Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

cisa.gov/uscert/ncas/alerts/aa22-083a

Summary

Actions to Take Today to Protect Energy Sector Networks:
• Implement and ensure robust network segmentation between IT and ICS networks.
• Enforce MFA to authenticate to a system.
• Manage the creation of, modification of, use of—and permissions associated with—privileged accounts.

This joint Cybersecurity Advisory (CSA)—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE)—provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and international Energy Sector organizations. CISA, the FBI, and DOE responded to these campaigns with appropriate action in and around the time that they occurred. CISA, the FBI, and DOE are sharing this information in order to highlight historical tactics, techniques, and procedures (TTPs) used by adversaries to target U.S. and international Energy Sector organizations.

On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and a Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) employee for their involvement in the following intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies.[1]

- **Global Energy Sector Intrusion Campaign, 2011 to 2018:** the FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
    - One of the indicted FSB officers was involved in campaign activity that involved deploying Havex malware to victim networks.
    - The other two indicted FSB officers were involved in activity targeting U.S. Energy Sector networks from 2016 through 2018.
- **Compromise of Middle East-based Energy Sector organization with TRITON Malware, 2017:** Russian cyber actors with ties to the TsNIIKhM gained access to and leveraged TRITON (also known as HatMan) malware to manipulate a foreign oil refinery's ICS controllers. TRITON was designed to specifically target Schneider Electric's Triconex Tricon safety systems and is capable of disrupting those systems. Schneider Electric has issued a patch to mitigate the risk of the TRITON malware's attack vector; however, network defenders should install the patch and remain vigilant against these threat actors' TTPs.
    - The indicted TsNIIKhM cyber actor is charged with attempt to access U.S. protected computer networks and to cause damage to an energy facility.
    - The indicted TsNIIKhM cyber actor was a co-conspirator in the deployment of the TRITON malware in 2017.

This CSA provides the TTPs used by indicted FSB and TsNIIKhM actors in cyber operations against the global Energy Sector. Specifically, this advisory maps TTPs used in the global Energy Sector campaign and the compromise of the Middle East-based Energy Sector organization to the MITRE ATT&CK for Enterprise and ATT&CK for ICS frameworks.

CISA, the FBI, and DOE assess that state-sponsored Russian cyber operations continue to pose a threat to U.S. Energy Sector networks. CISA, the FBI, and DOE urge the Energy Sector and other critical infrastructure organizations to apply the recommendations listed in the Mitigations section of this advisory and Appendix A to reduce the risk of compromise.

For more information on Russian state-sponsored malicious cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage. For more information on the threat of Russian state-sponsored malicious cyber actors to U.S. critical infrastructure as well as additional mitigation recommendations, see joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure and CISA's Shields Up Technical Guidance webpage.

Rewards for Justice Program

If you have information on state-sponsored Russian cyber operations targeting U.S. critical infrastructure, contact the Department of State's (DOS) Rewards for Justice program. You may be eligible for a reward of up to $10 million, which DOS is offering for information leading to the identification or location of any person who, while acting under the direction or control of a foreign government, participates in malicious cyber activity against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Contact +1-202-702-7843 on WhatsApp, Signal, or Telegram, or send information via the Rewards for Justice secure Tor-based tips line located on the Dark Web. For more details refer to rewardsforjustice.net.

Click here for a PDF version of this report.

Technical Details

Note: *This advisory uses the MITRE ATT&CK® for Enterprise framework, version 10, and the ATT&CK for ICSs framework. See the ATT&CK for Enterprise and ATT&CK for ICS frameworks for all referenced threat actor tactics and techniques.*

Global Energy Sector Intrusion Campaign, 2011 to 2018

From at least 2011 through 2018, the FSB (also known as Berserk Bear, Energetic Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala) conducted an intrusion campaign against international and U.S. Energy Sector organizations. The threat actor gained remote access to and deployed malware designed to collect ICS-related information on compromised Energy Sector networks, and exfiltrated enterprise and ICS data.

Beginning in 2013 and continuing through 2014, the threat actor leveraged Havex malware on Energy Sector networks. The threat actor gained access to these victim networks via spearphishing emails, redirects to compromised websites, and malicious versions of legitimate software updates on multiple ICS vendor websites. The new software updates contained installations of Havex malware, which infected systems of users who downloaded the compromised updates.

Havex is a remote access Trojan (RAT) that communicates with a command and control (C2) server. The C2 server deploys payloads that enumerate all collected network resources and uses the Open Platform Communications (OPC) standard to gather information about connected control systems devices and resources within the network. Havex allowed the actor to install additional malware and extract data, including system information, lists of files and installed programs, e-mail address books, and virtual private network (VPN) configuration files. The Havex payload can cause common OPC platforms to crash, which could cause a denial-of-service condition on applications that rely on OPC communications. **Note:** for additional information on Havex, see to CISA ICS Advisory ICS Focused Malware and CISA ICS Alert ICS Focused Malware (Update A).

Beginning in 2016, the threat actor began widely targeting U.S. Energy Sector networks. The actor conducted these attacks in two stages: first targeting third-party commercial organizations (such as vendors, integrators, and suppliers) and then targeting Energy Sector organizations. The threat actor used the compromised third-party infrastructure to conduct spearphishing, watering hole, and supply chain attacks to harvest Energy Sector credentials and to pivot to Energy Sector enterprise networks. After obtaining access to the U.S. Energy Sector networks, the actor conducted network discovery, moved laterally, gained persistence, then collected and exfiltrated information pertaining to ICS from the enterprise, and possibly operational technology (OT), environments. Exfiltrated information included: vendor information, reference documents, ICS architecture, and layout diagrams.

For more detailed information on FSB targeting of U.S. Energy Sector networks, See CISA Alert Russian Government Cyber Activity Targeting Energy Sector and Other Critical Infrastructure Sectors.

Refer to Appendix A for TTPs of Havex malware and TTPs used by the actor in the 2016 to 2018 targeting of U.S. Energy Sector networks, as well as associated mitigations.

Compromise of Middle East-based Energy Sector Organization with TRITON Malware, 2017

In 2017, Russian cyber actors with ties to TsNIIKhM gained access to and manipulated a foreign oil refinery's safety devices. TsNIIKhM actors used TRITON malware on the ICS controllers, which resulted in the refinery shutting down for several days.

TRITON is a custom-built, sophisticated, multi-stage malware affecting Schneider Electric's Triconex Tricon, a safety programmable logic controller (PLC) (also referred to as a safety instrumented system [SIS]), which monitors industrial processes to prevent hazardous conditions. TRITON is capable of directly interacting with, remotely controlling, and compromising these safety systems. As these systems are used in a large number of environments, the capacity to disable, inhibit, or modify the ability of a process to fail safely could result in physical consequences. **Note:** for additional information on affected products, see to CISA ICS Advisory Schneider Electric Triconex Tricon (Update B).

TRITON malware affects Triconex Tricon PLCs by modifying in-memory firmware to add additional programming. The extra functionality allows an attacker to read/modify memory contents and execute custom code, disabling the safety system.

TRITON malware has multiple components, including a custom Python script, four Python modules, and malicious shellcode that contains an injector and a payload. For detailed information on TRITON's components, refer to CISA Malware Analysis Report (MAR): HatMan: Safety System Targeted Malware (Update B).

Note: the indicted TsNIIKhM cyber actor was also involved in activity targeting U.S. Energy Sector companies in 2018, and other TsNIIKhM-associated actors have targeted a U.S.-based company's facilities in an attempt to access the company's OT systems. To date, CISA, FBI, and DOE have no information to indicate these actors have intentionally disrupted any U.S. Energy Sector infrastructure.

Refer to Appendix A for TTPs used by TRITON as well as associated mitigations.

Mitigations

Enterprise Environment

CISA, the FBI, and DOE recommend Energy Sector and other critical infrastructure organizations implement the following mitigations to harden their corporate enterprise network. These mitigations are tailored to combat multiple enterprise techniques observed in these campaigns (refer to Appendix A for observed TTPs and additional mitigations).

Privileged Account Management

Manage the creation of, modification of, use of—and permissions associated with—privileged accounts, including `SYSTEM` and root.

Password Policies

Set and enforce secure password policies for accounts.

Disable or Remove Features or Programs

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

Audit

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses.

Operating System Configuration

Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

Multifactor Authentication

Enforce multifactor authentication (MFA) by requiring users to provide two or more pieces of information (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system.

Filter Network Traffic

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

Network Segmentation

Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a demilitarized zone (DMZ) to contain any internet-facing services that should not be exposed from the internal network.

Limit Access to Resources over the Network

Prevent access to file shares, remote access to systems, and unnecessary services. Mechanisms to limit access may include use of network concentrators, Remote Desktop Protocol (RDP) gateways, etc.

Execution Prevention

Block execution of code on a system through application control, and/or script blocking.

Industrial Control System Environment

CISA, the FBI, and DOE recommend Energy Sector and other critical infrastructure organizations implement the following mitigations to harden their ICS/OT environment.

Network Segmentation

- Implement and ensure robust network segmentation between IT and ICS networks to limit the ability of cyber threat actors to move laterally to ICS networks if the IT network is compromised.
    - Implement a network topology for ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer. For more information refer to National Institute of Standard and Technology Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security. Further segmentation should be applied to portions of the network that are reliant on one another by functionality. Figure 5 on page 26 of the CISA ICS Defense in Depth Strategy document describes this architecture.
    - Use one-way communication diodes to prevent external access, whenever possible.
    - Set up DMZs to create a physical and logical subnetwork that acts as an intermediary for connected security devices to avoid exposure.
    - Employ reliable network security protocols and services where feasible.
- Consider using virtual local area networks (VLANs) for additional network segmentation, for example, by placing all printers in separate, dedicated VLANs and restricting users' direct printer access. This same principle can be applied to segmentation of portions of the process for which devices are used. As an example, systems that are only involved in the creation of one component within an assembly line that is not directly related to another component can be on separate VLANs, which allows for identification of any unexpected communication, as well as segmentation against potential risk exposure on a larger scale.
- Implement perimeter security between network segments to limit the ability of cyber threat actors to move laterally.
    - Control traffic between network segments by using firewalls, intrusion detection systems (IDSs), and rules for filtering traffic on routers and switches.
    - Implement network monitoring at key chokepoints—including egress points to the internet, between network segments, core switch locations—and at key assets or services (e.g., remote access services).
    - Configure an IDS to create alarms for any ICS traffic outside normal operations (after establishing a baseline of normal operations and network traffic).
    - Configure security incident and event monitoring to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts.

ICS Best Practices

- Update all software. Use a risk-based assessment strategy to determine which ICS networks, assets, and zones should participate in the patch management program.

- Test all patches in out-of-band testing environments before implementation into production environments.
- Implement application allow listing on human machine interfaces and engineering workstations.
- Harden software configuration on field devices, including tablets and smartphones.
- Replace all end-of-life software and hardware devices.
- Disable unused ports and services on ICS devices (after testing to ensure this will not affect ICS operation).
- Restrict and manage remote access software. Enforce MFA for remote access to ICS networks.
- Configure encryption and security for network protocols within the ICS environment.
- Do not allow vendors to connect their devices to the ICS network. Use of a compromised device could introduce malware.
- Disallow any devices that do not live solely on the ICS environment from communicating on the platform. 'Transient devices' provide risk exposure to the ICS environment from malicious activity in the IT or other environments to which they connect.
- Maintain an ICS asset inventory of all hardware, software, and supporting infrastructure technologies.
- Maintain robust host logging on critical devices within the ICS environment, such as jump boxes, domain controllers, repository servers, etc. These logs should be aggregated into a centralized log server for review.
- Ensure robust physical security is in place to prevent unauthorized personal from accessing controlled spaces that house ICS equipment.
- Regularly test manual controls so that critical functions can be kept running if ICS/OT networks need to be taken offline.

Contact Information

All organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

References

[1] https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical
[2] https://collaborate.mitre.org/attackics/index.php/Software/S0003
[3] https://collaborate.mitre.org/attackics/index.php/Software/S0003
[4] https://collaborate.mitre.org/attackics/index.php/Software/S0013

APPENDIX A: CAMPAIGN AND MALWARE TACTICS, TECHNIQUES, AND PROCEDURES

Global Energy Sector Campaign: Havex Malware

Table 1 maps Havex's capabilities to the ATT&CK for Enterprise framework, and table 2 maps Havex's capabilities to the ATT&CK for ICS framework. Table 1 also provides associated mitigations. For additional mitigations, refer to the Mitigations section of this advisory.

Table 1: Enterprise Domain Tactics and Techniques for Havex [2]

Tactic	Technique	Use	Detection/Mitigations
Persistence [TA0003]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	Havex adds Registry Run keys to achieve persistence.	**Monitor:** monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as `Sysinternals Autoruns` may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.
Privilege Escalation [TA0004]	Process Injection [T1055] **Note:** this technique also applies to: Tactic: Defense Evasion [TA0005]	Havex injects itself into `explorer.exe`.	**Behavior Prevention on End Point:** use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, Application Programming Interface (API) call, etc., behavior. Privileged Account Management: manage the creation of, modification of, use of, and permissions associated with privileged accounts, including `SYSTEM` and root.
Defense Evasion [TA0005]	Indicator Removal on Host: File Deletion [T1070.004]	Havex contains a cleanup module that removes traces of itself from victim networks.	**Monitor:** monitoring for command-line deletion functions to correlate with binaries or other files that an adversary may drop and remove may lead to detection of malicious activity. Another good practice is monitoring for known deletion and secure deletion tools that are not already on systems within an enterprise network, which an adversary could introduce. Some monitoring tools may collect command-line arguments but may not capture `DEL` commands since `DEL` is a native function within `cmd.exe`.

Credential Access [TA0006]	Credentials from Password Stores: Credentials from Web Browsers [T1555.003]	Havex may contain a publicly available web browser password recovery tool.	**Password Policies:** set and enforce secure password policies for accounts.
Discovery [TA0007]	Account Discovery: Email Account [T1087.003]	Havex collects address book information from Outlook	**Monitor:** monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation (WMI) and PowerShell.
File and Directory Discovery [T1083]	Havex collects information about available drives, default browser, desktop file list, My Documents, internet history, program files, and root of available drives.	**Monitor:** monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as WMI and PowerShell.	

Process Discovery [T1057]	Havex collects information about running processes.	**Monitor:** normal, benign system and network events that look like process discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as WMI and PowerShell.
System Information Discovery [T1082]	Havex collects information about the OS and computer name.	**Monitor:** monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as WMI and PowerShell. In cloud-based systems, native logging can be used to identify access to certain APIs and dashboards that may contain system information. Depending on how the environment is used, that data alone may not be useful due to benign use during normal operations.

System Network Configuration Discovery [T1016]	Havex collects information about the internet adapter configuration.	**Monitor:** monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as WMI and PowerShell.	
System Owner/User Discovery [T1033]	Havex collects usernames.		
Collection [TA0009]	Archive Collected Data [T1560]	Havex writes collected data to a temporary file in an encrypted form before exfiltration to a C2 server.	**Audit:** audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses.
Command and Control [TA0011]	Data Encoding: Standard Encoding [T1132.001]	Havex uses standard Base64 + bzip2 or standard Base64 + reverse XOR + RSA-2048 to decrypt data received from C2 servers.	**Detect:** analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes using the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.

Table 2: ICS Domain Tactics and Techniques for Havex [3]

Tactic	Technique	Use
Initial Access	Spearphishing Attachment [T0865]	Havex is distributed through a Trojanized installer attached to emails.

Supply Chain Compromise [T0862] **Note:** this activity also applies to Tactic: Drive by Compromise [T0817]	Havex is distributed through Trojanized installers planted on compromised vendor websites.	
Execution	User Execution [T0863]	Execution of Havex relies on a user opening a Trojanized installer attached to an email.
Discovery	Remote System Discovery [T0846]	Havex uses Windows networking (WNet) to discover all the servers, including OPC servers that are reachable by the compromised machine over the network.
Remote System Information Discovery [T0888]	Havex gathers server information, including CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth.	
Collection	Automated Collection [T0802]	Havex gathers information about connected control systems devices.
Point & Tag Identification [T0861]	Havex can enumerate OPC tags; specifically tag name, type, access, and ID.	
Inhibit Response Function	Denial of Service [T0814]	Havex has caused multiple common OPC platforms to intermittently crash.
Impact	Denial of Control [T0813]	Havex can cause PLCs inability to control connected systems.

Global Energy Sector Campaign: 2016 to 2018 U.S. Energy Sector Targeting

Table 3 maps the 2016 to 2018 U.S. Energy Sector targeting activity to the MITRE ATT&CK Enterprise framework. Mitigations for techniques are also provided in table. For additional mitigations, refer to the Mitigations section of this advisory.

Table 3: Energy Sector Campaign, 2016 to 2018 targeting U.S. Energy Sector: Observed MITRE ATT&CK Enterprise Tactics and Techniques

Tactic	Technique	Use	Detection/Mitigations

Reconnaissance [TA0043]	Gather Victim Identity Information: Credentials [T1589.001]	The threat actor harvested credentials of third-party commercial organizations by sending spearphishing emails that contained a PDF attachment. The PDF attachment contained a shortened URL that, when clicked, led users to a website that prompted the user for their email address and password. The threat actor harvested credentials of Energy Sector targets by sending spearphishing emails with a malicious Microsoft Word document or links to the watering holes created on compromised third-party websites. **Note:** this activity also applies to: Tactic: Reconnaissance [TA0043], Technique: Phishing for Information [T1598]: ◦ Spearphishing Attachment [T1598.002] ◦ Spearphishing Link [T1598.003]	**Software Configuration:** implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates. **User Training:** train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

Resource Development [TA0042]	Compromise Infrastructure: Server [T1584.004]	The threat actor created watering holes on compromised third-party organizations' domains.	This activity typically takes place outside the visibility of target organizations, making detection of this behavior difficult. Ensure that users browse the internet securely. Prevent intentional and unintentional download of malware or rootkits, and users from accessing infected or malicious websites. Treat all traffic as untrusted, even if it comes from a partner website or popular domain.
Initial Access [TA0001]	Valid Accounts [T1078]	The threat actor obtained access to Energy Sector targets by leveraging compromised third-party infrastructure and previously compromised Energy Sector credentials against remote access services and infrastructure—specifically VPN, RDP, and Outlook Web Access—where MFA was not enabled.	**Network Segmentation:** architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. **MFA:** enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system. **Privileged Account Management:** manage the creation of, modification of, use of, and permissions associated with privileged accounts, including `SYSTEM` and root.

Update Software: perform regular software updates to mitigate exploitation risk.

Exploit Protection: use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.

Application Isolation and Sandboxing: restrict execution of code to a virtual environment on or in transit to an endpoint system.

External Remote Services [T1133]	The threat actor installed VPN clients on compromised third-party targets to connect to Energy Sector networks.	**Network Segmentation:** architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. **MFA:** enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system. **Limit Access to Resource Over Network:** prevent access to file shares, remote access to systems, and unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc. **Disable or Remove Program:** remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.001]	During an RDP session, the threat actor used a PowerShell Script to create an account within a victim's Microsoft Exchange Server. **Note:** this activity also applies to: Tactic: Persistence [TA0003], Technique: Create Account: Local Account [T1136.001]	**Antivirus/Antimalware:** use signatures or heuristics to detect malicious software. **Code Signing:** enforce binary and application integrity with digital signature verification to prevent untrusted code from executing. **Disable or Remove Program:** remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries. **Privileged Account Management:** manage the creation of, modification of, use of, and permissions associated with privileged accounts, including SYSTEM and root.

Command and Scripting Interpreter: Windows Command Shell [T1059.003]	The threat actor used a JavaScript with an embedded Command Shell script to: • Create a local administrator account; • Disable the host-based firewall; • Globally open port 3389 for RDP access; and • Attempt to add the newly created account to the administrators group to gain elevated privileges. **Note**: this activity also applies to: • Tactic: Credential Access [TA0006], Technique: Input Capture [T1056] • Tactic: Execution [TA0002], Technique: Command and Scripting Interpreter: JavaScript [T1059.007] • Tactic: Persistence [TA0003], Technique: Create Account: Local Account [T1136.001]	**Execution Prevention:** block execution of code on a system through application control, and/or script blocking.

Scheduled Task/Job: Scheduled Task [T1053.005]	The threat actor created a Scheduled Task to automatically log out of a newly created account every eight hours.	**Audit:** audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses. **Harden Operating System Configuration:** make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques. **Privileged Account Management:** manage the creation of, modification of, use of, and permissions associated with privileged accounts, including `SYSTEM` and root. **User Account Management:** manage the creation of, modification of, use of, and permissions associated with user accounts.	
Persistence [TA0003]	Create Account: Local Account [T1136.001]	The threat actor created local administrator accounts on previously compromised third-party organizations for reconnaissance and to remotely access Energy Sector targets. MFA: enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system.	**MFA:** enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system. **Privileged Account Management:** manage the creation of, modification of, use of, and permissions associated with privileged accounts, including `SYSTEM` and root.

Server Software Component: Web Shell [T1505.003]	The threat actor created webshells on Energy Sector targets' publicly accessible email and web servers.	**Detect:** the portion of the webshell that is on the server may be small and look innocuous. Process monitoring may be used to detect Web servers that perform suspicious actions such as running cmd.exe or accessing files that are not in the Web directory. File monitoring may be used to detect changes to files in the Web directory of a Web server that do not match with updates to the Web server's content and may indicate implantation of a Web shell script. Log authentication attempts to the server and any unusual traffic patterns to or from the server and internal network.

Defense Evasion [TA0005]	Indicator Removal on Host: Clear Windows Event Logs [T1070.001]	The threat actor created new accounts on victim networks to perform cleanup operations. The accounts created were used to clear the following Windows event logs: System, Security, Terminal Services, Remote Services, and Audit. The threat actor also removed applications they installed while they were in the network along with any logs produced. For example, the VPN client installed at one third-party commercial facility was deleted along with the logs that were produced from its use. Finally, data generated by other accounts used on the systems accessed were deleted. **Note:** this activity also applies to: Tactic: Persistence [TA0003], Technique: Create Account: Local Account [T1136.001]	**Encrypt Sensitive Information:** protect sensitive information with strong encryption. **Remote Data Storage:** use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information. **Restrict File and Directory Permissions:** restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

Indicator Removal on Host: File Deletion [T1070.004]	The threat actor cleaned up target networks by deleting created screenshots and specific registry keys. The threat actor also deleted all batch scripts, output text documents, and any tools they brought into the environment, such as `scr.exe`. **Note:** this activity also applies to: Technique: Modify Registry [T1112]	**Monitor:** monitoring for command-line deletion functions to correlate with binaries or other files that an adversary may drop and remove may lead to detection of malicious activity. Another good practice is monitoring for known deletion and secure deletion tools that are not already on systems within an enterprise network that an adversary could introduce. Some monitoring tools may collect command-line arguments, but may not capture `DEL` commands since `DEL` is a native function within `cmd.exe`.
Technique: Masquerading [T1036]	After downloading tools from a remote server, the threat actor renamed the extensions.	**Restrict File and Directory Permissions:** restrict access by setting directory and file permissions that are not specific to users or privileged accounts. **Code Signing:** enforce binary and application integrity with digital signature verification to prevent untrusted code from executing. **Execution Prevention:** block execution of code on a system through application control, and/or script blocking.

Credential Access [TA0006]	Brute Force: Password Cracking [T1110.002]	The threat actor used password-cracking techniques to obtain the plaintext passwords from obtained credential hashes. The threat actor dropped and executed open-source and free password cracking tools such as Hydra, SecretsDump, and CrackMapExec, and Python.	**MFA:** enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system. **Password Policies:** set and enforce secure password policies for accounts.
Forced Authentication [T1187]	Microsoft Word attachments sent via spearphishing emails leveraged legitimate Microsoft Office functions for retrieving a document from a remote server over Server Message Block (SMB) using Transmission Control Protocol ports 445 or 139. As a part of the standard processes executed by Microsoft Word, this request authenticates the client with the server, sending the user's credential hash to the remote server before retrieving the requested file. (**Note:** transfer of credentials can occur even if the file is not retrieved.)	**Password Policies:** set and enforce secure password policies for accounts. **Filter Network Traffic:** use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.	
The threat actor's watering hole sites contained altered JavaScript and PHP files that requested a file icon using SMB from an IP address controlled by the threat actors.			

The threat actor manipulated `LNK` files to repeatedly gather user credentials. Default Windows functionality enables icons to be loaded from a local or remote Windows repository. The threat actor exploited this built-in Windows functionality by setting the icon path to a remote server controller by the actors. When the user browses to the directory, Windows attempts to load the icon and initiate an SMB authentication session. During this process, the active user's credentials are passed through the attempted SMB connection.

Note: this activity also applies to:

> Tactic: Persistence [TA0003], Technique: Boot or Logon Autostart Execution: Shortcut Modification [T1547.009]

OS Credential Dumping: Local Security Authority Subsystem Service (LSASS) Memory [T1003.001]	The threat actor used an Administrator PowerShell prompt to enable the WDigest authentication protocol to store plaintext passwords in the LSASS memory. With this enabled, credential harvesting tools can dump passwords from this process's memory.	**Operating System Configuration:** make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques. **Password Policies:** set and enforce secure password policies for accounts. **Privileged Account Management:** manage the creation of, modification of, use of, and permissions associated with privileged accounts, including `SYSTEM` and root. **Privileged Process Integrity:** protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defenses, or other process integrity enforcement measures. **User Training:** train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction. **Credential Access Protection:** use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.

OS Credential Dumping: NTDS [T1003.003]	The threat actor collected the files `ntds.dit`. The file `ntds.dit` is the Active Directory (AD) database that contains all information related to the AD, including encrypted user passwords.	**Monitor:** monitor processes and command-line arguments for program execution that may be indicative of credential dumping, especially attempts to access or copy the `NTDS.dit`. **Privileged Account Management:** manage the creation of, modification of, se of, and permissions associated with privileged accounts, including `SYSTEM` and root. **User Training:** train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

Discovery [TA0007]	Remote System Discovery [T1018]	The threat actor used privileged credentials to access the Energy Sector victim's domain controller. Once on the domain controller, the threat actors used batch scripts `dc.ba` t and `dit.bat` to enumerate hosts, users, and additional information about the environment. **Note:** this activity also applies to: • Tactic: Persistence [TA0003], Technique: Valid Accounts: Domain Accounts [T1078.002] • Tactic: Discovery [TA0007], Technique: System Owner/User Discovery [T1033]	**Monitor:** normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Monitor for processes that can be used to discover remote systems, such as `ping.exe` and `tracert.exe`, especially when executed in quick succession.
The threat actor accessed workstations and servers on corporate networks that contained data output from control systems within energy generation facilities. The threat actors accessed files pertaining to ICS or supervisory control and data acquisition (SCADA) systems.			

The actor targeted and copied profile and configuration information for accessing ICS systems on the network. The threat actor copied Virtual Network Connection (VNC) profiles that contained configuration information on accessing ICS systems and took screenshots of a Human Machine Interface (HMI). **Note:** this activity also applies to • Tactic: Discovery [TA0007], Technique File and Directory Discovery [T1083] • Tactic: [TA0009], Technique: Screen Capture [T1113]		
File and Directory Discovery [T1083]	The actor used `dirsb.bat` to gather folder and file names from hosts on the network. **Note:** this activity also applies to: Tactic: Execution [TA0002], Command and Scripting Interpreter: Windows Command Shell [T1059.003]	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information.

The threat actor conducted reconnaissance operations within the network. The threat actor focused on identifying and browsing file servers within the intended victim's network.			
Lateral Movement [TA0008]	Lateral Tool Transfer [T1570]	The threat actor moved laterally via `PsExec`, batch scripts, RDP, VNC, and admin shares. **Note:** this activity also applies to: Tactic: Lateral Movement [TA0008], Techniques: ◦ Remote Services: Remote Desktop Protocol [T1021.001] ◦ Remote Services: SMB/Windows Admin Shares [T1021.002] ◦ Remote Services: VNC [T1021.005]	**Network Intrusion Prevention:** use intrusion detection signatures to block traffic at network boundaries. **Network Segmentation:** architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. **Operating System Configuration:** make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques. **Privileged Account Management:** manage the creation of, modification of, use of, and permissions associated with privileged accounts, including `SYSTEM` and root. **User Account Management:** manage the creation of,

modification o, se of, and permissions associated with user accounts.

Disable or Remove Feature or Program: remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

Audit: audit or scan systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

MFA: enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system.

Limit Access to Resource Over Network: prevent access to file shares, remote access to systems, and unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.

Filter Network Traffic: use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

Limit Software Installation: block users or groups from installing unapproved software.

Collection [TA0009]	Data from Local System [T1005]	The threat actor collected the Windows `SYSTEM` registry hive file, which contains host configuration information.	**Monitor:** monitor processes and command-line arguments for actions that could be taken to collect files from a system. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as WMI and PowerShell.
Archive Collected Data: Archive via Utility [T1560.001]	The threat actor compressed the `ntds.dit` file and the `SYSTEM` registry hive they had collected into archives named `SYSTEM.zip` and `comps.zip`.	**Audit:** audit or scan systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.	

Screen Capture [T1113]	The threat actor used Windows' Scheduled Tasks and batch scripts, to execute `scr.exe` and collect additional information from hosts on the network. The tool `scr.exe` is a screenshot utility that the threat actor used to capture the screen of systems across the network. **Note:** this activity also applies to: Tactic: Execution [TA0002], Techniques: ◦ Command and Scripting Interpreter: Windows Command Shell [T1059.003] ◦ Scheduled Task/Job: Scheduled Task [T1053.005]	**Network Segmentation:** architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. **MFA:** enforce use of two or more pieces of evidence (such as username and password plus a token, e.g., a physical smart card or token generator) to authenticate to a system. **Limit Access to Resource Over Network:** prevent access to file shares, remote access to systems, and unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc. **Disable or Remove Feature or Program:** remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

The actor used batch scripts labeled `pss.bat` and `psc.bat` to run the PsExec tool. PsExec was used to execute `scr.exe` across the network and to collect screenshots of systems in a text file.

Note: this activity also applies to:

Tactic: Execution [TA0002],
Techniques:

- Command and Scripting Interpreter: Windows Command Shell [T1059.003]
- System Services: Service Execution [T1569.002]

Command and Control [TA0011]	Ingress Tool Transfer [T1105]	The threat actor downloaded tools from a remote server.	**Monitor:** monitor for file creation and files transferred into the network. Unusual processes with external network connections creating files on-system may be suspicious. Use of utilities, such as File Transfer Protocol, that does not normally occur may also be suspicious. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. Use intrusion detection signatures to block traffic at network boundaries.

TRITON Malware

Table 4 maps TRITON's capabilities to the ATT&CK for ICS framework. For mitigations to harden ICS/OT environments, refer to the Mitigations section of this advisory.

Table 4: ICS Domain Tactics and Techniques for TRITON [4]

Initial Access	Engineering Workstation Compromise [T0818]	TRITON compromises workstations within the safety network.
Execution	Change Operating Mode [T0858] **Note:** this technique also applies to Evasion.	TRITON can halt or run a program through the TriStation protocol. (**Note:** TriStation protocol is the protocol that Triconex System software uses to communicate with the Tricon PLCs.)

Execution through API [T0871]	TRITON leverages a custom implementation of the TriStation protocol, which triggers APIs related to program download, program allocation, and program changes.
Hooking [T0874] **Note:** this technique also applies to Tactic: Privilege Escalation.	TRITON's injector modifies the address of the handler for a Tristation protocol command so that when the command is received, the payload may be executed instead of normal processing.
Modify Controller Tasking [T0821]	Some TRITON components are added to the program table on the Tricon so that they are executed by the firmware once each cycle.
Native API [T0834]	TRITON's payload takes commands from `TsHi.ExplReadRam(Ex)`, `TsHi.ExplWriteRam(Ex)`, and `TsHi.ExplExec` functions to perform operations on controller memory and registers using `syscalls` written in PowerPC shellcode.
Scripting [T0853]	TRITON communicates with Triconex Tricon PLCs using its custom Python script. This Python script communicates using four Python modules that collectively implement the TriStation protocol via User Datagram Protocol (UDP) 1502. **Note:** this use also applies to: Tactic: Command and Control ⎪ Technique: Commonly Used Port [T0885]

Persistence	System Firmware [T0857] **Note:** this technique also applies to Tactic: Inhibit Response Function.	TRITON's injector injects the payload into the Tricon PLCs' running firmware. A threat actor can use the payload to read and write memory on the PLC and execute code at an arbitrary address within the firmware. If the memory address it writes to is within the firmware region, the malicious payload disables address translation, writes the code at the provided address, flushes the instruction cache, and re-enables address translation. This allows the malware to change the running firmware.
Privilege Escalation	Exploitation for Privilege Escalation [T0890]	TRITON can gain supervisor-level access and control system states by exploiting a vulnerability.
Evasion	Exploitation for Evasion [T0820]	TRITON's injector exploits a vulnerability in the device firmware to escalate privileges and then it disables and (later patches) a firmware RAM/ROM consistency check.
Indicator Removal on Host [T0872]	After running the malicious payload, TRITON's Python script overwrites the malicious payload with a "dummy" program.	
Masquerading [T0849]	TRITON's Python script masquerades as legitimate Triconex software.	
TRITON's injector masquerades as a standard compiled PowerPC program for the Triconex PLC.		
Discovery	Remote System Discovery [T0846]	TRITON's Python script can autodetect Triconex PLCs on the network by sending a UDP broadcast packet over port 1502.
Lateral Movement	Program Download [T0843]	TRITON leverages the TriStation protocol to download programs to the Tricon PLCs.
Collection	Detect Operating Mode [T0868]	A TRITON Python module provides string representations of different features of the TriStation protocol, including message and error codes, key position states, and other values returned by the status functions.
Program Upload [T0845]	TRITON uploads its payload to the Tricon PLCs.	

Impair Process Control	Unauthorized Command Message [T0855]	A threat actor can use TRITON to prevent the Tricon PLC from functioning appropriately.
Impact	Loss of Safety [T0880]	TRITON can reprogram the safety PLC logic to allow unsafe conditions or state to persist.

Revisions

March 24, 2022: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.