analysis of PipeMagic modules, including the asynchronous communication module, loader, and injector. In addition to the fake ChatGPT client loader, a Microsoft Help Index File loader was also used. Instead of code for reading .mshi container data, this loader contained C# code that decrypted and executed shellcode, which then extracted and executed the final malware code. A third loader variant used the DLL Hijacking technique, loading a malicious library into the legitimate Google Chrome update executable. In turn, BI.ZONE researchers conducted a technical analysis of the CVE-2025-29824 vulnerability itself. On the same day, Microsoft Threat Intelligence published their own analysis of PipeMagic's architecture and additional payloads, including a dedicated networking module.

Attacks with UpCrypter

Cybercriminal | Spear phishing | Backdoor | RAT

Researchers at Fortinet Labs detected a global campaign targeting organizations in various sectors, with manufacturing, technology, healthcare, construction, and retail/hospitality bearing the brunt of the attacks. As part of the campaign, the attackers used various social engineering tactics to lure users to realistic-looking phishing pages via emails related to purported voicemails for missed phone calls, purchase orders, and other topics that "require immediate attention." The attackers personalize these pages with the victim's email address and their company's logo to make them appear legitimate. The attack chain begins with a small, obfuscated script that redirects victims to a spoofed site. The pages are designed to entice recipients into downloading JavaScript files that act as droppers for UpCrypter, which is the malware that ultimately deploys various remote access tools (RATs). The deployed payloads observed in the attacks include PureHVNC, DCRat, and Babylon RAT.

EvilAI attacks

Unknown threat actor | Backdoor | AI-generated code | Disguised as AI-powered productivity toolset

Researchers at Trend Micro identified a new malware campaign dubbed EvilAI that masquerades as legitimate productivity and AI-enhanced tools, featuring professional-looking interfaces and valid digital signatures. According to Trend Research telemetry data, EvilAI infections have been detected globally, primarily affecting organizations in manufacturing, government, and healthcare, with a significant impact in Europe, the Americas, and the AMEA region. The malware leveraged an LLM to produce code that appears legitimate at first glance. It exfiltrates sensitive browser data and maintains encrypted communication with its command-and-control servers using AES-encrypted channels. To ensure persistence, it creates scheduled tasks, Registry Run key entries and malicious shortcuts. The backdoor functionality includes file downloads via a dedicated downloader, file write operations, registry operations, and process execution. EvilAI employs a sophisticated evasion tactic that makes malicious software appear legitimate at every level. This includes the use of plausible file names and silent execution of a JavaScript payload via Node.js. It utilizes MurmurHash3 32-bit hashing to generate unpredictable control flow conditions, creating loops that appear potentially infinite to static analysis tools, along with other

obfuscation and anti-analysis techniques. The malware establishes persistence by creating a scheduled task disguised as a legitimate Windows process. It also maintains autonomous communication with the C2 server, processing structured commands and ensuring uninterrupted control of the infected system.

Attacks with DarkCloud

Cybercriminal | Spear phishing | Spyware

In September 2025, researchers at ESentire detected a spear-phishing campaign targeting a customer in the manufacturing industry. The campaign attempted to deliver DarkCloud, malware used to steal information. The phishing email was sent to the client's Zendesk support email and featured a financial theme. It contained a malicious ZIP archive with a packed DarkCloud sample. The phishing lure was designed to appear as legitimate financial correspondence with a subject line and message body related to banking. DarkCloud has undergone numerous updates, including a full malware stub rewrite in VB6, string encryption and evasion updates. It targets sensitive information such as browser passwords, credit card details, keystrokes, FTP credentials, and cryptocurrency wallets. Stolen credentials and data are sent to endpoints controlled by the attacker, including Telegram, FTP, SMTP, and Web Panel (PHP). The version of DarkCloud used in this campaign was 3.2, an older version released earlier in 2025.
