Kaspersky ICS CERT

kaspersky

# APT and financial attacks on industrial organizations in Q4 2024

25.03.2025

Version 1.0

This summary provides an overview of the reports of APT and financial attacks on industrial enterprises disclosed in Q4 2024, as well as the related activities of groups that have been observed attacking industrial organizations and critical infrastructure facilities. For each topic, we summarize the key facts, findings and conclusions of researchers that we believe may be of use to professionals addressing practical issues of cybersecurity for industrial enterprises.

# Executive Summary

The cases that went public in Q4 2024 illustrate some of the many cybersecurity challenges of industrial enterprises and OT infrastructure. Here are a few highlights from the report that we'd like to draw reader attention to.

TIDRONE was once again caught spreading their malware via backdoored ERP software, most likely the result of a supply chain attack on niche Korean developers that only deliver their solutions to a limited number of customers. The campaign showcases that the supply chain attack vector, especially when dealing with small suppliers, is one of the most challenging risk factors for industrial enterprises.

OrpaCrab, a sophisticated Linux-based backdoor aimed at OT systems used at gas stations, was reportedly extracted from a fuel management system that had previously been compromised by a well-known hacking group. This serves as another example of OT-targeting being possible without implementing any OT-specific functionality (rather than introducing support for C2 communications via MQTT to hide them in legitimate traffic).

When targeting defence, energy, governmental, pharmaceutical, insurance and legal sectors in Europe, Ukraine and the U.S. for espionage and cybercrime, RomCom exploited a chain of two zero-day vulnerabilities (one in the browser and one in the OS) that ended up with zero-click remote code execution. This case emphasizes how important it is to educate personnel and raise security awareness.

Multi-factor authentication is a good security practice, but it must be carefully monitored and properly executed. Otherwise, it could be easily abused by intruders, as the pro-Iranian actors showcased in their campaign targeting organizations across multiple industrial sectors. The next move of the attackers was to exploit RDP to propagate laterally inside the victim's network, serving as one more reminder of how important it is to have remote access tool usage monitored and controlled within IT and OT perimeters.

A few interesting techniques were demonstrated by Shadow/Twelve (presumably the same, just switching between cybercrime and politically motivated hacktivism), showcasing that many industrial enterprises should take more care of their Linux-based system and virtualized system cybersecurity. Their abuse of Telegram to spy and put pressure on their victims' employees emphasizes that private messengers should not be treated as something outside corporate cybersecurity monitoring and control.

Attacks by Akira/Howling Scorpius targeting medium-size organizations in various sectors, including construction, transportation and logistics, government, telecommunications, technology and pharmaceuticals, bypassed cybersecurity solutions through a mix of well-known techniques, such as Bring You Own Vulnerable Driver, and a new one targeting virtualized infrastructures protected with EDR solutions. This is yet another argument for industrial organizations to invest in threat intelligence information gathering and analysis to proactively develop adequate security measures.

In their campaign targeting manufacturing and logistics companies in the Asia-Pacific region with infected USB disk drives for suspected industrial espionage, Turla (according to Mandiant and Cybereason) or Tomiris (according to Kaspersky), relied on a rarely reported technique. They hijacked an inactive botnet CnC (dismantled years ago by an international law force operation) and abused the malware for initial victim profiling. We consider this a reminder for industrial organization cybersecurity teams that a commodity malware infection attempt may be just a first step for a sophisticated APT inside the network.

BianLian ransomware used an interesting technique to notify their victims about the attack – the actor sent messages by printing them on printers connected to a compromised network. This is a sign to organization cybersecurity teams – it makes sense to periodically check what your printers are printing.

As well as LockBit, another ransomware now supports FreeBSD. The new Interlock ransomware, which has a version tailored for this OS, has been observed targeting industrial enterprises in India, Italy, Japan, Germany, Peru, South Korea, Turkey, and the United States. It is no longer possible to hope that servers running on this platform are secure due to the lack of malicious tools running on it.

# Southeast Asia and Korean Peninsula

## PhantomNet attacks

PhantomNet is a RAT first described by ESET in late 2020. In 2021, Kaspersky researchers released their analysis of the PhantomNet malware, which at the time was being used in attacks against the Vietnamese government sector. The Kaspersky report discussed in detail the plugins and commands it supported. Kaspersky researchers rediscovered PhantomNet during a recent investigation into a cyberattack on the Brazilian education and government sectors that occurred in April. This time, multiple scripts and commands executed by the attackers, and the PhantomNet builder tool, were recovered. The threat actor changed the persistence mechanism so the payload is now stored in an encrypted manner in the Windows registry with an associated loader to retrieve the payload from the registry. There are also some changes in the victimology: previously, PhantomNet infections were found in Asia, but now they are active in many regions around the world and affect a wide variety of industries, including manufacturing, agriculture and construction.

## SideWinder attacks

SideWinder is an APT group that has been active since at least 2012 and usually targets high-profile entities in South Asia. During an investigation, Kaspersky researchers discovered a previously unknown, final-stage tool named "StealerBot" used by the Sidewinder attacker. This unknown tool is an advanced modular implant specifically developed for espionage. The main component is usually protected with obfuscation layers and anti-analysis techniques. All components, including the main one used only to communicate with remote servers and load additional modules, are never stored on the file system as code. They always reside in encrypted files and are loaded in memory with other malware like the one dubbed "Backdoor Loader Module". The modules are not present by default, but selectively deployed by the attacker on specific systems, likely based on their requirements. In total, eight modules were discovered, with targets from Bangladesh, Djibouti, Jordan, Malaysia, the Maldives, Myanmar, Nepal, Pakistan, Saudi Arabia, Sri Lanka, Turkey and the United Arab Emirates. The targeted sectors include government and military entities, logistic companies and infrastructure, telecommunication companies, financial institutions, universities and oil trading companies. The attackers also targeted diplomatic entities in the following countries: Afghanistan, France, China, India, Indonesia and Morocco.

## DONOT/Origami Elephant attacks

DONOT APT group (aka APT-C-35, Origami Elephant, Brainworm) targeted maritime and defense manufacturing industries in Pakistan, according to the Cyble Research and Intelligence Labs (CRIL) report. The group has been active since 2016 and historically focused on government agencies, military entities, and diplomatic missions, with particular emphasis on countries in South Asia. The DONOT group has previously attacked organizations by exploiting vulnerabilities and using phishing emails and malicious attachments as initial infection vectors. The initial infection vector in the new campaign was a malicious LNK file sent in a spam email disguised as a legitimate RTF document. When clicked, the LNK file triggered several PowerShell commands that downloaded a DLL file and a lure RTF file. The lure document was linked to Karachi Shipyard & Engineering Works (KS&EW), a prominent Pakistani defense contractor. Once the DLL is executed, it initiates a process that extracts critical configuration data, including server addresses, encryption keys, and other task parameters, from an embedded JSON file. The malware then uses this information to communicate with the C&C server, requesting further instructions on how to proceed with the attack. A notable feature of this attack is the use of random domain generation served as a backup C&C server.

## P8 attacks

Kaspersky researchers identified a new attack framework dubbed P8, targeting financial and real estate sectors in Vietnam in H2 2022. In 2023, Elastic Lab reported on an OceanLotus (aka APT32) APT attack using a tool set named Spectral Viper. Although the campaigns are the same, Kaspersky researchers cannot conclusively attribute P8 to OceanLotus.

The P8 framework consists of a loader and various plugins downloaded from a C2 server and then loaded into memory, leaving no traces on the disk. Researchers believe P8 is based on the open-source C2Implant project, modified for espionage with advanced functions and protocols. The goal is presumably to implement another Cobalt Strike-like post-exploitation platform. Initial infections are believed to involve spear phishing, with medium to low confidence. These attacks use an outdated Kaspersky tool to side-load the P8 beacon. SMB and printer driver vulnerability exploitation has also been observed to move laterally through the network.

Kaspersky published a follow-up report that detailed 12 plugins for lateral movement, exfiltration, credential theft, taking screenshots, custom loading capabilities and file management. New attacks showed changes in TTPs while still predominantly affecting financial institutions in Vietnam, with one victim active in

the manufacturing industry. The initial infection vector remains unidentified, and no direct links to OceanLotus have been established.

# Chinese-speaking activity

## Estries/Salt Typhoon attacks

Researchers at Trend Micro have discovered a new backdoor, dubbed GHOSTSPIDER, found during attacks on Southeast Asian telecoms companies. They attribute the attacks to Earth Estries (aka Salt Typhoon, FamousSparrow, GhostEmperor and UNC2286), a Chinese-speaking threat actor. In addition to GHOSTSPIDER, Salt Typhoon uses a set of proprietary and shared tools for complex multi-stage attacks: SNAPPYBEE (aka Deed RAT), SparrowDoor, CrowDoor and MASOL RAT for Linux, the DEMODEX rootkit, NeoReGeorg, frpc, and Cobalt Strike. According to Trend Micro, Salt Typhoon targeted telecom, government, technology, consulting, chemical and transportation companies in Afghanistan, Brazil, Eswatini, India, Indonesia, Malaysia, Pakistan, the Philippines, South Africa, Taiwan, Thailand, U.S. and Vietnam. The report focuses on two campaigns: "Alpha," which targeted the Taiwanese government and chemical manufacturers using DEMODEX and SNAPPYBEE, and "Beta," a long-term espionage campaign against Southeast Asian telecom and government networks using GHOSTSPIDER and DEMODEX. Initial access is achieved by exploiting vulnerable public endpoints using CVE-2023-46805, CVE-2024-21887 (Ivanti Connect VPN service), CVE-2023-48788 (FortiClient EMS), CVE-2022-3236 (Sophos firewall), CVE-2021-26855, CVE-2021-26857-6858 and CVE-2021-27065 (ProxyLogon). Salt Typhoon uses LOLbin (Living-off-the-Land Binaries) tools to gather reconnaissance and move laterally across the network during the post-compromise phase.

## TIDRONE attacks

TIDRONE is a Chinese-speaking actor first identified by Trend Micro and then also described by Acronis in September 2024. In a blogpost we describe how TIDRONE attacks Taiwanese defense companies and drone manufacturers. ASEC researchers discovered that the group's CLNTEND malware was used in H1 2024 while also attacking Korean companies. In the cases reported by Trend Micro, researchers expected that TIDRONE spread their malware via backdoored ERP software most likely the result of a supply chain attack. In the cases described by ASEC, the malware was also spread via Trojanized ERP software exploited since July 2024, but this time the software was made by small Korean companies with no official websites. In addition to the usage of legitimate

winword.exe for malicious sideloading previously described by Trend Micro and Acronis, ASEC also observed legitimate VsGraphicsDesktopEngine.exe and rc.exe used for this purpose.

# Middle East-related activity

## CISA alert on Iranian cyber actors

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Communications Security Establishment Canada (CSE), Australian Federal Police (AFP) and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a joint cybersecurity advisory regarding Iranian cyber actors that have been actively targeting organizations across various critical infrastructure sectors, including healthcare, public health, government, IT, engineering and energy, since October 2023. They have gained unauthorized access to networks by employing brute force attacks like password spraying, and exploiting multifactor authentication (MFA) through tactics like "push bombing" and "MFA fatigue." With access secured, the attackers move quickly to register their own devices with MFA, thereby locking out legitimate users and reinforcing their control over the compromised accounts. In one documented case, attackers leveraged a self-service password reset (SSPR) tool on a public-facing Active Directory Federation Service (ADFS) to reset expired passwords and then registered new MFA devices through Okta for accounts that had not yet been protected. Once inside the network, the attackers further escalate attacks by moving laterally through systems using RDP. The advisory specifies that the actors exploited Citrix systems for external access, and used Microsoft Word to open PowerShell to launch the RDP binary mstsc.exe, thereby gaining broader access to the network. In multiple instances, they performed Kerberos Service Principal Name (SPN) enumeration of several service accounts to obtain Kerberos tickets for additional credentials, further increasing their access to sensitive systems.

## OrpaCrab/IOCONTROL backdoor

QiAnXin XLab researchers analyzed OrpaCrab, a sophisticated Linux-based backdoor aimed at industrial systems, particularly those associated with ORPAK, a company involved in gas stations and oil transportation. The malware was uploaded to VirusTotal in January 2024 from the U.S. One notable feature of OrpaCrab is its use of the MQTT (Message Queuing Telemetry Transport) protocol for C2 communication. The Trojan's primary infection vector remains unclear, but once installed, it establishes persistence through a script to be

autostarted from "/etc/rc3.d/". OrpaCrab employs AES-256-CBC encryption to obfuscate its configuration information and utilizes DNS over HTTPS (DoH) to resolve its C2 domain, effectively bypassing traditional DNS monitoring. The backdoor communicates with its C2 server using three main MQTT topics to upload initial device information, receive instructions, and return command execution results. Analysis of the malware's code reveals support for several commands, including arbitrary command execution, self-removal, and reconfiguration of the MQTT broker.

The OrpaCrab malware was also analyzed and codenamed IOCONTROL by Claroty. Claroty said the malware was extracted from a Gasboy fuel management system that was previously compromised by the CyberAv3ngers hacking group. This group has been previously linked to cyberattacks exploiting Unitronics PLCs to breach water systems. According to Claroty researchers, the malware was embedded within Gasboy's Payment Terminal, called OrPT. This implies that the threat actors, given their ability to control the payment terminal, also had the means to shut down fuel services and potentially steal credit card information from customers.

# Russian-speaking activity and targets

## Crypt Ghouls attacks

In December of 2023, new malicious activity appeared with ransomware infections in various Russian companies and government entities. Further investigation led Kaspersky researchers to discover the threat actor, dubbed "Crypt Ghouls", and its connections to other groups. Crypt Ghouls applied ransomware LockBit 3.0 and Babuk. The new malicious activity of the group overlaps with certain other cyber groups active nowadays like MorLock, BlackJack, Twelve/ExCobalt and Shedding Zmiy, reaffirming that most groups targeting Russian businesses and government agencies share tools and use similar TTPs. The Crypt Ghouls' other toolset consists of common tools such as Mimikatz, XenAllPasswordPro, PingCastle, Localtonet tool, Resocks, AnyDesk, PsExec and others. Victims were exclusively limited to Russian companies specializing in the following industries: mining, energy, finance and retail.

## Awaken Likho/Core Werewolf attacks

Kaspersky researchers detected a new campaign of the Awaken Likho APT group (aka Core Werewolf) against Russian government agencies, their contractors, and industrial enterprises, which began in June 2024 and lasted until

at least August. The attackers significantly modified the software in their attacks, preferring to use an agent for the legitimate MeshCentral platform instead of the UltraVNC module, which they had previously used to gain remote access to the system. Judging by the telemetry, the implant was downloaded to the victims' devices from a malicious URL presumably via phishing emails. The emails themselves could not be tracked, but attachments to emails from previous campaigns contained SFX archives and links to malicious modules. As in previous campaigns, the implant was distributed in a self-extracting 7-Zip archive. The archive includes five files, four of which are disguised as legitimate system services and command files, and one of which is the MeshAgent agent. The attackers create a scheduled task that runs a command file and then launches MeshAgent to establish a connection with the MeshCentral server. Kaspersky researchers believe that the new version of the malware is still in the development process.

According to F6 researchers, Core Werewolf updated its TTP in October and began using a chain of VBS scripts to install the legitimate UltraVNC remote access program. It also added a new SSH backdoor to its arsenal. The group continues to attack Russian industrial enterprises. In October, Core Werewolf disguised its lure documents as an official message from the Deputy Minister of Defense of the Russian Federation and as a message from the FSTEC of Russia. Judging by the context of the latter bait document, it was intended for organizations in the electric power industry and the defense and rocket and space industries.

## Shadow/Twelve attacks

F6 researchers released a detailed study of the dual-use group Shadow/Twelve, which attacks medium-sized and large Russian businesses, industrial enterprises and government organizations. Researchers concluded that these groups, which were thought to be independent, are actually parts of the same hacking group. Shadow is interested in money extortion, while Twelve sought to conduct hacktivist attacks to completely destroy the IT infrastructure of its victims. By July 2024, these attackers had attacked at least 50 targets in Russia. According to the researchers, over time the group changed its names to Comet and DARKSTAR. The group uses credentials purchased on closed marketplaces, external remote access services like RDP and VPN, and phishing messages as initial attack vectors. In some cases, they purchased access to corporate mailboxes to send dedicated phishing messages to compromised account contacts. They are also known to target software developers and system integrators for the sake of abusing access to their customers. Additionally, the attackers exploited the following vulnerabilities: Atlassian Confluence RCE

vulnerabilities (CVE-2023-22515, CVE-2023-22518), Zimbra vulnerability chain (CVE-2019-9670, CVE-2019-9621), MS Exchange vulnerability chain (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) and JetBrains TeamCity RCE vulnerability (CVE-2024-27198). As a first point of compromise for further development of their attacks, the attackers normally choose virtualized systems that company personnel rarely log in to. In the final stage of the attack, virtualized system files are encrypted on the compromised hypervisor. Compromised Linux systems are often used as a backup access channel (via SSH). Interestingly, when collecting confidential data, the attackers also restored it from hard drives using data restore tools.

The attacks associated with all four group names (Shadow, Twelve, Comet, DARKSTAR) involved use of the same tools, like Cobint, gpo.ps1, similar strings in Windows tasks created for running malware, and ngrok as one of the backup channels for the access and execution of other malicious actions. To create ransomware, the attackers use leaked builders and source codes of LockBit 3.0 (Black) and Babuk for ESXi. One of the group's signature techniques was stealing Telegram messenger sessions from company employee computers, which allowed them to spy on the employees of the attacked company and contact them to apply additional pressure.

## RomCom attacks

ESET researchers have linked Russia-aligned threat actor RomCom (aka Storm-0978, Tropical Scorpius, UNC2596), known for its opportunistic and targeted espionage operations, to a campaign exploiting two zero-day vulnerabilities: one in Mozilla Firefox (CVE-2024-9680) and the other in Microsoft Windows (CVE-2024-49039). If a victim uses a vulnerable browser and visits a fake website that redirects to a server hosting the exploit, an adversary can run arbitrary code without any user interaction required (zero click). The shellcode loads an embedded library that implements a sandbox escape by exploiting the Windows Task Scheduler vulnerability to obtain elevated privileges. The library makes use of an undocumented RPC endpoint, which would not have been callable from an untrusted process level, to launch a hidden PowerShell process that downloads and executes RomCom RAT on the compromised system. Telemetry data gathered by ESET shows that a majority of the victims who visited the exploit-hosting site were located in Europe and North America. In the same research paper, researchers reported that in 2024, RomCom was observed targeting state entities and the defense and energy sector in Ukraine, and state entities in Europe for espionage, as well as pharmaceutical and insurance sectors in the U.S. and the legal sector in Germany for cybercrime.

## Cloud Atlas attacks

A Kaspersky researcher published a report describing a previously undocumented toolset that the Cloud Atlas group used heavily in 2024. Cloud Atlas continues to use phishing emails with malicious attachments targeting the CVE-2018-0802 vulnerability to obtain initial access. When opened, the document downloads a malicious RTF template that contains a formula editor exploit that downloads and runs an HTA file. The RTF and HTA downloads are restricted to certain time slots and victim IP addresses: requests are only allowed from target regions. The malicious HTA file extracts and writes several files to disk that are parts of the VBShower backdoor. In the new campaign VBShower then downloads and installs the PowerShower backdoor, a tool introduced by the group in 2019 to steal browser credentials, and a new implant called VBCloud, which is similar to PowerShower.

The use of PowerShell Inveigh was also observed, a machine-in-the-middle attack utility used for data packet spoofing attacks and collecting hashes and credentials by intercepting packets and using protocol-specific sockets.

According to Kaspersky telemetry, the threat actor has been active in Russia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Slovakia, and Turkey. There are no significant changes in the targeted industries, which continue to primarily include organizations from the government, military, telecommunications, manufacturing, non-profit and energy sector.

## Venture Wolf attacks

BI.ZONE researchers discovered a previously unknown cluster called Venture Wolf, which has been active since at least November 2023 and targets industrial companies and the construction, IT, telecom and other industries in Russia using various downloaders to deliver MetaStealer. Venture Wolf distributes archives containing a downloader with the .com extension (less often .exe), as well as one or more phishing documents that are either images (JPG or PNG) or PDF, DOC/DOCX and ODT files. Once launched, the downloader either creates a .NET dummy file that has the MetaStealer malicious payload embedded in it or injects the malicious payload into the RegAsm.exe process. The downloaders are PE executable files with obfuscated code. MetaStealer is implemented in C# and is a fork of another stealer, RedLine. An important difference between MetaStealer and RedLine is that MetaStealer developers do not prohibit its use for attacks on Russia and countries in the CIS. During execution, MetaStealer collects information about the system and receives data from browsers, crypto wallets, email clients, as well as various applications such as Steam and FileZilla. Venture Wolf uses the .NET Reactor protector to obfuscate MetaStealer code.

## Unicorn attacks

The Unicorn group's activity was first revealed in September by Kaspersky researchers. The group targets Russian energy companies, industrial enterprises, and suppliers and developers of electronic components using Trojan-Spy.VBS.Unicorn. Later F6 researchers found out that the threat actor distributed variants of custom malware under the guise of a commercial offer to purchase equipment for military operation at a discount and an offer to donate equipment to a fund for soldiers' needs. During the investigation of the Unicorn group, experts managed to discover additional infrastructure and related files, including new VBS scripts, a .HTA file, phishing LNK files and bait PDF files. One of the LNK files and a bait PDF file have references to a Russian developer of electronic components.

## Sticky Werewolf/Angry Likho attacks

According to F6 researchers, Sticky Werewolf continued the MimiStick campaign targeting industry companies in Russia by deploying the Sliver Implant and Quasar RAT. In addition to the ongoing MimiStick campaign, malicious mailings were detected targeting a research and development enterprise and a supplier of materials, equipment and quarry machinery, where the Darktrack RAT was installed as the final payload. The malicious emails distributed password-protected RAR archives that would lead to execution of the NSIS installer, a batch file, Powershell downloader and an executable downloader/injector, this chain eventually leading to the installation of the Darktrack RAT.

Kaspersky researchers shared the TTP of the same group, also observing the ZIP archives, VBS files and Ande Loader involved in the attack chain that ends with the download of the Darktrack RAT, in addition to what was described by F6 researchers. According to Kaspersky, the group also targets Belarusian in addition to Russian organizations. Attackers use third-party services to host and download malicious files. A study of the attackers' infrastructure showed that they have many other malicious tools in their arsenal, including stealers and remote access trojans.

## Andromeda/Gamarue attacks

Cybereason Security Services Team discovered a new cluster of Command and Control servers associated with the Andromeda/Gamarue malware, which has been targeting manufacturing and logistics companies in the Asia-Pacific region for suspected industrial espionage. Based on the available telemetry, the researchers assessed that the initial infection vector was through infected USB disk drives. In this case, the creation of LNK shortcuts with generic file names

was observed, mimicking familiar USB stick names or familiar file names designed to trick the victim into clicking the LNK file. On one environment, researchers detected multiple instances of rundll32.exe being launched to load different DLLs with a naming convention of ~$W*.USBDrv or ~$W*.FAT32. On multiple instances, shortly after rundll32.exe executes the DLL with specific arguments and parameters, the process establishes a C2 connection, which ultimately leads to Andromeda/Gamarue backdoor executables being loaded and injected into svchost.exe. Continuing the investigation on VirusTotal, researchers identified a cluster of IP addresses being used as C2 in conjunction with the Andromeda backdoor.

Research led to the discovery that one of Andromeda's malicious domains has been associated with Turla (aka UNC4210) by AlienVault's Open Threat Exchange (OTX). According to Mandiant's research, Turla/UNC4210 has been seen repurposing an old Andromeda sample with a C2 hijacked by Turla/UNC4210. The sample was first uploaded to VirusTotal in 2013, and spreads from infected USB keys. Given the level of data available, Cybereason assessed with low to medium confidence that it is linked with this particular Turla campaign. According to Kaspersky researchers, not Turla but another Russian-speaking threat actor called Tomiris may have actually hijacked extinct Andromeda hostnames or domains. Though Kaspersky researchers see connections between Turla and Tomiris, we continue tracking these two as different actors.

# Cybercriminal and other

## CISA alert on BianLian ransomware group

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a joint cybersecurity advisory regarding BianLian ransomware and its IOCs and TTPs identified through FBI and ASD'S ACSC investigations. BianLian group actors have affected organizations in multiple U.S. critical infrastructure sectors since June 2022, including the critical manufacturing sector. They have also targeted Australian critical infrastructure sectors in addition to professional services and property development. The group gains access to victim systems through valid RDP credentials, uses open-source tools and command-line scripting for discovery and credential harvesting, and exfiltrates victim data via FTP, Rclone, or Mega. BianLian originally employed a double-extortion model in which they encrypted victims' systems after exfiltrating data. However, they shifted to exclusively exfiltration-based extortion around January 2024, abandoning file encryption tactics. The

group targets Windows and ESXi infrastructure, possibly leveraging the ProxyShell exploit chain (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) for initial access. It uses Ngrok and modified Rsocks to mask traffic destinations using SOCK5 tunnels, exploits CVE-2022-37969 to escalate privileges on Windows 10 and 11, and renames binaries and tasks after legitimate Windows services and security products for evasion. The group uses PowerShell scripts to compress collected data before exfiltration, including the new Tox ID for victim communication using ransom notes, and prints ransom notes on printers connected to the compromised network.

## Interlock attacks

Fortinet researchers released a report on a new ransomware called Interlock. It was first submitted to a publicly available file-scanning site in early October 2024, but apparently was also distributed earlier. Interlock is available in two versions: for Windows (Vista, 7, 8, 8.1 and 10) and FreeBSD. The initial infection vector of Interlock is still unknown, but researcher Sina Kheirkhah reported that a previously unknown Supper backdoor was found on the victim's machine, through which the ransomware could have been deployed. Interlock encrypts files on victim computers using the AES-CBC encryption algorithm. At the time of investigation, six victims were listed on the DLS Interlock website, five of whom were in the U.S. and one in Italy. For each victim, DLS in TOR provides a separate page with a description of the victim's organization and a list of stolen files. However, telemetry data points to a broader victimology. Interlock ransomware samples have been spotted in India, Italy, Japan, Germany, Peru, South Korea, Turkey and the U.S., and victims have been found in the education, finance, government, healthcare, and manufacturing sectors.

## TA866/Asylum Ambuscade attacks

Cisco Talos researchers identified the activities of TA866 (aka Asylum Ambuscade), a financially motivated threat actor involved in malware campaigns and also potentially espionage since at least 2020. TA866 uses a mix of commodity and custom tools in their campaigns, often collaborating with other cybercriminal groups. Since early 2023, their malware distribution methods have evolved, utilizing malspam and malvertising to redirect victims to traffic distribution systems (TDS), such as 404 TDS, which deliver malware. The group has been observed using tactics such as email thread hijacking. The infection chain generally starts with a malicious JavaScript downloader, leading to the deployment of WasabiSeed, which fetches further payloads, including ScreenShotter and AHK Bot. Their key malware tools also include Resident backdoor, Cobalt Strike beacons, CSharp-Streamer-RAT and Rhadamanthys

during post-compromise stages. TA866 often installs remote access tools like AnyDesk and Remote Utilities on infected systems. Most of the cases where follow-on payloads were observed have been in the U.S., with additional cases spread across Canada, the United Kingdom, Germany, Italy, Austria and the Netherlands. The most affected industry was the manufacturing sector, followed closely by government and financial services. Recent links have been found between TA866's activities and those of other cybercrime groups like ShadowSyndicate and ransomware campaigns involving ALPHV and IcedID.

## Akira/Howling Scorpius attacks

Palo Alto Networks Unit 42 published research on how the Howling Scorpius group impacts both Windows and Linux/ESXi systems through its Akira ransomware, frequently updating its attack methods. According to researchers, Howling Scorpius targets small to medium-sized businesses in North America, Europe and Australia across various sectors. Affected industries include education, construction, consulting, transportation and logistics, government, telecommunications, technology and pharmaceuticals, with manufacturing being affected the most. Howling Scorpius' initial access methods include exploiting vulnerable VPN services that lack multi-factor authentication using valid accounts, often purchased through initial access brokers on the dark web, targeting external-facing services like RDP and conducting spear phishing campaigns. Mimikatz and LaZagne are the group's primary tools for extracting credentials for privilege escalation. Howling Scorpius affiliates employ the Kerberoasting attack to achieve control over service accounts and exploit credentials stored in memory. The group's affiliates copy the SYSTEM registry hive and NTDS.dit file from the domain controller to obtain a complete listing of user accounts and their corresponding domain password hashes. The group created new domain accounts to establish persistence. Lateral movement within compromised networks primarily involves exploiting remote services such as RDP and SMB. Affiliates use network scanning tools like NetScan and Advanced IP Scanner, and also execute PowerShell and Windows Net Commands to query Active Directory for information on users and administrators. Howling Scorpius affiliates use the BYOVD (Bring Your Own Vulnerable Driver) technique with tools that abuse the Zemana antimalware driver to terminate antimalware-related processes. The group creates their own fresh new VMs where they disable Windows Defender, mount the data storage drives on the hypervisor, stop (shut down) the VMs to release locked disk image files, and then execute the ransomware, thus bypassing EDR tools.

## Water Makara attacks

A new spear-phishing campaign targeting companies in Latin America, with a particular focus on organizations in Brazil, has been found delivering banking malware called Astaroth (aka Guildma) by making use of obfuscated JavaScript. Trend Micro tracks the threat activity cluster under the name Water Makara. According to Trend Micro researchers, the spear phishing campaign targeted various industries, with manufacturing companies, retail firms, and government agencies being the most affected. Construction, automotive and agriculture also made it into the top victims. Mandiant has assigned the moniker PINEAPPLE to a similar intrusion set that delivers the same malware to Brazilian users. Both these campaigns are similar in that they begin with phishing messages that impersonate official entities such as Receita Federal and aim to trick recipients into downloading a ZIP archive attachment that masquerades as income tax documents. Inside the malicious ZIP file is a Windows shortcut (LNK) that abuses mshta.exe and executes obfuscated JavaScript to establish connections to a C2 server.

## Operation Cobalt Whisper

SEQRITE Labs' APT team has revealed an advanced cyber-espionage campaign known as Operation Cobalt Whisper, impacting multiple industries including defense, education, environmental engineering, electrotechnical engineering, energy, cybersecurity, aviation and healthcare in Hong Kong and Pakistan.

SEQRITE identified over 20 infection chains utilizing RAR and ZIP archives containing decoy PDF and LNK files. Researchers revealed a two-stage infection process, where an initial LNK executes a VBScript to achieve persistence and hide activity, followed by a Cobalt Strike beacon disguised as a legitimate executable that connects back to the attacker. Through file path artifacts, machine IDs, and configuration similarities, SEQRITE links clusters of activity to Operation Cobalt Whisperer. These campaigns also have consistent command-and-control patterns registered with Tencent's network infrastructure.

## UAC-0185 attacks

The Ukrainian CERT described a campaign aimed at defense and industrial sectors in Ukraine. The attackers send an email impersonating the Ukrainian League of Industrialists and Entrepreneurs (ULIE) with a URL leading to the download of an LNK file. Once executed, the lure document is downloaded and JS code is executed, which in turn runs two Powershell commands. Ultimately, a ZIP file is downloaded and the MESHAGENT RAT gets installed. According to the Ukrainian CERT, the group responsible for this attack is UAC-0185 (aka

UNC4221), which has been active since at least 2022. The group's aim is to steal credentials for messaging apps, such as Signal and Telegram, but also for military systems such as DELTA and TENETA.

## SmokeLoader attacks

In September 2024, FortiGuard Labs observed an attack using SmokeLoader malware to target companies in Taiwan, including those in manufacturing, healthcare, IT and other sectors. The starting point of the attack chain discovered by FortiGuard Labs is a phishing email with a Microsoft Excel attachment that, when executed, exploits multi-year security vulnerabilities (including CVE-2017-0199 and CVE-2017-11882) to install the Ande Loader through VBS, which is then used to deploy SmokeLoader on the compromised host. SmokeLoader includes two components: a stager and a main module. The stager's purpose is to establish persistence, decrypt, unpack and inject the main module into the explorer.exe process. The main module is responsible for communicating with C2 and downloading plugins. The malware supports several plugins that can steal login and FTP credentials, email addresses, cookies, and other information from browsers, Outlook, Thunderbird, FileZilla and WinSCP.

## Attacks with Lumma stealer and Amadey bot

Cyble Research and Intelligence Labs identified a malicious campaign targeting the manufacturing industry, leveraging a deceptive LNK file. This file is disguised as a PDF file and hosted on a remote WebDAV share likely sent in a spear phishing email. The malicious LNK file is hosted on a URL that impersonates LogicalDOC, a cloud-based document management system commonly used in manufacturing and engineering firms. This campaign leverages multiple Living-off-the-Land Binaries (LOLBins), such as ssh.exe, powershell.exe and mshta.exe. The attack chain leverages DLL sideloading via legitimate syncagentsrv.exe and IDAT Loader to deploy the Lumma stealer and Amadey bot, enabling the attacker to gain control and exfiltrate sensitive information from the victim's machine. The unattributed threat actor behind the campaign uses a Google Accelerated Mobile Pages (AMP) URL along with a shortened URL to evade detection by traditional URL scanners. To maintain persistence on compromised systems, the attackers use Task Scheduler.

**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