Kaspersky ICS CERT

kaspersky

APT and financial attacks on industrial organizations in H1 2023

25.09.2023

Version 1.0

Contents

This summary provides an overview of reports of APT and financial attacks on industrial enterprises that were disclosed in H1 2023, as well as 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 the researchers that we believe may be of use to professionals addressing the practical issues of cybersecurity for industrial enterprises.

Korean-speaking activity

Lazarus attacks

Kaspersky researchers observed a Lazarus campaign, active until January 2023, leveraging a backdoored UltraVNC client to deliver an updated BLINDINCAN payload. The payload has new features, including plug-in-based expanding capabilities. Backdooring prominent open-source programs is one of the means that the Lazarus group has been using to deliver its malware. When executed, the compromised application functions normally, but covertly collects victim information and transmits it to the C2 servers.

The telemetry shows evidence of a memory-resident payload being retrieved by the backdoored client. The delivered payload was identified as BLINDINCAN, which has been delivered as second-stage malware before. This updated version of BLINDINCAN shares similar characteristics with previous iterations, such as C2 communication, encryption methods and infection procedure.

However, it introduced new features, including plug-in-based expanding capabilities. By analyzing and cracking the Trojanized application's communications, Kaspersky researchers discovered information about possible victims in the manufacturing and real estate sectors being targeted in India. Additional analysis of the C2 servers, compromised since early 2020, suggests further targeting of telecoms companies in Pakistan and Bulgaria. Kaspersky researchers believe that this campaign is not limited to these countries and sectors.

WithSecure published an investigation into a new cyber-espionage campaign called No Pineapple! that researchers attributed to Lazarus. According to the researchers, the threat actor was able to discreetly steal 100 GB of data from the victim without causing any damage. The campaign ran from August to November 2022 and targeted organizations in scientific research, healthcare, chemical engineering, energy, defense and a leading research university.

Lazarus hackers compromised the victim's network on August 22, 2022, using the RCE vulnerabilities CVE-2022-27925 and CVE-2022-37042 to bypass Zimbra authentication by dropping the web shell on the mail server. Following a successful breach of the network, the Plink and 3Proxy tunneling tools were deployed, allowing the attackers to bypass the firewall. Less than a week later, the attackers used modified scripts to extract 5 GB from the mail server, saving it in a CSV file that was later uploaded to the attacker's server.

Over the next two months, Lazarus deployed its Dtrack and a new version of GREASE (known to be related to Kimsuky) to locate Windows administrator accounts, spread laterally through the network, and steal data from devices. The WithSecure investigation identified several changes to Lazarus, including: a new infrastructure using IP addresses without domain names, updated Dtrack software, and GREASE (used to create an administrator account and bypass security).

The new Dtrack variant no longer uses its own C2 server to steal data, relying on a separate backdoor to transfer locally collected data in a password protected archive. The new GREASE variant being run via 'Printnightmare' Windows Print Spooler RCE/LPE vulnerability (CVE2021-34527) exploit that as a dll with SYSTEM privileges. It now uses RDPWrap to install the RDP service on the host to create privileged user accounts using 'net user' commands.

The actor accidentally exposed a North Korean IP address during its operations. WithSecure also found many matches in TTP, infrastructure and targeting with Symantec and Cisco Talos reports. In addition, the researchers observed the attackers manually entering various commands on compromised network devices using the Impacket atexec module.

3CX supply chain attack

On March 29, CrowdStrike published an alert about a supply chain attack occurring via 3CXDesktopApp, a popular VoIP app. In their report, they tentatively attributed the ongoing attack to a Korean-speaking APT group called LABYRINTH CHOLLIMA, which Kaspersky researchers are tracking as Lazarus. 3CX has an estimated 600 000 customers worldwide, including Toyota, McDonald's, Pepsi, Chevron and manufacturing companies.

Researchers believe the campaign has been ongoing for some time. A GitHub repository associated with the campaign dates back to December 2022, and other infrastructure dates back to February 2022. Early indications suggest that the attackers attempted to compromise more than 1,000 targets by Trojanizing both Windows and macOS installation packages.

According to Sentinelone, the date of the first infection attempt was registered by their telemetry on March. Kaspersky has been tracking a related campaign since March 2023, when Kaspersky researchers observed a spike in activity related to a backdoor dubbed Gopuram. Gopuram has been tracked internally since 2020, when it was observed alongside the AppleJeus backdoor on infected machines.

APT43 attacks

Mandiant researchers have identified a previously unknown APT threat actor, dubbed APT43, that they believe supports the interests of the North Korean government. The group's targeting is regionally focused on South Korea and the US, as well as Japan and Europe, specifically in the areas of government, education/research/think tanks focused on geopolitical and nuclear policy, business services and manufacturing.

They believe that this threat actor's activities, which date back more than five years, have sometimes been attributed to other threat actors – specifically Kimsuky or Thallium. The group mostly uses spear-phishing and fake websites to gather information. The threat actor's preferred tool is LATEOP – a backdoor based on Visual Basic scripts. They also use some other malicious tools exclusively available to them, as well as lots of publicly available malware, such as gh0st RAT, QUASARRAT, AMADE and many other families. The group has also shared infrastructure and tools with other North Korean-nexus threat actors.

Andariel attacks

Kaspersky researchers have revisited an Andariel campaign from 2022, expanding on the commands the attackers used to deploy DTrack and the accompanying post-exploitation tools and malware. Kaspersky researchers believe the attackers exploited Log4j to gain an initial foothold.

Investigation of the attacker's infrastructure helped connect additional Yamabot infections to this incident. Several target profiles for related Yamabot deployments were identified, including biomedical research and production, genetic and botanical soil science research, as well as the energy sector. A new malware family, EarlyRat, was also identified as being dropped by the phishing documents.

MATA attacks

In early September 2022, the Kaspersky team discovered several malware detections from the MATA cluster, previously attributed to the Lazarus group, targeting defense contractors in Eastern Europe. The campaign remained active until March 2023. New, active actor campaigns with full infection chains were discovered, including an implant designed to work in air-gapped networks via USB sticks, as well as a Linux MATA backdoor.

The malware was distributed using spear-phishing techniques, with the attackers deploying their malware in multiple stages using validators. In the course of the attack the threat actor also abused various security solutions, by different vendors, used by the victims. The new MATA Orchestrator introduced several modifications to its encryption, configuration and communication protocols and appears to have been rewritten from scratch.

Kaspersky researchers have also discovered a new version of MATA, written from scratch. MATAv5 provides attackers with a rich set of commands and communication options. MATAv5 is capable of functioning as both a service and a DLL within different processes. The malware leverages Inter-Process Communication (IPC) channels internally and employs a diverse range of commands, enabling it to establish proxy chains across various protocols, including within the victim's environment. While MATAv5 has undergone significant evolution and shares minimal code sections with its predecessors, there are still similarities in protocols, commands, and plug-in structures. These similarities suggest a consistent approach to functionality across different generations of the malware.

Chinese-speaking activity

Blackfly/APT41 attacks

According to Symantec researchers, the Blackfly threat actor (aka APT41, Winnti and Bronze Atlas) targeted two subsidiaries of an Asian materials and composites conglomerate. The attacks, which occurred late last year and early this year, relied more on open-source tools than custom malware and included Backdoor.Winnkit, a credential-dumping tool, a screenshotting tool, a process-hollowing tool, an SQL tool, Mimikatz, ForkPlayground, and proxy configuration tools. Researchers believe this is part of a broader campaign targeting various sectors in the region.

Volt Typhoon/VANGUARD PANDA attacks

Researchers from Microsoft have reported that a Chinese-speaking threat actor, Volt Typhoon, was able to establish persistent access inside critical infrastructure targets in the US, including the communications, manufacturing, utilities, transportation, construction, maritime, government, information technology, and education sectors. The aim is espionage, but, according to Microsoft it potentially provides the threat actor with the ability to disrupt communications in the event of a military conflict in the South China Sea and broader Pacific region.

The attackers gain initial access by compromising internet-facing Fortinet FortiGuard devices, using the device's privileges to extract credentials from Active Directory and authenticate to other devices on the network. They then use command line and legitimate software binaries available on the compromised systems to find information on the system, discover additional devices on the network, and exfiltrate data.

The threat actor covers its tracks by proxying its network traffic through compromised SOHO routers and other edge devices. In a coordinated release, the National Security Agency along with other US domestic agencies and counterparts in Australia, the UK, New Zealand and Canada issued an advisory that referred to Microsoft's finding and provided broader warnings about a "recently discovered cluster of activity" originating in China.

The Volt Typhoon group has been active since at least mid-2021. In the most recent campaign, the group targeted organizations in the communications, manufacturing, utilities, transportation, construction, maritime, government, information technology, and education sectors.

CrowdStrike researchers observed this group, which they dubbed VANGUARD PANDA, using a novel tradecraft to gain initial access to target networks. CrowdStrike reported that the group employed Zoho ManageEngine

ADSelfService Plus exploits to gain initial access, then the attackers relied on custom web shells for persistent access, and living-off-the-land (LOTL) techniques for lateral movement.

Other detected malicious activity included listing processes, testing network connectivity, gathering user and group information, mounting shares, enumerating domain trust over WMI, and listing DNS zones over WMI. VANGUARD PANDA's actions indicated a familiarity with the target environment based on the rapid succession of its commands, as well as having specific internal hostnames and IPs to ping, remote shares to mount, and plaintext credentials to use for WMI.

The attackers used a web shell to replace tomcat-websocket.jar in the Apache Tomcat library with the backdoored version. The use of a backdoored Apache Tomcat library is a previously undisclosed persistence TTP used by VANGUARD PANDA. This backdoor was likely used by VANGUARD PANDA to provide persistent access to high-value targets downselected after the initial access phase of operations using what were then zero-day vulnerabilities.

Earth Longzhi attacks

After several months of inactivity, Earth Longzhi (believed to be a sub-group of APT41) targeted healthcare, manufacturing, technology and government organizations in Taiwan, Thailand, the Philippines and Fiji. The campaign abuses a Windows Defender executable to perform DLL side-loading, while also exploiting a vulnerable driver to disable security products installed on the hosts via a Bring Your Own Vulnerable Driver (BYOVD) attack. Researchers at TrendMicro also observed the threat actor using a new method to disable security products, a technique dubbed “stack rumbling” that abuses undocumented MinimumStackCommitInBytes values in the Image File Execution Options (IFEO) registry key – a new DoS technique seen in the wild.

Lancefly attacks

Researchers at Symantec have observed a new APT threat actor, dubbed Lancefly, targeting government, aviation and telecoms organizations in South and Southeast Asia using a custom backdoor. The backdoor used by the group, called Merdoor, has been developed since 2018. The initial infection vector remains unknown, although there is evidence that the attackers use phishing emails, brute forcing of SSH credentials, and exploitation of public-facing server vulnerabilities to gain access to target systems. The group also uses a newer version of the ZXShell rootkit, a tool used by the APT17 and APT41 threat actors. Lancefly has also been observed using Impacket's atexec feature to instantly execute a scheduled task on a remote machine via SMB. The Lancefly APT group has also been seen using PlugX and ShadowPad RAT, tools traditionally used by several Chinese-speaking APT groups.

Cyberattacks on Taiwan

According to Trellix researchers, there has been an increase in cyberattacks on Taiwan in the wake of rising geopolitical tensions between Taiwan and China. The attacks are mainly designed to deliver malware and steal sensitive information. The sectors most affected during the period monitored by the researchers were networking, manufacturing and logistics. There has also been

a marked increase in detections of PlugX, a Windows backdoor used by many China-based threat actors to control target computers. Other malware families targeting Taiwan included Zmutzy .NET spyware, Formbook infostealer and unknown malware identified only by its anti-emulation, anti-debugging and code obfuscation capabilities under the Kryptik name.

Russian-speaking activity

YoroTrooper attacks

Cisco Talos has identified a new threat actor it calls YoroTrooper that has been conducting cyber-espionage campaigns targeting government and energy organizations in CIS (Commonwealth of Independent States) countries since June 2022. The threat actor behind the campaigns has also compromised the accounts of a critical EU health agency, the World Intellectual Property Organization (WIPO), and various CIS embassies.

Researchers believe the actor may also have targeted organizations in the EU and Turkey. The tools used, which include commodity information stealers, RATs (such as AveMaria/Warzone RAT, LodaRAT), Python-based RATs and information stealers, and Python- and Meterpreter-based reverse shells, are delivered via phishing emails containing malicious LNK attachments and decoy PDF documents. The attackers registered malicious domains, created subdomains, and also used domains with typos similar to legitimate ones. Kaspersky researchers observed overlaps between YoroTrooper and Tomiris in terms of malware samples, network indicators, targets and TTPs.

COSMICENERGY tool

Mandiant researchers have identified a toolset dubbed COSMICENERGY that is designed to simulate attacks on power grids. They discovered it after it was uploaded to VirusTotal. They believe it was likely developed by a Russian contractor as a red-teaming tool for simulated power disruption exercises hosted by Rostelecome-Solar, a Russian cybersecurity company. The toolset targets IEC 60870-5-104 (IEC-104) devices, including remote terminal units (RTUs). It appears to be similar to Industroyer. So far, researchers haven't seen any targeting with this tool in the wild.

BlueDelta/Sofacy attacks

According to Ukraine's Computer Emergency Response Team (CERT-UA), BlueDelta (aka Sofacy, APT28, Fancy Bear and Sednit) exploited vulnerabilities in Roundcube Webmail to hack more than 40 Ukrainian organizations, including government institutions and military entities connected to aviation infrastructure.

The threat actor used news stories about the Russo-Ukrainian conflict to trick targets into opening malicious emails that exploited vulnerabilities (CVE-2020-35730, CVE-2020-12641 and CVE-2021-44026). Using a malicious script, the attackers redirected their targets' incoming emails to an email address controlled by the attackers and gathered data from the compromised accounts. The BlueDelta activity appears to have been ongoing since November 2021.

Midnight Blizzard attacks

Microsoft experts have discovered a surge in attacks by the Midnight Blizzard group (Nobelium, APT29, Cozy Bear, Iron Hemlock and The Dukes) that focus on the theft of credentials. Midnight Blizzard garnered worldwide attention with the SolarWinds supply chain compromise in December 2020.

The attackers use a variety of techniques in these attacks, including password spraying, brute force, token theft, and session replay, to gain unauthorized access to cloud resources. APT29 also uses residential proxy services to conceal malicious traffic and obscure the connections it establishes via stolen credentials. These attacks target governments, IT service providers, NGOs, the defense industry, and critical manufacturing.

Middle East-related activity

Mint Sandstorm/Charming Kitten attacks

The threat actor Mint Sandstorm (aka Charming Kitten group, previously tracked as Phosphorous), which researchers believe is linked to the Iranian government, is conducting cyberattacks against US critical infrastructure, particularly organizations in the energy and transportation sectors.

The group often uses proof-of-concept exploits as soon as they become public, with researchers observing an attack using a Zoho ManageEngine PoC the same day it was released. The threat actor also uses known vulnerabilities, such as Log4Shell, to breach unpatched devices. After gaining access to a

target network, the threat actor launches a custom PowerShell script to gather information about the environment to determine if it is high-value. After moving laterally on the network, the actor deploys custom backdoors to maintain persistence and deploy additional payloads. Bitdefender researchers also observed Mint Sandstorm victims in the US, Europe, Turkey and India, and provided additional details on the group's toolset and IoCs.

Watering hole attack on shipping and logistics websites

ClearSky Cyber Security uncovered a watering hole attack on at least eight Israeli websites belonging to shipping, logistics, and financial services companies, attributing them with low confidence to the Iran-linked APT group Tortoiseshell (aka TA456 or Imperial Kitten).

According to the company's report, the Tortoiseshell threat actor has been active since at least July 2018. The threat actor used a script on the compromised websites to collect preliminary user information, including the user's OS language, IP address, screen resolution, and the URL from which the website was visited. The attackers used four domains that mimicked the legitimate jQuery JavaScript framework by using "jQuery" in their domain names. The trick of using domain names impersonating jQuery was observed in a previous Iranian campaign from 2017.

Other

Vice Society Ransomware Group attacks

Vice Society, aka DEV-0832, is a targeted ransomware group active since at least June 2021 that was previously focused primarily on the education and healthcare sectors in the US. Although one group, they use different ransomware families (e.g., BlackCat, QuantumLocker and Zeppelin).

In January, TrendMicro published a blogpost sharing its telemetry data and summarizing the observed group's TTPs. For example, custom PS scripts are used, and the group relies on vulnerable public-facing websites and compromised RDP credentials for initial infection.

Researchers have observed that the group has also targeted the manufacturing sector, indicating they have the ability and desire to penetrate different industries. The presence of Vice Society has been detected in Brazil (primarily affecting the country's manufacturing industry), Argentina, Switzerland, and Israel.

Royal ransomware

Following the CISA alert on the Royal ransomware group, Trend Micro also issued its own report on the group. The report introduces new indicators of compromise, infection chain and techniques, and shares statistics on targeted organizations and geography.

According to Trend Micro, from September 2022 to January 2023, manufacturing and transportation were the leading industries among Trend Micro customers targeted by Royal, with 33.7% of attack attempts each.

Several attacks by the Royal group were seen in 2022, primarily against organizations in the US and Brazil. According to the Royal ransomware group's leak site, small businesses accounted for just over half of Royal's victims in Q4, while midsize organizations accounted for approximately 30%. Large companies accounted for 14% during this period.

The group uses a mix of old and new techniques in its operations. On the one hand, they use callback phishing to trick victims into installing remote desktop malware. On the other hand, the use of intermittent encryption and the development of Linux variants of ransomware that also target ESXi servers show they are investing in modern ransomware trends.

APT attacks with CommonMagic and CloudWizard framework

Kaspersky researchers discovered an ongoing campaign, active since Q3 2021, targeting government, agricultural and transportation organizations in the conflict-affected region of Eastern Europe, using a previously unknown malware set. Observed victims downloaded an archive containing a malicious LNK file that downloads and installs a PowerShell backdoor, "PowerMagic", which then deploys a sophisticated modular framework called CommonMagic. CommonMagic plug-ins are capable of stealing files from USB devices, as well as capturing screenshots and sending them to the attacker.

Further investigation led to the discovery of the CloudWizard framework, which has been deployed since at least 2017 and was seen to be active in 2023. The framework has a modular architecture and its capabilities include taking screenshots, recording the microphone, and stealing files and passwords. The information collected by this framework is uploaded to cloud storage. CloudWizard has ties to the Operation Groundbait (Prikormka), BugDrop and CommonMagic campaigns. Malwarebytes researchers have also been tracking this activity, dubbing the threat actor RedStinger, responsible for espionage operations against both pro-Ukrainian and pro-Russian targets

since 2020. They highlight two campaigns, both notable for their persistence and aggressiveness.

The targets of "Operation Four" included a member of the Ukrainian military working on Ukraine's critical infrastructure. The attackers compromised the targeted devices to exfiltrate screenshots and documents, and record audio. "Operation Five" targeted several election officials involved in referendums in the cities of Donetsk and Mariupol. One was an adviser to Russia's Central Election Commission. Another worked on transportation – possibly railroad infrastructure – in the region.

RA Group attacks

Cisco Talos researchers discovered a previously unknown ransomware operation called RA Group that has been active since at least April 22, 2023. The group is targeting companies in the US and South Korea with malware built from leaked Babuk ransomware source code.

Compromised organizations operate in various industries, including manufacturing, wealth management, insurance, and pharmaceuticals. Like other ransomware operations, RA Group also uses a double extortion model and operates a data leak site to sell the stolen information. The ransomware only targets files and folders that are not included in a hardcoded list, a trick that allows it to avoid encrypting files that could impair the infected system.

Void Rabisu attacks

The Russo-Ukrainian conflict has blurred the lines between APT threat actors, hacktivists and cybercriminals. The change in use of the RomCom backdoor is one example of this. The threat actor behind this malware, Void Rabisu (aka Tropical Scorpius), was thought to be a financially motivated threat actor – based on its links to the Cuba ransomware.

However, researchers at TrendMicro have noted the use of RomCom against Ukrainian government and military targets, as well as water, energy and financial entities in the country. The attackers used spear phishing and a Google Ads advertisement that redirects users to a RomCom lure site. These sites offer Trojanized versions of genuine applications, such as AstraChat and Signal, PDF readers, password managers and remote desktop apps.

CISA alerts

CISA Royal ransomware alert

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint alert to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as January 2023.

CISA wrote that Royal actors have targeted several critical infrastructure sectors, including manufacturing, communications, education and healthcare. Malicious activity by threat actors using a specific malware variant has been detected since September 2022.

The FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used 'Zeon' as a loader. After gaining initial access to networks through phishing, RDP and other techniques, the threat actors were observed disabling antivirus software on victims' machines and exfiltrating large amounts of data. Finally, they deployed the ransomware and encrypted systems. CISA made a number of recommendations to reduce the likelihood and impact of ransomware incidents.

CISA advisory on Snake malware

The US Cybersecurity and Infrastructure Security Agency (CISA) has published a detailed analysis of Snake, one of the implants attributed to Turla.

This malware is designed to perform long-term intelligence gathering on high-priority targets using a peer-to-peer network of compromised systems around the world. Infrastructure associated with the threat actor has been identified in more than 50 countries across North America, South America, Europe, Africa, Asia and Australia, targeting government networks, research facilities, and journalists. Targeted sectors in the US include education, small business, media and critical manufacturing.

The US Department of Justice issued a warrant that allowed the FBI to remotely access eight Snake-infected computers in the US and terminate the malware running on them.

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