



Custom Tools Targeting ICS/SCADA Devices

CRITICALITY 

17/04/202٢

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

Custom advanced tools have been developed by Advanced Persistent Threat (APT) actors for targeting Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) devices.



Threat Details

Custom advanced tools have been developed by Advanced Persistent Threat (APT) actors for targeting Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA) devices. These tools allow APT actors to emulate their capabilities and advanced skills of exploiting by automating the process through utilizing a supported virtual console with a command interface. The target devices will be scanned for details to upload malicious configuration/code, backup or restore contents, and modify device parameters.

As reported in the joint Cybersecurity Advisory (CSA), which was published by the Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), The threat actors' endeavor to exploit the AsrDrv103.sys (CVE-2020-15368) vulnerability of ASRock motherboard driver. Successful exploitation leads to executing malicious code in the Windows kernel and disrupting critical devices or functions across the target environment by leveraging the lateral movement technique.

The threatened ICS/SCADA devices include Schneider Electric programmable logic controllers (PLCs), OMRON Sysmac NEX PLCs, and Open Platform Communications Unified Architecture (OPC UA) servers.

- The Schneider Electric devices tool allows APT actors to:
 - Quick scan with the purpose of identifying the Schneider PLCs on the LAN via UDP multicast destination port 27127.
 - Brute-force the Schneider PLC passwords by applying CODESYS via UDP port 1740.
 - DoS attack to prevent network communications from reaching the PLC.
 - Capture credentials for the sever connections that required users to re-authenticate to the PLC.
 - Crash the PLC temporarily through a "packet of death" attack until configuring and recovering the power cycle.
 - Send custom Modbus commands via TCP port 502.
- The OMRON devices tool allows APT actors to:
 - Utilizing FINS protocol to scan for OMRON.



- Parsing HTTP response from OMRON devices.
 - Retrieving the MAC address of the device.
 - Polling for specific devices connected to the PLC.
 - Backing up/restoring arbitrary files to/from the PLC
 - uploading a custom malicious agent on OMRON PLCs which provides threat actors the ability to connect and initiate commands for file manipulation, packet capturing, and code execution via HTTP and/or HTTPS.
- The OPC UA servers tool allows APT actors to connect to an OPC UA server using default or previously compromised credentials.

According to the CSA, the energy sectors are most vulnerable to these exploits. However, DOE, CISA, NSA, and the FBI advise all critical infrastructure organizations to implement detection and mitigation measures.

Recommendations

 <u>Prevention</u> • Appendix A contains the recommendations to prevent such attacks.	 <u>MITRE ATT&CK</u> • Appendix B contains the Mitre ATT&CK details.
---	--



References

DOE, CISA, NSA, FBI . (2022, April 13). *APT Cyber Tools Targeting ICS/SCADA Devices*. Retrieved from Joint Cybersecurity Advisory :
https://www.cisa.gov/uscert/sites/default/files/publications/Joint_Cybersecurity_Advisory_APT%20Cyber%20Tools%20Targeting%20ICS%20SCADA%20Devices.pdf

McKeon, J. (2022, April 15). *CISA, FBI Warn of APT Cyber Tools Affecting ICS/SCADA Devices*. Retrieved from Health IT Security: <https://healthitsecurity.com/news/cisa-fbi-warn-of-apt-cyber-tools-affecting-ics-scada-devices>



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to follow the below steps:

- 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 MFA 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.
- Enforce the principle of least privilege.
- Monitor systems for loading of unusual drivers, especially for ASRock driver if no ASRock driver is normally used on the system.
- Limit ICS/SCADA systems' network connections to only specifically allowed management and engineering workstations.



Appendix B – MITRE ATT&CK

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 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	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 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 Model – T0868 Monitor Process State – T0801 Program Upload – T0845
Command and Control	Commonly Used Port – T0885 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



Appendix D – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix E – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.