Kaspersky ICS CERT

APT and financial attacks on industrial organizations in Q1 2024

10.06.2024

Version 1.0

This summary provides an overview of the reports of APT and financial attacks on industrial enterprises that were disclosed in Q1 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.

As always, social engineering (phishing) and exploitation of vulnerable internet-facing devices were the most common methods used to penetrate a target organization. Vulnerabilities in the Ivanti Secure VPN solution and a Microsoft Outlook vulnerability were zero-days at the time they were exploited, requiring a great deal of effort and some luck for the targeted organizations to detect the attacks in their early stages. Enterprises considering protection against such threats should pay close attention to their information infrastructure. It should be divided into separate security domains in such a way that the compromise of one system, even a very important one, does not automatically allow the attacker to gain access to adjacent systems and move laterally in the infrastructure. This requires a lot of effort and investment, including highly qualified personnel.

The other cases demonstrate that while timely patching of internet-facing systems and educating personnel may not look like rocket science, in the real world even mature organizations with ample budgets and all the policies and procedures in place can still be compromised.

One case stands out for detailing an adversary-in-the-middle (AitM) scenario used to deliver a malicious implant instead of legitimate software updates and to hide CnC communications in attacks targeting victims located in different countries – China, Japan and the UK. Defending against an attacker with such capabilities on your own is not an easy task.

South-East Asia and Korean Peninsula

Attacks on South Korean semiconductor manufacturers

South Korea's National Intelligence Service (NIS) warned that North Korean hackers are targeting domestic semiconductor manufacturers in cyber-espionage attacks.

According to the NIS, these attacks increased in the second half of 2023 until recently, targeting internet-exposed servers vulnerable to known flaws for initial access to corporate networks. Once the network was breached, the threat actors stole data from servers holding sensitive documents and data. In the cases observed by the NIS, the North Korean adversaries used living-off-the-land (LotL) techniques.

The NIS cited at least two cyberattacks on separate entities, occurring in December 2023 and February 2024, in which the company's configuration management and security policy servers were hacked, resulting in the compromise of product design drawings and facility site photos, among other sensitive data. The NIS believes these cyberattacks are aimed at gathering valuable technical information that North Korea could use to develop its own chip manufacturing program and cover its military equipment needs.

The NIS notified the hacking victim of the facts and assisted in establishing security measures. In addition, to prevent further damage, threat information was provided to major domestic semiconductor companies to conduct their own security checks.

SideWinder attacks

The APT actor known as SideWinder has launched hundreds of attacks against high-profile entities in Asia and Africa in recent months. The infection chain is consistent with the process described in previous Kaspersky reports.

Most attacks begin with a Microsoft Word document sent via spear-phishing email or a ZIP archive containing an LNK file. The attachment triggers a chain of events that lead to the execution of multiple intermediate stages composed by the malware in JavaScript and .NET, and finally compromises the system with a malicious implant developed in .NET that runs only in memory and is loaded with custom-packed loaders.

During the investigation, Kaspersky researchers observed a rather large infrastructure consisting of many different VPSs and dozens of subdomains. Many subdomains are believed to have been created for specific victims, and the naming scheme suggests that the attacker was trying to disguise malicious communications as legitimate traffic for websites related to government entities or logistics companies. SideWinder has historically targeted government and military entities in South Asia, but in this case an expansion of its targets was observed. The actor also compromised victims located in South-East Asia and Africa. In addition, Kaspersky telemetry revealed that different diplomatic entities in Europe, Asia and Africa were compromised. The expansion of targets also includes new industries, as evidenced by the discovery of new targets in the logistics sector, specifically maritime logistics.

Chinese-speaking activity

Blackwood attacks

ESET researchers have discovered a sophisticated implant, dubbed "NSPX30", being used by a new APT threat actor they believe is aligned to China. The threat actor, dubbed Blackwood, uses adversary-in-the-middle techniques to hijack update requests from legitimate software to deliver the implant to the targets and to intercept its traffic on the telecom side, therefore hiding its C2 communication by disguising it as HTTP and UDP requests sent to legit internet services belonging to Baidu.

NSPX30 is a multi-stage implant that includes several components such as a dropper, installer, loaders, orchestrator, and backdoor. The latter two have their own sets of plugins. The implant was designed around the attackers' ability to perform packet interception, allowing NSPX30 operators to hide their infrastructure. NSPX30 has been mapped to an earlier backdoor named Project Wood – the oldest sample found was compiled in 2005.

The group has conducted cyber-espionage operations against individuals and companies from China, Japan and the UK. Victims include a large manufacturing and trading company in China and the Chinese office of a Japanese engineering and manufacturing corporation.

The researchers believe that traffic interception has been implemented some place closer to the targets rather than to Baidu or at a Chinese telecom side since Baidu has a geographically spread infrastructure, partially located outside China, and accessible via anycast.

Ivanti Connect Secure VPN Exploitation

Researchers have discovered targeted attacks exploiting two zero-day vulnerabilities affecting Ivanti Connect Secure (ICS) VPN appliances (CVE-2024-21887 and CVE-2024-46805). The attackers chained together two vulnerabilities to obtain unauthenticated remote code execution.

The vulnerabilities were initially exploited by a threat actor tracked as UTA0178, believed to be based in China. However, other threat actors have since launched attacks using the same vulnerabilities.

Volexity researchers have found evidence of at least 1,700 compromises. According to them, victims are globally distributed, vary greatly in size and span multiple industries, including: global government and military departments, national telecommunications companies, defense contractors, aerospace, aviation, engineering, and others.

Ivanti has issued mitigation advice, pending a patch for the two vulnerabilities.

VOLTZITE attacks

According to Dragos, the threat actor dubbed “Voltzite” has been conducting reconnaissance and enumeration of multiple US electric companies since early 2023.

The threat group overlaps with an adversary described by the US Cybersecurity and Infrastructure Security Agency (CISA) in May 2023, and the Microsoft threat group Volt Typhoon. Dragos also discovered evidence that VOLTZITE overlaps with UTA0178, a threat activity cluster tracked by Volexity that exploits zero-day vulnerabilities in Ivanti Connection Secure VPN.

The actor primarily uses living-off-the-land (LOTL) techniques, exhibits a high level of operational security practices, uses open-source tooling and web shells, and leverages credential theft to facilitate lateral movement.

VOLTZITE has targeted emergency management services, telecommunications, satellite services, and African electric transmission and distribution providers.

While the attackers weren't able to infiltrate the operational technology network after compromising a US water and electric utility, Voltzite was able to steal geographic information system data, SCADA system configurations, and lists of critical customers. Some of the devices and software compromised by the attackers include Fortinet FortiGuard, PRTG Network Monitor appliances, ManageEngine ADSelfService Plus, FatePipe WARP, Ivanti Connect Secure VPN, and Cisco ASA, according to the Dragos report.

Volt Typhoon CISA alert

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) published a joint guidance and advisory on February 7 focusing on the Chinese-speaking threat actor, Volt Typhoon, which infiltrated a critical infrastructure network in the United States and remained undetected for at least five years before being discovered.

Volt Typhoon compromised the IT environments of multiple organizations primarily in communications, energy, transportation, water and wastewater sectors in the continental and non-continental United States and its territories, including Guam.

Volt Typhoon hackers are known to make extensive use of living-off-the-land (LOTL) techniques and stolen accounts as part of their attacks. The actor leverages strong operational security, which allows it to evade detection and maintain long-term persistence on compromised systems.

US authorities are also concerned that Volt Typhoon may exploit access to critical networks to cause disruption, particularly in the midst of potential military conflicts or geopolitical tensions.

The advisory and guidance are accompanied by a technical guide with information on how to detect Volt Typhoon techniques and mitigation measures.

Russian-speaking activity

RedCurl attacks

Group-IB researchers reported new attacks by the Russian-speaking hacker group RedCurl in Australia, Singapore and Hong Kong targeting companies in the construction, logistics, aviation and mining industries.

The files involved in the observed campaigns were captured by researchers in October 2023. RedCurl was first noticed by Group-IB in late 2019, but was active since at least 2018. So far, RedCurl has carried out more than 40 attacks: half of them in Russia, the rest in the UK, Germany, Canada, Norway, and Ukraine. At the time, Group IB believed the group may be related to Cloud Atlas APT – but only based on the victim profile, the use of the LaZagne tool and the WebDav protocol. No other intersections were noticed. The attacks have always used their own unique homemade tools.

The attackers were exclusively engaged in cyber-espionage to order. Typically, RedCurl was able to implement its plan from the time of infection to data theft in a period of two to six months. The attackers stole business information of interest: corporate correspondence, personal files of employees, legal documents and other secrets of the victim company.

The entry point for new RedCurl attacks remains the same – sending an email to employees with attachments in the form of SVG files or RAR archives containing SVG (in the past they used links in the emails). SVG files contain links to RedCurl.ISO, which contains an LNK file and a directory with many DLLs.

Once the shortcut is opened, a command is executed via rundll32.exe, which runs RedCurl.SimpleDownloader to download the next stage and display the bait site. If the necessary checks are passed, RedCurl.Downloader gathers information about the system and sends it to the C2 server.

After that, the next stage RedCurl.Extractor is initiated, which is used for extraction and persistence of RedCurl.FSABIN. RedCurl.FSABIN makes requests to the C2 server to obtain a decryption key and an encrypted BAT script, which is decrypted and executed on the infected system (RedCurl.Commands).

Pawn Storm/Sofacy/APT28 attacks

TrendMicro reported that Pawn Storm (aka APT28, Sofacy, Fancy Bear, Sednit, and Forest Blizzard) launched NTLMv2 hash relay attacks between April 2022 and November 2023 to brute-force its way into government, defense, military, energy and transportation networks worldwide.

The threat actor exploited the CVE-2023-23397 critical elevation of privilege zero-day vulnerability at the time, to collect NTLMv2 digests from targeted Outlook accounts via a hash relay attack and send malicious calendar invitations.

Pawn Storm used a variety of tools to cover its tracks, including VPN services, Tor, data center IP addresses, and compromised EdgeOS routers. In addition, Pawn Storm compromised numerous email accounts around the world and used them as launch pads to send spear-phishing emails.

The campaign evolved with the use of more sophisticated methods, including scripts hosted on Mockbin and URLs redirecting to PHP scripts on free web hosting domains. Pawn Storm also exploited the CVE-2023-38831 WinRAR vulnerability for hash relay attacks. A credential phishing campaign in late 2023 targeted various organizations in Europe and North America using webhook[.]site URLs and VPN IP addresses.

The Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners released a joint Cybersecurity Advisory (CSA) in February warning that the actor was compromising Linux-based Ubiquiti EdgeRouters (EdgeRouters) to facilitate malicious cyber operations worldwide.

According to the CSA, these operations have targeted various industries, including aerospace and defense, education, energy and utilities, governments, hospitality, manufacturing, oil and gas, retail, technology, and transportation. Targeted countries include the Czech Republic, Italy, Lithuania, Jordan, Montenegro, Poland, Slovakia, Turkey, Ukraine, the United Arab Emirates, and the US.

An FBI investigation revealed that APT28 actors accessed EdgeRouters compromised by Moobot, a botnet that installs OpenSSH Trojans on compromised hardware. APT28 actors have used compromised EdgeRouters to collect credentials, proxy network traffic, and host spoofed landing pages and custom post-exploitation tools. With root access to compromised devices, actors had unfettered access to Linux-based operating systems and installed publicly available tools, such as Impacket ntlmrelayx.py and Responder, to execute NTLM relay attacks and host NTLMv2 rogue authentication while conducting malicious campaigns.

Middle East-related activity

UNC1549 attacks

Mandiant reported on an ongoing cyber-espionage campaign targeting the aerospace and defense industries in Israel, the United Arab Emirates, and possibly Turkey, India and Albania.

The campaign began as early as June 2022 and was conducted by a group Mandiant tracks as UNC1549, which researchers have linked to Iran and which overlaps with another hacking operation called Tortoiseshell.

Mandiant observed UNC1549 deploy multiple evasion techniques to mask its activity, most prominently the extensive use of Microsoft Azure cloud infrastructure, as well as social engineering schemes to disseminate two unique backdoors: MINIBIKE and MINIBUS.

The MINIBIKE malware was first spotted in June 2022 and last seen in October 2023. It’s capable of exfiltrating and uploading files, executing commands, and using Azure cloud infrastructure. MINIBUS is a custom backdoor that provides a more flexible code-execution interface and enhanced reconnaissance capabilities. It was first discovered in August 2023 and seen as recently as January. The two pieces of malware cover the usual cyber-espionage checklist, including harvesting of login credentials to enable further spying, or running other malicious code to clear the way for more activity.

The researchers also spotted a custom tunneler they dubbed LIGHTRAIL, which is likely based on an open-source Socks4a proxy that communicates using Azure cloud infrastructure.

Other

Scaly Wolf attacks

BI.ZONE researchers reported new Scaly Wolf campaigns targeting logistics and industrial facilities in Russia.

Attackers send phishing emails in the name of domestic government agencies (Roskomnadzor, Investigative Committee, Military Prosecutor’s Office, court orders, and other regulatory requirements) and trick recipients into launching a malicious file, after which they deliver the White Snake stealer to the victim's computer. The malware is almost always contained in a protected ZIP archive with the password stored in the archive filename.

White Snake is the main tool in Scaly Wolf's arsenal. The stealer first appeared on the darknet in February 2023. White Snake can be run cross-platform using a downloader written in Python. On the Windows platform, the stealer implements the functionality of a remote access Trojan, including a keylogger, and supports customization based on XML configuration. In addition, the stealer uses the Serveo.net service for SSH access to the infected machine, giving the attacker the ability to execute commands on the compromised host. Another functionality of the stealer is the sending of notifications about new infected devices to the Telegram bot.

The Scaly Wolf actor managed to bypass the restrictions imposed by the stealer developers, which prohibited its use in Russia and the CIS. In order to do this, the attackers modified the functionality of the software, disabling IP filtering that determines whether the victim belonged to a blocked segment.

Operation FlightNight

EclecticIQ researchers uncovered a new espionage campaign targeting Indian government agencies and the country’s energy industry with a modified version of an open-source information stealer called HackBrowserData that can collect browser login credentials, cookies and history. The researchers dubbed the intrusion “Operation FlightNight” and didn’t attribute it to a specific threat actor.

The information stealer was delivered to its victims via a phishing PDF document disguised as an invitation letter from the Indian Air Force. Researchers believe the original PDF file was most likely stolen during a previous intrusion and repurposed by the attackers. The document contained a shortcut LNK file that pointed to the malware. Once executed, the malware immediately began exfiltrating documents and cached web browser data from the victim's device to channels on the workplace app Slack. The stolen information included internal documents, private email messages and cached web browser data.

Although the hacker group behind this campaign hasn’t been identified, similarities in the malware and the delivery technique metadata strongly suggest a connection to an attack reported in January, when cybercriminals targeted Indian Air Force officials with credential stealer malware called GoStealer. According to EclecticIQ, both campaigns are likely the work of the same threat actor.

Rhadamanthys stealer attacks

According to Cofense research, an updated version of an information-stealing malware called Rhadamanthys has been used in phishing campaigns targeting the oil and gas sector. The campaign uses carefully crafted phishing emails and a PDF file disguised as a communication from the Federal Bureau of Transportation.

The phishers created several provocative subject lines such as "Notification: Incident Involving Your Vehicle" and "Attention Needed: Your Vehicle's Collision." The email message contains a malicious link that exploits an open redirect flaw to direct recipients to a link that appears to host a PDF document, but is actually an image that, when clicked, downloads a ZIP archive with the stealer payload.

StrelaStealer attacks

Palo Alto Networks researchers identified a wave of large-scale StrelaStealer campaigns that impacted more than 100 organizations in the EU and US, including manufacturing, utilities and energy, construction, high tech, and other industries. The campaign aimed to exfiltrate email account credentials and peaked from late January to early February.

The attacks involved the delivery of phishing emails with ZIP attachments deploying JScript files that, when executed, facilitate the execution of a DLL and the delivery of the StrelaStealer payload, representing a change from the old tactic that executed the malware through phishing emails with .ISO files.

While StrelaStealer's primary function is to compromise email credentials, the malware has been updated to better bypass detection through control flow obfuscation and PDB string removal, the researchers said.

Magnet Goblin attacks

Check Point researchers identified a new, financially motivated threat actor, dubbed “Magnet Goblin”, that targeted US medical, manufacturing and energy companies by exploiting vulnerabilities in Ivanti’s products.

The attackers are thought to have targeted vulnerable Ivanti Connect Secure VPN servers and used them to deploy backdoors in the targeted IT systems. The malware used by the attackers includes a Linux backdoor called MiniNerbian, a new version of NerbianRAT, a JavaScript credential stealer called WARPWIRE, and Ligolo, an open-source tunneling tool written in GO. They also use legitimate remote monitoring and management tools such as ScreenConnect and AnyDesk.

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