INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems

mandiant.com/resources/incontroller-state-sponsored-ics-tool

In early 2022, Mandiant, in partnership with Schneider Electric, analyzed a set of novel industrial control system (ICS)-oriented attack tools—which we call INCONTROLLER (aka PIPEDREAM)—built to target machine automation devices. The tools can interact with specific industrial equipment embedded in different types of machinery leveraged across multiple industries. While the targeting of any operational environments using this toolset is unclear, the malware poses a critical risk to organizations leveraging the targeted equipment. INCONTROLLER is very likely state sponsored and contains capabilities related to disruption, sabotage, and potentially physical destruction.

INCONTROLLER represents an exceptionally rare and dangerous cyber attack capability. It is comparable to TRITON, which attempted to disable an industrial safety system in 2017; INDUSTROYER, which caused a power outage in Ukraine in 2016; and STUXNET, which sabotaged the Iranian nuclear program around 2010. To help asset owners find and defend against INCONTROLLER, we have included a range of mitigations and discovery methods throughout this report. As future modifications to these tools are likely, we believe behavior-based hunting and detection methods will be most effective.

If you need support responding to related activity, please contact Mandiant Consulting. Further analysis of related threats is available as part of Mandiant Advantage Threat Intelligence.

This report is related to information shared in CISA Alert (AA22-103A).For more information from Schneider Electric, please see their bulletin. For more information from CODESYS, please see their advisory.

INCONTROLLER is comprised of three main components:

Table 1: Description of tools

Tool	Description
TAGRUN	A tool that scans for OPC servers, enumerates OPC structure/tags, brute forces credentials, and reads/writes OPC tag values.
CODECALL	A framework that communicates using Modbus—one of the most common industrial protocols—and Codesys. CODECALL contains modules to interact with, scan, and attack at least three Schneider Electric programmable logic controllers (PLCs).
OMSHELL	A framework with capabilities to interact with and scan some types of Omron PLCs via HTTP, Telnet, and Omron FINS protocol. The tool can also interact with Omron's servo drives, which use feedback control to deliver energy to motors for precision motion control.

INCONTROLLER Was Built to Manipulate and Disrupt Industrial Processes

Industrial automation networks rely on a variety of equipment that enable operators to translate information and instructions into chains of physical actions. Given the diversity of assets present in industrial networks, industrial automation equipment typically speaks different languages across different portions of the network, which is possible using standardized industrial communication protocols.

INCONTROLLER includes three tools that enable the attacker to send instructions to ICS devices using industrial network protocols, such as OPC UA; Modbus; Codesys, which is used by EcoStruxure Machine Expert and SoMachine; and Omron FINS. While the tool's capabilities could enable the actor to communicate with a variety of products from different original equipment manufacturers (OEMs), the actor developed modules for specific controllers from Schneider Electric and Omron. The targeted equipment consists of machine automation solutions whose use cases span from supporting simple, repetitive machines to complex modular machines in distributed architectures:

- OPC servers
- Schneider Electric Modicon M251, Modicon M258, and Modicon M221 Nano PLCs
  Other devices leveraging Modbus and Codesys may also be affected
- Omron NX1P2 and NJ501 PLCs and R88D-1SN10F-ECT servo drive
  Other devices from NJ and NX PLC series may also be affected

We highly doubt that the threat actor would target these devices at random. It is more likely they were chosen because of reconnaissance into specific target environment(s). We note that this would be consistent with previous ICS malware, such as TRITON, which targeted a critical safety system that was almost certainly identified prior to compromising the target's industrial environment.

INCONTROLLER: Tooling Overview

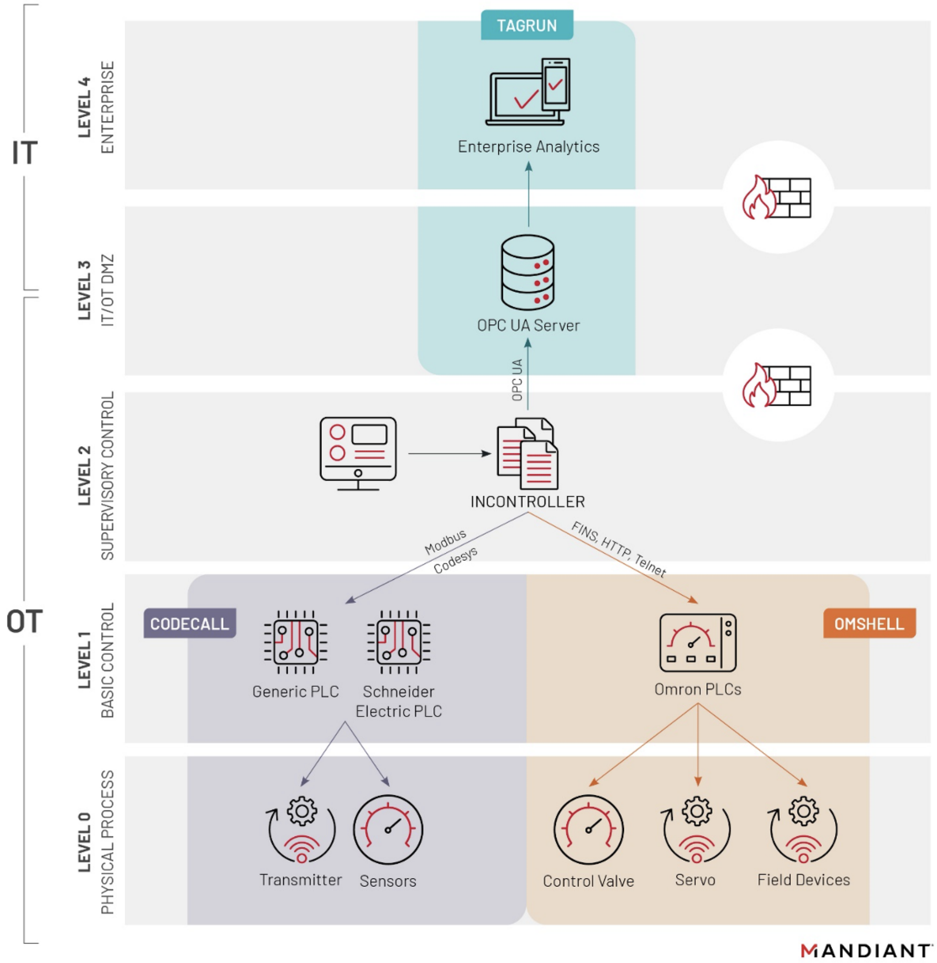


Figure 1: INCONTROLLER tooling overview

TAGRUN

TAGRUN's capabilities, such as the ability to scan for and enumerate OPC UA servers, suggests a reconnaissance role. OPC acts as a central communications protocol to collect and store data from ICS assets in industrial environments. Access to this data can provide attackers with a detailed overview of production systems and control processes. The tool was likely developed for reconnaissance, but it can also write and change tag values, which could be used to modify data to either support an attack or mask process changes. TAGRUN also verifies whether the target environment is running a Windows operating system and provides different ping commands depending on this check's return value. This suggests that the actor may use non-Windows devices to execute TAGRUN.

TAGRUN’s capabilities include:

- Scanning for OPC UA servers on a network
- Reading the structure of OPC UA servers
- Reading/writing tag values for data on an OPC UA server
- Brute forcing credentials
- Outputting log files

CODECALL

CODECALL communicates with ICS devices using the Modbus protocol, which potentially gives it the ability to interact with devices from different manufacturers. However, the tool contains a specific module to interact with, scan, and attack Schneider Electric's Modicon M251 (TM251MESE) PLC using Codesys, which is used by the company's proprietary EcoStruxure Machine Expert protocol. We have reason to believe the tool also targets Schneider Electric's Modicon M221 Nano PLC and the Modicon M258 PLC, and it potentially affects additional devices leveraging these protocols.

CODECALL’s general capabilities include:

- Identifying Schneider Electric and Modbus-enabled devices on a network
- Connecting to specific devices over Modbus or Codesys
- Reading/writing device registers over Modbus
- Requesting device ID from a session over Modbus
- Defining, dumping, or loading command macro file(s)
- Executing device specific commands over Codesys, such as:
    - Attempting to login using a username/password and by brute forcing credentials with a provided dictionary file
    - Downloading/uploading files to the PLC device
    - Retrieving file/directory listings
    - Deleting files
    - Disconnecting sessions from the PLC device
    - Attempting a DDoS attack
    - Crashing the device with a specifically crafted packet
    - Adding a route if the device gateway IP exists on a different interface
    - Sending custom raw packets

OMSHELL

OMSHELL is designed to obtain shell access to Omron PLCs, including Omron NX1P2, NJ501, R88D-1SN10F-ECT servo drive, and possibly other similar devices from the NJ/NX product lines. The tool primarily operates using the HTTP protocol, however it also utilizes Omron's proprietary FINS over UDP protocol for scanning and device identification. The framework is modular, which means the attacker can develop and deploy additional capabilities into the tool.

OMSHELL's capabilities include:

- Scanning for and identifying Omron devices on the network
- Wiping the device's program memory and resetting the device
- Loading backup configuration and backup data from or restoring data to the device
- Activating the telnet daemon on the device
- Connecting to the device via the telnet daemon, uploading and optionally executing an arbitrary payload or command
- Connecting to a backdoor present on a device and providing arbitrary command execution
- Performing a network traffic capture
- Killing arbitrary processes running on the device
- Transferring files to the device
- Connecting and communicating with attached servo drives

We have reason to believe that indicator-based detections would not be effective at detecting INCONTROLLER in victim environments, in part because the attacker would almost certainly modify or customize the tool prior to using it in a specific victim environment. Instead, defenders should focus their efforts on behavior-based hunting and detection methods for these tools.

Potential Supporting Windows Tooling

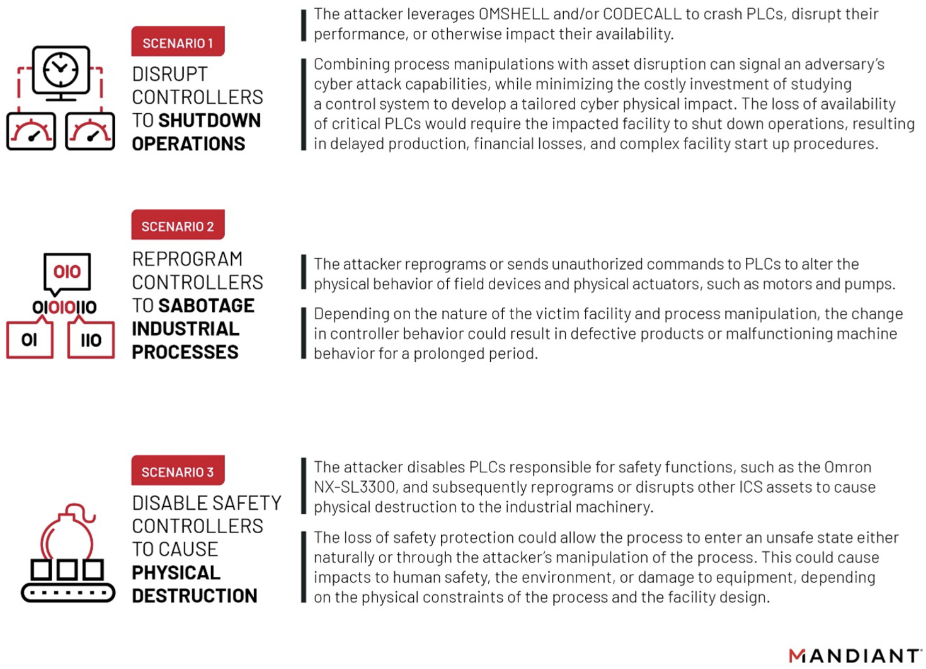
We are also tracking two additional tools affecting Windows-based systems that may be related to this threat activity. It is possible that these tools could be used to support the overall attack lifecycle in an INCONTROLLER attack by exploiting Windows-based systems in IT or operational technology (OT) environments.

- One of the tools exploits CVE-2020-15368 in the AsrDrv103.sys driver, which would result in installation and exploitation of a vulnerable driver. ASRock motherboards may be leveraged in some human-machine interfaces (HMIs) and engineering workstations in OT environments.
- The other tool, which we track as ICECORE, is a backdoor providing reconnaissance and command and control functionality.

Attack Scenarios

It is feasible that each tool could be used independently, or the actor may use the three tools to attack a single environment. We highlight that the devices targeted by INCONTROLLER are often integrated in automation machinery (e.g., a milling machine or press) and could plausibly be present in a variety of industrial sectors and processes even without the user's explicit knowledge.

We developed three cyber physical attack scenarios that highlight a range of possible outcomes from an attack using INCONTROLLER. In each of the three cases, TAGRUN could have been used at earlier stages to enumerate the victim environment, identify its targets, and learn about the physical process.



SCENARIO 1

DISRUPT CONTROLLERS TO **SHUTDOWN OPERATIONS**

The attacker leverages OMSHELL and/or CODECALL to crash PLCs, disrupt their performance, or otherwise impact their availability.

Combining process manipulations with asset disruption can signal an adversary's cyber attack capabilities, while minimizing the costly investment of studying a control system to develop a tailored cyber physical impact. The loss of availability of critical PLCs would require the impacted facility to shut down operations, resulting in delayed production, financial losses, and complex facility start up procedures.

SCENARIO 2

REPROGRAM CONTROLLERS TO **SABOTAGE INDUSTRIAL PROCESSES**

The attacker reprograms or sends unauthorized commands to PLCs to alter the physical behavior of field devices and physical actuators, such as motors and pumps.

Depending on the nature of the victim facility and process manipulation, the change in controller behavior could result in defective products or malfunctioning machine behavior for a prolonged period.

SCENARIO 3

DISABLE SAFETY CONTROLLERS TO CAUSE **PHYSICAL DESTRUCTION**

The attacker disables PLCs responsible for safety functions, such as the Omron NX-SL3300, and subsequently reprograms or disrupts other ICS assets to cause physical destruction to the industrial machinery.

The loss of safety protection could allow the process to enter an unsafe state either naturally or through the attacker's manipulation of the process. This could cause impacts to human safety, the environment, or damage to equipment, depending on the physical constraints of the process and the facility design.

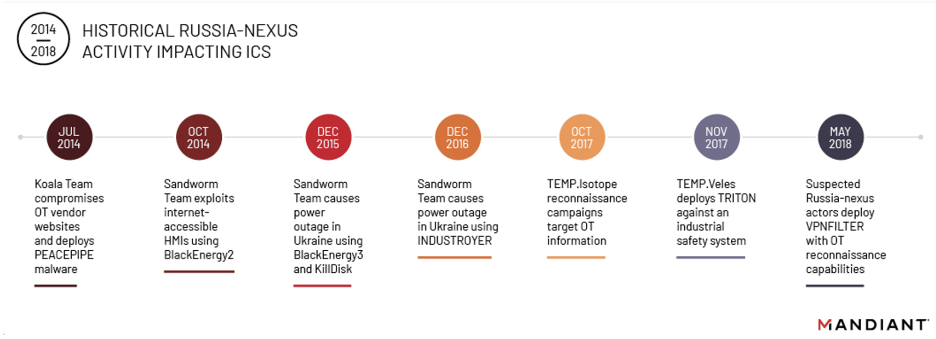
Figure 2: INCONTROLLER attack scenarios

The impact of these scenarios would depend on the nature of the victim facility and the extent of the attacker's understanding of and interaction with the controlled physical process. We note that our current understanding of INCONTROLLER is still limited given that it leverages an extensible structure that can support new features implemented by the author.

INCONTROLLER Is Very Likely State-Sponsored Malware

We believe INCONTROLLER is very likely linked to a state-sponsored group given the complexity of the malware, the expertise and resources that would be required to build it, and its limited utility in financially motivated operations. We are unable to associate INCONTROLLER with any previously tracked group at this stage of our analysis, but we note the activity is consistent with Russia's historical interest in ICS. While our evidence connecting INCONTROLLER to Russia is largely circumstantial, we note it given Russia's history of destructive cyber attacks, its current invasion of Ukraine, and related threats against Europe and North America.

> Since at least 2014, Russia-nexus threat actors have targeted ICS assets and data with multiple ICS-tailored malware families (PEACEPIPE, BlackEnergy2, INDUSTROYER, TRITON, and VPNFILTER).



JUL 2014: Koala Team compromises OT vendor websites and deploys PEACEPIPE malware

OCT 2014: Sandworm Team exploits internet-accessible HMIs using BlackEnergy2

DEC 2015: Sandworm Team causes power outage in Ukraine using BlackEnergy3 and KillDisk

DEC 2016: Sandworm Team causes power outage in Ukraine using INDUSTROYER

OCT 2017: TEMP.Isotope reconnaissance campaigns target OT information

NOV 2017: TEMP.Veles deploys TRITON against an industrial safety system

MAY 2018: Suspected Russia-nexus actors deploy VPNFILTER with OT reconnaissance capabilities

Figure 3: Historical Russia-nexus activity impacting ICS

> INCONTROLLER's functionality is consistent with the malware used in Russia's prior cyber physical attacks. For example, the 2015 and 2016 Ukrainian blackouts both involved physical process manipulations combined with disruptive attacks against embedded devices. INCONTROLLER similarly allows the malware operator to manipulate physical processes, while also containing denial-of-service (DoS) capabilities to disrupt the availability of PLCs.

Recommendations

While the nature of any potential intended victims remains uncertain, INCONTROLLER poses a critical risk to organizations with compatible devices. The targeted devices are embedded in multiple types of machinery and could plausibly be present in many different industrial sectors. Given the consistencies with prior Russia-nexus threat activity, we suggest that INCONTROLLER poses the greatest threat to Ukraine, NATO member states, and other states actively responding to Russia's invasion of Ukraine. Organizations should take immediate action to determine if the targeted ICS devices are present in their environments and begin applying vendor-specific countermeasures.

We also recommend that at-risk organizations conduct threat hunts to detect this activity in their networks. Mandiant Advantage Threat Intelligence subscribers have access to additional reporting containing threat hunting guidance and YARA detections.

If you need support responding to related activity, please contact Mandiant Consulting. Further analysis is available as part of Mandiant Advantage Threat Intelligence.

Mitigations

OPC UA

We recommend several steps to mitigate risk and counter malicious activity in environments using this protocol:

- Proper segmentation of IT and OT networks to aid in preventing attackers pivoting from corporate networks into industrial environments.
- Allow listing accepted primary/subordinate devices, behavior patterns, and commands to aid in establishing approved baselines and detecting anomalies with the aid of network monitoring.
- Implementation of an industrial firewall with deep packet inspection to aid in controlling access and approved capabilities.
- Implementation of ICS-aware intrusion protection systems to aid in monitoring for function codes from potentially malicious sources.
- Monitoring and blocking of external traffic to OPC UA ports, when possible, to aid in detecting anomalous traffic and prevent external network traffic directed at OPC UA-associated ports.
- Enabling and aggregating audit logs for OPC servers and clients.
- Periodic reviewing of audit logs for inconsistent or nefarious connections, security options negotiations, configuration changes, and user interaction.

Schneider Electric

To help keep your Schneider Electric products secure and protected, it is in your best interest that you implement the cyber security best practices as indicated in the Cybersecurity Best Practices document provided on the Schneider Electric website: Recommended Cybersecurity Best Practices White paper | Schneider Electric.

Additionally, *Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment User Guide* could help you ensure that only legitimate users can access your Schneider Electric product: Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment, User Guide | Schneider Electric.

You should pay special attention to features and cyber security devices that help to restrict access to authorized users only. This includes examples such as intrusion detection systems, network firewalls, secure remote access, device authentication, device firewall, disabling/filtering unsecure or programming protocols.

Omron

According to public vulnerability notices, Omron has previously identified other vulnerabilities that use the same or similar FIN ports that are used by OMSHELL. Omron's guidance for unpatched vulnerabilities, as noted in their security brief, indicates that external firewall filtering of identified FIN ports can be used as a mitigation. Mandiant believes that the recommended methodology may be a viable mitigation, though this mechanism has not been tested with INCONTROLLER. Additional guidance related to Omron's previous recommendations can be found in the related ICS Advisory for that older vulnerability.

Discovery Methods

TAGRUN

- Search for and investigate irregular connections to OPC UA endpoints and enable robust audit logging for OPC UA applications. Aggregate OPC UA logs and audit records to a central location where applicable.
- Review OPC UA audit records for evidence of credential bruteforcing, nefarious certificate usage, irregular connection attempts, configuration changes, and changes to OPC tags.
- Search for and investigate TAGRUN ping command execution.
- Review OT network traffic for evidence of pingsweep activity.

CODECALL

- Enable robust logging for Schneider Electric PLC devices and aggregate logs to a central location where applicable.
- Review Schneider Electric device logs for evidence of the following activity:
  - Credential bruteforcing
  - Error codes associated with abnormal device crashes/reboots
  - Files uploaded or downloaded
  - File deletion
  - Unauthorized changes in device configuration and execution of commands
  - Connections to devices outside of documented norms for the device and environment
- Search for and investigate evidence of ARP scanning followed by abnormal Modbus/Codesys traffic differing from environment baselines.
- Search for abnormal Modbus and Codesys traffic flows compared to environment baselines.

OMSHELL

- Search for and investigate evidence of the creation/existence of OMSHELL-related host-based indicators on systems with access to OT resources and connectivity (e.g., packet captures).
- Enable robust logging for Omron PLC devices and aggregate logs to a central location where applicable.
- Review Omron device logs for evidence of the following activity:
  - Activation of Telnet daemon on the device.
  - Unauthorized Telnet connection attempts including the use of default credentials.
  - Wiping of PROGRAM memory and device resets.
  - Unauthorized changes in device configuration and execution of commands.
  - Connections to devices outside of documented norms for the device and environment.
  - Files uploaded or downloaded.
- Identify and investigate nefarious pingsweep scanning activity, telnet traffic, and HTTP traffic on systems with access and connectivity to OT resources/devices:
- Search for and investigate evidence of Omron FINS traffic outside of standard norms and environment baselines.

Collect, identify, and investigate nefarious HTTP POST data to Omron devices containing Omron API commands.

Appendix: MITRE ATT&CK for ICS Mapping

Table 2: TAGRUN MITRE ATT&CK for ICS mapping

Module	Tactic	Technique
TAGRUN	Execution	T0807: Command-Line Interface
TAGRUN	Execution	T0853: Scripting
TAGRUN	Lateral Movement	T0859: Valid Accounts
TAGRUN	Discovery	T0888: Remote System Information Discovery

TAGRUN	Discovery	T0846: Remote System Discovery
TAGRUN	Persistence	T0859: Valid Accounts
TAGRUN	Collection	T0801: Monitor Process State
TAGRUN	Collection	T0861: Point & Tag Identification
TAGRUN	Command and Control	T0885: Commonly Used Port
TAGRUN	Command and Control	T0869: Standard Application Layer Protocol
TAGRUN	Impact	T0832: Manipulation of View
TAGRUN	Impact	T0882: Theft of Operational Information

Table 3: CODECALL MITRE ATT&CK for ICS mapping

Module	**Tactic**	**Technique**
CODECALL	Execution	T0807: Command-Line Interface
CODECALL	Execution	T0853: Scripting
CODECALL	Persistence	T0859: Valid Accounts
CODECALL	Persistence	T0857: System Firmware
CODECALL	Persistence	T0889: Modify Program
CODECALL	Discovery	T0846: Remote System Discovery
CODECALL	Discovery	T0888: Remote System Information Discovery
CODECALL	Lateral Movement	T0812: Default Credentials
CODECALL	Lateral Movement	T0843: Program Download
CODECALL	Lateral Movement	T0859: Valid Accounts
CODECALL	Collection	T0801: Monitor Process State
CODECALL	Collection	T0845: Program Upload
CODECALL	Collection	T0801: Monitor Process State
CODECALL	Command and Control	T0885: Commonly Used Port

CODECALL	Command and Control	T0869: Standard Application Layer Protocol
CODECALL	Inhibit Response Function	T0804: Block Reporting Message
CODECALL	Inhibit Response Function	T0803: Block Command Message
CODECALL	Inhibit Response Function	T0814: Denial of Service
CODECALL	Inhibit Response Function	T0809: Data Destruction
CODECALL	Inhibit Response Function	T0816: Device Restart/Shutdown
CODECALL	Inhibit Response Function	T0857: System Firmware
CODECALL	Impair Process Control	T0836: Modify Parameter
CODECALL	Impair Process Control	T0855: Unauthorized Command Message
CODECALL	Impact	T0813: Denial of Control
CODECALL	Impact	T0815: Denial of View
CODECALL	Impact	T0826: Loss of Availability
CODECALL	Impact	T0827: Loss of Control
CODECALL	Impact	T0828: Loss of Productivity and Revenue
CODECALL	Impact	T0831: Manipulation of Control
CODECALL	Impact	T0882: Theft of Operational Information

Table 4: OMSHELL MITRE ATT&CK for ICS mapping

Module	Tactic	Technique
OMSHELL	Initial Access	T0886: Remote Services
OMSHELL	Execution	T0807: Command-Line Interface
OMSHELL	Execution	T0853: Scripting
OMSHELL	Execution	T0858: Change Operating Mode
OMSHELL	Execution	T0821: Modify Controller Tasking
OMSHELL	Execution	T0834: Native API

OMSHELL	Persistence	T0889: Modify Program
OMSHELL	Persistence	T0859: Valid Accounts
OMSHELL	Evasion	T0858: Change Operating Mode
OMSHELL	Discovery	T0842: Network Sniffing
OMSHELL	Discovery	T0846: Remote System Discovery
OMSHELL	Discovery	T0888: Remote System Information Discovery
OMSHELL	Lateral Movement	T0812: Default Credentials
OMSHELL	Lateral Movement	T0867: Lateral Tool Transfer
OMSHELL	Lateral Movement	T0843: Program Download
OMSHELL	Lateral Movement	T0886: Remote Services
OMSHELL	Lateral Movement	T0859: Valid Accounts
OMSHELL	Collection	T0868: Detect Operating Mode
OMSHELL	Collection	T0801: Monitor Process State
OMSHELL	Collection	T0845: Program Upload
OMSHELL	Command and Control	T0885: Commonly Used Port
OMSHELL	Command and Control	T0869: Standard Application Layer Protocol
OMSHELL	Inhibit Response Function	T0881: Service Stop
OMSHELL	Impair Process Control	T0836: Modify Parameter
OMSHELL	Impair Process Control	T0855: Unauthorized Command Message
OMSHELL	Impact	T0879: Damage to Property
OMSHELL	Impact	T0837: Loss of Safety
OMSHELL	Impact	T0831: Manipulation of Control
OMSHELL	Impact	T0882: Theft of Operational Information

Appendix: YARA Rules

```
rule MTI_Hunting_AsRockDriver_Exploit_PDB
{
          meta:
                    author = "Mandiant"
                    date = "03-23-2022"
                    description = "Searching for executables containing strings associated with AsRock driver Exploit."

          strings:
                    $dos_stub = "This program cannot be run in DOS mode"
                    $pdb_bad = "dev projects\\SignSploit1\\x64\\Release\\AsrDrv_exploit.pdb"
                    $pdb_good = "c:\\asrock\\work\\asrocksdk_v0.0.69\\asrrw\\src\\driver\\src\\objfre_win7_amd64\\amd64\\AsrDrv103.pdb"

          condition:
                    all of them and (@pdb_bad < @dos_stub[2]) and (#dos_stub == 2) and (@pdb_good > @dos_stub[2])
}
rule MTI_Hunting_AsRockDriver_Exploit_Generic
{
          meta:
                    author = "Mandiant"
                    date = "03-23-2022"
                    description = "Searching for executables containing strings associated with AsRock driver Exploit."

          strings:
                    $dos_stub = "This program cannot be run in DOS mode"
                    $pdb_good = "c:\\asrock\\work\\asrocksdk_v0.0.69\\asrrw\\src\\driver\\src\\objfre_win7_amd64\\amd64\\AsrDrv103.pdb"

          condition:
                    all of them and (#dos_stub == 2) and (@pdb_good > @dos_stub[2])
}
```

Acknowledgements

This research was made possible thanks to the hard work of many people not listed on the byline. A huge thanks to the Schneider Electric Team, Mandiant Advanced Practices, FLARE, Consulting, Managed Defense, and everyone else who supported this effort.

Special thanks to Jared Scott Wilson, Glen Chason, Benjamin Read, Jonathan Leathery, Conor Quigley, and Wesley Mok.