Radiflow

# INCONTROLLER:

## New State-Sponsored Cyber Attack Tools

May 2022

# Introduction

The US DHS CISA and other US Government agencies published (on April 14, 2022) a joint cybersecurity advisory regarding APT cyber tools targeting ICS/SCADA devices.

According to the advisory and other cyber intelligence sources (such as this blog from Mandiant Threat Research team), these tools enable APT actors to scan for, compromise, and control affected devices once they've established initial access to the ICS/OT network.

In addition, one of the tools listed can be used to compromise Windows-based engineering workstations, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising and maintaining full system access to ICS devices, threat groups could elevate privileges, move laterally within a network, and eventually disrupt critical devices or functions.

The purpose of this brief is to advise Radiflow customers and partners using its iSID industrial threat detection system how to detect various Indicators of Compromise (IOCs) of these advanced attack tools.

In this report we will use Mandiant code-names for these tools for the sake of simplicity, and advise on detection methods and alert descriptions based in analysis done in CISA advisory and Mandiant blog.

# Attack tools arsenal

The INCONTROLLER package is comprised of three main components:

- A tool for targeting Schneider Electric MODICON and MODICON Nano PLCs (a.k.a. "CODECALL")
- A tool for targeting OMRON Sysmac NJ and NX PLCs (a.k.a. "OMSHELL")
- A tool for targeting OPC-UA servers (a.k.a. "TAGRUN")

The APT actors' tools have a modular architecture. They enable cyber-actors to conduct highly-automated exploits against targeted devices: establish initial access in an OT network, and scan for, compromise, and control ICS devices.

These tools have a virtual console with a command interface that mirrors that of the targeted ICS/SCADA device. The tools different modules interact with targeted devices to enable operations by lower-skilled cyber actors that emulate higher-skilled actor capabilities.

| Tool | Capabilities |
|---|---|
| TAGRUN | Capabilities include scanning for OPC servers; enumerating OPC structure/tags; brute forces credentials; and reading and writing of OPC tag values. |
| CODECALL | The CODECALL framework communicates using Modbus and Codesys. CODECALL contains modules to interact with, scan, and attack at least three Schneider Electric PLCs. |
| OMSHELL | Capabilities include scanning some types of Omron PLCs via HTTP, Telnet, and Omron FINS protocol. OMSHELL can also interact with Omron's servo drives, which use feedback control to power servo motors for precision motion control. |

# Detection by iSID

## CODECALL: 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).

| Attack capability | Detection in ISID |
|---|---|
| Run a rapid scan that identifies all Schneider PLCs on the local network via UDP multicast, with a destination port of 27127 (UDP 27127 is a standard discovery scan used by SE EcoStruxure Machine software (engineering workstations) to discover PLCs). | Any device that generates UDP traffic over port 27127 will be identified as an "Engineering Station". Applications that generate such traffic are identified as "EcoStruxure" or "SoMachine". |
| Brute-force on Schneider Electric PLC passwords, using CODESYS and other available device protocols via UDP port 1740. This is done using password defaults or a dictionary word list. | iSID will alert on Brute-force or scanning via UDP port 1740 (Schneider Electric Machine Expert protocol) aim at Schneider PLCs.<br>In addition, "UMAS, initialize a UMAS communication" alert in "Asset Management" category will be generated multiple times. |
| Conduct a denial-of-service attack to prevent network communications from reaching the PLC | iSID will generate a denial-of-service alert for Schneider PLCs. Examples for such alerts:<br>► Modbus - Illegal Packet Size, Possible DOS Attack<br>► Modbus - Incorrect Packet Length, Possible DOS Attack |
| Server connections, requiring users to re-authenticate their credentials to access the PLC, likely to facilitate capturing of credentials | In case of "Man-in-the-Middle" attacks by threat actor in order to gather the credentials, a large number of ARP poisoning alerts will be generated for PLC and Engineering Station.<br>Additional alert example:<br>► PROTOCOL-SCADA Schneider Modicon TM221CE16R password retrieval attempt |
| Conduct a 'packet of death' attack to crash the PLC until a power cycle and configuration recovery is conducted | The crafted packet will be identified by the SNORT signatures – Wrong length, wrong CRC. Examples for such alerts:<br>► Modbus - Illegal Packet Size, Possible DOS Attack<br>► Modbus - Incorrect Packet Length, Possible DOS Attack |
| Send custom Modbus commands (beyond commands that are specific to Schneider Electric PLCs) | "Asset Management" commands that indicates on changing of the PLC behavior will be identified by respective alerts, such as:<br>► UMAS, Copy Block from engineering PC to PLC<br>► UMAS, Write System bits, System Words and Strategy variables |

# Detection of APT Tool for Schneider Electric Devices - continued

### Additional SNORT signatures that may be triggered during an attack:

- Schneider Stop Controller Command
- SERVER-WEBAPP Schneider Electric quantum Modicon Ethernet module unauthenticated password change attempt
- SERVER-WEBAPP Schneider Electric Quantum Modicon Ethernet module unauthenticated password reset attempt
- UMAS: Copy Block from PLC to engineering PC
- UMAS: Finish copy from PLC to engineering PC
- UMAS: Read a memory block of the PLC

## OMSHELL – APT Tool for OMRON Devices

The OMSHELL APT actors' tool for OMRON devices has modules that interact via normal management protocols as well as via the OMRON Factory Interface Network Service (FINS) protocol (UDP 9600).

| Attack capability | Detection in ISID |
|---|---|
| Scanning for OMRON using Factory Interface Network Service (FINS) protocol | "New device/link" alerts will be generated on detection of multiple FINS communications with OMRON PLCs on UDP port 9600 |
| Parsing the HTTP response from OMRON devices | "New links created" alerts will be generated to the OMRON PLCs on HTTP |
| Retrieving devices' MAC addresses<br>Polling for specific devices connected to the PLC | ARP poisoning alerts will be triggered upon intercepting multiple ARP packets (a large number of ARP packets are typically involved in retrieving OMRON PLCs' MAC addresses.) |
| Backing up/restoring arbitrary files to/from the PLC | "New link created" or "new device" alerts may be triggered. |
| Loading a custom malicious agent on OMRON PLCs for additional attacker-directed capability | "New link created" alert following with FINS alert related to file write will be triggered (eg. SNORT signature: PROTOCOL-SCADA OMRON-FINS single file write attempt) |
| 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 HTTPS | SNORT alerts that have triggered suspicious\ malicious HTTP/HTTPS and related to OMRON PLC Alerts generated on newly-detected links between OT devices and OMRON PLCs on HTTP/HTTPS. |

### Additional SNORT rules that may be triggered during an attack:

- PROTOCOL-SCADA OMRON-FINS memory area write overflow attempt
- FILE-OTHER OMRON CX-One arbitrary code execution attempt
- FILE-IDENTIFY Omron CX-Supervisor project file attachment detected
- PROTOCOL-SCADA OMRON-FINS program area protect clear brute force attempt

## TAGRUN – APT Tool for OPC-UA Servers

The APT actors' tool for OPC UA has modules with a basic functionality to identify OPC UA servers and to connect to an OPC UA server using default or previously-compromised credentials.

| Attack capability | Detection in ISID |
|---|---|
| ► Request whether the target environment is running a Windows operating system<br>► Send different ping commands depending on return value | SNORT alerts will be triggered:<br>► NF - ICMP Payload contains - Windows PowerShell Running - Covert Channel<br>► ET SCAN ICMP PING IPTools |
| ► Scan for OPC UA servers on a network<br>► Reading the structure of OPC UA servers | ► Detection of new devices and links<br>► New link on port 4840/4843 (OPC UA & OPC UA-TLS) |
| Brute forcing credentials | Brute force attempt alert triggered |
| Output log files | New link from OPC server to other devices; also, in most cases, change in amount of data transferred between devices may be observed |

## Summary

iSID helps asset owners detect and defend against advanced attack tools for ICS environments (e.g. INCONTROLLER) using a wide range of discovery and detection methods, as described in this report.

As future modifications to these tools are likely, we believe that a mix of signature-based and behavior-based detection methods, combined with deep knowledge of asset inventory and network behavior, will prove to be most effective.

In order to ensure the effectiveness of signature-based detection, iSID customers should regularly update its cyberattack signature database provided by Radiflow.

Radiflow's additional recommendations:

- Check the traffic between zones (conduits) – Enterprise to Supervisory to Basic and vice versa - to detect attempts to install these tools
- Audit remote connections to supervisory/operations/basic control zones based on approved protocols and workstations. Additionally, whenever possible, make sure to enforce multifactor authentication for remote access to ICS networks and devices.
- Regularly change all passwords to ICS/SCADA devices and systems, especially default passwords, to strong per-device passwords. This will significantly help to mitigate password brute force attacks and to provide defender monitoring systems with opportunities to detect common attacks.
- Ensure basic cyber-hygiene practices:
  - Implementation of effective network segmentation
  - The use of EOL OSs is unfortunately still very common in ICS environments. You should upgrade all EOL Windows operating systems to modern OSs such as Windows 10.
  - Install Endpoint Protection, Detection and Response (EDR) solutions and configure strong anti-malware file reputation settings

If you suspect malicious ICS network activity, or for additional guidance, you are welcome to reach out to the Radiflow cyber analytics team.

**About Radiflow**

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 7000 sites around the globe.