Kaspersky ICS CERT

APT attacks on industrial companies in H2 2021

28.02.2022

Version 1.0

This summary provides an overview of APT attacks on industrial enterprises disclosed in H2 2021 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.

Threat groups linked to China

During 2020 and 2021, Kaspersky detected a new ShadowPad loader module, dubbed ShadowShredder. The module was used against critical infrastructure in multiple countries, including but not limited to India, China, Canada, Afghanistan, and Ukraine. Upon further investigation, additional implants deployed through both ShadowPad and ShadowShredder, such as the Quarian backdoor, PlugX, Poison Ivy, and other hack tools were discovered. Notably, the Quarian backdoor and Poison Ivy showed similarities with earlier IceFog activity targeting users in Central Asia. This information was disclosed in a private report, which includes a technical analysis of ShadowShredder and related activities that use second-stage payloads linked to ShadowShredder and ShadowPad.

In Q3 2021, Kaspersky also discovered another set of TTPs that targeted aerospace and defense research establishments in India between 2019 and the end of June 2021, featuring two previously unknown backdoors: LGuarian and HTTP_NEWS. The former appears to be a new variant of the Quarian backdoor, a little-known malicious program that Chinese-speaking actors have used since around 2012, which this attacker also uses. Extensive information on the attacker's post-exploitation process was obtained, and detailed descriptions of the various tools used by the attackers during this phase, as well as actions performed on the victims' machines, were provided in a private report.

Kaspersky's advanced exploit prevention technology detected attacks that use a zero-day exploit in multiple versions of Windows. The corresponding zero-day vulnerability was reported to Microsoft. It was assigned CVE-2021-40449 and patched as part of the October 2021 Patch Tuesday. Previously unknown malware used in conjunction with the exploit, dubbed "MysterySnail", was analyzed. Other variants of the malware, which were used in widespread espionage campaigns, were found and studied. It was found that the malware had been used against IT companies, military/defense contractors and diplomatic entities. Code similarity and the re-use of C2 infrastructure connected these attacks with an actor known as IronHusky, as well as with Chinese-speaking APT activity dating back to 2012.

Lazarus attacks

Kaspersky observed the Lazarus group attacking the defense industry using the MATA malware framework. Historically, Lazarus had used MATA to attack various industries for cybercrime-related intentions: stealing customer databases and spreading ransomware. However, in these cases, Lazarus was seen using MATA for cyber-espionage purposes. The actor delivered a Trojanized version of an application known to be used by their victim of choice, representing a known characteristic of Lazarus. Executing the application starts a multi-staged infection chain beginning with a downloader. The downloader fetches additional malware from compromised servers used as C2 servers. Kaspersky researchers were able to acquire several MATA components, including plugins,. The MATA malware discovered in this campaign has evolved compared to its earlier versions and uses a legitimate, stolen certificate to sign some of its components. Through this research, a stronger connection between MATA and the Lazarus group was discovered, including the fact that the downloader malware fetching MATA malware showed ties to TangoDaiwbo, which previously was attributed to the Lazarus group.

WildPressure attacks

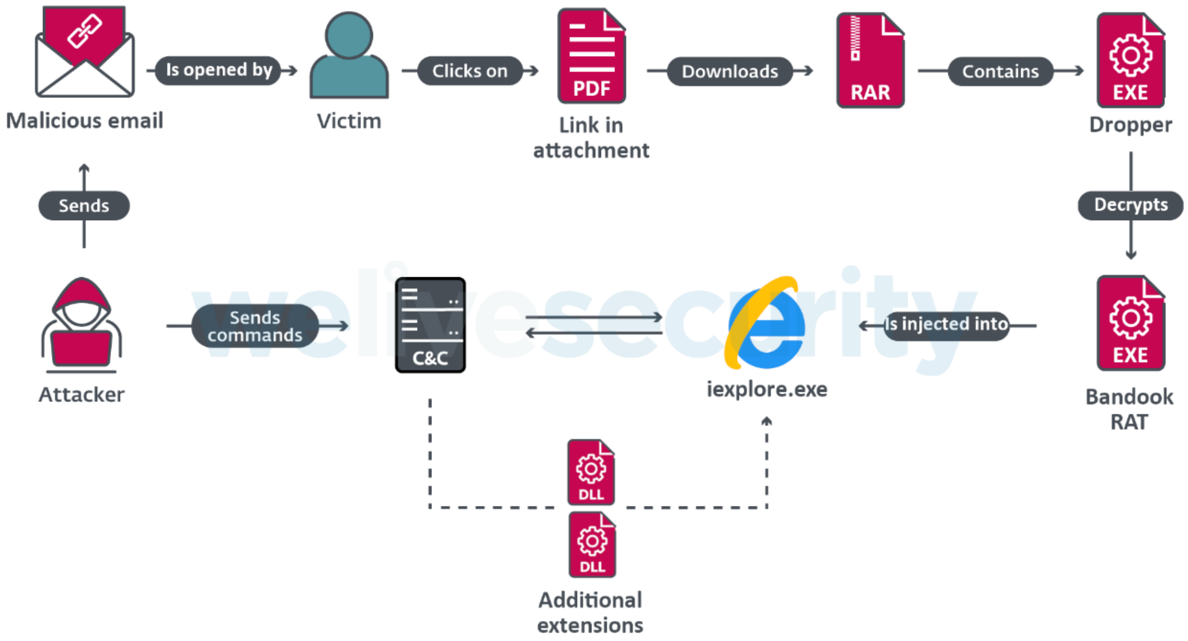
New WildPressure samples have been found following earlier research on the WildPressure campaign against industrial-related targets in the Middle East. The samples include a Python multi-OS Trojan that works both on Windows and macOS, a self-decrypting VBScript, a C++ Milum Trojan, an orchestrator, and several plugins. Suspected targets in the same region of the Middle East were related to the oil and gas industry.

TortoiseShell

On July 15, Facebook took down around 200 accounts that it says were run by an Iranian-based hacker group called “TortoiseShell” as part of a cyber-espionage operation that mainly targeted US military personnel and people working in defense and aerospace companies. The group’s TTPs include social engineering, phishing and credential theft, RATs, device and network reconnaissance tools, keystroke loggers, Syskit malware.

Bandook RAT spying campaign in Latin America

Updated versions of the Bandook RAT are being used in a campaign targeting corporate networks in Spanish speaking countries, mainly Venezuela. The main targets of the campaign, which has been dubbed “Bandidos”, are corporate networks in Venezuela - some in manufacturing, others in construction, healthcare, software services and retail. The infection chain features spear phishing emails with a PDF file containing a URL that leads to an encrypted RAR file which in turn installs Bandook malware. Bandook is an old remote access Trojan: there are references to it being available online as early as 2005, though its use by organized groups was not documented until 2016.



Bandook RAT infection process (Source: ESET)

Another report about this activity was published by ProofPoint, who track the actor as TA2721 (aka “Caliente Bandits”).

APT31

According to research by the Positive Techologies Expert Security Center (PT ESC), emails containing a previously unknown malicious RAT were sent to targets in Mongolia in April. Similar attacks were subsequently identified in Russia, Belarus, Canada, and the US. Ten attacks were carried out using the malware between January and July 2021. Targeted sectors include government, aerospace, defense, international finance and high-tech. Based on an analysis of malware samples, working directory and registry key names, and TTPs used by the attackers, researchers attribute the attacks to the APT31 group (aka Judgment Panda and Zirconium), which is believed to be of Chinese origin. Attacks on companies in France, which were uncovered in July and involved hacking home and office routers, have also been linked to the group. Recent findings about the group suggest that it is expanding the geography of its interests to countries where its growing activity can be detected, particularly Russia.

Attacks on Iranian railway system and gas stations

A previously unseen wiper, dubbed “Meteor”, was used in an attack on Iran’s train system that occurred on July 9th, 2021. The attack disrupted rail services and directed customers, via displays and message boards, to dial 64411 – the number for the office of Supreme Leader Ali Khamenei – for more information. At the time when information about the Meteor wiper was published, this activity wasn’t tied to any previously identified threat group or to any additional attacks. However, the artifacts suggest that the wiper was developed in the past three years and was designed for reuse. The attackers, believed by SentinelLabs researchers to be a new group, also hit the website and computer systems of Iran’s Ministry of Roads and Urban Development.

A cyberattack on the system that enables car drivers to buy subsidized fuel with government-issued smart cards caused long lines at gas stations in Iran in October 2021. A group calling itself “Predatory Sparrow” claimed responsibility for the attack. The attackers also hacked digital billboards in Tehran and elsewhere to display a message saying “Khamenei, where is our fuel?”. Iran has said that an unnamed foreign state was behind the attack.

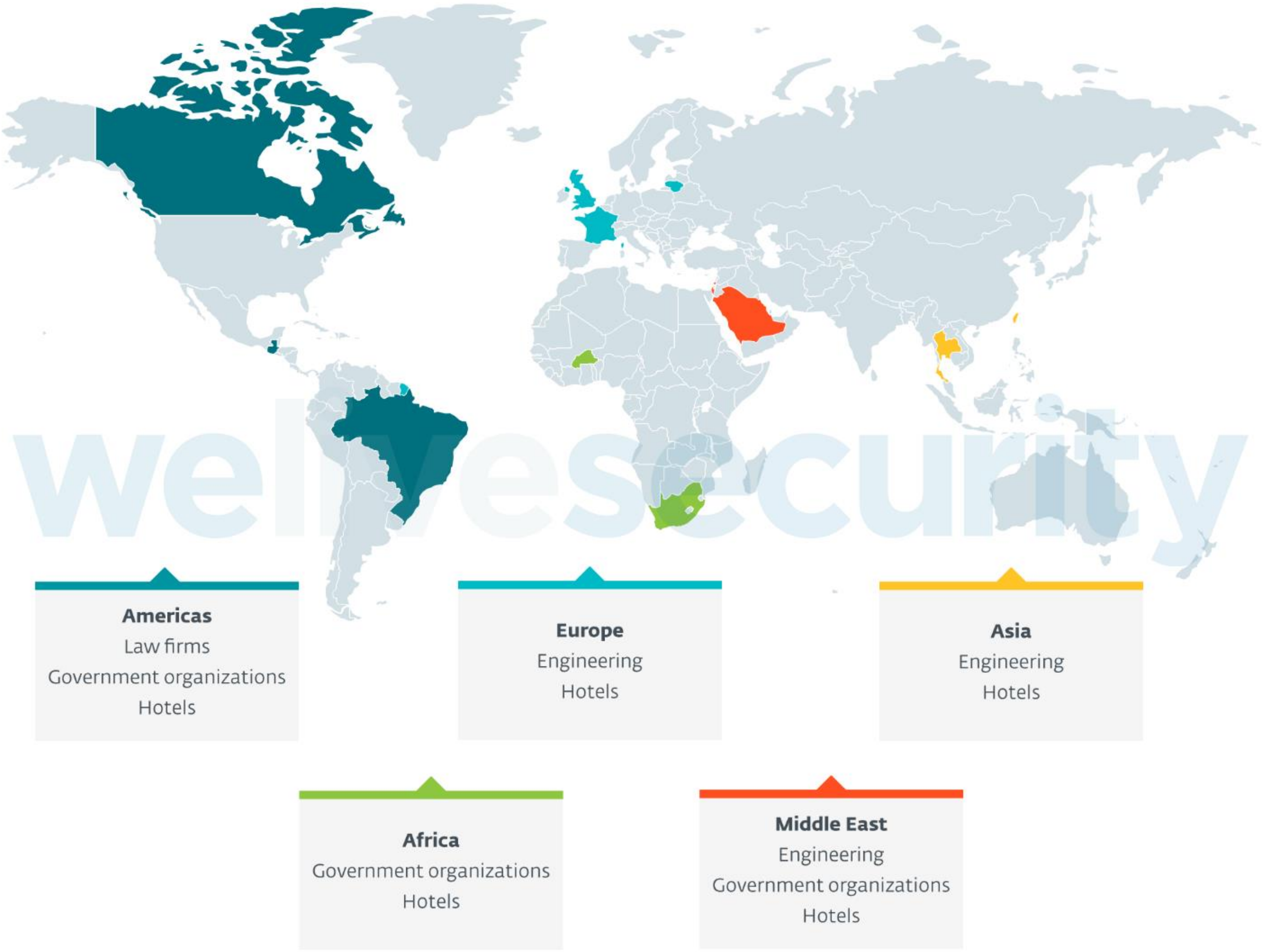
Operation Layover targeting aviation industry

Researchers at Cisco Talos believe that a Nigerian-based threat actor has been launching attacks against the aviation industry for at least the past two years. The actor has consistently used off-the-shelf malware and cryptors sourced from online forums to conceal its activities. The attackers have been spreading AsyncRAT and njRAT using specific lure documents centered around the aviation industry. Victims of the attacks could face data theft, financial fraud or future cyberattacks with much worse consequences.

FamousSparrow group and attacks on engineering firms

According to ESET research, a new backdoor dubbed “SparrowDoor” is being used to target government organizations, engineering firms, law offices and hotels in Europe, the Middle East, the Americas (but not the US), Asia, and Africa. Researchers attribute the backdoor to a new APT threat actor called

"FamousSparrow". The group can be traced back to 2019, but the current attacks leverage the ProxyLogon vulnerability in Microsoft Exchange that was discovered in March. Kaspersky researchers also investigated the case and believe with medium to high confidence, that ESET's description of "FamousSparrow" actually covers several sets of malicious activities from different operators.



Geographic distribution of FamousSparrow targets (Source:ESET)

Kaspersky has observed an overlap in one server that was mentioned as used by FamousSparrow to deliver SparrowDoor and as a staging server used by Chinese-speaking threat actor GhostEmperor, possibly around the same time in July 2020. According to Kaspersky telemetry, GhostEmperor's targets include government entities and telecommunication companies in South East Asia, with multiple high-profile entities targeted in Malaysia, Thailand, Vietnam and Indonesia, and additional victims of a similar nature in countries such as Egypt, Ethiopia and Afghanistan.

APT actors exploiting vulnerabilities in Zoho ManageEngine

On September 16, the FBI, CISA, and United States Coast Guard Cyber Command said in a joint advisory that they believe state-backed APT threat actors have been actively exploiting a newly identified vulnerability (CVE-2021-40539) in the Zoho ManageEngine ADSelfService Plus password management and single sign-on solution that can lead to remote code execution (RCE), providing attackers with a broader access to the corporate network. Threat actors exploiting the vulnerability have targeted academic institutions, defense contractors, and critical infrastructure entities in multiple industries, including transportation, IT, manufacturing, communications, logistics, and finance.

As part of the campaign, the attackers attempted to breach the network of the Port of Houston, one of the largest port authorities in the US. Port officials said in a statement that they had successfully defended their systems against the attack, and “no operational data or systems were impacted as a result” of the attempted intrusion.

In December, CISA and the Federal Bureau of Investigation (FBI) released a new joint advisory, which stated that a newly identified vulnerability in Zoho ManageEngine ServiceDesk Plus (CVE-2021-44077) is being actively exploited. The FBI and CISA assess that APT cyber actors are among those exploiting the vulnerability and have targeted Critical Infrastructure Sector industries, including the healthcare, financial services, electronics and IT consulting industries.

According to a Palo Alto report, there were no public proof-of-concept exploits for CVE-2021-44077 at the time of releasing the advisory (which is no longer the case). This suggests that the APT group may have developed the exploit code itself. Over the three fall months of 2021, at least 13 organizations across the technology, energy, healthcare, education, finance and defense industries were compromised. Additionally, upon exploitation, the actor has been observed uploading a new dropper to victim systems. Similar to the previous tactics used against the ADSelfService software, this dropper deploys a Godzilla webshell which provides the actor with further access to and persistence in compromised systems. Palo Alto Networks has named the combined activity “TiltedTemple“ and has seen evidence that may connect these attacks to the APT27 group (Emissary Panda), who have previously deployed Godzilla against high-profile targets, but the clues are insufficient for clear attribution.

APT-C-36 attacks

Trend Micro has reported a new campaign involving spear-phishing emails that deliver BitRAT as their payload. The campaign was attributed to an actor known as APT-C-36 (aka Blind Eagle), which has retooled its techniques to include a wide range of commodity remote-access Trojans (RATs) and geolocation filtering to avoid detection. Organizations in multiple sectors, including government, financial, healthcare, telecommunications, energy, and oil-and-gas, are said to have been affected, with the majority of the latest campaign's targets located in Colombia and a smaller proportion in Ecuador, Spain, and Panama.

DarkOxide targeting the semiconductor industry

Since September 2019, Crowdstrike has been tracking an as yet unattributed actor, conducting targeted operations against organizations within the Asia Pacific (APAC) semiconductor industry. CrowdStrike Intelligence tracks this activity cluster under the name DarkOxide. CrowdStrike Intelligence has not yet determined the motivation of this activity cluster, but its tactics, techniques and procedures (TTPs) and target scope indicate it is more likely focused on the theft of sensitive information than on direct financial gain. Initially, the actor engages a target via a business-oriented social media platform under the guise of carrying out a recruitment drive. The target is then encouraged to download a lure document purportedly relating to a job opening, which is in fact an executable with a double file extension. The executables in these lures have used non-standard executable file extensions such as .PIF (program information file) and .SCR (screensaver). When the payload is executed, it utilizes a number of scripting interfaces, including PowerShell and Visual Basic Script, to download a further malicious binary executable. This second executable, also with a .PIF or .SCR extension, in turn installs a copy of the legitimate remote access tool, Remote Utilities, with a preconfigured command-and-control (C2) address. In a small number of cases, in addition to Remote Utilities, the actor also installed the Total Manager Pro file manager. It is likely that this was in order to conduct file system searches, or to package files for exfiltration.

ChamelGang attacks

In Q2 2021 the Positive Technologies Expert Security Center (PT ESC) incident response team conducted an investigation in an energy company. The investigation revealed that the company's network had been compromised by an unknown group for the purpose of data theft. The experts dubbed the group ChamelGang. After investigating the initial incident, on August 16, 2021, PT ESC specialists detected a server compromise in a Russian company from the aviation production sector, in which a chain of ProxyShell vulnerabilities were exploited to gain access to the server. During further threat intelligence of the group's activity, the researchers identified 13 more compromised organizations in ten countries of the world. The attackers used such well-known malicious programs as FRP, Cobalt Strike Beacon, and Tiny SHell. They also used new, previously unknown malware named ProxyT, BeaconLoader, and the DoorMe backdoor.

PseudoManuscrypt: a mass-scale spyware attack campaign

In June 2021, Kaspersky ICS CERT experts identified malware whose loader has some similarities to the Manuscrypt malware, which is part of the Lazarus APT group's arsenal. During the period from January 20 to November 10, 2021, the loader identified had been used to attack over 35,000 systems in 195 countries across the globe. At least 7.2% of all systems attacked by the PseudoManuscrypt malware are part of industrial control systems (ICS). Targets of PseudoManuscrypt attacks include a significant number of industrial and government organizations, including enterprises in the military-industrial complex and research laboratories. The main PseudoManuscrypt module has extensive and varied spying functionality. Stealing VPN connection data, logging keypresses, capturing screenshots and videos of the screen, recording sound with the microphone, stealing clipboard data and operating system event log data (which, together, can be used to steal RDP authentication data), etc. Many indirect clues point to the actor behind the attack probably being connected with China. Specifically, some malware samples have comments in Chinese, etc. Data is sent to the attackers' server over the KCP protocol using a library that has previously been seen used only in the malware of the Chinese APT41 group.

Operation GhostShell

Cybereason Nocturnus has reported on Operation GhostShell, a highly-targeted cyber espionage campaign targeting the Aerospace and Telecommunications industries mainly in the Middle East, with additional victims in the U.S., Russia and Europe. Operation GhostShell aims to steal sensitive information about critical assets, infrastructure and technology. A previously undocumented and stealthy RAT, dubbed “ShellClient”, was employed as the primary espionage tool: this has been under ongoing development since at least 2018. Researchers attribute the campaign to a new Iranian threat actor that they are calling “MalKamak”. Their investigation points to possible connections with the Chafer APT (APT39) and the Agrius APT (which Kaspersky tracks as “BlackShadow”).

TA2722 attacks

Proofpoint has identified a new and highly active cybercriminal threat actor dubbed TA2722 / Balikbayan Foxes. Throughout 2021, a series of campaigns by the threat actor impersonated multiple Philippine government entities including the Department of Health, the Philippine Overseas Employment Administration (POEA), and the Bureau of Customs. TA2722 typically targets Shipping/Logistics, Manufacturing, Business Services, Pharmaceutical, and Energy entities, among others. Geographic targeting includes North America, Europe, and Southeast Asia. The email phishing campaign uses OneDrive URLs linking to RAR files with embedded UUE files, a PDF email attachment with an embedded OneDrive link or other malicious URL leading to compressed executables (.iso files) that download and run malware, or Compressed MS Excel documents containing macros which, if enabled, download malware. The campaign’s goal is to distribute Remcos and Nanocore Remote Access Trojans to gain access to the target’s computer and later to steal information from it.

Attacks of Iranian state-sponsored APT actors

A joint advisory from CISA, the FBI, the Australian Cyber Security Centre (ACSC) and the UK National Cyber Security Centre (NCSC) highlights an ongoing malicious cyberattack they link to an Iranian government-sponsored APT threat actor targeting organizations in the healthcare and transportation sectors. The group has been exploiting Fortinet vulnerabilities since at least March and a Microsoft Exchange ProxyShell vulnerability since at least October. Having gained initial access, the threat actor follows up with ransomware, data exfiltration and extortion.

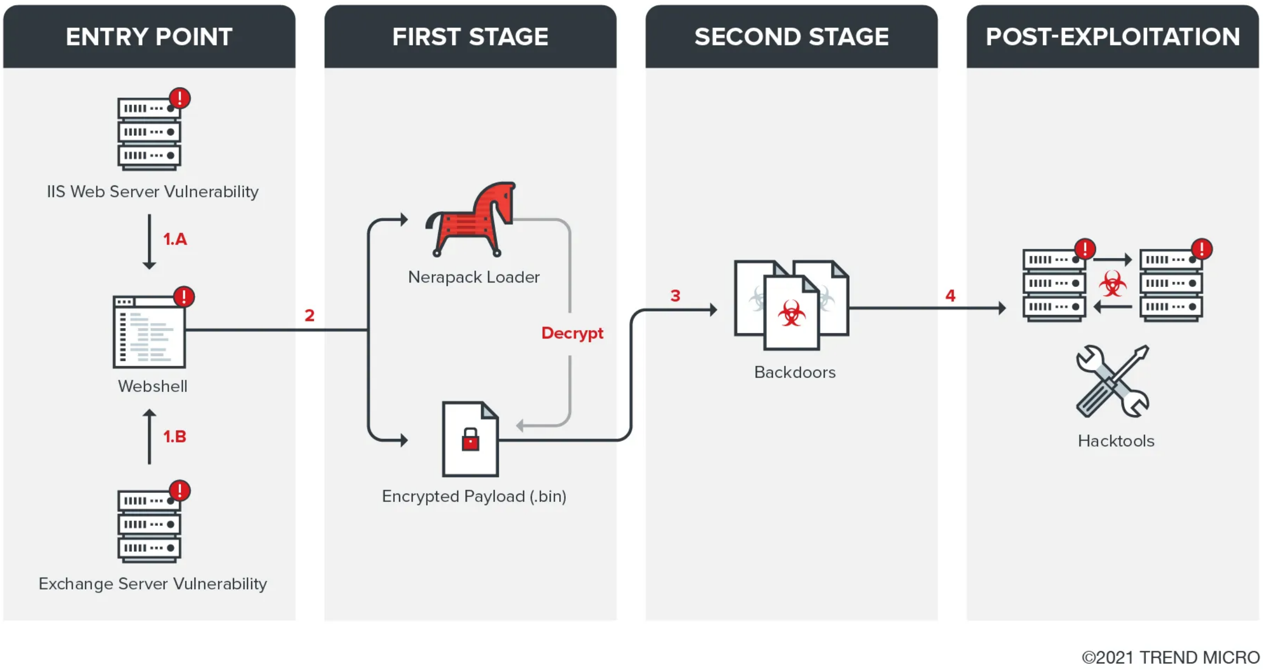
According to a report published by Symantec, they discovered a series of attacks conducted over the second half of 2021 and targeting telecoms, a number of IT services organizations and a utility company. The attacks, which targeted organizations in Israel, Jordan, Kuwait, Saudi Arabia, the United Arab Emirates, Pakistan, Thailand, and Laos, are most likely associated with Iranian state-sponsored hackers. While the identity of the attackers remains unconfirmed, there is some evidence to suggest a link to the Iranian Seedworm (aka MuddyWater) group. While in most attacks the initial attack vector is yet unclear, there is some evidence that a spear-phishing email was possibly used in one case. In one attack against a utility company in Laos that researchers called an "outlier", the threat group appeared to exploit a public-facing service to gain initial entry, as the first compromised machine was an IIS web server, according to the report. Attackers then used PowerShell to deliver malicious tools and scripts to the company's network and ultimately to connect to a webmail server of an organization in Thailand as well as IT-related servers of another Thai company.

Tardigrade malware attacks on Biomanufacturing companies

The Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) has published an advisory describing malware that has been used to target biomanufacturing firms. Dubbed Tardigrade, the malware was first detected in the wake of a ransomware attack but its goals may also include espionage. It has the functionality of a Trojan and uses sophisticated detection evasion techniques. The researchers found that Tardigrade resembles a popular malware downloader known as SmokeLoader/Dofoil but it is more advanced and offers an expanded array of customization options. It is able to decide on lateral movement based on its internal logic.

Tropic Trooper targets transportation and government

Trend Micro has determined that the TropicTrooper/Earth Centaur APT actor targeted organizations in the transportation industry and transport-related government agencies in July 2020. It was observed that the group tried to access some internal documents (such as flight schedules and documents for financial plans) and personal information on the compromised hosts (such as search histories). The threat group used Internet Information Services (IIS) server and Exchange server vulnerabilities as entry points to further deploy webshells, .NET loader and first stage backdoors. Depending on the target, it uses backdoors with different protocols, and it can also use the reverse proxy to bypass the monitoring of network security systems. The group uses opensource frameworks to make customized backdoors. This enables it to create new backdoor variants more efficiently. After successfully exploiting a vulnerable system, the threat actor will use multiple hacking tools to discover and compromise machines on the victim's intranet and tools for exfiltration. It exploits vulnerable websites and uses them as C2 servers.



Stages of Earth Centaur's intrusion process (Source: Trend Micro)

Karakurt group attacks

Accenture Security has identified a new threat group, which calls itself Karakurt Hacking Team. The threat group is financially motivated, opportunistic in nature and focuses solely on data exfiltration and subsequent extortion. Accenture Security is currently aware of over 40 victims spanning multiple industry verticals, including energy, industrial and manufacturing, and organization sizes. Of known victims, 95% are based in North America and the remaining 5% in Europe. It typically uses credential access as the initial vector into victims' networks and utilizes applications already installed to move laterally and exfiltrate data, if available. In addition, the threat group will typically contact the victim multiple times, using different communication methods, to apply additional pressure during extortion attempts.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky 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