Kaspersky ICS CERT

APT and financial attacks on industrial organizations in Q2 2024

03.10.2024

Version 1.0

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

The second quarter of 2024 was rich in interesting technical details of disclosed attacks on industrial organizations. Advanced attackers continue to demonstrate unconventional approaches to solving their tasks. Creating fake profiles on social networks and mockups of entire companies to gain the trust of potential victims has been seen before, but developing a full-fledged IT product, such as a computer game – a tank simulator with a Trojan inside – is something new. No effort or resources were spared in the preparation.

Attackers are often aided by developers of security tools. The magnitude of failures is especially great when a solution is not a natural response to a security challenge, but rather a formal requirement dictated by foreign policy, situational circumstances, established traditions, or – as happened in South Korea – a mix of all these factors. Attackers have long begun to exploit the chaos surrounding the "security applications" required by local banks to work with client portals created by South Korean developers. An interesting target and means of spreading malware is WIZVERA VeraPort – an orchestrator application that helps install these very same "security applications." And while this vector was previously used mainly to attack banks and their customers, more recently the victims have been visitors to the website of an association related to the construction sector.

Reading the reports of research teams, it is both curious and alarming to observe how the threat landscape for industrial enterprises is evolving in line with our forecasts. Attackers are changing their targets and breaking traditional notions of their modus operandi. Financially motivated groups are getting involved in geopolitical confrontations and joining hacktivism. An APT targeting maritime logistics attacks not only office and port systems but also ships, and ICS systems suddenly become entry points for attacks targeting not production assets, but corporate resources and office systems – reaching them from the technological network through an ICS product developed by a "domestic" vendor not very concerned with security becomes easier than directly from the internet.

Southeast Asia and Korean Peninsula

Andariel attacks

Researchers at the AhnLab Security Intelligence Center (ASEC) have uncovered attacks by the threat actor Andariel (aka Onyx Sleet) targeting educational institutions and manufacturing and construction businesses in South Korea. The attackers employed tools they had already used in previous attacks, including a keylogger, infostealer, proxy tools and the Nestdoor backdoor. They also used a new backdoor called Dora. The Dora RAT is relatively simple malware that supports reverse shell and file download/upload functions.

Kimsuky attacks

In December 2023, ESET detected Kimsuky malware on several machines belonging to a construction-related entity in South Korea. Analysis of the attack revealed that the malware was downloaded and executed by employees on the entity's compromised servers running the WIZVERA VeraPort solution. According to ESET, the attack continued until January 2024. The malware was only available for download during specific time frames. Outside of these time frames, the compromised servers served legitimate binaries. This was confirmed in an AhnLab report published in February 2024. In additionally, AhnLab estimated the total number of affected machines to be over 3,000, indicating that this attack had a relatively large number of victims.

In mid-2023, Kimsuky was observed using AlphaSeed, a newly developed malware written in Go, as well as proxy malware. Throughout the rest of 2023 and early 2024, Kimsuky continued the trend of developing new malware strains in Go. In particular, various security vendors described and named TrollAgent, Endoor, and Nikidoor. ESET researchers attribute all of this new malware to the Kimsuky AppleSeed cluster.

According to a BlackBerry research post, Kimsuky has targeted a weapons manufacturer in Western Europe in a sophisticated cyber-espionage campaign. The threat actor used the General Dynamics brand as a lure in a spear-phishing email containing a malicious JavaScript file. The JS file decodes a lure PDF file and an executable library, which is a new espionage tool containing functions for remote execution by the attacker.

SmallTiger malware attacks

The AhnLab Security intelligence Center (ASEC) discovered cases where a downloader named SmallTiger was used to attack South Korean businesses, including defense contractors, automotive parts manufacturers, and semiconductor manufacturers, among other confirmed targets. The initial access method has not yet been identified, but the threat actor distributed SmallTiger to the companies' systems during the lateral movement phase. The unidentified actor's attacks were first observed in November 2023. The threat actor exploited the companies' software update programs during the internal propagation phase. The backdoor installed at the end was DurianBeacon, a malware strain found in previous attacks by Andariel. The same threat actor resumed the attacks in February 2024, and the final distributed malware was replaced by SmallTiger. Researchers believe the attacks are also related to Kimsuky group. As of May 2024, the malware was still being used in attacks.

Moonstone Sleet attacks

A new threat actor, dubbed Moonstone Sleet by Microsoft researchers (formerly tracked as Storm-1789), has been targeting individuals and organizations in the software, IT, education and defense industrial base sectors using social engineering tactics. The attackers established fake companies that engage with potential targets via email and social networks, used Trojanized versions of legitimate tools (such as PuTTY) and malicious npm packages, and even created a fully functional tank game that loads a custom malware loader DLL Microsoft tracks as YouieLoad. The threat actor's primary goal is espionage. But the actor is also interested in financial gain. In April 2024, Microsoft observed Moonstone Sleet delivering a new custom ransomware variant, dubbed FakePenny, against a company it had previously compromised in February. According to researchers, Moonstone Sleet initially overlapped with Diamond Sleet, but later shifted to its own infrastructure and attacks, establishing itself as a separate threat actor.

Xctdoor malware attacks

The AhnLab Security Intelligence Center (ASEC) identified an attack using the Xctdoor malware that targeted South Korean companies in the defense and manufacturing industries. In one case, the attackers infiltrated systems by targeting the update server of a South Korean enterprise resource planning (ERP) solution. They inserted a malicious routine to execute a DLL from a specific path into the update program of the ERP solution. This method is similar to a case in 2017, when the Andariel group used it to install the HotCroissant backdoor. In another attack case, a vulnerable web server was attacked to distribute malware.

LilacSquid attacks

A previously undocumented cyber-espionage threat actor, dubbed LilacSquid by Cisco Talos, has been linked to targeted attacks as part of a data theft campaign since at least 2021. Targets include information technology organizations developing software for the research and industrial sectors in the USA, energy companies in Europe, and the pharmaceutical sector in Asia. The attack chains are known to either exploit publicly known vulnerabilities to breach internet-facing application servers or use compromised RDP credentials to deliver a mix of open-source tools and custom malware. The most distinctive feature of the campaign is the use of an open-source remote management tool called MeshAgent, which delivers a customized version of the Quasar RAT codenamed PurpleInk. In the case of infection methods that leveraged compromised RDP credentials, the threat actors chose to either deploy MeshAgent or use a .NET-based loader dubbed InkLoader to drop PurpleInk. Cisco Talos identified another custom tool called InkBox that the adversary used to deploy PurpleInk before the switch to InkLoader. The use of MeshAgent is notable because it was previously used by the Andariel threat actor, an offshoot of the Lazarus group. Another overlap with Andariel/Lazarus is the use of tunneling tools to maintain secondary access, with LilacSquid using Secure Socket Funneling (SSF) to create a communication channel to its infrastructure.

Transparent Tribe attacks

According to BlackBerry researchers, the threat actor Transparent Tribe (aka APT36, ProjectM, Mythic Leopard, Earth Karkaddan) is responsible for attacks carried out between late 2023 and April 2024 that targeted the Indian government, defense and aerospace sectors using cross-platform malware written in Python, Golang and Rust. A notable feature of the actor's spear-phishing campaign is the abuse of popular online services, including Discord, Google Drive, Slack and Telegram, to deliver malicious payloads using malicious ZIP archives or links. Transparent Tribe first used ISO images as an attack vector in October 2023, which BlackBerry noted in Transparent Tribe's current campaigns. The researchers also discovered a new Golang-compiled "all-in-one" espionage tool used by the group that can find and exfiltrate files with popular extensions, take screenshots, upload and download files, and execute commands. The researchers also observed the distribution of a Python downloader script compiled into ELF binaries.

Chinese-speaking activity

APT31 attacks

Following the March publication of the US Department of Justice's indictment of seven hackers associated with APT31 (aka BRONZE VINEWOOD, Judgment Panda and Zirconium), researchers have been reviewing the indictment. They believe it contains information consistent with existing knowledge of APT31's tradecraft and the nature of cooperation between public and private Chinese entities in cybercrime matters. APT31 has targeted high-profile entities in the Western world. The targets named in the indictment include government, defense and industrial organizations, such as a US steel company and various aerospace companies. The indictment provides a comprehensive view of the group's interests, ranging from diplomatic intelligence to the theft of trade secrets and financial data. Moreover, researchers believe the fact that call data records for "millions of Americans" were obtained by the attackers indicates that at least one US telecoms provider was compromised.

Mustang Panda attacks

In the first quarter of 2024, ESET researchers identified the presence of Chinese-language APT Mustang Panda (aka Stately Taurus, Bronze President, Earth Preta, HoneyMyte, Camaro Dragon, RedDelta) Korplug loaders on computer systems belonging to cargo shipping companies based in Norway, Greece, and the Netherlands, including some that appeared to be on board the cargo ships themselves. These samples have been used in previous campaigns, suggesting that Mustang Panda operators are reusing samples across multiple campaigns. In some instances, the initial dropper appears to have been launched from a USB drive and had filenames such as Usb Disk(29GB).exe or SONY_8GR.exe.

Some of the samples deployed at these cargo shipping companies have invalid Authenticode signatures and probably used DLL search order hijacking against an old version of Nero WaveEditor. One invalid signature was copied from a binary legitimately signed by Klaas Nekeman. Another sample used a signature copied from a binary legitimately signed by AVG Technologies USA, a firm specializing in computer security.

RedJuliett attacks

From November 2023 to April 2024, Insikt Group researchers identified cyber-espionage activities by RedJuliett targeting government, academic, technology (especially electronics), and diplomatic organizations in Taiwan.

The group also targeted organizations in Hong Kong, Malaysia, Laos, South Korea, the USA, Djibouti, Kenya, and Rwanda. RedJuliett exploited vulnerabilities in firewalls, VPNs, and load balancers to gain initial access. The group also used SQL injection and directory traversal exploits. It also created a SoftEther VPN bridge or client in victim networks. Additionally, the group conducted reconnaissance and attempts at exploitation using Acunetix Web Application Security Scanners. Post-exploitation, the group used open-source web shells and exploited an elevation of privilege vulnerability in the Linux operating system. RedJuliett's activities are consistent with aliases Flax Typhoon and Ethereal Panda.

UNC3886 attacks

In recent years, a cyber-espionage actor tracked by Mandiant as UNC3886 has used publicly available open-source rootkits, called “Reptile” and “Medusa”, to hide on VMware ESXi virtual machines. UNC3886 has also made use of custom malware such as “Mopsled” and “Riflespine”, using GitHub and Google Drive for C2 communications. The threat actor has targeted organizations in the government, telecoms, technology, aerospace, defense and utilities sectors in North America, Southeast Asia and Oceania, with other targets in Europe, Africa and elsewhere in Asia. The group has exploited vulnerabilities in FortiOS (CVE-2022-41328) and VMware technologies (CVE-2022-22948, CVE-2023-20867), including a zero-day vulnerability in VMware vCenter (CVE-2023-34048).

Middle East-related activity

POLONIUM attacks

In November 2023, ESET researchers observed that POLONIUM, a threat actor aligned with Hezbollah interests, used a Python backdoor MegaPy and an exfiltrator to exploit four Israeli organizations in the technology and social services sectors. The backdoor uses MEGA and Nextcloud for C&C communication and, in the case of the exfiltrator, to store data. An interesting feature of the exfiltrator is that it uses the WebDAV protocol. Then, in January 2024, POLONIUM deployed an update of its Python backdoor to construction, manufacturing, and healthcare companies in Israel. This iterative update employs encrypted payloads with customized content for each victim, probably to mask some of the exploit chain from defenders and make it more difficult for researchers to track. During this campaign, POLONIUM changed the service providers it used for its C&Cs: Supabase and Backendless. In one particular case, the initial payload was hosted on a typo-squatting domain: yutube.com[.]de.

MuddyWater attacks

Beginning in late October 2023, researchers observed a significant increase in the use by MuddyWater (aka Mango Sandstorm, Boggy Serpens) of installation packages for legitimate RMM (remote monitoring and management) tools called Atera Agent and Tactical RMM. The tools seen in this campaign were registered using a mix of compromised business and personal user email accounts. The threat actor uses free file hosting platforms to host these RMM installers (as it has done with other RMM installers in the past), employing spear-phishing emails to direct recipients to these files. Furthermore, researchers observed abuse of the AutodialDLL registry key using PowerShell through a scheduled task to side-load the malicious DLL and install/deploy the C2 framework.

MuddyWater targeted various organizations in Israel, India, Alegria, Turkey, Italy and Egypt. Based on the accounts used to register Atera Agent and analyzed emails, researchers believe MuddyWater targeted the following types of organizations between October 2023 and April 2024: airlines, IT, telecommunications and pharmaceutical companies, automotive manufacturers, logistics companies, travel and tourism agencies, employment/immigration services, as well as small businesses.

Russian-speaking activity and targets

Sandworm attacks

WithSecure researchers have observed a previously undocumented backdoor called Kapeka being used in attacks against targets in Central and Eastern Europe since at least mid-2022. Kapeka functions as a versatile backdoor, providing both initial toolkit capabilities and long-term access to victims. Kapeka includes a dropper that loads and executes a backdoor component on the target computer, after which it removes itself. Researchers found overlaps between Kapeka, GreyEnergy and Prestige ransomware attacks, suggesting that Kapeka is a new addition to the Sandworm (aka APT44 and Seashell Blizzard) toolset. In February, Microsoft discovered a backdoor with similar characteristics to Kapeka and named it KnuckleTouch. WithSecure confirmed to Recorded Future News that KnuckleTouch and Kapeka are the same backdoor. WithSecure said it found traces of Kapeka in mid-2023 while analyzing an attack on an Estonian logistics company that occurred in late 2022.

According to a report released on April 19 by Ukraine's computer emergency response team (CERT-UA), hackers deployed several new and previously known malware variants to infect about 20 power, water, and heating utilities in 10 regions of the country in March. Sandworm used the Kapeka backdoor in the latest attacks on Ukraine's critical infrastructure. CERT-UA also identified new Linux-based variants of Kapeka developed by Sandworm, called Biasboat. The Linux payload injector using the ptrace API was called Loadgrip. Biasboat and Loadgrip were installed on Ukrainian Linux devices designed to automate technological processes in critical facilities. The compromised Linux ICS computers were running "special purpose software" from an unnamed Ukrainian developer that contained vulnerabilities and backdoors. The agency confirmed that at least three successful supply chain attacks by the hackers for three initial compromises correlate with the first installation of the software. This suggests the attackers either exploited vulnerabilities in the software or compromised suppliers to gain access to target systems. The compromised systems of critical infrastructure objects were then used for lateral movement to the corporate networks of the enterprises. The attackers also deployed Gossipflow malware, a tunneling tool that provides SOCKS5 proxy functionality using the Yamux multiplexor library on computers running Windows OS. Since 2022, Gossipflow has been used by Sandworm in conjunction with SDELETE in destructive attacks on water supply facilities in Ukraine. According to researchers, one of the factors that led to these attacks was a lack of server isolation and software security practices by suppliers that could lead to RCE.

Forest Blizzard/STRONTIUM/Fancy Bear attacks

Microsoft Threat Intelligence researchers have published the results of their investigation into malware developed by Forest Blizzard (aka Strontium and Fancy Bear). Since at least June 2020, the threat actor has used a tool dubbed "GooseEgg" to exploit a Windows Print Spooler vulnerability (CVE-2022-38028) to elevate privileges and steal credentials from compromised systems. The threat actor has targeted entities in Ukraine, Western Europe and North America, as well as non-governmental organizations and the education and transportation sectors.

FIN7 attacks

In late 2023, BlackBerry analysts detected a spear-phishing campaign launched by FIN7 (aka Carbon Spider, Elbrus and Sangria Tempest) targeting a US-based automotive manufacturer. BlackBerry said its cyber defenders detected the campaign early on, locating an infected system and isolating it before hackers had a chance to penetrate deeper into the network through lateral movement. BlackBerry attributed the attack to FIN7 with high confidence based on the group's signature obfuscation techniques. In this campaign, the group used spear-phishing emails containing links to a malicious URL – "advanced-ip-sccanner.com" – designed to mimic a legitimate IP scanning website. The website ultimately redirected victims to an attacker-owned Dropbox account, where they unknowingly downloaded a malicious executable that reads and decrypts a .wav file to extract the encoded payload. The initial payload initiated a multi-stage execution process to deploy the final payload, a backdoor known as Anunak or Carbanak. BlackBerry's analysis of the attacker's network infrastructure revealed an interconnected network of domains and proxy servers used by FIN7 to facilitate delivery and maintain access to compromised systems.

Hellhounds attacks

Researchers at Positive Technologies have reported a continuation of attacks against Russian companies by the Hellhounds threat actor, with at least 48 companies attacked, including public sector, IT, aerospace, energy, transportation and logistics, and mining companies. They discovered previously unreported attacks on Windows-based infrastructure, in addition to previously known TTPs and attacks on Linux hosts. Hellhounds has been successfully targeting Russian companies since at least 2021. The threat actor is believed to compromise target networks through supply chain attacks. Hellhounds disguises its tools as legitimate software processes. While virtually the entire Hellhounds toolkit is based on the open-source Pupy RAT project and is almost identical to the previously analyzed Decoy Dog for Linux, the threat actor has been able to evade malware defenses and maintain persistence in target networks.

PhantomCore attacks

F.A.C.C.T. researchers have found a new malicious downloader PhantomDL (PhantomGoDownloader), which is probably closely related to the cyber-espionage group PhantomCore and has been in use since March 2024. Since January 2024, PhantomCore has been targeting organizations in Russia that are likely related to the military-industrial complex.

At the end of March, researchers found a password-protected RAR archive on the VirusTotal platform that contained an executable file and a legitimate PDF file. The decoy document contained information about the act of acceptance and transfer of a construction site for work on the territory of a Russian enterprise from the nuclear industry. The attackers used a variant of CVE-2023-38831 in WinRAR. The executable file is a loader written in the Go language and presumably obfuscated using the Garble utility. Just over a month after the initial discovery of the Go loader, researchers were able to identify a new sample that, unlike the earlier one, did not obfuscate classes and methods. This allowed the researchers to identify the project name

D:\github\phantomDL and assign the name PhantomDL to this loader. The researchers found overlaps between the PhantomDL loader and PhantomRAT, which is known to be the main tool of the PhantomCore APT.

Werewolves attacks

Researchers at F.A.C.C.T. reported a new wave of attacks with malicious mailings from the Werewolves ransomware group, which specializes in extortion using a version of the LockBit3 (Black) ransomware program compiled from a leaked builder. In early April, the extortionists were observed carrying out mass mailings on the topic of the spring military draft and court cases. The targets of the new attacks were Russian industrial enterprises, telecommunications and IT companies, financial and insurance organizations. Using the HTTrack Website Copier, the attackers created a fake website of a large Russian manufacturer of special equipment, completely copying the content of the original portal. They registered the same domain name, but in the .ru zone (the original was in .com). Emails with the subject "Court case" and "Complaint" contained malicious attachments that downloaded Cobalt Strike Beacon. After the victim opens the attached document "Complaint.doc", an RTF document is downloaded that exploits the CVE-2017-11882 vulnerability. An HTA (HTML application) is delivered to the victim's device, which executes a PowerShell command. This command unpacks and runs the Cobalt Strike Stager shellcode, which loads the Cobalt Strike Beacon with the specified watermark in its configuration.

Sapphire Werewolf attacks

BI.ZONE researchers reported the activity of Sapphire Werewolf, which carried out attacks for the purpose of cyber-espionage. Since March 2024, Sapphire Werewolf has conducted more than 300 attacks against Russian organizations in the education, industrial, IT, military-industrial complex and aerospace sectors using the Amethyst stealer, which is based on the open-source program called SapphireStealer. The attackers distributed the malware using phishing emails under the guise of a resolution to initiate legal proceedings, a Central Election Commission information bulletin, and a decree of the President of the Russian Federation. The dropped stealer collects Telegram messenger configuration files, files with various extensions and from external media, data from browsers (Chrome, Opera, Yandex, Brave, Edge, etc.), as well as PowerShell usage logs and FileZilla and SSH configurations. The collected data is archived and sent to the C&C, and in the latest stealer versions, a password-protected archive is created. The C&C server for sending the archive is implemented on the basis of a Telegram bot. The bot token is stored in the stealer.

Sticky Werewolf attacks

Threat actor Sticky Werewolf, believed to be a hacktivist group, has targeted organizations in the aviation industry in Russia and Belarus in a new phishing campaign, according to a Morphisec report. Having previously targeted government agencies, the attackers have now expanded their choice of targets to include a pharmaceutical company and a research institute. The phishing emails purported to be from the general director of Moscow-based aircraft and spacecraft manufacturer AO OKB Kristall, and used password-protected archives, two LNK files, and a fake PDF document. Clicking on the LNK file resulted in the installation of commodity RATs and infostealers designed to steal sensitive data, including the Rhadamanthys and Ozone RATs.

Shedding Zmiy attacks

Solar 4RAYS researchers have released a report describing the activities of the Shedding Zmiy hacker group, which has attacked dozens of Russian companies in the energy sector, public sector, IT and other sectors since the beginning of 2022 with the goal of cyber-espionage. The attackers used compromised data from Russian companies not only for subsequent attacks, but also published them in the public domain, mainly in pro-Ukrainian Telegram channels. Each time, the hackers managed to change their arsenal beyond recognition, finding new methods of attack: custom loaders, backdoors and web shells. Researchers associate Shedding Zmiy with the Cobalt ((ex)Cobalt) group, known since 2016, which, according to public reports, exclusively attacked credit and financial organizations, pursuing only material gain.

In total, researchers found traces of the use of 35 different tools for reconnaissance, privilege escalation, malware delivery, lateral movement and data theft. Both publicly available and the group's own unique malware are used. The attackers used up to 20 known vulnerabilities in common corporate software to penetrate the network, elevate privileges and gain a foothold. In addition to technical means, Shedding Zmiy is also skilled in social engineering. The group has learned to cover its tracks perfectly: it has an extensive network of C2 servers in Russia and abroad, renting resources from hosting providers and on cloud platforms to avoid GeoIP blocking. Researchers combined seemingly disparate incidents with similar signs of malware, vulnerability, and infrastructure use into a single cluster.

Other

ChamelGang attacks

Researchers at SentinelLabs and Recorded Future tracked two distinct clusters of activity targeting government and critical infrastructure sectors globally between 2021 and 2023. Cyber-espionage actors, particularly the APT group ChamelGang, have been using ransomware as a final stage in their operations. ChamelGang used CatB ransomware to target AIIMS in India and the Brazilian presidency in 2022. They also attacked a government organization in East Asia and critical infrastructure in the Indian subcontinent in 2023. Another cluster of attacks involving the BestCrypt and BitLocker encryption tools affected various industries in North America, South America, and Europe, primarily targeting the US manufacturing sector. The attribution for the secondary cluster remains unclear, but there are overlaps with previous intrusions that involve artifacts associated with suspected Chinese and North Korean APT clusters.

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