Kaspersky ICS CERT

APT and financial attacks on industrial organizations in H2 2023

02.04.2024

Version 1.0

This summary provides an overview of reports on APT and financial attacks on industrial enterprises that were disclosed in H2 2023, 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.

Among many APT-related stories, three stand out. Two of them involve attack vectors that resulted in gaining access to the automated control system and these attacks led to a physical effect – an attack on a Ukrainian energy company and attacks on an Israeli-made Unitronics PLC.

The third story – an attack on industrial companies using MATA tools – is interesting due to the high complexity of the tools used by the attackers, a fascinating story about the lateral movement of attackers within the network of a compromised organization, and the intrigue that arose when attributing the tools to the known APT groups.

Korean-speaking activity

Lazarus attacks

Campaign targeted the defense industry and nuclear engineers

Kaspersky researchers discovered a Lazarus campaign beginning in 2023 that targeted the defense industry and nuclear engineers.

They use Trojanized apps, especially backdoored VNC apps, to access enterprise systems. In this campaign, Lazarus tricks job seekers on social media into opening malicious apps for fake job interviews. To avoid detection by behavior-based security solutions, this backdoored application operates discreetly, activating only when the user selects a server from the Trojanized VNC client's drop-down menu. Upon opening this initial infection vector, the application proceeds to launch additional payloads into memory and retrieve further malicious code.

Kaspersky researchers observed an additional payload known as LPEClient, which has been previously employed multiple times by the Lazarus group. Furthermore, it employs sophisticated C2 communication methods and disables application behavior monitoring of security solutions by unhooking user-mode syscalls. The use of an updated version of COPPERHEDGE as an additional backdoor was identified, exhibiting a complex infection chain. In addition, the presence of a malware variant specifically designed to transfer targeted files to a remote server was observed. This particular malware serves the purpose of exfiltrating specific files chosen by the Lazarus group and sending them to their designated remote server.

Our telemetry confirms numerous instances of compromised companies. The majority of affected entities are directly involved in defense manufacturing, encompassing radar systems, unmanned aerial vehicles (UAVs), military vehicles, vessels, weaponry, and companies related to the navy. Furthermore, in one of the cases, the username associated with the initial infection vector was identified. Through conversations with the victim, Kaspersky researchers found out that this individual was a nuclear engineer based in Hungary who received the malicious file after getting into contact with a suspicious account via Telegram and WhatsApp.

Attacks with LightlessCan backdoor

Researchers at ESET detected a malware campaign involving a previously unknown backdoor named LightlessCan. The Lazarus Group managed to compromise an aerospace company in Spain. The initial vector of attack was a spear phishing email in which the hackers pretended to be recruiters from Meta and sent messages to developers via LinkedIn Messaging.

LightlessCan backdoor Windows functions include the ability to mimic the functionality of many native Windows commands like ping, ipconfig, systeminfo, sc, net, and more. ESET speculated that in developing LightlessCan, Lazarus may have reverse-engineered closed-source system binaries to add additional functionality to the RAT. The threat actor also rigged LightlessCan in such a manner that its encrypted payload can only be decrypted using a decryption key specific to the compromised machine. The goal is to ensure that the payload decryption is only possible on target systems and not in any other environment, Kálnai noted, such as a system belonging to a security researcher.

Operation Blacksmith

A new Lazarus group campaign dubbed “Operation Blacksmith” by Cisco Talos researchers has been using at least three new DLang-based malware strains in attacks on organizations worldwide from manufacturing, agriculture, and physical security sectors since as early as March 2023. This campaign consists of continued opportunistic targeting of enterprises globally that publicly host and expose their vulnerable infrastructure to n-day vulnerability exploitation, such as CVE-2021-44228 (Log4j). Two of the malware variants are RATs, one of which, NineRAT” uses Telegram bots and channels for C2 communications. The non-Telegram-based RAT is tracked by researchers as DLRAT, and the DLang-based downloader is tracked as BottomLoader. Researchers observed an overlap between the TTPs used in this campaign and those of Onyx Sleet (aka PLUTONIUM and Andariel).

Attack on a Russian missile engineering company

SentinelLabs researchers reported that two APT threat actors gained persistent access to the internal systems of a Russian missile and satellite developer. ScarCruft was responsible for the compromise of the company's email systems, while Lazarus compromised the network using a Windows backdoor called OpenCarrot. The analyzed OpenCarrot variant implements over 25 backdoor commands with a wide range of functionality representative of Lazarus group backdoors. According to research, these findings establish connections between two distinct DPRK-affiliated threat actors, suggesting the potential for shared resources, infrastructure, implants, or access to victim networks.

Andariel attacks

AhnLab Security Emergency Response Center (ASEC) researchers analyzed recent attacks carried out by Andariel against universities, ICT, electronic equipment, shipbuilding, and manufacturing companies in South Korea. A characteristic of the attacks is the use of new malware developed in the Go language, including Goat RAT and DurianBeacon. The latter also features a version developed in the Rust language. One of the attacks detected by ASEC in February 2023 is said to have involved the exploitation of security flaws in an enterprise file transfer solution called Innorix Agent to distribute backdoors such as Volgmer and Andardoor, as well as a Golang-based reverse shell known as 1th Troy.

A major cyber espionage campaign in which Andariel APT group hacked a wide range of companies and stole sensitive defense information in South Korea was reported. The investigation is being led by the Seoul Police Department with the involvement of the U.S. FBI. Officials believe that the hackers managed to steal information about laser weapons used to support the operation of the national air defense system. The agencies believe the intrusions were part of a larger cyber campaign that resulted in a total data breach of more than 1.2 TB, including corporate, government and personal data.

Andariel was able to successfully hack 14 organizations, also participating in attacks using ransomware, which were carried out from a loosely monitored South Korean proxy server used by hackers 83 times from December 2022 to March 2023 from Pyongyang's Ryugyong-dong district. The server was used to access the websites of firms and institutions, with the group taking advantage of a South Korean hosting service that rents servers to unidentified clients. Among those compromised were large companies in the field of communications, information security and IT, technology centers, universities and research institutes engaged in advanced developments and technologies, pharmaceutical companies, defense enterprises, and financial organizations.

Attacks on defense contractors with the use of updated MATA framework

Kaspersky experts discovered a new, active campaign of the MATA cluster malware compromising defense contractors in Eastern Europe. The campaign spanned over six months and remained active until May 2023 and featured three new generations of the MATA.

One of them is an evolution of previous MATA generation 2. Second, the malware we dubbed “MataDoor”, has been rewritten from scratch and may be considered as generation 4, and then generation 5 has been rewritten from scratch as well. All of them introduce several modifications to its encryption, configuration, and communication protocols.

The actor demonstrated high capabilities of navigating through and leveraging security solutions deployed in the victim’s environment. In situations where no communication line to a desired target host was possible, the actor used a USB propagation module capable of bridging the air-gapped networks. Attackers used many techniques to hide their activity: rootkits and vulnerable drivers, disguising files as legitimate applications, using ports open for communication between applications, multi-level encryption of files and network activity of malware, setting long wait times between connections to control servers – this and much more shows how sophisticated modern targeted attacks can be.

From the very first versions of MATA the experts have had some doubt as which APT it belongs to. This doubt grew with the latest MATA generations. On one side, there are obvious arguments that tie the MATA family to the Lazarus group. At the same time, the latest MATA generations have more techniques similar to ones used by Five Eyes APT groups.

Middle East-related activity

Dark Caracal attacks

While tracking Dark Caracal's activity, Kaspersky researchers discovered an ongoing campaign targeting public and private sector entities in multiple Spanish-speaking countries. Dark Caracal is known to have been conducting cyber-espionage campaigns since at least 2012. The group's campaigns target governments, military entities, utilities, financial institutions, manufacturing companies, and defense contractors worldwide. Thousands of victims suffered from Dark Caracal – valuable data is found to have been stolen, including intellectual property and personally identifiable information. This group has been referenced as a "cyber mercenary threat group" due to the variety of targets and apparent targeting of multiple governments throughout its campaigns. Since 2021, the activity of this group has been reported focusing on Spanish-speaking countries.

Ballistic Bobcat/Charming Kitten attacks

ESET researchers uncovered a sophisticated cyber-espionage campaign carried out by suspected Iranian-aligned threat actor Ballistic Bobcat (aka APT35, APT42, Charming Kitten, TA453, and PHOSPHORUS). The group used a new backdoor named Sponsor to target organizations in Brazil, Israel, and the UAE: the targeted entities include automotive, manufacturing, engineering, financial services, media, healthcare, technology, and telecoms sectors. The Sponsor backdoor is written in C++ and designed to collect information about the host and process commands received from a remote server, the results of which are sent back to the server.

According to the report, the latest campaign, codenamed Sponsoring Access, involves gaining initial access by exploiting known vulnerabilities in Microsoft Exchange servers. In one of the incidents described by ESET, an Israeli company was compromised by an attacker in August 2021, and the delivery of tools for the next stage (PowerLess, Plink, and a number of open source post-exploitation tools written in Go) was implemented over several months.

As experts concluded, Ballistic Bobcat continues to find opportunities to exploit unpatched vulnerabilities on Microsoft Exchange servers accessible from the network using a new and diverse arsenal of tools.

Imperial Kitten/Yellow Liderc/Tortoiseshell attacks

According to PwC researchers, threat actor Yellow Liderc (aka Imperial Kitten, Tortoiseshell, TA456, and Crimson Sandstorm) has launched watering-hole attacks to distribute IMAPLoader malware, which exploits Windows utilities to identify target systems and deploy additional payloads. The targets of the campaign include maritime, shipping and logistics organizations across the Mediterranean; nuclear, aerospace, and defense industries in the U.S. and Europe, and IT-managed service providers in the Middle East. While new attacks involved compromising legitimate websites with malicious JavaScript designed to exfiltrate data, the threat actor has also used a fraudulent Microsoft Excel document as an initial attack vector.

After the PwC report, CrowdStrike reported that the same actor referred to as Imperial Kitten has been targeting transportation, logistics, and technology sectors in the Middle East, including Israel, since the onset of the Israel-Hamas conflict. The group's activity is characterized by the use of social engineering, particularly job recruitment-themed content, to deliver custom .NET-based implants. The attackers use compromised websites to profile visitors using bespoke JavaScript and exfiltrate the information. In addition to the use of watering holes, the threat actor also uses one-day exploits, stolen credentials, and phishing, and targets upstream IT service providers for initial access.

OilRig attacks

ESET researchers analyzed a series of new OilRig (aka APT34, Lyceum, Crambus, or Siamesekitten) downloaders that the threat actor used in 2022 campaigns to target organizations in Israel, including a healthcare organization, a manufacturing company, and a local governmental body. All targets were previously affected by multiple OilRig campaigns. The new downloaders named SampleCheck5000 (SC5k v1-v3), OilCheck, ODAgent, and OilBooster, are notable for using legitimate cloud storage and cloud-based email services for C2 communications and data exfiltration as a way to hide malicious communication and mask the group's network infrastructure:
Microsoft OneDrive, Exchange Online and Office 365 through via Microsoft Graph and Outlook API, as well as Microsoft Office Exchange Web Services (EWS). These downloaders share similarities with MrPerfectionManager and PowerExchange backdoors, other recent additions to OilRig's toolset that use email-based C&C protocols.

Peach Sandstorm/APT33 attacks

According to Microsoft, the threat actor Peach Sandstorm (aka APT33, Elfin, and Refined Kitten) targeted organizations in the defense industrial base sector using a new backdoor called FalseFont. This is a custom backdoor that allows attackers to remotely access infected systems, launch additional files, and send information to its C2. This malware strain was first observed in the wild around early November 2023. The development and use of FalseFont is consistent with Peach Sandstorm activity observed by Microsoft over the past year, suggesting that Peach Sandstorm is continuing to improve their tradecraft.

Chinese-speaking activity

TEMP.Hex and UNC4698 USB attacks

Researchers at Mandiant reported a threefold increase in attacks involving USB drives in the first half of this year. In one such campaign, threat actor TEMP.Hex (aka HoneyMyte) used USB drives to distribute the Sogu malware, designed to steal sensitive information from host systems. They believe that TEMP.Hex is using Sogu to collect information of economic and national security interest to China. TEMP.Hex is targeting a variety of sectors, including construction and engineering, business services, government, health, transportation, and retail organizations in Europe, Asia, and the U.S.

Another threat actor tracked as UNC4698 is also using USB drives to spread the SnowyDrive malware, which creates a backdoor on infected systems, providing attackers a way to remotely interact with the device and issue commands. The backdoor supports many commands that perform file operations, data exfiltration, reverse shelling, command execution, and reconnaissance. It also spreads to other USB drives and over the network. The malware uses DLL search order hijacking to load a malicious DLL via legitimate executables such as Notepad++, Microsoft Silverlight, VentaFax Software, and CAM UnZip Software. UNC4698 is targeting oil and gas organizations in Asia.

Space Pirates attacks

Positive Technologies released a report on new large-scale attacks on organizations in Russia and Serbia carried out by the Chinese-speaking Space Pirates group tracked by researchers since 2022. The main goal of the group is espionage and data theft. The group has expanded the areas of interest. Over the past year, at least 16 organizations in Russia and one (a ministry) in Serbia have become victims, including state and educational institutions, enterprises of the aviation, rocket-space, and agricultural industries, the military-industrial and fuel-energy complex, and infosec companies.

An Acunetix scanner was found on one of the control servers. This indicates a likely attack vector through the exploitation of vulnerabilities, which has not been observed before. The group also targeted PST mail archives.

The Godzilla web shell and obfuscated Neo-reGeorg tunnel were found on the C2 server. The group also began to use ShadowPad malware. In almost every investigation, there were traces of Deed RAT being used, which is still under development. When investigating the incident, a 64-bit version of this malware was found on one of the infected devices, which is almost the same as the 32-bit version. Two new plugins were found on computers infected with Deed RAT. The first one is called Disk and is used to work with disks. The second plugin is called Portmap, which was based on the ZXPortMap utility. The plugin is used for port forwarding and supports three network commands.

During one of the investigations, a previously unknown sample of malware was found which was delivered through the already installed Deed RAT and subsequently named Voidoor. The life cycle of this malware included interaction through GitHub and the voidtools forum. The latter together with the analysis of GitHub repositories led researchers to the hacker's blog on the Chinese Software Developer Network. Positive Technologies researchers assume with a certain degree of confidence that the author is one of the malware developers (if not the only one).

APT31 attacks

Kaspersky ICS CERT identified over 15 implants and their variants planted by the APT31 (aka Judgment Panda and Zirconium) threat actor in a series of attacks against industrial organizations in Eastern Europe designed to steal sensitive data. The malware is typically installed using DLL hijacking and covers its tracks by using the RC4 algorithm to encrypt data until just prior to being injected. The malware includes a worm component able to infect removable drives and steal sensitive data, including data on an air-gapped device. Other implants include Variants of FourteenHi backdoor, MeatBall backdoor, Implant using Yandex Cloud as C2, and implants used to upload files to Dropbox.

UNC4841 attacks

Following up on earlier research into the exploitation of a remote command injection vulnerability affecting the Barracuda Email Security Gateway (ESG) appliance (CVE-2023-2868) by UNC4841, Mandiant researchers provided further detail on TTPs used by the threat actor.

UNC4841 deployed new malware designed to maintain presence at a small subset of high priority targets compromised either before the patch was released or shortly afterwards. This includes use of the SKIPJACK and DEPTHCHARGE backdoors and the FOXTROT/FOXGLOVE launcher.

The threat actor targeted a wide variety of verticals: primary targets include national governments, high-tech and IT entities, local governments, telecoms providers, manufacturing entities, and colleges and universities.
The US Cybersecurity and Infrastructure Security Agency (CISA) provided additional IoCs associated with the exploitation of this vulnerability.

Flax Typhoon attacks

Microsoft researchers report that a newly discovered Chinese-speaking threat actor dubbed Flax Typhoon targeted dozens of organizations in Taiwan. Flax Typhoon has been active since mid-2021 and has targeted government agencies and education, critical manufacturing, and information technology organizations in Taiwan. The purpose of the attacks is cyber-espionage.

The group seeks to maintain access to organizations across a broad range of industries for as long as possible. Flax Typhoon uses minimal malware, primarily relying on “living-off-the-land” techniques. The attackers obtained initial access by exploiting known vulnerabilities in public-facing servers (in VPN, web, Java, and SQL applications) and deploying web shells, including China Chopper.

The threat actor is thought by some researchers to have been operating since mid-2021. However, Taiwanese threat intelligence group TeamT5 has disputed this, dating the group’s activities back to at least 2020 and giving it the temporary code name SLIME13.

Volt Typhoon attacks

The Black Lotus Labs team at Lumen Technologies linked the threat actor Volt Typhoon (aka BRONZE SILHOUETTE) to a botnet called KV-botnet used to target routers, firewalls, and VPN devices to camouflage malicious traffic within legitimate traffic. The targeted devices include Netgear ProSAFE firewalls, Cisco RV320s, DrayTek Vigor routers, and Axis IP cameras.

The KV-botnet has been used in attacks targeting telecoms and ISPs, a U.S. territorial government entity in Guam, a renewable energy firm in Europe, and U.S. military organizations, though researchers classify the majority of the KV infections as opportunistic.

Beginning in August 2023, researchers observed an uptick in the exploitation of new bots for KV-botnet. This cluster infected SOHO devices associated with a handful of high value networks. While no prebuilt functions in the original binary to enable targeting of the adjacent LAN were discovered, there was the ability to spawn a remote shell on the SOHO device. This capability could have been used to either manually run commands or potentially retrieve a yet-to-be discovered secondary module to target the adjacent LAN.

Redfly attacks

A new threat actor was discovered by Symantec dubbed Redfly that infiltrated the national power grid of an Asian country using the ShadowPad Trojan. The report states that the attackers managed to steal credentials and compromise several computers on the organization's network, and that this attack is the latest in a series of espionage intrusions against the country's critical national infrastructure.

The ShadowPad variant disguises itself as VMware files and directories on infected machines and establishes persistence by registering a service that starts when Windows starts. In addition to ShadowPad, Redfly was seen deploying PackerLoader, a tool for downloading and executing shellcode, and a keylogger, which was installed under different names on different machines. The group acted quite methodically and consistently changed permissions for the driver, which was later used to create file system dumps and download credentials from the Windows registry. Hackers used a tool to dump credentials from LSASS, and a scheduled task was used to execute Oleview for side-loading and lateral movement. To install a keylogger on a compromised machine, the attackers tried to dump credentials using ProcDump.

According to Symantec, the most obvious motive of the group is espionage. Identified tools and infrastructure used in the recent campaign targeting the national power grid overlaps with previously reported attacks attributed to a cluster of APT41 activity (aka Brass Typhoon, Wicked Panda, Winnti, and Red Echo).

Attacks on semiconductor companies in East Asia

Semiconductor companies in East Asia (Taiwan, Hong Kong, Singapore) have been targeted using messages purporting to come from the Taiwan Semiconductor Manufacturing Company (TSMC).

The attacks used the HyperBro backdoor, which leveraged a digitally signed CyberArk binary (fv_host.exe, renamed by malicious actors to vfhost.exe) for DLL side-loading, resulting in the in-memory execution of a Cobalt Strike beacon. The C2 address hardcoded into the Cobalt Strike implant was disguised as a legitimate jQuery CDN, allowing it to bypass firewall protection.

In the second attack variant, hackers used a compromised Cobra DocGuard web server to download an additional McAfee binary (mcods.exe) and a malicious file (which is loaded in the mcods.exe using DLL side-loading), and an encrypted Cobalt Strike shellcode. In this case, the hackers deployed a previously undocumented Go-based backdoor called ChargeWeapon designed to collect and transmit victim's data to the C2 in Base64 encoded form.

EclecticIQ researchers have attributed the campaign to a China-linked threat actor due to its use of HyperBro, which has been almost exclusively used by Lucky Mouse (aka APT27, Budworm, and Emissary Panda). They also found tactical overlaps with RedHotel and Earth Lusca.

Russian-speaking activity

Attacks with DroxiDat/SystemBC

An unknown actor targeted an electric utility in Africa with Cobalt Strike beacons and DroxiDat, a newer variant of the SystemBC payload. This attack occurred in the third and fourth week of March 2023 as part of a small wave of attacks across the world. In one of several related incidents, Nokoyawa ransomware was detected, which is linked with zero-day exploitation and a potential link to a group that deployed the Hive ransomware. To date, the group behind Nokoyawa ransomware activity has not seen publicly available precise political attribution, but appears to be used by an older Russian-speaking crimeware group/ransomware affiliate (probably Pistachio Tempest or FIN12).

APT29/Midnight Blizzard/Nobelium attacks

Microsoft researchers report that Midnight Blizzard (aka Nobelium) has been using Microsoft Teams chats to target individuals in government, NGOs, IT services, technology, discrete manufacturing, and media sectors. Overall, the current investigation indicates this campaign has affected fewer than 40 unique global organizations.

The attackers used compromised Microsoft 365 accounts to create domains that masquerade as organizations offering tech support. They then use these domains to send chat messages with links to web pages where they try to phish recipient's credentials, specifically MFA code.

The FortiGuard Incident Response team reported that in October 2023, a U.S.-based biomedical manufacturing organization was compromised due to a critical CVE-2023-42793 TeamCity vulnerability that the publicly accessible exploit had been released for on September 27, 2023. TeamCity is a product by JetBrains used to manage and automate software compilation, building, testing, and release.

The attack was initially exploited using a custom-built exploit script written in Python. The threat actor used the TeamCity exploit to install an SSH certificate, which they used to maintain access to the victim's environment. After executing the discovery commands, the actor downloaded a DLL file, AclNumsInvertHost.dll, on the TeamCity host and again used the TeamCity RCE vulnerability to create a Windows-scheduled task referencing the DLL file for persistence.

The AclNumsInvertHost.dll library and multiple other DLL files pulled from the threat actors' webserver matched on a Yara rule for a known malware family called GraphicalProton that was historically linked to APT29 (aka the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard/BlueBravo). Given the technique crossover with previously reported activity and the identification of the GraphicalProton payload, FortiGuard believes with medium confidence that this attack was part of a new BlueBravo/APT29 campaign.

In a joint advisory published on December 13, the FBI, the Cybersecurity & Infrastructure Security Agency (CISA), the NSA, the Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the UK National Cyber Security Centre (NCSC) warned that APT29 has been exploiting an authentication bypass vulnerability (CVE-2023-42793) in TeamCity. The agencies have alerted dozens of companies in the U.S., Europe, Asia, and Australia after discovering hundreds of compromised devices.

Attacks exploiting WinRAR vulnerability

The vulnerability CVE-2023-38831 in WinRAR, a Windows file archiving utility, is the high-severity bug which has been exploited since early 2023. RARLabs released WinRAR 6.23 in August to address the vulnerability.

Sandworm attacks

Google's Threat Analysis Group (TAG) observed multiple government-backed hacking groups exploiting the vulnerability CVE-2023-38831. In April 2023, TAG reported on FROZENBARENTS (aka SANDWORM) targeting the energy sector and continuing hack-and-leak operations. In an early-September attack, Sandworm hackers delivered Rhadamanthys infostealer malware in phishing attacks using fake invitations to join a Ukrainian drone training school. Rhadamanthys is a commodity infostealer that collects and exfiltrates browser credentials and session information among other things. It operates on a subscription-based model and can be rented out for as low as $250 for 30 days.

APT28 attacks

The APT28 group (aka Frozenlake, Fancy Bear, Strontium, or Sednit) also used the flaw to deliver malware targeting energy infrastructure in Ukraine via a phishing campaign that used a decoy document inviting targets to an event hosted by Razumkov Center, a public policy think tank in Ukraine.

Proofpoint also reported the use of the vulnerability CVE-2023-38831 by TA422 (aka APT28). According to Proofpoint researchers, TA422 used the vulnerabilities as initial access against government, aerospace, education, finance, manufacturing, and technology sector targets likely to either disclose user credentials or initiate follow-on activity.

In September 2023, the actor sent malicious emails spoofing geopolitical entities and using the BRICS Summit and a European Parliament meeting as subject lures to entice targets to open the emails. The researchers also observed that between September 2023 and November 2023, the attackers sent lures to targets which included a link that, if clicked, initiated a chain of malicious activity from Mockbin service.

In November 2023, TA422 abandoned the use of Mockbin for initial filtering and redirection in favor of direct delivery of InfinityFree URLs.

Mysterious Werewolf

Researchers from Cyble Research and Intelligence Labs (CRIL) uncovered a targeted spear phishing attack on a Russian semiconductor supplier. The phishing email was disguised as an official communication from the Ministry of Industry and Trade of Russia, the email contained a deceptive archive file named resultati_sovehchaniya_11_09_2023.rar.

The threat actors behind this attack also used this vulnerability.

The malicious .NET payload, the Athena agent of the Mythic C2 framework, is equipped with an extensive tool of pre-installed commands tailored to perform various actions on the targeted systems. Athena comes loaded with features, such as Crossplatform for Windows, Linux, and OSX, SOCKS5 Support, Reverse Port Forwarding, Reflective loading of Assemblies, Modular loading of commands, and much more. In this case, it was configured to use Discord as the C2 communication channel.

The BI.ZONE Cyber Threat Intelligence team also tracked this activity cluster dubbed Mysterious Werewolf and uncovered another attack in the campaign, this time targeting industry facilities in Russia. Attackers posed as the Russian Ministry of Industry and Trade and used phishing emails that contained archives named Pismo_izveshcanie_2023_10_16.rar with malicious CMD files that exploited the CVE-2023-38831 vulnerability to launch a PowerShell script and ultimately download an Athena agent. The attackers used a dynamic DNS service and post-exploitation frameworks, as well as a scheduled task to run the agent every 10 minutes.

Other APT28/Fancy Bear attacks

CERT-UA reported a targeted cyberattack against a critical energy infrastructure facility in Ukraine. The attackers sent emails designed to lure targets into downloading a seemingly innocent archive file. This archive contained malicious scripts that hijacked the computer and exfiltrated sensitive data using services such as mockbin.org and mocky.io.

Zscaler researchers analyzed the key components of this attack and another campaign dubbed Steallt with similar TTPs that align with the APT28 (Fancy Bear) threat actor. According to researchers, the attackers stole and exfiltrated NTLMv2 hashes using customized versions of Nishang's Start-CaptureServer PowerShell script and executed various system commands. Threat actors focused on targeting regions including Australia, Poland, and Belgium in this campaign.

Since March, Microsoft researchers have observed phishing attacks by TA422 (aka APT28, Forest Blizzard, Strontium, Fancy Bear, and Fighting Ursa) targeting government, energy, transportation, and non-governmental organizations in the U.S., Europe, and the Middle East.

The threat actor is exploiting two vulnerabilities. The first (CVE-2023-23397) is a Microsoft Outlook elevation of privilege vulnerability. The vulnerability doesn't require any user interaction. Palo Alto researchers have observed the threat actor exploiting this vulnerability over the past 20 months to target at least 30 organizations in 14 countries including in the energy, transportation, and telecommunications sectors, and the military industrial base. The campaigns all used Ubiquiti networking devices to harvest NTLM authentication messages from victim networks. Microsoft initially patched the Outlook vulnerability in March, warning that it was being actively exploited, and has since updated its guidance for customers.

The use of the second vulnerability – CVE-2023-38831 – was reported by Proofpoint (see above).

Other Sandworm/Hades attacks

According to Mandiant researchers, Sandworm (aka Hades) carried out a cyberattack on a Ukrainian electric utility that began in June 2022 and culminated in October 2022, causing a power blackout. The initial access vector into the IT environment wasn't identified.

At first, the attackers deployed the Neo-REGEORG webshell on a server exposed on the public internet. After one month, the hackers executed the Golang-based GOGETTER tunneler to proxy encrypted communications for the command and control server using the Yamux open-source library.

Sandworm gained access to the OT environment through a hypervisor that hosted a supervisory control and data acquisition (SCADA) management instance for the victim's substation environment and maintained access for up to 3 months.

The attack culminated in activity that had a physical effect.

First, Sandworm used an ISO CD-ROM image file to run the native ABB utility scilc.exe, likely to run malicious commands written in the SCIL (Supervisory Control Implementation Language) by ABB – that would switch off the substations on October 10, 2022.

Based on the file timestamp analysis, Mandiant believes the actors needed 2 months to develop the OT capability. Loading the ISO image was possible because the virtual machine that the MicroSCADA was running on had the autorun feature enabled, allowing CD-ROMs, physical or virtual (e.g. an ISO file), to run automatically. The scilc.exe utility is part of the MicroSCADA software suite, and Sandworm used it to run SCIL commands that the server would convert to IEC 101/104 commands and relay them to the remote terminal units in the substation. According to the researchers' findings, the compromised MicroSCADA server was running an end-of-life software version that allowed default access to the SCIL-API. Using a native binary in the attack indicates the hackers' shift to living-off-the-land (LoL/LOTL) techniques that rely on more lightweight and generic tools, which make threat activity more difficult to detect.

Then, on October 12, 2022, Sandworm deployed a new version of the CADDYWIPER data-destroying malware, perhaps in an attempt to hamper analysis of the intrusion. Mandiant did not reveal the location of the targeted energy facility, or the length and scale of the blackout.

Other

RedEnergy attacks

Zscaler ThreatLabz researchers discovered .NET RedEnergy malware used in attacks on enterprises in the energy, oil and gas, telecom, and machinery industries. The malware allows attackers to steal information from various browsers, and also has ransomware functionality (Stealer-as-a-Ransomware).

The attackers use the FAKEUPDATES tactic to deceive victims and force them to download RedEnergy malware disguised as browser updates. The attackers used LinkedIn pages to target victims and redirect them to a fraudulent URL using quite authoritative profile pages, including Philippines Industrial Machinery Manufacturing Company and several organizations in Brazil.

The malware operates through multiple stages, starting with the execution of disguised malicious executables. It establishes persistence, communicates with DNS servers, and downloads additional payloads from remote locations. RedStealer communicates with servers over HTTPS, stores itself in the Windows startup directory, and creates a start menu entry. The researchers also found suspicious activity related to the File Transfer Protocol (FTP), which suggests that it's used by attackers to steal data. After a successful attack, a module is used to encrypt data with the addition of the .FACKOFF! extension to encrypted files, deleting backup copies along the way.

QR code phishing campaign

Researchers at Cofense identified a phishing campaign that uses malicious QR codes to steal Microsoft account credentials. The campaign has been operating since at least May 2023. One of the targets is an unnamed U.S. energy company that received about 29% of the over 1,000 emails.

Most of the phishing emails appear to be Microsoft security notifications. Top organizations were in manufacturing, insurance, technology, and financial services that received 15%, 9%, 7%, and 6% of the emails, respectively.

Most of the identified phishing links were Bing redirect URLs (26%), followed by two domains associated with the Salesforce application (15%) and Cloudflare's Web3 services. The use of Bing URL redirects, coupled with hiding the phishing links in QR codes embedded in images or documents and other obfuscation tactics, helped the malicious messages bypass security controls and land in the recipients' inboxes.

Cofense researchers didn't attribute the new campaign to a specific actor.

Mysterious Team Bangladesh attacks

Group-IB Threat Intelligence researchers analyzed the activities of hacktivist group Mysterious Team Bangladesh. This group, which typically targets logistics, government, and financial sectors in India and Israel (and, to a lesser extent, in Australia, Senegal, the Netherlands, Sweden, and Ethiopia), has been linked to more than 750 DDoS attacks and 78 website defacements since June 2022. The threat actor, thought to be Bangladeshi in origin, reportedly also gained access to web servers and administrative panels, probably by exploiting known security flaws (like vulnerable versions of PHPMyAdmin and WordPress) or poorly-secured passwords.

Cuba ransomware attacks

Kaspersky researchers presented an analysis of Cuba ransomware about the history of the group and typical TTPs.

The group first came to attention in 2020 when it was called Tropical Scorpius. Cuba targeted organizations in the U.S., Canada, Australia, and Europe with a series of high-profile attacks on oil companies, manufacturing, financial services, government agencies, healthcare providers, and others.

The group uses a classic double extortion model, stealing and then encrypting data using the Xsalsa20 symmetric algorithm, and the encryption key uses the asymmetric RSA-2048 algorithm. The ransomware encrypts documents, images, and archives. It also stops all SQL services to encrypt all available databases, and searches for data both locally and within network shares.

In addition to encryption, the group steals sensitive data that it discovers inside the victim's organization. The type of data that hackers look for depends on the industry of the target company. The group uses both well-known classic credential access tools and custom applications: Bughatch, Burntcigar, Cobeacon, Hancitor (Chanitor), Termite, SystemBC, Veeamp, Wedgecut, RomCOM RAT, Mimikatz, PowerShell, PsExec, and Remote Desktop Protocol. Already known software vulnerabilities are mainly exploited, such as the combination of ProxyShell and ProxyLogon to attack Exchange servers, as well as security holes in the Veeam data backup and recovery service.

In the report, Kaspersky researchers present the results of an investigation into one of the incidents with an emphasis on analysis of previously undocumented software, group TTPs, and also share IoCs, Sigma, and YARA rules.

Core Werewolf attacks

Researchers from BI.ZONE Threat Intelligence reported new attacks by the Core Werewolf group in their Telegram channel, targeting enterprises in the defense and energy industries in Russia, as well as other critical infrastructure facilities for espionage purposes.

The attackers sent emails with an attached UKAZ.PDF.ZIP archive, which contained an executable malicious file named "О предоставлении информации по согласованию и наградам.exe" ("On the provision of information on approvals and awards.exe"). The executable file is a self-extracting archive that, when launched, displays the expected PDF or Microsoft Word document on the victim's screen. In the last identified campaign, it was a document with an order from the deputy general director of a well-known industrial company. At the same time, a legitimate UltraVNC tool is installed in the background that allows the attackers to gain full control over the compromised device.

According to BI.ZONE, Core Werewolf has been active since at least December 2021, and its TTPs were shared previously.

Attacks on Russian industrial organizations

Researchers at Kaspersky Lab reported an espionage campaign targeting a number of Russian government and industrial organizations using a custom backdoor written in Go.

The attack vector began with an email with a malicious archive named finansovyy_kontrol_2023_180529.rar. The archive contained a decoy PDF used to distract the victim, as well as an NSIS script that extracts and runs the backdoor from an external URL.

The functionality of the backdoor is limited to spyware and is mainly focused on searching for files of certain extensions and reading the contents of the clipboard. All data sent to C2 is encrypted with AES, and the malware checks the environment it's located in to avoid analysis. The results of these checks are sent to C2 at the initial stage of infection and are used to profile the victim.

Malicious activity was detected in June 2023, and in mid-August, researchers discovered a new version of the malware. The updated malware provided improved evasion of security measures, which indicates ongoing systematic work to optimize attacks.

XDSpy attacks

F.A.C.C.T. researchers report that the XDSpy APT group attacks Russian metallurgists and military-industrial complex enterprises. New malicious mailings were discovered on November 21-22 addressed to a Russian metallurgical enterprise, as well as a research institute specializing in the development of military missiles. In both cases, the email signature displayed the logo of a nuclear research institute, and the email address of a logistics company from Kaliningrad was indicated as the sender. In addition, another email was discovered sent to Russian metallurgists, but from a Belarusian address.

The group's Kill Chain of the new November campaign corresponds to the previously described XDSpy attacks. The emails contain a link to a PDF that leads to downloading a malicious ZIP archive. The archive contains an lnk file and a command line file, which ultimately results in the C# code being compiled into malicious .NET payloads and launched. XDSpy's victimology correlates with previous targets among military, financial, energy, research, and mining companies in the Russian Federation.

Despite the fact that APT has been active since 2011, international researchers still don't know in the interests of which country it works.

DarkWatchman RAT attacks

F.A.C.C.T. researchers detected a new campaign using the fileless JavaScript-based DarkWatchman associated with attacks on Russian companies under the guise of mailings from the Pony Express courier delivery service. The list included 30 recipients from banking institutions, marketplaces, telecom operators, agricultural and fuel and energy companies, and logistics and IT companies.

In the messages, the recipient is informed that the free storage period for their packages has expired, while the attached archive with the invoice contains the malicious DarkWatchman RAT. The emails were sent from the ponyexpress[.]site domain, which has previously been used for phishing. Moreover, the multi-line phone number indicated in the email actually belongs to the Pony Express courier service.

The DarkWatchman RAT has long been observed targeting Russian entities. Previously, DarkWatchman RAT operators distributed malware under the guise of an archive with the results of a fake tender from the Russian Ministry of Defense, fake summonses from the military registration and enlistment office, and also through the fake website of a Russian developer in the field of cryptography.

Hellhounds attacks

Positive Technologies researchers have uncovered the activities of a new group, Hellhounds, which is aimed at Russian commercial and government organizations. The campaign was called Operation Lahat because telemetry from infected hosts was sent to an account with the username “lahat”.

Research started in October 2023, when PT CSIRT discovered the compromise of an energy company using the Decoy Dog trojan. Decoy Dog has been used in attacks against Russian organizations since at least September 2022. However, the sample found on the victim’s host was a new, more refined modification of the trojan.

Researchers reported that Hellhounds makes significant efforts to hide their activity on hosts and the network. At the first stage, attackers use the Decoy Dog Loader, which is protected by a modified version of the UPX packer. Unlike regular UPX, this modification does not unpack an executable file, but rather a shellcode written entirely in the assembly language and using only Linux system calls. The loader itself runs on the system and disguises itself as a legitimate cron service. The second stage uses the main payload, which is a modified version of Pupy RAT (a cross-platform multi-functional backdoor) that researchers call Decoy Dog.

At least 20 Russian organizations have been affected, most of which are in the public sector, information technology, space industry and energy sector, but also including construction, transportation, and logistics companies.

TTP’s analysis didn’t allow researchers to link the attackers to any previously known APT groups.

According to PT, Hellhounds are involved in hacking a Russian telecommunications operator where they managed to put some of its services out of operation. This was reported by Solar 4RAYS researchers as part of their presentation "Thanos' blip for the telecom operator" at SOC-Forum 2023.

Cloud Atlas attacks

F.A.C.C.T. researchers discovered a new cyber espionage campaign by the Cloud Atlas APT group (aka Clean Ursa, Inception, Oxygen) targeting a Russian agro-industrial enterprise and a state-owned research company. The threat actor is known for its persistent campaigns targeting Russia, Belarus, Azerbaijan, Turkey, and Slovenia.

The starting point of the new campaign are phishing messages under the guise of supporting participants in the Special Military Operation and military registration with a lure document that exploits CVE-2017-11882, a six-year-old memory corruption flaw in Microsoft Office's Equation Editor, a technique Cloud Atlas has employed as early as October 2018. The emails originate from popular Russian email services Yandex Mail and VK's Mail.ru. Successful exploitation of the vulnerability leads to executing a shellcode that's responsible for downloading and running an obfuscated HTA file. The downloaded malicious HTML application subsequently launches Visual Basic Script (VBS) files that are ultimately responsible for retrieving and executing an unknown VBS code from a remote server. At the time of the study, the next stage VBS code was unavailable.

Grayling attacks

Symantec researchers shared evidence of a new APT group dubbed “Grayling” that targeted mainly Taiwanese organizations in a cyber-espionage campaign lasting at least four months. The group’s activity began in February 2023 and continued until at least May 2023, stealing sensitive information from manufacturing, IT, and biomedical companies in Taiwan, as well as victims in the U.S., Vietnam, and Pacific Islands.

The group deployed DLL side-loading through the exported API SbieDll_Hook to load tools such as a Cobalt Strike Stager leading to the popular post-exploitation tool Cobalt Strike Beacon. It also installed “Havoc”, an open-source, post-exploitation command-and-control (C2) framework used in a similar way to Cobalt Strike. Grayling used the publicly available spyware tool NetSpy, exploited legacy Windows elevation of privileges bug CVE-2019-0803, and downloaded and executed shellcode, the report noted. Other post-exploitation activities carried out by these attackers includes using kill processes to kill all processes listed in a file called processlist.txt and using Mimikatz for credential-dumping.

Attack against Danish critical infrastructure

Denmark's SektorCERT reported a simultaneous cyberattack on 22 companies associated with the country's energy sector on May 11, 2023. Among the shared details was that one organization lost visibility into three of its remote locations and the organization's employees had to drive out to all that locations.

The attackers exploited a critical command injection vulnerability (CVE-2023-28771) affecting Zyxel firewalls. Eleven companies were successfully compromised: the threat actors executed malicious code to conduct reconnaissance of the firewall configurations and determine the next course of action. Some of the deployed payloads were related to the Mirai Moobot variant.

The agency has attributed the attacks or at least part of them to Sandworm (aka Hades), but without complete certainty. The traffic in one of the affected organizations was linked to an IP address that had previously been used by Sandworm. However, SektorCERT insisted that attribution could not be made with confidence due to the overall lack of evidence.

AeroBlade attacks

BlackBerry researchers discovered a previously unknown cyber espionage hacking group dubbed AeroBlade targeting organizations in the U.S. aerospace sector. The campaign unfolded in two phases: a testing wave in September 2022, and a more advanced attack in July 2023.

The attacks employed spear-phishing with weaponized documents dropping a reverse-shell payload. In both attacks, a reverse shell connected to the same C2 IP address, and the threat actors used the same lure documents in the phishing stage. The final reverse shell of the 2023 attack was stealthier, used more obfuscation and anti-analysis techniques, and included an option to list directories from infected victims.

BlackBerry assesses with medium to high confidence that the goal of the attacks was commercial cyber espionage aiming to gather valuable information.

USB attacks with Vetta Loader

In an investigation conducted by Yoroi's malware ZLab team, a persistent threat was unveiled affecting several Italian companies, primarily in the industrial, manufacturing, and digital printing sectors. The modus operandi of this threat involves the utilization of infected USB drives, exploiting the heavy reliance on pen-drives for data sharing within these sectors.

Researchers identified at least four different variants of the same malware loader dubbed Vetta Loader being launched as part of an infection chain using USB drives, all written in different programming languages: NodeJS, Golang, Python, and .NET. All of them work with the same logic to communicate with C2s and then download other payloads. The final downloaded payloads were no longer available at the time of analysis. The initial USB Infector responsible for infecting the USB devices along with other modules capable of collecting systeminfo and Bitcoin clipper malware were found.

Yoroi researchers say with a medium-high level of confidence that the attacks were implemented by an Italian-speaking threat actor.

CISA alerts

CISA advisory on CVE-2022-47966 and CVE-2022-42475

The attacks on a U.S. aeronautical organization were detailed in an advisory authored by the CISA, FBI, and the Cyber National Mission Force (CNMF). The attacks are believed to have begun in January.

The advisory stated that nation-state advanced persistent threat (APT) groups were exploiting a critical remote code execution vulnerability (CVE-2022-47966) to gain unauthorized access to the organization's Zoho ManageEngine ServiceDesk Plus instance, then moving laterally through their network. Other APT groups exploited a heap-based buffer overflow vulnerability (CVE-2022-42475) in FortiOS SSL-VPN to establish presence on the organization's Fortinet firewall device.

Through the Zoho exploit, the threat actors were able to achieve root level web server access and create a local user account with administrative privileges. Actors were further able to download malware, enumerate the network, collect administrative user credentials, and move laterally through the organization's network.

It was unclear if the attacks resulted in data being accessed, altered, or exfiltrated due to the organization not clearly defining where their data was centrally located and the CISA having limited network coverage.

The advisory did not attribute the attack to any specific threat groups, but noted CISA's investigation uncovered overlapping tactics, techniques and procedures (TTPs) that could be ascribed to multiple APT groups.

CISA advisory on Snatch Ransomware

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA) to disseminate known ransomware IOCs and TTPs associated with the Snatch ransomware variant identified through FBI investigations as recently as June 1, 2023.

The alert warned of the threat actor targeting a wide range of critical infrastructure sectors, including the IT sector, the U.S. defense industrial base, and the food and agriculture vertical.

Since mid-2021, Snatch threat actors have consistently evolved their tactics to take advantage of current trends in the cybercriminal space and have been observed purchasing previously stolen data from other ransomware groups in an attempt to further exploit victims into paying a ransom to avoid having their data released on Snatch's extortion blog.

In many attacks, Snatch operators have targeted weaknesses in the Remote Desktop Protocol (RDP) to gain administrator-level access to a target network. In other instances, they have used stolen or purchased credentials to gain an initial foothold. Once on a network, the threat actor can sometimes spend up to three months moving around the network searching for files and folders to target.

The FBI and CISA advisory described Snatch operators as using a combination of legitimate and malicious tools on compromised networks. These include post-compromise tools such as the Metasploit open-source penetration testing tool, Cobalt Strike for later movement, and utilities such as sc.exe to create, query, add, and delete services and perform other tasks.

CISA alert on BlackTech attacks

A joint advisory from the U.S. National Security Agency (NSA), FBI, Cybersecurity and Infrastructure Security Agency (CISA), Japan National Police Agency (NPA), and Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) warned that a threat group called BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda) has been stealthily modifying Cisco IOS router firmware and taking advantage of routers' domain-trust relationships to move/traverse from subsidiary organizations to primary target organizations in the U.S. and Japan. The hacks targeted government agencies, as well as industrial, technology, media, electronics, and telecommunication companies.

In the advisory, the agencies said BlackTech used the attacks to deploy a customized firmware backdoor. The backdoor functionality is enabled and disabled through specially crafted TCP or UDP packets. They urged multinational organizations to review all network connections with their subsidiary offices and listed a range of security measures they should take to mitigate the APT gang's potential risk.

Cisco has released a bulletin noting that the most prevalent initial access vector in these attacks involves stolen or weak administrative credentials. There was no indication that any Cisco vulnerabilities were exploited.

CISA alert on Rhysida ransomware

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint alert that provides defenders with Rhysida Ransomware indicators of compromise (IOCs), detection information, and tactics, techniques, and procedures (TTPs) discovered during investigations as of September 2023.

The threat actors behind the Rhysida ransomware engage in opportunistic attacks targeting organizations in various industry sectors. Observed as a Ransomware-as-a-Service (RaaS) model, Rhysida actors have compromised organizations in education, manufacturing, information technology, and government sectors since May 2023, and any ransom paid is split between the group and affiliates.

Rhysida actors leverage external-facing remote services, such as VPNs, Zerologon vulnerability (CVE-2020-1472), and phishing campaigns to gain initial access and persistence within a network. It's also said to share overlaps with another ransomware crew known as Vice Society (aka Storm-0832 or Vanilla Tempest).

CISA alert on LockBit 3.0 ransomware

On November 21, 2023, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing & Analysis Center (MS-ISAC), and Australian Signals Directorate's Australian Cyber Security Center (ASD's ACSC) released a joint alert that disseminates Indicators of Compromise (IOCs), Tactics, Techniques and Procedures (TTPs), and detection methods associated with LockBit 3.0 ransomware exploiting CVE-2023-4966, labeled Citrix Bleed, affecting Citrix NetScaler web application delivery control (ADC) and NetScaler Gateway appliances. The vulnerability allows adversaries to bypass password requirements and multi-factor authentication (MFA), allowing them to take control of user sessions on Citrix NetScaler ADC and Gateway appliances.

LockBit is a ransomware family active since September 2019 that operates under the Ransomware-as-a-Service (RaaS) model. LockBit 3.0 affiliates have conducted attacks against organizations of varying sizes across multiple critical infrastructure sectors, including education, energy, financial services, food and agriculture, government and emergency services, healthcare, manufacturing, and transportation.

CISA alert on CyberAv3ngers attacks

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), NSA, EPA, and Israel's National Cyber Directorate published a joint Cybersecurity Advisory (CSA) on December 14 on the threat actor calling itself CyberAv3ngers responsible for the attack on the Municipal Water Authority of Aliquippa in Pennsylvania. In addition to the November CISA alert, the authoring agencies released the joint CSA to share indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with the actor's cyber operations.

The actor is focused on targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. Once the devices are compromised, the hackers defaced their user interface, potentially making the PLC inoperable.

The agencies said IRGC-affiliated threat actors targeted multiple U.S. water sector facilities that rely on Unitronics Vision PLCs since November 22. The victims were located in multiple states.

CISA alert on Star Blizzard

In a joint advisory published on December 7, the “Five Eyes” security agencies (the Cybersecurity and Infrastructure Security Agency (CISA) in coordination with the United Kingdom’s National Cyber Security Centre (UK-NCSC), Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ), and the U.S. National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cyber Command Cyber National Mission Force (CNMF)) warned about the evolving phishing techniques employed by Star Blizzard and its targeting of individuals and organizations, including the U.S. government and defense industrial base.

The alert shares the group’s tactics and techniques based on real-world observations. The attacker uses typical phishing tradecraft and shares a link in an email message or document allegedly leading to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials.

Star Blizzard uses the open-source framework EvilGinx in their spear-phishing activity, which allows them to harvest credentials and session cookies to successfully bypass the use of two-factor authentication. Star Blizzard then uses the stolen credentials to log in to a target’s email account, where they are known to access and steal emails and attachments from the victim’s inbox. They have also set up mail-forwarding rules, giving them ongoing visibility of victim correspondence, and have also used compromised email accounts for further phishing activity.

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