APT attacks on industrial organizations in H2 2022

ics-cert.kaspersky.com/publications/reports/2023/03/24/apt-attacks-on-industrial-organizations-in-h2-2022/

March 24, 2023

24 March 2023

Download PDF

This summary provides an overview of APT attacks on industrial enterprises disclosed in H2 2022 and related activity of groups that have been observed attacking industrial organizations and critical infrastructure facilities. For each story, we sought to summarize the most significant facts, findings, and conclusions of researchers, which we believe can be of use to experts who address practical issues related to ensuring the cybersecurity of industrial enterprises.

Southeast Asia and Korean Peninsula

DEV-0530 attacks

Researchers have attributed an emerging ransomware threat to a North Korean based threat actor they call DEV-0530 (the group calls itself “H0lyGh0st”). DEV-0530 has targeted small-to-medium businesses in multiple countries since September 2021, including manufacturing organizations, banks, schools, and event and meeting planning companies. The attackers employ “double extortion”, encrypting data and also threatening to publish data if the target refuses to pay. Researchers have found connections of DEV-0530 with the PLUTONIUM APT group (aka DarkSeoul and Andariel).

Between June 2021 and May 2022, the Microsoft Threat Intelligence Center (MSTIC) classified H0lyGh0st ransomware under two new malware families: SiennaPurple and SiennaBlue. Researchers suspect that DEV-0530 may have exploited vulnerabilities such as CVE-2022-26352 (a DotCMS remote code execution vulnerability) on public-facing web applications and content management systems to gain initial access into target networks.

Tropic Trooper attacks

For over a decade, the Tropic Trooper APT actor has been actively targeting victims in East and Southeast Asia. Kaspersky has been tracking this threat actor for several years and has published a report describing its malicious operations. The report is available to subscribers of the Threat Intelligence Reporting service.

In February 2022, Symantec published a report describing a campaign called “Antlion”, which has been observed targeting financial institutions and a manufacturing company in Taiwan. In the manufacturing target, where the attackers maintained their presence for about 175 days, researchers saw the attackers attempting to download malicious files via SMB shares. While analyzing the IoCs of this campaign, Kaspersky found strong connections with the Tropic Trooper threat actor, which led to the conclusion that the group was behind the Antlion campaign.

In the Kaspersky investigation, different attacks conducted by this threat actor using the malware families described by Symantec were discovered and studied, together with new versions of the malware that were discussed in an earlier Kaspersky report on the Tropic Trooper APT actor. The infection chain for these attack cases, the attack infrastructure, lateral movement and post-exploitation activities carried out by this actor were analyzed. Additional target verticals besides the finance sector were identified, including the tech hardware & semiconductors industry, as well as a political entity.

Furthermore, Kaspersky discovered a previously unknown, multi-module backdoor deployed to a victim machine in August 2021, which uses the MQTT protocol for network communication with its C&C server. Tracing the history of the backdoor, it appears that the module has been used by this threat actor since at least 2019 and only with a selected set of targets.

GwisinLocker ransomware attacks

ReversingLabs researchers discovered a new ransomware family targeting Linux-based systems with features specially designed to operate and interact with VMWare ESXI virtual machines. The malware, which was dubbed GwisinLocker, was detected in successful campaigns targeting South Korean industrial and pharmaceutical firms.

Analysis and public reporting of the larger GwisinLocker campaign suggests that the ransomware is in the hands of sophisticated threat actors who gain access to target environments prior to the deployment of the ransomware and steal sensitive data for use in so-called “double extortion” campaigns. Details in samples of the group’s ransom notes suggest a familiarity with the Korean language as well as South Korean government and law enforcement. This has led to speculation that the attackers belong to a North Korean-linked advanced persistent threat (APT) group.

Lazarus attacks

The threat actor Lazarus has used a signed malicious macOS executable to target engineers. It drops a fake job document named Coinbase_online_careers_2022_07.pdf. The executable, which targets systems based on both Apple and Intel chips, was disguised as a job description from Coinbase seeking an engineering manager for product security. The second executable used by the threat actor is a downloader that fetches the next-stage payload from a remote location. Researchers have linked the malware to “Operation In(ter)ception”, a Lazarus campaign targeting high-profile aerospace and defense industries.

DTrack is a backdoor used by subsets of the Lazarus group. The backdoor has been used in a variety of attacks, including ransomware attacks and espionage campaigns. Kaspersky experts identified and investigated new DTrack samples. These new samples are packed in a different way and with relatively minor changes in the code. This latest set of samples was analyzed in detail in a public report that describes these changes and packing mechanisms. According to KSN telemetry, DTrack activity has been detected in Brazil, Germany, India, Italy, Mexico, Saudi Arabia, Switzerland, Turkey, and the United States, indicating that DTrack is being distributed into more parts of the world. Targeted sectors were education, chemical manufacturing, governmental research centers and government ministries, an IT services provider, utility providers, and telecommunications.

Researchers from Cisco Talos reported on Lazarus attacks that targeted energy providers in the US, Canada and Japan between February and July, with the aim of stealing data and trade secrets. The attacks start by exploiting Log4j vulnerabilities in VMware Horizon, followed by the deployment of three custom malware implants. The first, “VSingle”, executes arbitrary code from a remote network and can download and execute plugins. The second,

“YamaBot”, is a custom-made Golang implant that communicates with the C&C servers. The third, MagicRAT, is a Remote Access Trojan that launches additional payloads such as custom-built port scanners.

ESET researchers uncovered and analyzed a set of malicious tools that were used by the Lazarus APT group in attacks during the autumn of 2021. The campaign started with spearphishing emails containing malicious Amazon-themed documents and targeted an employee of an aerospace company in the Netherlands and a political journalist in Belgium. The primary goal of the attackers was data exfiltration. The most notable tool used in this campaign represents the first recorded abuse of the CVE-2021-21551 vulnerability, which affects Dell DBUtil drivers. This BYOVD (Bring Your Own Vulnerable Driver) technique was used to disable 7 Windows OS monitoring mechanisms and to blind the security solutions on compromised machines. In this campaign, Lazarus also used their fully featured HTTP(S) backdoor known as BLINDINGCAN.

Kaspersky researchers uncovered an ongoing Lazarus campaign targeting defense contractors in South Africa and Brazil and dating back to March. The actor contacted potential victims via social networks or email and sent the initial malware through Skype. The malware is a Trojanized PDF application that initiates a multi-stage infection chain, loading additional payloads that contain C&C communication capability via the DLL side-loading technique. The attackers also deployed additional malware to the initial host to pivot and perform lateral movement. In this process, the operator took advantage of a relatively new DLL side-loading technique named “ServiceMove”. The technique was introduced by a red team researcher and abused the “Windows Perception Simulation Service” to load arbitrary DLL files for malicious purposes. The Lazarus group is equipped with a variety of tools, which it employs with various infection chains. While examining all the samples in this case, different clusters were observed: ThreatNeedle, Bookcode, and DeathNote.

UNC4034/ZINC attacks

Mandiant researchers have uncovered Trojanized versions of the PuTTY SSH client being used by a threat actor known as UNC4034 to deploy a backdoor, “AIRDRY.V2”, on target devices. This activity seems to be a continuation of the “Operation Dream Job” campaign, which has been ongoing since June 2020 and is suspected to have a North Korean nexus. The attackers approach potential targets via email with a lucrative job offer, purportedly from Amazon, and then move the communication to WhatsApp, where they share an ISO file. The file contains a readme file with an IP address and login credentials, and a Trojanized version of PuTTY, a popular open-source SSH console application.

Microsoft has been tracking the actor behind these attacks under the name ZINC. The group uses weaponized open-source software in its attacks. Microsoft experts have observed activity targeting employees in organizations across multiple industries, including media, defense and aerospace, and IT services in the USA, UK, India, and Russia. They have

observed ZINC weaponizing a wide range of open-source software for these attacks, including PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and muPDF/Subliminal Recording software installer.

Middle East

UNC3890 attacks

A suspected Iranian threat activity cluster has been linked to attacks aimed at Israeli shipping, government, energy, and healthcare organizations, in a campaign stretching back to late 2020. Researchers believe that the data harvested during the campaign could be used to support various activities. UNC3890, the threat actor behind the attacks, deployed two proprietary pieces of malware – a backdoor named “SUGARUSH” and a browser credential stealer called “SUGARDUMP”, which exfiltrates password information to email addresses registered with Gmail, ProtonMail, Yahoo and Yandex email services. The threat actor also employs a network of C&C servers that host fake login pages impersonating legitimate platforms such as Office 365, LinkedIn and Facebook. These servers are designed to communicate with the targets and also with a watering hole hosted on the login page of a legitimate Israeli shipping company.

POLONIUM attacks

Researchers have discovered previously undocumented custom backdoors and cyberespionage tools deployed by the POLONIUM APT threat actor against targets in Israel. The targets include organizations in the engineering, IT, law, communications, branding and marketing, media, insurance, and social services sectors. The threat actor targeted more than a dozen organizations between September 2021 and September 2022.

POLONIUM’s toolset consists of seven custom backdoors: CreepyDrive, which abuses OneDrive and Dropbox cloud services for C&C; CreepySnail, which executes commands received from the attackers’ own infrastructure; DeepCreep and MegaCreep, which make use of Dropbox and Mega file storage services, respectively; and FlipCreep, TechnoCreep, and PapaCreep, which receive commands from attackers’ servers. The group has also developed several custom modules to spy on its targets by taking screenshots, logging keystrokes, spying via the webcam, opening reverse shells, exfiltrating files, and more. According to the researchers, “most of the group’s malicious modules are small, with limited functionality” such as “one module for taking screenshots and another for uploading them to the C&C server”. The attackers like to divide the code, distributing malicious functionality into various small DLLs, perhaps expecting this to prevent defenders or researchers from observing the complete attack chain.

Chinese-speaking activity

TA428 attacks

Kaspersky ICS CERT experts have detected a wave of targeted attacks on military industrial complex enterprises and public institutions in several countries. The attack targeted over a dozen organizations, including industrial plants, design bureaus and research institutes, government agencies, ministries and departments in several East European countries (Belarus, Russia, and Ukraine), as well as Afghanistan. Some of the malware used in these attacks had previously been observed in attacks conducted by the IronHusky APT group. The research has also identified malware and command-and-control (C&C) servers previously used in attacks attributed by other researchers to the TA428 APT group.

The attackers penetrate the enterprise network using carefully crafted phishing emails containing information some of which is not publicly available. In the new series of attacks, the attackers used six different backdoors (PortDoor, nccTrojan, Cotx, DNSep, Logtu, and CotSam) at the same time – probably to set up redundant communication channels with infected systems in case one of the malicious programs was removed by an antivirus solution. The backdoors used provide extensive functionality for controlling infected systems and collecting confidential data. The attack's final stage involves hijacking the domain controller and gaining complete control of all of the organization's workstations and servers.

After gaining domain administrator privileges, the attackers search for and exfiltrate documents and other files containing the attacked organization's sensitive data to their servers, which are hosted in different countries and which are also used as C&C servers. The attackers compress stolen files into encrypted and password-protected ZIP archives, possibly to bypass DLP systems. After receiving the data collected, the C&C servers forward the archives received to a stage two server located in China.

APT31 attacks

In April 2022, the Positive Technologies Expert Security Center detected an attack on a number of Russian energy and media companies using a malicious document. The investigation subsequently revealed a number of other documents used in attacks on the same companies. The campaigns contained identical snippets of code for harvesting information about network adapters and collecting data about the infected system; the document stubs had clear similarities, and in all cases cloud servers were used to control the malware. An investigation of the tools showed that the attackers used Yandex.Disk as the C&C server.

The malware samples analyzed date from November 2021 to June 2022. In all cases legitimate files were used, whose main task was to pass control to a malicious library using, for instance, DLL side-loading, as well as to generate an initialization package to be sent to

C&C. A significant part of the legitimate executable files identified turned out to be Yandex.Browser components and were signed with a valid digital signature. An analysis of the malware samples showed that the APT31 group was behind the attacks.

TA423/Red Ladon attacks

Proofpoint and PwC Threat Intelligence teams published a joint research paper about a cyberespionage campaign that focused on government, energy and manufacturing organizations in the Asia-Pacific region. It deployed phishing emails directing targets to a fake news outlet. The attackers — referred to as TA423, Red Landon, or APT40 — designed the site to deliver malware known as ScanBox.

ScanBox delivers JavaScript code either in a single block or, as in the April 2022 campaign, as a plugin-based modular architecture. The primary payload sets its configuration, including the information to be gathered, and the C&C server to be contacted. It harvests detailed data on the browser being used.

Subsequent ScanBox plugins delivered to the victim include a keylogger, browser plugin identification, browser fingerprinting, a peer connection plugin, which can be used to establish connections with the infected node through NATs and to bypass firewalls and other security solutions installed on the same network device as the NAT (see our blog for details on the attack vector), as well as a security check for Kaspersky Internet Security (KIS).

Espionage activity against Asian governments

According to Symantec, government and state-owned organizations in a number of Asian countries have been targeted by a group of cyber-espionage hackers formerly associated with the ShadowPad RAT. The attackers use a wide range of legitimate software packages to load their malware payloads using DLL side-loading.

The campaign targets government institutions, state-owned media, IT, telecoms firms and government-owned aerospace and defense companies. The payloads used include information stealers, keyloggers, PowerSploit scripts, PlugX/Korplug, Trochilus RAT, QuasarRAT, publicly available tools, etc. The researchers couldn't make a solid attribution but found limited evidence to suggest links to past attacks by a number of known groups, including Blackfly/Grayfly (APT41) and Mustang Panda.

Budworm attacks

Researchers at Symantec have published a report detailing a cyber espionage campaign that has targeted the government of a Middle Eastern country, a multinational electronics manufacturer, and a US State Legislature. The hacking group, which is called Budworm, is believed to have ties to China's government.

According to the report, Budworm leveraged the Log4j vulnerabilities (CVE-2021-44228 and CVE-2021-45105) in recent attacks to compromise the Apache Tomcat service on servers in order to install web shells. The attackers used Virtual Private Servers (VPS) hosted on Vultr and Telstra as command-and-control (C&C) servers. While the threat actor's main tool is HyperBro, it has also used other tools, including CyberArk Viewfinity, Cobalt Strike, LaZagne, IOX, Fast Reverse Proxy and Fscan.

Earth Longzhi attacks

According to Trend Micro research, a previously undocumented sub-group of APT41 (aka Winnti) has been targeting organizations in East and Southeast Asia and Ukraine since at least 2020.

In its first wave of attacks, the threat actor, which has been dubbed Earth Longzhi, targeted government organizations, infrastructure companies, and healthcare companies in Taiwan, as well as Chinese banks. In the second wave, the group infiltrated high-profile victims in Ukraine and several countries in Asia, including defense, aviation, insurance, and urban development companies.

Both campaigns used spear-phishing emails as the primary entry vector to deliver Earth Longhzhi's malware, which was either embedded in a password-protected archive or downloaded via a Google Drive link hosting a password-protected archive. In both cases, the archive contained a customized Cobalt Strike loader.

For the post-exploitation operations of one of the campaigns Earth Longzhi prepared an all-in-one tool to combine all the necessary tools in one package, including a proxy, a port scanner, password scans and others. Most of the tools included in this one package are either publicly available or were used in previous attack deployments. Multiple hacking tools used for privilege escalation (PrintNightmare and PrintSpoofer), credential dumping (custom standalone Mimikatz), and defense evasion (disablement of security products) were collected during the investigation of the second campaign. The threat actors were able to reimplement or develop their own tools based on some open-source projects.

Russian-speaking activity

IRIDIUM/Sandworm attacks

In October, researchers at Microsoft reported on new ransomware named "Prestige", which was used to target transport and logistics industries in Ukraine and Poland. Initially, the malware was given a temporary name, DEV-0960. There is an overlap in victims between Prestige and HermeticWiper malware, although it is unclear whether the two are controlled by the same attacker – DEV-0960. Prior to deploying ransomware, the DEV-0960 activity included the use of RemoteExec and an open-source utility called Impacket WMIexec. To

gain access to highly privileged credentials, in some of the environments, DEV-0960 used the winPEAS open-source utility for privilege escalation, a tool for dumping the memory of the LSASS process and stealing credentials, and a tool for backing up the Active Directory database. In November, MSTIC (Microsoft Threat Intelligence Center) researchers updated their original blogpost and attributed the attack to the threat actor IRIDIUM (aka Sandworm, Hades).

Cloud Atlas/Inception attacks

Researchers at CheckPoint have observed Cloud Atlas (aka Inception) campaigns focused on very specific targets in Belarus, mainly in the country's transportation and military radio-electronics sectors, and in Russia, including the government sector, energy and metal industries, since June 2022. The actor has also maintained its focus on the Crimean Peninsula, as well as Lugansk and Donetsk regions. Cloud Atlas has used spear-phishing emails containing malicious attachments as their initial attack vector for many years, using current geo-political issues directly related to the target country as a lure. They mostly use public email services such as Yandex, Mail.ru and Outlook.com, but in some cases, they have also attempted to spoof existing domains of other entities that are likely to be trusted by the target. The next stage of a Cloud Atlas attack is usually a PowerShell-based backdoor called PowerShower.

Researchers at Positive Technologies have also reported on the actor and specified some additional countries in which the group targets the government sector. The report provides information on the actor's attack chain and toolset.

Other

Woody Rat attacks

The Malwarebytes Threat Intelligence team has identified a previously unknown Remote Access Trojan they dubbed Woody Rat, which has been in the wild for at least one year. This advanced custom RAT is mainly used by a threat actor that targets Russian entities by using lures in an archive file format (filenames "anketa_brozhik.doc.zip" and "zayavka.zip") and, more recently, Office documents ("Памятка.docx") leveraging the Follina vulnerability (CVE-2022-30190). Researchers believe that a Russian aerospace and defense entity known as OAK was targeted by Woody RAT, based on a fake domain registered by the threat actor. According to current research, there weren't any solid indicators to attribute this campaign to a specific known threat actor.

Worok attacks

ESET researchers have discovered targeted attacks against high-profile companies and local government bodies, mostly in Asia but also in the Middle East and Africa. The attacks were conducted by a previously unknown cyberespionage group, active since at least 2020, that they named “Worok”. Targets included companies from the telecoms, banking, maritime, energy, government and public sectors. In some cases, Worok exploited the infamous ProxyShell vulnerabilities to gain initial access. Once access had been acquired, the operators deployed multiple publicly available tools for reconnaissance, including Mimikatz, EarthWorm, ReGeorg, and NBTscan, and then deployed their custom implants: a first-stage loader, followed by a second stage .NET loader (PNGLoad). The final payloads couldn’t be retrieved.

Avast researchers were able to provide additional details on the actor’s compromise chain and confirmed the use of steganography to hide malware in PNG images. While the initial infection method remains unknown, they believe that the threat actor probably uses DLL side-loading to execute the CLRLoader malware loader in memory. This loads a second-stage DLL, PNGLoader, which extracts bytes embedded in PNG files and uses them to assemble two malicious payloads. The first payload implementation is a PowerShell script. Researchers don’t have a sample of this payload yet, but expect it to have similar functionality to the second payload implementation. The second payload is a .NET C# backdoor called DropBoxControl, which communicates with the attackers via the DropBox service. The victims of this campaign observed by Avast researchers were similar to those described by ESET and included companies and government institutions in Asia (Vietnam and Cambodia) and North America, specifically in Mexico.

CISA alerts

Iran-backed APT actors

CISA (Cybersecurity and Infrastructure Security Agency), the FBI, the NSA (National Security Agency), U.S. Cyber Command (USCC) – Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury) have released a joint advisory, which warns of APT actors affiliated with the Islamic Revolutionary Guard Corps (IRGC) of Iran targeting a broad range of entities, including entities across multiple U.S. critical infrastructure sectors. The advisory was also written in collaboration with Australian, Canadian, and British cybersecurity agencies. This new advisory updates a November 2021 advisory, which warned of these same APT actors exploiting Microsoft, Fortinet, and ProxyShell vulnerabilities. In addition to these prior vulnerabilities, it became known that the VMware Horizon Log4j vulnerability has now been added to the list of attack methods in the threat actors’ tool box and is used to gain initial access to target environments. The APT groups have used the initial access to carry out malicious activity, such as disk encryption and data

extortion that supports ransom operations. The agencies that collaborated on the joint advisory urge organizations, especially critical infrastructure organizations, to use the mitigation list provided in the advisory to minimize any risk of compromise by this APT group.

Military contractor hack

According to a joint alert from the US Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), between November 2021 and March 2022 attackers hid inside a US Defense Industrial Base organization's enterprise network and stole sensitive data. The CISA alert provides technical details of incident response activities. It was determined that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment. The attackers compromised the organization's Exchange Server and used a compromised administrator account to query Exchange via its EWS API. They also used the Impacket open source network toolkit to control computers remotely and perform lateral movement.

Download PDF