Kaspersky ICS CERT

APT and financial attacks on industrial organizations in Q3 2024

26.12.2024

Version 1.0

Highlights of the quarter ... 3
Southeast Asia and Korean Peninsula ... 4
Andariel attacks ... 4
Kimsuky attacks ... 5
UNC2970 attacks ... 6
SideWinder attacks ... 6
SloppyLemming attacks ... 6
Chinese-speaking activity ... 7
APT41 attacks ... 7
MirrorFace attacks ... 8
TIDRONE attacks/Operation WordDrone ... 9
Flax Typhoon/Raptor Train attacks ... 10
Attacks with MSC file/AppDomainManager Injection ... 10
Middle East-related activity ... 11
Peach Sandstorm attacks ... 11
Spanish-speaking activity ... 11
BlindEagle attacks ... 11
Russian-speaking activity and targets ... 12
BlackJack attacks ... 12
ReaverBits attacks ... 13
Attacks with Unicorn scripts ... 13
PhantomCore/Head Mare attacks ... 13
Unit 29155 attacks ... 15
Librarian Ghouls attacks ... 15
Attacks with Loki agent ... 16
Stone Wolf attacks ... 17
CMoon worm attacks ... 17
OldGremlin attacks ... 18
Other ... 19
UAC-0180 attacks ... 19
FrostyGoop attacks ... 19
Attacks on transportation and logistics in North America ... 19
RansomHub attacks ... 20
Attacks abusing Microsoft Sway ... 20

This summary provides an overview of the reports of APT and financial attacks on industrial enterprises that were disclosed in Q3 2024, as well as the related activities of groups that have been observed attacking industrial organizations and critical infrastructure facilities. For each topic, we have sought to summarize the key facts, findings and conclusions of researchers that we believe may be of use to professionals addressing the practical issues of cybersecurity for industrial enterprises.

Highlights of the quarter

During the quarter, a number of research papers and technical advisories were published detailing attacks that either targeted or affected organizations in the industrial sector. From our perspective, the following are likely to be the most interesting for researchers and useful for cybersecurity practitioners.

FrostyGoop is one of the rare instances where an OT-specific toolset was found and disclosed. The tool, which allows communication via the Modbus protocol, is believed to have been used in an attack on a utility company in western Ukraine that resulted in 600 apartment buildings being left without heating for two days during a cold winter period in late 2023.

Librarian Ghouls is another campaign targeting industrial organizations. Although this time the attackers did not specifically target OT systems, their espionage campaign sought industrial 2D and 3D design and modelling data, as well as design and project files from various CAD systems, demonstrating their interest in the design and development of new industrial products and technologies.

The **CMoon worm**, which spread through a compromised the website of a Russian energy company, and the **TIDRONE/Operation WordDrone** attacks, which appear to be either supply chain attacks or exploiting a vulnerability in an ERP product to gain initial access to the victim's systems, reiterate the point that these widely discussed attack vectors, when a third-party service is compromised by the attacker to infect other systems, should by no means be excluded from the threat models of modern industrial enterprises.

Attacks on transportation and logistics in North America – the campaign used dialog boxes referencing Samsara, AMB Logistic, and Astra TMS – software that would only be used in transportation and fleet operations management – to leverage a social engineering technique called ClickFix, which tricks the victim into copying and running a malicious PowerShell script to “fix a technical problem”. Interestingly, researchers identified at least 15 compromised email accounts used in the campaign. The use of legitimate corporate accounts makes such attacks much more effective than the usual use of malicious infrastructure to send phishing emails with forged headers.

PhantomCore/Head Mare attacks – another case where the attackers sent malicious emails from compromised email addresses. They also planted malware in the infrastructure of hacked organizations.

Some of the more recent first-stage attack techniques were demonstrated in the following papers:

- **MSC file/AppDomainManager Injection attacks.** Among the reported attack techniques that deserve attention is a new one called GrimResource that uses a Windows XSS vulnerability that was reported to Microsoft almost six years ago and still remains unaddressed by the vendor. Curiously, the same attack campaign utilizes another Microsoft security flaw that was reported by researchers a few years ago and since then has been mostly used by red teams, and rarely seen in the wild – the AppDomainManager Injection.
- **Attacks abusing Microsoft Sway.** Free access to public cloud services was reportedly abused in a non-trivial way for the initial compromise. The attackers deployed phishing pages for a Microsoft 365 credential harvesting campaign in Microsoft Sway. The pages contained only QR codes that prompted victims to open malicious login pages on their mobile devices. The attackers abused Cloudflare Turnstile to trick victims into passing a captcha test that hides the malicious page from static analysis by automatic tools, thus ensuring it has a good domain reputation. Finally, the attackers abused the Cloudflare Workers free tier service as a malicious reverse proxy for the original (legitimate) Microsoft login pages, allowing them to implement the attacker-in-the-middle phishing that logs the user into the legitimate page and then collects credentials and one-time login tokens and cookies for future use.
- **TA415/APT41.** A phishing campaign abusing the .search-ms file format.

An outlier case is that of the **Flax Typhoon/Raptor Train attacks** – a complex three-tiered botnet consisting of 200,000 SOHO routers that has not been observed conducting DDoS attacks, though some network activity originating from it has been detected targeting critical sectors in the USA and Taiwan.

Southeast Asia and Korean Peninsula

Andariel attacks

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) and other authoring partners published a Cybersecurity Advisory on July 25 focusing on the statesponsored cybergroup known publicly as Andariel, Onyx Sleet (formerly PLUTONIUM), DarkSeoul, Silent Chollima, and Stonefly/Clasiopa. The authoring agencies identified the threat actor as primarily targeting defense, aerospace, nuclear, and engineering organizations in the USA, Japan, South Korea, and India. The group has evolved from conducting destructive attacks targeting US and South Korean organizations to conducting specialized cyber-espionage and ransomware operations. The Advisory describes the group's tools, tactics, techniques, and indicators of compromise.

Researchers from Microsoft and Mandiant also published reports on the activities of Andariel/APT45/Onyx Sleet sharing tools, TTPs, IoCs and targeted industries. Some of the information presented there includes an operation Kaspersky covered in 2021 and 2022.

Kimsuky attacks

According to Der Spiegel, a hacking team linked to the North Korean government attacked German weapons manufacturer Diehl Defence using a phishing campaign with fake job offers and advanced social engineering tactics. The attack, carried out by Kimsuky APT (aka APT43), combined the use of PDF files with spear-phishing lures offering Diehl Defence employees jobs with US defense contractors. According to the article, researchers at Mandiant investigated the compromise and found the attackers performed detailed reconnaissance on Diehl Defense ahead of the spear-phishing attacks. According to Der Spiegel, the Kimsuky hackers hid their attack server behind an address containing "Uberlingen", a reference to Diehl Defence's location in Überlingen in southern Germany. The attack server also hosted authentic-looking, German-language login pages that resembled those of telecommunications provider Telekom and email service GMX, suggesting the attackers were bulk harvesting login credentials of German users. It was not clear how successful the attack was or how much information the hackers were able to obtain.

South Korea's National Cyber Security Center (NCSC) warned that threat actors Kimsuky and Andariel have targeted organizations in the country. The NCSC believes the attackers were attempting to steal trade secrets. In January, a Kimsuky campaign targeted construction companies, public institutions and local governments, distributing digitally signed, trojanized installers. In April, Andariel exploited a vulnerability in a domestic VPN to distribute fake software updates that installed DoraRAT in construction and machinery companies. DoraRAT is a lightweight remote access Trojan (RAT) with minimal functionality that allows it to operate more stealthily. The variant observed in this particular attack was configured to steal large files and exfiltrate them to the attacker's command and control server.

UNC2970 attacks

Researchers at Mandiant observed a threat actor, tracked as UNC2970, targeting executives in the energy and aerospace sectors with job-related phishing messages in an attempt to obtain confidential data. Organizations in the USA, UK, Netherlands, Cyprus, Sweden, Germany, Singapore, Hong Kong and Australia have been targeted. The attackers engage with the targets via email and WhatsApp to establish a relationship of trust, and then send a malicious ZIP file masquerading as a job description. The ZIP archive contains an encrypted PDF file and a trojanized version of SumatraPDF, an open source PDF viewer application. The attackers use this to start an attack-chain that ultimately installs a previously undocumented backdoor dubbed MISTPEN. The activities of this threat actor overlap with those of TEMP.Hermit.

SideWinder attacks

BlackBerry researchers have uncovered a new cyber-espionage campaign by the SideWinder threat actor (aka Razor Tiger, Rattlesnake and T-APT-04) targeting ports and maritime facilities in the Indian Ocean and Mediterranean. The targets are located in Pakistan, Egypt, Sri Lanka, Bangladesh, Myanmar, Nepal and the Maldives. The attack began with phishing emails containing a malicious document with very specific logos and themes familiar to the targets, often related to specific port infrastructure. The actor used spear-phishing documents that exploited the remote template injection technique (CVE-2017-0199). The final-stage payload delivered by the documents is JavaScript malware. This activity overlaps with the Kaspersky SideWinder report.

SloppyLemming attacks

According to Cloudflare, the threat actor SloppyLemming (aka Outrider Tiger) has been targeting organizations in the government, law enforcement, energy, education, telecoms and technology sectors in Pakistan, Bangladesh, Sri Lanka, Nepal and China. The attackers use phishing emails to trick targets into clicking a malicious link that takes them to a credential harvesting page. They also use a custom-built tool named CloudPhish to create a malicious Cloudflare Worker that handles the credential logging logic and credential exfiltration. Some of SloppyLemming's attacks used similar techniques to capture Google OAuth tokens, and also used infected RAR archives to exploit a CVE-2023-38831 RCE vulnerability in WinRAR. The RAR contains a PDF file and an executable that, in addition to displaying a decoy document, covertly downloads a DLL that acts as a downloader to extract the RAT hosted on Dropbox.
Another SloppyLemming infection chain uses phishing lures to direct victims

to a website posing as the Punjab Information Technology Board (PITB) in Pakistan, after which they are redirected to another URL containing a file. The downloaded file is a legitimate executable that is used to sideload a DLL that communicates with the Cloudflare Worker.

Chinese-speaking activity

APT41 attacks

According to Mandiant researchers, the threat actor APT41 (aka Barium, Wicked Panda, Wicked Spider, Earth Baku, Axiom, Blackfly, Brass Typhoon, Barium, Bronze Atlas, HOODOO, Red Kelpie, TA415 and Winnti) launched data exfiltration attacks against global shipping and logistics, media, technology and automotive sectors, primarily in Italy, Spain, Taiwan, Thailand, Turkey and the UK.
The attackers used variants of previously known malware and publicly available tools to infiltrate target organizations and maintain persistence since 2023. APT41 used the ANTSWORD and BLUEBEAM web shells to execute the DUSTPAN malware in order to execute the BEACON backdoor for C2 communications. The threat actor then used DUSTTRAP to proceed with hands-on keyboard activity, SQLULDR2 to copy data from databases, and PINEGROVE to exfiltrate data to Microsoft OneDrive. Interestingly, the DUSTTRAP malware and its components – both those used in the campaign and those found on VirusTotal – were signed with legitimate certificates, presumably stolen from South Korean gaming companies.
One of the certificates was previously observed by Mandiant being used by another Chinese-speaking actor, UNC3914.

Proofpoint researchers discovered a cyber-espionage campaign using malware dubbed Voldemort. The attackers sent messages impersonating tax authorities from countries in Europe, Asia and the USA, targeting more than 70 organizations. The threat actor targeted 18 different industries, but nearly a quarter of the organizations targeted were insurance companies. Aerospace and transportation companies and higher education institutions made up the rest of the top 50%, with automotive, energy, and manufacturing organizations also among the targets. The email messages contained a link that redirected the user to a landing page where they were invited to view a document. If the user agent contains "windows", the browser is redirected to a TryCloudflare-tunneled URI ending in .search-ms, prompting the victim to open Windows Explorer. If the victim agrees to open Windows Explorer, a silent Windows Search query is performed as directed by the .search-ms file. The .search-ms file abuses the file format and causes a decoy LNK or ZIP file from an external share to be displayed in Windows Explorer as if the LNK/ZIP file was located directly in the Downloads folder of recipient's host. The LNK/ZIP file uses a PDF icon to masquerade as a different file type, and these two techniques may lead the recipient to believe there is a local PDF file on disk, increasing the likelihood they will click the malicious file icon.

If the LNK is executed, it invokes PowerShell to run a Python script. The Python script collects information about the computer, downloads a decoy PDF and opens it. It then downloads a password-protected ZIP file and extracts the contents: a legitimate executable related to WebEx and a Voldemort DLL to be side-loaded. Voldemort is a backdoor with information gathering capabilities and can load additional payloads. Voldemort uses Google Sheets for C2 communication. Proofpoint observed Cobalt Strike being hosted on the actor's infrastructure and it is likely that this is one of the payloads that would be delivered.

Proofpoint analysts attribute the campaign to the China-aligned threat group TA415 (aka APT41 and Brass Typhoon). This attribution is based on multiple newly identified high confidence links between the campaign distributing Voldemort and known infrastructure associated with TA415, including overlap with activity publicly reported by Mandiant. Furthermore, in late August 2024, Proofpoint identified a targeted campaign featuring an almost identical attack chain to deliver the Voldemort backdoor. This activity spoofed a Taiwanese aerospace industry association and repeatedly targeted fewer than five aerospace companies in the USA and Taiwan, consistent with the more typical targeting associated with TA415 and other China-aligned actors. In this campaign, TA415/APT41 used phishing emails with Google AMP Cache URLs that redirected to password-protected 7-Zip files hosted on OpenDrive. These archives contained malicious Microsoft Shortcut (LNK) files that attempted to download a Python script hosted on paste[.]ee. This activity continued into late September 2024 and also targeted a small number of organizations in the chemical, insurance, and manufacturing industries.

MirrorFace attacks

JPCERT/CC has observed attacks on Japanese organizations by the threat actor MirrorFace using LODEINFO and NOOPDOOR malware. While previous MirrorFace attacks targeted media, political organizations, think tanks and universities, the latest attacks since 2023 have targeted manufacturers and research institutes. The threat actor’s TTPs have also changed: previous attacks made use of phishing emails, but the attackers now exploit vulnerabilities in Array AG and FortiGate. The group uses the NOOPDOOR shellcode to inject itself into legitimate applications using XML or DLL files, communicate with a command and control (C2) server over port 443, and perform reconnaissance, lateral movement, and information exfiltration. NOOPDOOR also employs a number of evasion tactics including time stamp manipulation, Windows event log deletion, and file deletion. The attackers also use tools other than LODEINFO and NOOPDOOR. In some cases, JPCERT confirmed the use of GO Simple Tunnel (GOST), an HTTP/SOCKS5 proxy tool.

TIDRONE attacks/Operation WordDrone

According to Trend Micro researchers, a previously undocumented cyber-espionage threat actor dubbed TIDRONE, with likely ties to Chinese-speaking groups, has been targeting drone manufacturers in Taiwan as part of a cyberattack campaign that commenced in 2024. One commonality among the various victims is the presence of the same enterprise resource planning (ERP) software, raising the possibility of a supply chain attack. The exact initial access vector used to breach the targets remained unknown, with Trend Micro's analysis uncovering the deployment of custom malware such as CXCLNT and CLNTEND using remote desktop tools like UltraVNC. Both CXCLNT and CLNTEND are initiated by sideloading a rogue DLL via the Microsoft Word application. CXCLNT comes with basic file upload and download capabilities, as well as features to clean up traces, collect victim information such as file listings and computer names, and download next-stage EXE and DLL files for execution. CLNTEND, first detected in April 2024, is a remote access tool (RAT) that supports a wider range of network protocols for communication, including TCP, HTTP, HTTPS, TLS, and SMB (port 445).

Acronis has published its own findings related to the campaign, which it has dubbed Operation WordDrone, stating that it observed the attacks between April and July 2024. The intrusions are characterized by the use of a technique called Blindside to evade detection by endpoint detection and response (EDR) software before deploying CLNTEND (aka ClientEndPoint). Acronis also revealed that the malicious artifacts were detected inside the folder of a Taiwanese ERP software called Digiwin, suggesting the possibility of either a supply chain attack or exploitation of a vulnerability in the product to gain initial access. A DLL with unclear functionality was also found, but researchers speculate that it is used to proxy execution of ClientEndPoint/CLNTEND backdoor commands so that they are executed with dllhost in user context as the parent, rather than winword.exe in SYSTEM context, which could raise suspicions.

Flax Typhoon/Raptor Train attacks

Researchers at Black Lotus Labs have shared details of a botnet dubbed Raptor Train that is thought to be linked to a Chinese-speaking cyber-espionage group known as Flax Typhoon. The botnet consisted of more than 200,000 SOHO routers, NVR/DVR devices, NAS devices, and IP cameras. To date, no DDoS attacks have been observed originating from Raptor Train, and the researchers suspect this capability was being preserved for future use. Nevertheless, some network activity from the botnet has been detected over the last four years targeting critical sectors in the USA and Taiwan, including military, government, higher education, telecoms, defense industrial base, and IT. The botnet infrastructure was managed by a series of distributed payload and C2 servers, a centralized Node.js backend, and a cross-platform Electron application front end called Sparrow. This service enables a full range of activities, including scalable bot exploitation, vulnerability and exploit management, remote management of C2 infrastructure, file uploads and downloads, remote command execution, and the ability to tailor IoT-based DDoS attacks at scale. In most cases, the operators did not build in a persistence mechanism capable of surviving a reboot. The primary implant used on most of the Tier 1 nodes, called Nosedive, is a custom variation of the Mirai implant. Possible exploitation attempts against Atlassian Confluence servers and Ivanti Connect Secure appliances originated from nodes associated with this botnet.

On the same day the report was published, the Five Eyes agencies published an advisory about the botnet with recommendations for mitigations. Also on the same day, the US Department of Justice announced that a court-authorized law enforcement operation was conducted to disrupt the botnet, which involved taking control of the botnet infrastructure and sending commands to disable the malware on compromised devices.

Attacks with MSC file/AppDomainManager Injection

Researchers at NTT identified a wave of attacks starting in July 2024 that targeted government agencies in Taiwan, the military in the Philippines, and energy organizations in Vietnam. The observed attacks had two patterns: one where a ZIP file is downloaded from a website prepared by the attacker, and another in which a ZIP file is attached to a spear-phishing email. In both cases, the ZIP file contains a malicious MSC file, and the attack proceeds when the user opens it. The malicious MSC file exploits an unpatched Windows XSS flaw in apds.dll using the GrimResource technique to execute embedded JavaScript code. The final VBScript code is executed, which downloads and saves four files and executes oncesvc.exe, which is the legitimate Microsoft dfsvc.exe. The downloaded config file “oncesvc.exe.config” contains information to load an assembly version that is different from the one pre-defined in the application. Attackers use this to make a legitimate EXE file load an external DLL file. This malicious behavior is called AppDomainManager Injection. This technique is used by red teams, but has rarely been observed in the wild. In this attack campaign, the CobaltStrike beacons were ultimately used to compromise the target environment. After examining the characteristics of the loader and attacker infrastructure used in the attack, the researchers believe that this method is similar to that used by the APT41 group. An AhnLab report described a similar attack case involving a decoy PDF in Korean about Japan's defense industry and a “readme.docx”.

Middle East-related activity

Peach Sandstorm attacks

Between April and July, Microsoft researchers observed the Peach Sandstorm threat actor (aka APT33, Elfin and Refined Kitten) deploy a new custom multi-stage backdoor dubbed Tickler in attacks against the satellite, communications equipment and oil and gas sectors, as well as federal and state government sectors in the USA and UAE. The threat actor also continued its password spray attacks against the education sector for infrastructure procurement, and the satellite, government, and defense sectors as primary targets for intelligence gathering. Researchers also observed intelligence gathering and possible social engineering targeting organizations in the higher education, satellite, and defense sectors via LinkedIn. Once Peach Sandstorm gains access to an organization, the threat actor is known to perform lateral movement and actions on targets using the SMB protocol. In an older intrusion against a multinational pharmaceutical company, the threat actor also downloaded and installed AnyDesk, a commercial RMM tool. In at least one intrusion against a satellite operator based in the Middle East, Peach Sandstorm actors compromised a user by using a malicious ZIP file delivered via a Microsoft Teams message, followed by dropping AD Explorer and taking an AD (Active Directory) snapshot.

Spanish-speaking activity

BlindEagle attacks

Kaspersky researchers reported on an APT group known as Blind Eagle (APT-C-36). The group has been active since at least 2018 and targets organizations and individuals in Colombia, Ecuador, Chile, Panama, and other Latin American countries, focusing on various sectors, including government, finance, energy, oil and gas. Blind Eagle has demonstrated adaptability and flexibility in the targeting of its attacks, switching between purely financially motivated campaigns and cyber-espionage operations. The APT group is known for using spear phishing to impersonate government agencies or banking institutions to distribute various publicly available Trojans, such as AsyncRAT, BitRAT, Lime RAT, NjRAT, Quasar RAT, and Remcos RAT. The phishing emails contain a link that purports to take targets to the official website of the organization being impersonated. The emails also include a PDF or Microsoft Word file containing the same URL and, in some cases, additional details to add urgency and legitimacy to the message. The first set of URLs redirects users to subject-controlled sites hosting the initial dropper, but only if the victim has been identified as belonging to a target country; otherwise, they are redirected to the real site. The initial dropper is delivered as a compressed ZIP archive, which in turn embeds a Visual Basic Script responsible for extracting the next-stage payload from a hard-coded remote server, ranging from an image host to Pastebin, Discord, and GitHub. The second-stage malware, often disguised using steganographic techniques, is a DLL or .NET injector that then contacts another server to retrieve the final stage Trojan. The group often uses process injection techniques to execute the RAT in the memory of a legitimate process. BlindEagle uses open source RATs as the final link in its attack chain, which it modifies to suit the goals of its campaign. While BlindEagle's TTPs appear simple, their effectiveness allows the group to maintain a high level of activity.

Russian-speaking activity and targets

BlackJack attacks

The BlackJack threat actor has been targeting government, telecoms and industrial organizations in Russia, using open source tools and malware. Kaspersky research revealed that the group employed the LockBit ransomware and Shamoon wiper, written in Go, to inflict destructive damage on its victims. To maintain persistent access to compromised victim resources, the attackers used tunneling with the popular ngrok utility. BlackJack installed various remote access tools (RATs) such as Radmin utility, AnyDesk, and the PuTTY SSH client. Kaspersky's telemetry and similarity technologies have revealed overlap with other hacktivist groups, such as the Twelve group and an unattributed cluster of activity, sharing malicious tools and distinct TTPs.

ReaverBits attacks

F.A.C.C.T. researchers reported about the new ReaverBits group targeting Russian companies via malicious emails purportedly on behalf of companies and ministries. The attacks were aimed at a federal fund and Russian companies in the retail, telecommunications, manufacturing, and agro-industrial sectors. About five mailings from the group were detected, two in December 2023, two more in January 2024, and the last one in May. The group actively relies on spoofing, using MetaStealer as a payload. In one of the attacks, the group used the LuckyDownloader downloader, presumably using the services of a third-party actor tracked under the name LuckyBogdan.

Attacks with Unicorn scripts

In early September, Kaspersky researchers detected a malicious mailing designed to steal confidential data. The attack targeted Russian energy companies and industrial enterprises, as well as suppliers and developers of electronic components. The malware is distributed as an email attachment or as a file on Yandex Disk via a link in the email. The delivered RAR archive contains a file with the double extension PDF + LNK. The malicious shortcut contains a command to launch the mshta application, which downloads and executes the HTML Application (HTA) file. When HTA is launched, a malicious VBS script is executed that creates two scripts on the disk. The scripts are automatically launched by two tasks created in the scheduler and certain registry keys. The first one searches for documents, archives and images smaller than 50 MB, and also copies the contents of the Telegram Desktop folder. The second script sends the collected files to the attackers' server using the decrypted code from the registry. Kaspersky solutions detect these scripts as Trojan-Spy.VBS.Unicorn. No connections to known groups have been traced.

PhantomCore/Head Mare attacks

F.A.C.C.T. researchers tracked new activities and cyberattacks by the PhantomCore group, which has been targeting Russian organizations since early 2024. F.A.C.C.T. first reported on the activities of the PhantomCore cyber-espionage group in March, naming the group after its unique remote access Trojan, PhantomRAT. The attackers were able to rewrite their PhantomRAT from C# to Go, enriching it with additional commands. In addition, the hackers developed PhantomDL loader version 3 (v.3), and then released another version (v.4), which they partially supplemented with PhantomRAT capabilities. Using these tools, the group managed to carry out a number of new attacks against various Russian facilities: an instrumentation manufacturer, a polymer materials plant, a mechanical plant, a technology park, a leasing company, an oil and gas company, and an IT company. Analyzing the observed attacks, the researchers noted that the attackers first compromise third-party organizations and use them to launch attacks on the primary targets. In particular, they send malicious emails from compromised email addresses and place malware in the infrastructure of the hacked organizations. The attackers were able to compromise a household and industrial chemical manufacturer, a software developer, a medical device developer and integrator, a distributor of metallurgical products, and a construction company for use in further attacks.

On September 5, F.A.C.C.T. researchers detected new attacks by the PhantomCore group targeting an IT company, a design bureau, and a manufacturer of high-tech wireless communication equipment in Russia. Throughout the spring and summer, PhantomCore attacked Russian organizations in various sectors, but the majority were in the industrial sector. A distinctive feature of the attackers' activities is that they first compromise third-party organizations and use them to launch attacks via phishing emails.

Researchers noted several mailings from a likely compromised address belonging to a company specializing in the construction and automation of power and transport facilities. The attackers sent phishing emails with a password-protected archive attached. The archive contained a legitimate PDF bait and an executable malicious file. When the archive is opened, the CVE-2023-38831 vulnerability was used to automatically launch the program. The main tool used was the PhantomCore.KscDL_trim malware, which is a stripped-down version of the PhantomCore.KscDL loader written in C++ and packed with the UPX tool. The loader has the following capabilities: downloading and running files from a C2 address, executing arbitrary commands in the Windows command interpreter. During analysis, the researchers were able to obtain several commands from the command and control server and established that the attackers pre-profile the victim and decide whether they are of interest for developing the attack.

Kaspersky researchers believe that the hacktivist group known as Head Mare, which appeared in 2023, is behind the PhantomDL and PhantomRAT attacks. As part of Kaspersky’s investigation into attacks on organizations based in Russia, the researchers were able to determine how and with what tools Head Mare carries out its attacks, and to establish a connection with malicious activity investigated by F.A.C.C.T. to gain initial access. They confirmed that the group carries out various phishing campaigns in which it distributes RAR archives that exploit CVE-2023-38831 in WinRAR, enabling the execution of arbitrary code in the system. The group uses custom PhantomDL and PhantomCore malware for initial access and exploitation. For other tasks, Head Mare primarily uses publicly available software in its attacks, such as Sliver (the main C2 framework for attackers), ngrok, rsockstun (both used for pivoting), XenAllPasswordPro, and Mimikatz. In addition, Head Mare uses LockBit and Babuk ransomware in its attacks (generated using a publicly available builder). The attackers create scheduler tasks and registry values named MicrosoftUpdateCore and MicrosoftUpdateCoree to disguise their activity as tasks related to Microsoft software. Many of the tools used by Head Mare had names typical of legitimate programs and were located on standard or standard-like paths. The malware samples analyzed were predominantly found in organizations based in Russia, but there were also a few samples in Belarus. The organizations targeted by this group primarily operate in sectors related to government, manufacturing, technology, energy, transportation, and entertainment.

Unit 29155 attacks

The US Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and security agencies from nine other countries published a joint Cybersecurity Advisory (CSA) on September 5 highlighting the activities of Unit 29155, which they believe is linked to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (formerly the GRU). They believe Unit 29155 is responsible for targeting the Ukrainian government, critical infrastructure organizations, and key resource sectors, including the government services, financial services, transportation systems, energy, and healthcare sectors of NATO members, the EU, as well as Central American and Asian countries. WhisperGate wiper attacks are linked to Unit 29155. The document lists technical details, including the vulnerabilities the threat actors exploited to gain initial access, indicators of compromise, and tactics, techniques and procedures. Unit 29155 cyber actors use common red team techniques and publicly available tools to conduct cyber operations. The actors are known to use VPNs to anonymize their operational activity and attempt to exploit weaknesses in internet-facing systems. Five officers from Unit 29155, along with one civilian, have been indicted in the US for alleged attacks in Ukraine and 26 NATO countries.

Librarian Ghouls attacks

In early July, Kaspersky researchers reported a new wave of targeted attacks in which attackers sent malicious files disguised as documents in order to collect sensitive information from computers belonging to various companies. Since then, Kaspersky has continued to monitor the activity of the group dubbed Librarian Ghouls and has identified changes in their tactics. The targets of the new attacks included companies engaged in design and development in various industries, research institutes, rocket, space and aviation companies, as well as enterprises operating in the gas processing, petrochemical and defense sectors. In addition, manufacturers of diving equipment, communications and radar systems, automotive components, automated control systems and semiconductor devices were targeted.

The attack method remained the same: malicious files are distributed as RAR archives containing fake documents in the .SCR format. Once launched, the .SCR malware downloads additional malicious components to the computer, collects the data of interest, and sends it to the attackers' server. The group's goals and the format of the collected data have changed: instead of focusing solely on office documents and data from the Telegram messenger, the attackers have begun to target files related to software for modeling and designing industrial systems. Several extensions typical of highly specialized software were added to the list of files collected by the malware, such as files for the SolidWorks automated design system used for industrial design, the Russian KOMPAS-3D CAD system, .m3d files used by various programs for creating three-dimensional models of objects, .dwg files used by CAD software packages such as AutoCAD, CorelCAD and others. In addition, the malware began to steal documents in *.pdf format.

Attacks with Loki agent

Kaspersky researchers discovered a previously unknown Loki backdoor that was used in a series of targeted attacks in July. More than a dozen Russian companies from various industries, including mechanical engineering and healthcare, have already been hit by this threat, but the number of potential victims may be higher. By analyzing the malicious file and open sources, the researchers determined that Loki is a private version of an agent for the open source Mythic framework. The discovered Loki agent is a Mythic-compatible version of an agent for another framework, Havoc. However, unlike the agent for Havoc, Loki has been split into a loader and a DLL where the main functionality of the malware is implemented. Both versions of the agent use the djb2 hashing algorithm to hide functions and API commands, with minor differences. Once executed, the Loki loader generates a packet containing information about the infected system and sends it encrypted to the C2 server. In response, the server sends a DLL that executes in memory. After a detailed analysis, the researchers managed to find about 15 versions of the loader and two active C2s, and eventually obtained a sample of the main DLL module from the May version. The main module, like the loader, is based on the Havoc agent version, but the list of supported commands is partially borrowed from other Mythic agents. It is not stored as plain text in the DLL – instead a series of hashes are specified in the library code. When a command is received from the server, its name is hashed and compared with the hash stored in the DLL. The agent itself does not support traffic tunneling, so the attackers use the publicly available third-party utilities ngrok and gTunnel to access private network segments. Due to insufficient data, Loki could not be assigned to any group.

Stone Wolf attacks

BI.ZONE researchers uncovered a new hacker group dubbed Stone Wolf, which is using the commercial infostealer Meduza to attack Russian organizations. The attackers send phishing emails in the name of a legitimate organization involved in industrial automation with the aim of delivering the Meduza stealer. As part of the detected campaign, Stone Wolf distributed an archive named Dostavka_Promautomatic.zip containing three files: a digital signature, a *.p7s file, a legitimate decoy *.docx document, and a malicious link disguised as a PDF document (Scan_127-05_24_dostavka_13.05.2024.pdf.url). After accessing the malicious link, a file located on a remote SMB server was downloaded and executed, ultimately delivering the Meduza stealer. According to the Meduza developers, the executable file has a built-in module that limits the possibility of implementing attacks in the CIS, but the sample in question had no such check. The stealer gathers system information: OS version, device name, time, information about the processor, RAM and graphics adapter, screen resolution and external IP of the device. In addition, it has the functionality to steal credentials from Outlook, browsers, crypto wallets, Telegram and Steam sessions, Discord tokens, password managers, data from Windows Credential Manager and Windows Vault, as well as read the list of active processes and installed applications. The collected data is sent via TCP to the C2 server.

CMoon worm attacks

In late July, Kaspersky researchers discovered a previously unknown malware that was distributed via the website of a Russian energy company. The attackers replaced links to download regulatory documents in several sections of the resource with others that led to malicious executable files. In total, the attackers replaced approximately two dozen links on the energy company's website, each of which downloaded a self-extracting archive. It contained the original document and the same executable file – a new piece of malware that Kaspersky analysts dubbed CMoon, after the strings in the malicious file's code. The complexity of the attack indicates that it was aimed at visitors to a specific organization's website and was carefully prepared.

CMoon is capable of downloading confidential and payment data from an infected device, launching DDoS attacks, and spreading to other devices. The worm was able to search for files from the user's Desktop, Documents, Photos, Downloads and external media folders that contained the substrings “secret”, “service”, “password” and other keywords in the text and send them to the attackers' server – a sign of a targeted attack. Files containing information about system protection, user actions and their credentials could also be downloaded. The malware was also able to take screenshots. Files containing saved passwords, cookies, bookmarks, browsing history, and information for autofilling forms, including credit card information, could be collected from web browsers. The worm can also monitor connected USB drives. The company was notified of the compromise and the malicious files and links were removed from the site on July 25.

OldGremlin attacks

F.A.C.C.T. researchers reported the return of the OldGremlin ransomware gang, which attacked Russian companies in 2020-2022. The group had been inactive since September 2022, but almost two years later, the attackers made a comeback by sending a new mailing and using a new tool, OldGremlin.JsDownloader. F.A.C.C.T. discovered an email uploaded to AnyRun in the name of a Diadoc employee using the address makarova@diadok[.]net, the recipient of which was an employee of a large Russian petrochemical company. The email was sent on August 12, and the diadok[.]net domain from which the malicious email was sent mimics the original domain of the Kontur.Diadoc company – diadoc[.]ru. The email included a link to download “invoice.xlsx”. Clicking the link downloaded an archive containing an LNK file that connected to a WebDav server and executed a command to download a next-stage JavaScript file and legitimate Node.js interpreter that is used to launch this JavaScript file. Running this script opens a decoy XLS file via the WebDav path and also decodes and runs a malicious downloader (OldGremlin.JsDownloader) in Base64 format. This OldGremlin.JsDownloader retrieves, decrypts and executes the next JavaScript code from a C2 server.

Other

UAC-0180 attacks

CERT-UA has warned of malicious activity by the UAC-0180 group targeting Ukrainian defense enterprises. The attackers distribute fake emails related to procurement in an attempt to trick their targets into opening an attached ZIP file containing a PDF document. If the target clicks the attachment, it triggers the execution of the GLUEEGG malware, which decrypts and executes the DROPCLUE loader. This starts an infection chain that results in the installation of legitimate ATERA remote management software.

FrostyGoop attacks

Previously unseen malware dubbed FrostyGoop is believed to have been used in a targeted attack on a municipal district energy company in Ukraine that provides central heating to more than 600 apartment buildings in Lvov. The attack targeted the utility's ENCO temperature controllers, first by downgrading the firmware to a version that does not send telemetry, and second by sending commands to the controllers causing them to report inaccurate readings. According to Dragos, this "resulted in the disruption of power to the heating system". FrostyGoop is an ICS-specific tool written in Golang – it is believed this is the first reported case involving the use of the Modbus protocol to directly affect systems. FrostyGoop can read and write to an ICS device that holds registers containing inputs, outputs, and configuration data. It accepts optional command line execution arguments, uses separate configuration files to specify target IP addresses and Modbus commands, and logs output to a console and/or JSON file. Investigation of the attack in Ukraine revealed that the adversaries may have gained access to the victim's network through an unspecified vulnerability in an externally facing Mikrotik router. The network assets, including the Mikrotik router, four management servers, and district heating system controllers, were not adequately segmented, which facilitated the attack.

Attacks on transportation and logistics in North America

Proofpoint detected a campaign targeting the transportation and logistics sector in North America. Proofpoint had been tracking the activity since late May and said it could not attribute it to a specific threat actor, but determined that the group is likely financially motivated. The hackers use compromised legitimate email accounts belonging to transportation and shipping companies, and then injected Google Drive URLs that led to an internal URL file, or attached a URL file into existing conversations. When clicked, malware such as Lumma, StealC, NetSupport, DanaBot, or Arechclient2 is installed – all designed to steal information from the victims' devices. Proofpoint identified at least 15 compromised email accounts used in the campaign, but it remains unclear how the hackers gained access to those accounts. The campaigns also used dialog boxes referencing Samsara, AMB Logistic, and Astra TMS – software that would only be used in transportation and fleet operations management – to leverage a technique called ClickFix. The dialog boxes trick users into copying, pasting and running a Base64-encoded PowerShell script contained within the HTML. The PowerShell scripts led to an MSI file that was used to load DanaBot.

RansomHub attacks

The US Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), and Department of Health and Human Services (HHS) issued a joint Cybersecurity Advisory (CSA) on August 29 containing information relevant to the RansomHub ransomware-as-a-service (RaaS) group (formerly known as Cyclops and Knight). Since its inception in February 2024, RansomHub has encrypted and exfiltrated data from at least 210 victims from sectors including water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, communications, and critical infrastructure. The document lists technical details, including the vulnerabilities that RansomHub threat actors exploit to gain initial access, as well as indicators of compromise and tactics, techniques and procedures. After initial access, RansomHub affiliates created user accounts for persistence, re-enabled disabled accounts, and used Mimikatz. The affiliates then moved laterally inside the network using methods such as RDP, PsExec, AnyDesk, Connectwise, N-Able, Cobalt Strike, Metasploit, and others. Data exfiltration has been observed through the use of tools such as PuTTY, Amazon AWS S3 buckets/tools, HTTP POST requests, WinSCP, Rclone, Cobalt Strike, Metasploit, and other methods. The agencies also listed BITSAdmin, Sliver, SMBExec, CrackMapExec, Kerberoast and AngryIPScanner among the tools used.

Attacks abusing Microsoft Sway

According to Netskope Threat Labs, a massive QR code phishing campaign abused Microsoft Sway, a cloud-based tool for creating online presentations, to host landing pages designed to trick Microsoft 365 users into handing over their credentials. The attacks were spotted by researchers in July 2024 after they noticed a 2,000-fold increase in traffic to phishing pages served through Microsoft Sway. This spike is in stark contrast to the minimal activity reported in the first half of the year, indicating the large scale of this campaign. The primary targets were users in Asia and North America, in the technology, manufacturing, and financial sectors. The emails directed potential victims to phishing landing pages where they were asked to scan QR codes that redirected them to other malicious websites. The attackers used a transparent phishing technique that abused the Cloudflare Workers free tier service to act as a malicious reverse proxy server for legitimate login pages. This allowed them to steal the credentials and multi-factor authentication codes for the victims' Microsoft accounts while displaying the legitimate login page. The attackers also used Cloudflare Turnstile, a tool intended to protect websites from bots, to hide the phishing content of their landing pages from static scanners, helping to maintain the phishing domain's good reputation and avoid being blocked by web filtering services.

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