APT Cyber Tools Targeting ICS/SCADA Devices

cisa.gov/uscert/ncas/alerts/aa22-103a

Summary

Actions to Take Today to Protect ICS/SCADA Devices:
• Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
• Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks.
• Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors.

The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising and maintaining full system access to ICS/SCADA devices, APT actors could elevate privileges, move laterally within an OT environment, and disrupt critical devices or functions.

DOE, CISA, NSA, and the FBI urge critical infrastructure organizations, especially Energy Sector organizations, to implement the detection and mitigation recommendations provided in this CSA to detect potential malicious APT activity and harden their ICS/SCADA devices.

Click here for a PDF version of this report.

Technical Details

APT actors have developed custom-made tools that, once they have established initial access in an OT network, enables them to scan for, compromise, and control certain ICS/SCADA devices, including the following:

- Schneider Electric MODICON and MODICON Nano PLCs, including (but may not be limited to) TM251, TM241, M258, M238, LMC058, and LMC078;
- OMRON Sysmac NJ and NX PLCs, including (but may not be limited to) NEX NX1P2, NX-SL3300, NX-ECC203, NJ501-1300, S8VK, and R88D-1SN10F-ECT; and
- OPC Unified Architecture (OPC UA) servers.

The APT actors' tools have a modular architecture and enable cyber actors to conduct highly automated exploits against targeted devices. The tools have a virtual console with a command interface that mirrors the interface of the targeted ICS/SCADA device. Modules interact with targeted devices, enabling operations by lower-skilled cyber actors to emulate higher-skilled actor capabilities.

The APT actors can leverage the modules to scan for targeted devices, conduct reconnaissance on device details, upload malicious configuration/code to the targeted device, back up or restore device contents, and modify device parameters.

In addition, the APT actors can use a tool that installs and exploits a known-vulnerable ASRock-signed motherboard driver, `AsrDrv103.sys,` exploiting CVE-2020-15368 to execute malicious code in the Windows kernel. Successful deployment of this tool can allow APT actors to move laterally within an IT or OT environment and disrupt critical devices or functions.

APT Tool for Schneider Electric Devices

The APT actors' tool for Schneider Electric devices has modules that interact via normal management protocols and Modbus (TCP 502). Modules may allow cyber actors to:

- Run a rapid scan that identifies all Schneider PLCs on the local network via User Datagram Protocol (UDP) multicast with a destination port of 27127 (Note: UDP 27127 is a standard discovery scan used by engineering workstations to discover PLCs and may not be indicative of malicious activity);
- Brute-force Schneider Electric PLC passwords using CODESYS and other available device protocols via UDP port 1740 against defaults or a dictionary word list (Note: this capability may work against other CODESYS-based devices depending on individual design and function, and this report will be updated as more information becomes available);
- Conduct a denial-of-service attack to prevent network communications from reaching the PLC;
- Sever connections, requiring users to re-authenticate to the PLC, likely to facilitate capture of credentials;

- Conduct a ‘packet of death’ attack to crash the PLC until a power cycle and configuration recovery is conducted; and
- Send custom Modbus commands (Note: this capability may work against Modbus other than in Schneider Electric PLCs).

Refer to the appendix for tactics, techniques, and procedures (TTPs) associated with this tool.

APT Tool for OMRON

The APT actors’ tool for OMRON devices has modules that can interact by:

- Scanning for OMRON using Factory Interface Network Service (FINS) protocol;
- Parsing the Hypertext Transfer Protocol (HTTP) response from OMRON devices;
- Retrieving the media access control (MAC) address of the device;
- Polling for specific devices connected to the PLC;
- Backing up/restoring arbitrary files to/from the PLC; and
- Loading a custom malicious agent on OMRON PLCs for additional attacker-directed capability.

Additionally, the OMRON modules can upload an agent that allows a cyber actor to connect and initiate commands—such as file manipulation, packet captures, and code execution—via HTTP and/or Hypertext Transfer Protocol Secure (HTTPS).

Refer to the appendix for TTPs associated with this tool.

APT Tool for OPC UA

The APT actors’ tool for OPC UA has modules with basic functionality to identify OPC UA servers and to connect to an OPC UA server using default or previously compromised credentials. The client can read the OPC UA structure from the server and potentially write tag values available via OPC UA.

The threat from this tool can be significantly reduced by properly configuring OPC UA security. Refer to the Mitigations below for more information.

Refer to the appendix for TTPs associated with this tool.

Mitigations

Note: these mitigations are provided to enable network defenders to begin efforts to protect systems and devices from new capabilities. They have not been verified against every environment and should be tested prior to implementing.

DOE, CISA, NSA, and the FBI recommend all organizations with ICS/SCADA devices implement the following proactive mitigations:

- Isolate ICS/SCADA systems and networks from corporate and internet networks using strong perimeter controls, and limit any communications entering or leaving ICS/SCADA perimeters.
- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
- Have a cyber incident response plan, and exercise it regularly with stakeholders in IT, cybersecurity, and operations.
- Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks.
- Ensure OPC UA security is correctly configured with application authentication enabled and explicit trust lists.
- Ensure the OPC UA certificate private keys and user passwords are stored securely.
- Maintain known-good offline backups for faster recovery upon a disruptive attack, and conduct hashing and integrity checks on firmware and controller configuration files to ensure validity of those backups.
- Limit ICS/SCADA systems' network connections to only specifically allowed management and engineering workstations.
- Robustly protect management systems by configuring Device Guard, Credential Guard, and Hypervisor Code Integrity (HVCI). Install Endpoint Detection and Response (EDR) solutions on these subnets and ensure strong anti-virus file reputation settings are configured.
- Implement robust log collection and retention from ICS/SCADA systems and management subnets.
- Leverage a continuous OT monitoring solution to alert on malicious indicators and behaviors, watching internal systems and communications for known hostile actions and lateral movement. For enhanced network visibility to potentially identify abnormal traffic, consider using CISA's open-source Industrial Control Systems Network Protocol Parsers (ICSNPP).
- Ensure all applications are only installed when necessary for operation.
- Enforce principle of least privilege. Only use admin accounts when required for tasks, such as installing software updates.
- Investigate symptoms of a denial of service or connection severing, which exhibit as delays in communications processing, loss of function requiring a reboot, and delayed actions to operator comments as signs of potential malicious activity.
- Monitor systems for loading of unusual drivers, especially for ASRock driver if no ASRock driver is normally used on the system.

Resources

For additional guidance on securing OT devices, see

- Layering Network Security Through Segmentation,
- Stop Malicious Cyber Activity Against Connected Operational Technology, and
- NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems.

For additional guidance on securing OPC UA enabled devices, see:

> Practical Security Recommendations for building OPC UA Applications

For more information on APT actors' tools and TTPs, refer to:

- Mandiant's Blog – INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems
- Dragos' Blog – CHERNOVITE'S PIPEDREAM: Malware Targeting Industrial Control Systems

Disclaimer

The information in this report is being provided "as is" for informational purposes only. DOE, CISA, NSA, and the FBI do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the DOE, CISA, NSA, or the FBI, and this guidance shall not be used for advertising or product endorsement purposes.

Acknowledgements

The DOE, CISA, NSA, and the FBI would like to thank Dragos, Mandiant, Microsoft, Palo Alto Networks, and Schneider Electric for their contributions to this joint CSA.

Appendix: APT Cyber Tools Tactics, Techniques, and Procedures

See tables 1 through 3 for TTPs associated with the cyber actors' tools described in this CSA mapped to the MITRE ATT&CK for ICS framework. See the ATT&CK for ICS framework for all referenced threat actor tactics and techniques.

Table 1: APT Tool for Schneider Electric ICS TTPs

Tactic	Technique
Execution	Command-Line Interface [T0807]
Scripting [T0853]	
Persistence	Modify Program [T0889]
System Firmware [T0857]	

Tactic	Technique
Valid Accounts [T0859]	
Discovery	Remote System Discovery [T0846]
Remote System Information Discovery [T0888]	
Lateral Movement	Default Credentials [T0812]
Program Download [T0843]	
Valid Accounts [T0859]	
Collection	
Monitor Process State [T0801]	
Program Upload [T0845]	
Monitor Process State [T0801]	
Command and Control	Commonly Used Port [T0885]
Standard Application Layer Protocol [T0869]	
Inhibit Response Function	Block Reporting Message [T0804]
Block Command Message [T0803]	
Denial of Service [T0814]	
Data Destruction [T0809]	
Device Restart/Shutdown [T0816]	
System Firmware [T0857]	
Impair Process Control	Modify Parameter [T0836]
Unauthorized Command Message [T0855]	
Impact	Denial of Control [T0813]
Denial of View [T0815]	
Loss of Availability [T0826]	
Loss of Control [T0827]	
Loss of Productivity and Revenue [T0828]	

Tactic	Technique
Manipulation of Control [T0831]	
Theft of Operational Information [T0882]	

Table 2: APT Tool for OMRON ICS TTPs

Tactic	Technique
Initial Access	Remote Services [T0886]
Execution	Command-Line Interface [T0807]
Scripting [T0853]	
Change Operating Mode [T0858]	
Modify Controller Tasking [T0821]	
Native API [T0834]	
Persistence	Modify Program [T0889]
Valid Accounts [T0859]	
Evasion	Change Operating Mode [T0858]
Discovery	Network Sniffing [T0842]
Remote System Discovery [T0846]	
Remote System Information Discovery [T0888]	
Lateral Movement	Default Credentials [T0812]
Lateral Tool Transfer [T0867]	
Program Download [T0843]	
Remote Services [T0886]	
Valid Accounts [T0859]	
Collection	Detect Operating Mode [T0868]
Monitor Process State [T0801]	
Program Upload [T0845]	
Command and Control	Commonly Used Port [T0885]

Tactic	Technique
Standard Application Layer Protocol [T0869]	
Inhibit Response Function	Service Stop [T0881]
Impair Process Control	Modify Parameter [T0836]
Unauthorized Command Message [T0855]	
Impact	Damage to Property [T0879]
Loss of Safety [T0837]	
Manipulation of Control [T0831]	
Theft of Operational Information [T0882]	

Table 3: APT Tool for OPC UA ICS TTPs

Tactic	Technique
Execution	Command-Line Interface [T0807]
Scripting [T0853]	
Persistence	Valid Accounts [T0859]
Discovery	Remote System Discovery [T0846]
Remote System Information Discovery [T0888]	
Lateral Movement	Valid Accounts [T0859]
Collection	Monitor Process State [T0801]
Point & Tag Identification [T0861]	
Command and Control	Commonly Used Port [T0885]
Standard Application Layer Protocol [T0869]	
Impact	Manipulation of View [T0832]
Theft of Operational Information [T0882]	

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. When available, please

include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

Revisions

April 13, 2022: Initial Version

April 14. 2022: Added Resources

May 25, 2022: Added Additional Mitigations and Resources

Please share your thoughts.

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