



How SCADAfence Detects Triton

Based on the MITRE ATT&CK Framework

What you can learn about the Triton Attack and how SCADAfence helps prevent attacks on industrial control systems (ICS)



SUMMARY OF THE TRITON ATTACK

The Triton malware attack was far from the first time that cyber attackers have attempted to target the networks of an industrial facility, but it was the first time that malware designed to attack safety systems was ever seen in the wild. Only a year after the attack, it was reported in 2018 that the malware most likely came from the Central Scientific Research Institute of Chemistry and Mechanics (CNIHM), a research entity in Russia.

The malware was designed to manipulate Schneider Electric's Triconex Safety Instrumented System (SIS) controllers – emergency shutdown systems – and was uncovered on the network at a critical infrastructure operator in the Middle East.

The malware campaign was extremely stealthy and was only uncovered because the attackers made a mistake and triggered the safety system, shutting down the plant. The outcome could've been much worse. Following the initial point of compromise, the malware was able to use techniques such as harvesting credentials and moved across the network to reach the SIS controllers.

However, Triton was only able to reach its goal because of some lax attitudes to security throughout the facility: the safety controllers were using improper network segmentation and the network was connected to internet-facing operational systems, allowing attackers to gain

access using compromised valid credentials. Other failures -- like a key being left inside a machine -- provided attackers with access they should never have gained without physically being inside the facility.

While the malware has the potential to be highly damaging to valves, switches and sensors in an industrial environment, the threat can be countered by implementing some relatively simple cybersecurity techniques that make movement between systems almost impossible.

Triton targeted critical infrastructure in the Middle East, but there are lessons from the incident that can be applied to organizations in every sector, no matter where they are in the world.

THE MITRE ENGENUITY EVALUATION FOR ICS THREAT DETECTION

There is a lot of buzz recently on the topic of MITRE ATT&CK for ICS and rightfully so. The **Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)** project by MITRE is an initiative started in 2015 with the goal of providing a “globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.” The knowledge base helps security professionals make sense of the numerous varieties of tactics and techniques attackers use to infiltrate networks, steal data and other methods of exploiting organizations.

The MITRE ATT&CK framework enables security professionals to move beyond identifying the simplest and most common attack methods and instead allocate resources to get a better understanding of adversaries’ behaviors.

MITRE Engenuity ran its first evaluation of the ICS threat detection market. One of the challenges we face in ICS cybersecurity is the lack of detection and collection capability within most ICS environments. MITRE Engenuity ATT&CK Evaluations are intended to help vendors and end-

users better understand a product’s capabilities in relation to MITRE’s publicly accessible ATT&CK for the ICS framework. As a true community-led effort, more than 100 participants from 39 organizations reviewed, provided comments, or contributed to the ATT&CK for ICS framework which was first launched in early 2020.

For the ATT&CK Evals, MITRE Engenuity used the MITRE ATT&CK for ICS knowledge base to emulate the tactics, techniques, and procedures (TTPs) associated with the TRISIS/TRITON malware.

HOW THE TRITON ATTACK OCCURRED

The attacker moved from the IT network to the OT network through systems that were accessible to both environments and gained remote access to an SIS engineering workstation and deployed the Triton attack framework to reprogram the SIS controllers.



Initial Compromise

- Utilized captured valid credentials to log into windows-based engineering workstation within the process environment - Remote Desktop (RDP) over port 3389 (T0885)



Persistence

- Outgoing SSH request was made over port 445 to the application to disguise as SMB traffic (T0885)
- Open SSH backdoor was masqueraded as a proprietary Rockwell protocol, listening on port 2223 and a service name of rockwell-csp3 (T0849).



Collection/Discovery

- Uses custom network and EtherNet/IP tools to conduct a stealth scan across the network on TCP port 44818 to identify any EtherNet/IP capable assets (T0846).
 - [to discover Rockwell devices]
- The script conducts a Rockwell broadcast discovery (T0888), gathers the device type (T0888), PLC operating mode (T0868), and a dump of all tag names (T0871).
- Triton is capable of auto detecting Triconex controllers by sending a specific UDP broadcast packet over port 1502 (T0888).
- The attacker leverages the Rockwell engineering tools to initiate a Program Upload (gets the PLC logic from Rockwell PLC) (T0871) and saves this file into their temp Rockwell directory.



Impair Process Control

- Sent ENIP command: to change the operating mode (T0858) of the safety PLC to Program Mode to allow for a full program download (T0843).
- Modifies the safety controller program (T0889) over EtherNet/IP using the custom python script through an online edit or program append action (T0843).
- Monitors their command-and-control tags before actuating the malicious logic (T0855):
 - TriStation 'get main processor diagnostic data' command.
 - Switch device operating mode [to "Running"]
- Stop the safety system: 'enable all forces' command (T0843) (forces values on the equipment)



Impact

- Safety system is disabled, resulting in Loss of safety (T0880)

How The SCADAfence Platform Prevents Attacks on ICS Networks Such As Triton

This analysis was based on the MITRE Engenuity scenario which used the MITRE ATT&CK for ICS knowledge base to emulate the tactics, techniques, and procedures (TTPs) associated with the TRISIS/TRITON malware.

 **Attack method:**

Adversaries communicated over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection.

 **Tactic:**

Command and Control (TA0101)

 **Technique:**

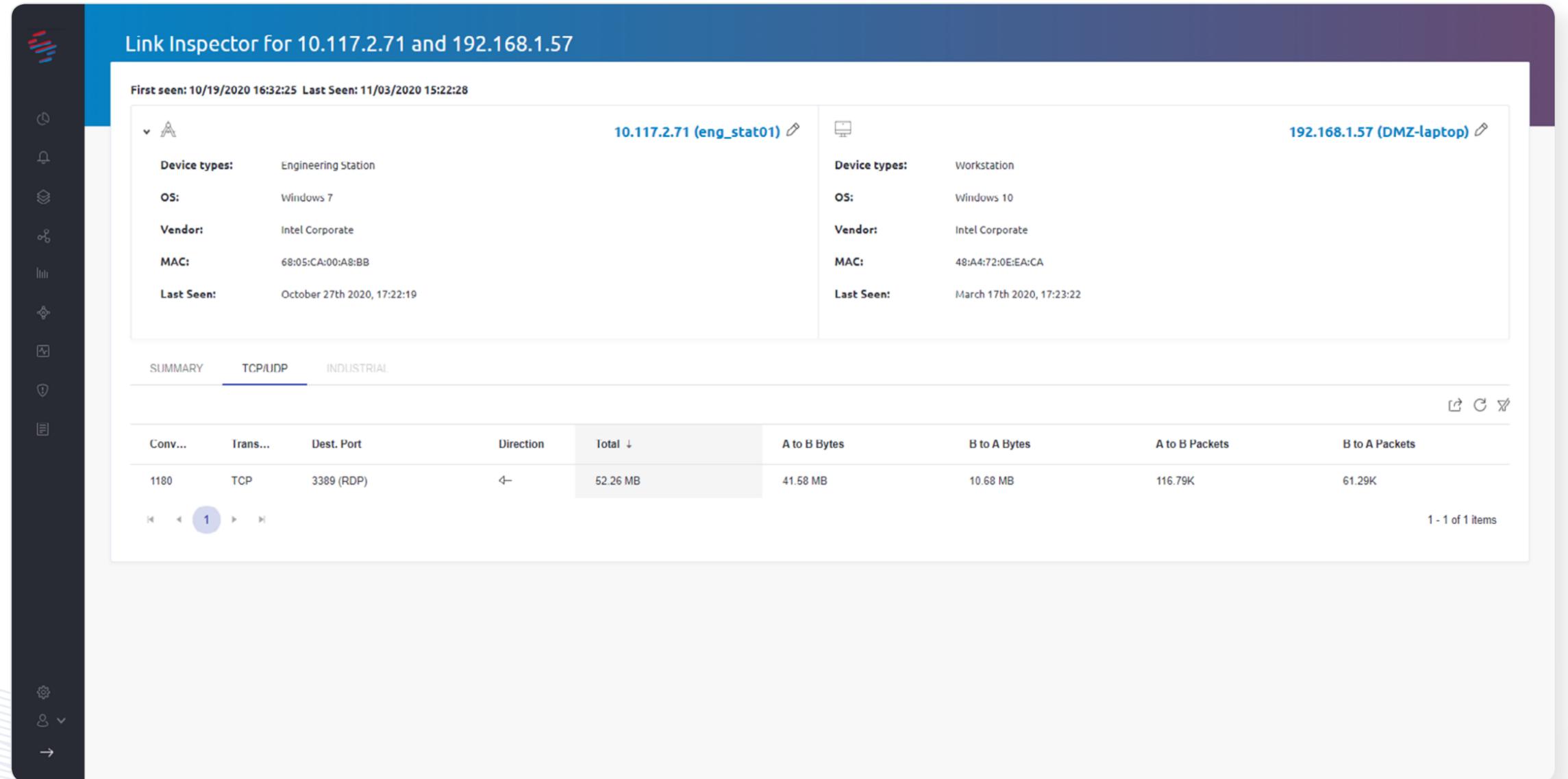
Commonly Used Port (T0885)

 **Criteria:**

Evidence of an established network connection over TCP port 3389 as RDP.

1.A.1.1 - Link Inspector:

Port 3389 (RDP) connection between adversary and engineering-station



Link Inspector for 10.117.2.71 and 192.168.1.57

First seen: 10/19/2020 16:32:25 Last Seen: 11/03/2020 15:22:28

Property	10.117.2.71 (eng_stat01)	192.168.1.57 (DMZ-laptop)
Device types:	Engineering Station	Workstation
OS:	Windows 7	Windows 10
Vendor:	Intel Corporate	Intel Corporate
MAC:	68:05:CA:00:A8:BB	48:A4:72:0E:EA:CA
Last Seen:	October 27th 2020, 17:22:19	March 17th 2020, 17:23:22

TAB: SUMMARY | TCP/UDP | INDUSTRIAL

Conv...	Trans...	Dest. Port	Direction	Total ↓	A to B Bytes	B to A Bytes	A to B Packets	B to A Packets
1180	TCP	3389 (RDP)	←	52.26 MB	41.58 MB	10.68 MB	116.79K	61.29K

1 - 1 of 1 items

1.A.1.2 - Traffic Analyzer - Protocols:
RDP connections

The screenshot displays the Traffic Analyzer interface with the 'Protocols' tab selected. The main table lists various protocols and their traffic statistics. Below it, a detailed view of a conversation is shown.

Protocol	Dest. Port	Trans...	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total ↓
+ DACnet/IP	47000	UDP	836.77K	831.72K	197.35 MB	253.34 MB	450.68 MB
+ Modbus/TCP	502	TCP	2.28M	2.06M	135.72 MB	123.01 MB	248.54 MB
+ iPulse-ICS	20222	TCP	49.17K	85.17K	3.01 MB	101.41 MB	104.42 MB
+ HTTPS	443	TCP	102.99K	80.75K	12.69 MB	88.81 MB	101.5 MB
+ MS-SQL-s	1433	TCP	638.64K	637.78K	40.64 MB	41.37 MB	82.01 MB
+ VAT	3456	TCP	68.38K	66.02K	4.13 MB	75.1 MB	79.23 MB
+ Kerberos	88	TCP	157.51K	116.21K	54.03 MB	30.67 MB	70.35 MB
+ EPMAP	135	TCP	1.61M	1.61M	43.85 MB	46.25 MB	68.73 MB
+ SunProxyAdmin	8081	TCP	104.6K	100.75K	6.32 MB	61.43 MB	65.12 MB
+ SMD	445	TCP	907.27K	1.05M	43.62 MB	68.95 MB	64.53 MB
- RDP	3389	TCP	244.5K	148.04K	57.44 MB	21.23 MB	60.62 MB

Conv...	Source IP	Src. Port	Dest. IP	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total ↓	In...
1180	192.168.1.57	65536	10.117.2.71	116.79K	61.29K	41.58 MB	10.68 MB	52.26 MB	
48	10.130.78.217	65536	10.117.0.51	12.32K	2.45K	1.15 MB	971.86 KB	2.12 MB	
57	10.130.78.213	65536	10.117.0.51	10.48K	3.98K	1.12 MB	880.72 KB	2 MB	
1	192.168.1.54	generic	10.11.0.200	526	1.4K	40.63 KB	1.74 MB	1.78 MB	
132	10.130.80.212	65536	10.117.0.142	4.82K	3.47K	902.83 KB	801.7 KB	1.7 MB	
52	10.130.80.226	65536	10.117.0.142	1.95K	680	334.09 KB	103.21 KB	437.3 KB	

1.A.1.3 - Alerts Manager:

New host and new connection to industrial device alerts

The screenshot displays the Alerts Manager interface with a table of alerts. The interface includes a top navigation bar with filters for 'Open 176', 'Resolved 140', 'Don't show 1', 'Stale 93', and 'All 316'. A search bar and a 'Mark 0 selected as Resolved' button are also present. The table columns are: ID, Severity, Description, Status, IP, Hostname, Details, and Last Event Time. The table contains 18 rows of alert data.

ID	Severity	Description	Status	IP	Hostname	Details	Last Event Time
26	Blue	New host detected	In Progress	192.168.0.102	desktop-cs7vbm1u	New host detected: 192.168.0.102 (desktop-cs7vbm1u) from source: communication fro...	12/02/2020 12:21:41
560	Blue	New host detected	Created	172.31.16.1		New host detected: 172.31.16.1 from source: ARP Packet.	11/12/2020 10:09:25
51888	Yellow	TeamViewer Inbound connection established	In Progress	10.11.0.200	powersvr1	TeamViewer Inbound connection was established from device 192.168.1.135 (scadafen...	08/16/2020 09:34:08
50103	Yellow	TeamViewer inbound connection established	In Progress	192.168.1.135	scadafence-rbi10d	TeamViewer inbound connection was established from device 213.227.181.133 to devic...	08/16/2020 09:34:08
501	Purple	New Source IP Connecting to industrial device	In Progress	192.168.0.123	Eng_SIA_1	Unexpected conversation detected between IP address 192.168.0.123 (Eng_SIA_1) (H...	07/22/2020 10:22:29
555	Blue	New host detected	Created	172.31.27.226	ip-172-31-27-226...	New host detected: 172.31.27.226 (ip-172-31-27-226.eu-central-1.compute.interna...) tro...	07/20/2020 09:35:08
35	Blue	New host detected	In Progress	192.168.1.57		New host detected: 192.168.1.57 from source: communication from this IP.	07/15/2020 16:10:47
12	Blue	New host detected	In Progress	192.168.0.176	HMI-L345	New host detected: 192.168.0.176 (HMI-L345) from source: communication from this IP.	06/13/2020 23:53:42
95	Blue	New host detected	In Progress	192.168.0.137		New host detected: 192.168.0.137 from source: communication from this IP.	05/28/2020 11:24:51
36	Purple	New Source IP Connecting to industrial device	In Progress	10.117.2.71	(Eng_STA_1)	Unexpected conversation detected between IP address 10.117.2.71 (Eng_STA_1) (othe...	05/27/2020 11:45:12
50100	Red	Group-to-group communication	In Progress			User rule "Unauthorized Traffic": Communication between group "DMZ_Plant_3" and gr...	05/26/2020 20:02:25
51803	Blue	New host detected	Created	192.168.1.135	scadafence-rbi10d	New host detected: 192.168.1.135 (scadafence-rbi10d) from source: communication fro	05/26/2020 16:56:41
51796	Blue	New host detected	Created	10.11.0.200	powersvr1	New host detected: 10.11.0.200 (powersvr1) from source: communication from this IP.	05/26/2020 16:56:41
51794	Blue	New host detected	Created	10.11.38.100		New host detected: 10.11.38.100 from source: communication from this IP.	05/26/2020 16:56:39
51807	Blue	New host detected	Created	10.11.0.202		New host detected: 10.11.0.202 from source: communication from this IP.	05/26/2020 16:56:38

Attack method:

Adversaries may use the protocol associated with the port, or a completely different protocol to bypass firewalls or network detection systems and to blend in with normal network activity

Tactic:

Command and Control (TA0101)

Technique:

Commonly Used Port (T0885)

Criteria:

Successful logon as user "Engineer" on RDP (3389) may be present or as a part of the connection and process creation.

1.A.2.1 - User Activity Analyzer:

RDP connections and operations

The screenshot shows the 'User Activity Analyzer' interface with a table of network activity. The table has columns for Source IP, Src Hostname, VPN, Dest. IP, Dest Hostname, Application, Operation, Service, Username, and Time. The interface includes a sidebar with navigation icons, a top navigation bar with filters, and a pagination bar at the bottom.

Source IP ↑	Src Hostname	VPN	Dest. IP	Dest Hostname	Application	Operation	Service	Username	Time
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.2.17	xperion_srvb	RDP	disconnect(inact)	XPERION_SRVB.lin...	*****	10/26/2020 14:36:10
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.2.17	xperion_srvb	RDP	login	XPERION_SRVB.lin...	*****	10/22/2020 13:35:50
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.0.53	phdsrv_hw01 line3 L...	RDP	disconnect(inact)	PHDSRV_HW01 lin...	*****	10/22/2020 14:04:29
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.2.17	xperion_srvb	RDP	disconnect(inact)	XPERION_SRVB.lin...	*****	10/26/2020 14:38:23
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.2.17	xperion_srvb	RDP	login	XPERION_SRVB.lin...	*****	10/22/2020 14:16:48
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.0.53	phdsrv_hw01.line3.L...	RDP	login	PHDSRV_HW01.lin...	*****	10/22/2020 13:59:50
10.117.0.51	phd_hw01	<input type="checkbox"/>	10.117.2.17	xperion_srvb	RDP	disconnect(inact)	XPERION_SRVB lin...	*****	10/26/2020 14:37:21
10.128.19.169		<input type="checkbox"/>	10.117.0.142	hmi_hw01	RDP	disconnect(inact)	HMI_HW01.line3.local	*****	10/27/2020 16:06:48
192.168.1.57	DMZ-laptop	<input type="checkbox"/>	10.117.2.71	eng_stat01	RDP	login	REFAPC01.area3.lo...	*****	10/20/2020 15:53:45
10.128.19.169		<input type="checkbox"/>	10.117.0.142	hmi_hw01	RDP	disconnect(inact)	HMI_HW01.line3.local	*****	10/27/2020 16:09:51
10.128.19.169		<input type="checkbox"/>	10.117.0.142	hmi_hw01	RDP	disconnect(inact)	HMI_HW01.line3.local	*****	10/20/2020 15:56:45
192.168.1.57	DMZ-laptop	<input type="checkbox"/>	10.117.2.71	eng_stat01	RDP	login	REFAPC01.area3.lo...	*****	10/27/2020 16:04:08
192.168.1.57	DMZ-laptop	<input type="checkbox"/>	10.117.2.71	eng_stat01	RDP	disconnect(inact)	REFAPC01.area3.lo...	*****	10/20/2020 15:56:45
10.128.19.169		<input type="checkbox"/>	10.117.0.142	hmi_hw01	RDP	login	HMI_HW01.line3.local	*****	10/27/2020 16:04:08
10.128.19.169		<input type="checkbox"/>	10.117.0.142	hmi_hw01	RDP	login	HMI_HW01.line3.local	*****	10/20/2020 15:53:45

1.A.2.2 - Connection Inspector:

Port 3389 (RDP) connection between adversary and engineering-station

The screenshot displays the 'Source Connection Inspector for 192.168.1.57' interface. It shows a connection between the source IP 192.168.1.57 and the destination IP 10.117.2.71. A popup window titled 'Last Logins between 192.168.1.57 and eng_stat01' is open, showing a table of login events.

Username	Application	Service	Operation	Time ↑
*****	RDP	REFAPC01.ar...	login	10/20/2020 15:53:45
*****	RDP	REFAPC01 ar...	disconnect(ina	10/20/2020 15:56:45

Additional details for the connection to 10.117.2.71:
Login: 10/20/20 15:53:45
User: *****/RDP
Srv: REFAPC01.area3.it

Attack method:

Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:

Execution (TA0104)

Technique:

Execution through API (T0871)

Criteria:

Evidence of an adversary initiated program upload action of the control PLC to collect the current running configuration.

2.B.1.1 - Alerts Manager:

Program Upload (programming read) alert

ID	Severity	Description	Status	IP	Hostname	Details	Last Event Time
50100	High	Group-to-group communication	In Progress			User rule "Unauthorized Traffic": Communication between group "DMZ_Plant_3" and gr...	05/26/2020 20:02:25
1446	High	Trickbot trojan communication detected	In Progress	192.168.0.102	desktop-cs7vbm	192.168.0.102 (desktop-cs7vbm) is communicating with a Trickbot C&C server 92.53....	07/18/2020 09:33:16
554	High	Security Incident Detected	In Progress	192.168.0.222	WSTA_4	Multiple alerts on this IP.	05/20/2020 16:08:03
465	High	SMB exploitation attempt - MS17-10 Fter ...	In Progress	192.168.1.24	tech-ws-18	SMB exploit detected - device 192.168.1.24 (tech-ws-18) sent an exploit to device 192...	02/19/2020 18:18:14
10	High	Vulnerability assessment tool detected - ...	In Progress	192.168.1.16	scadafence-pc	Nessus communication detected from 192.168.1.16 (scadafence-pc) to target IP 192.16...	02/12/2020 15:31:08
50103	Medium	TeamViewer inbound connection establis...	In Progress	192.168.1.135	scadafence-rb10d	TeamViewer inbound connection was established from device 213.227.181.133 to devic...	08/16/2020 09:34:08
51888	Medium	TeamViewer inbound connection establis...	In Progress	10.11.0.200	powersvr1	ToamViewor inbound connection was established from device 192.168.1.135 (scadafen...	08/16/2020 09:34:08
559	Medium	Communication with vulnerable device	In Progress	192.168.0.132	plc_32	Industrial device 192.168.0.132 (plc_31) has communicated with device 192.168.0.123 ...	11/05/2020 15:12:37
510	Medium	Domain reputation alert	In Progress	192.168.0.101	WS-yk75	Device 192.168.0.101 (WS-yk75) tried to resolve a known malicious domain name "aak...	02/12/2020 15:31:00
50102	Low	New Source IP Connecting to industrial d...	In Progress	10.11.0.202		Unexpected conversation detected between IP address 10.11.0.154 (Engineering Statio...	05/22/2020 10:22:29
50101	Low	Industrial parameter value out of range	In Progress	10.11.38.100		User rule Analog Value Validation (profile-based): Device 10.11.38.100 reported value ...	08/29/2017 04:59:23
51867	Low	Programming read command detected	In Progress	10.11.0.202		10.117.2.71 (Eng_STA_1) sent a programming read sequence to PLC on 10.11.0.202. us...	05/26/2020 17:07:34
50042	Low	Programming write command detected	In Progress	10.77.60.131	PLC_131	10.77.1.60 (win-k4tva/53kkg) sent a programming write sequence to PLC on 10.77.60...	07/29/2018 12:44:20
50019	Low	PLC stop command issued	In Progress	10.77.0.140	PLC_140	10.77.1.60 (win-k4tva/753kkg) sent a PLC stop command to PLC on 10.77.0.140 (PLC_...	01/16/2019 15:30:38
50001	Low	PLC stop command issued	In Progress	192.168.60.150		192.168.60.11 sent a PLC stop command to PLC on 192.168.60.150, using melsoft prot...	05/17/2020 18:58:10

2.B.1.1.1 - Alerts Manager:

Program Upload (programming read) alert

The screenshot displays the Alerts Manager interface for a 'Programming read command detected' alert. The alert is currently in an 'In Progress' state. The main content area is divided into several sections: a header with the alert title and a 'Resolve' button; a summary section with details like ID, severity, and last event time; an 'Explanation' section describing the event; a 'Resolution recommendations' section with two steps; a 'Last comment & Actions' section with a comment from 'Admin'; and an 'Affected Asset' section for IP 10.11.0.202, which includes a table of device details and an 'Additional Details' table.

Alerts Manager > Programming read command detected Resolve

Programming read command detected In Progress

10.117.2.71 sent a programming read sequence to PLC on 10.11.0.202 using cip protocol
ID: 11 Severity: **Threat** Last Event Time: 04/12/2020 19:28:55 Total Events: 36
MITRE ATT&CK: Collection > Automated Collection, Collection > Data From Information Repositories, ...

Explanation

A programming read sequence was sent to a PLC. This command is used in the process of reading code or memory on a PLC, and might indicate malicious activity.

Resolution recommendations

1. Check if the source is authorized to perform read operations on this PLC.
2. Validate with the operator what was the purpose of the read operations on this PLC

Last comment & Actions All + Add Comment

Admin 17-08-21 23:48 Alert first seen by admin

Affected Asset 10.11.0.202

10.11.0.202 1 Information 6 Threat **Connections:** 3 Internal

Device types:	PLC
Vendor:	Rockwell Automation
MAC:	F4:54:33:AD:39:7A
First seen:	March 15th 2020, 11:00:27
Last Seen:	February 2nd 2021, 19:03:34

Additional Details

Asset name:	1769-L30ER/A LOGIX5330ER
Serial number:	60D5ED50
Firmware version:	32.11
Device Type:	PLC

2.B.1.2 - User Activity Analyzer: ICS connections and operations

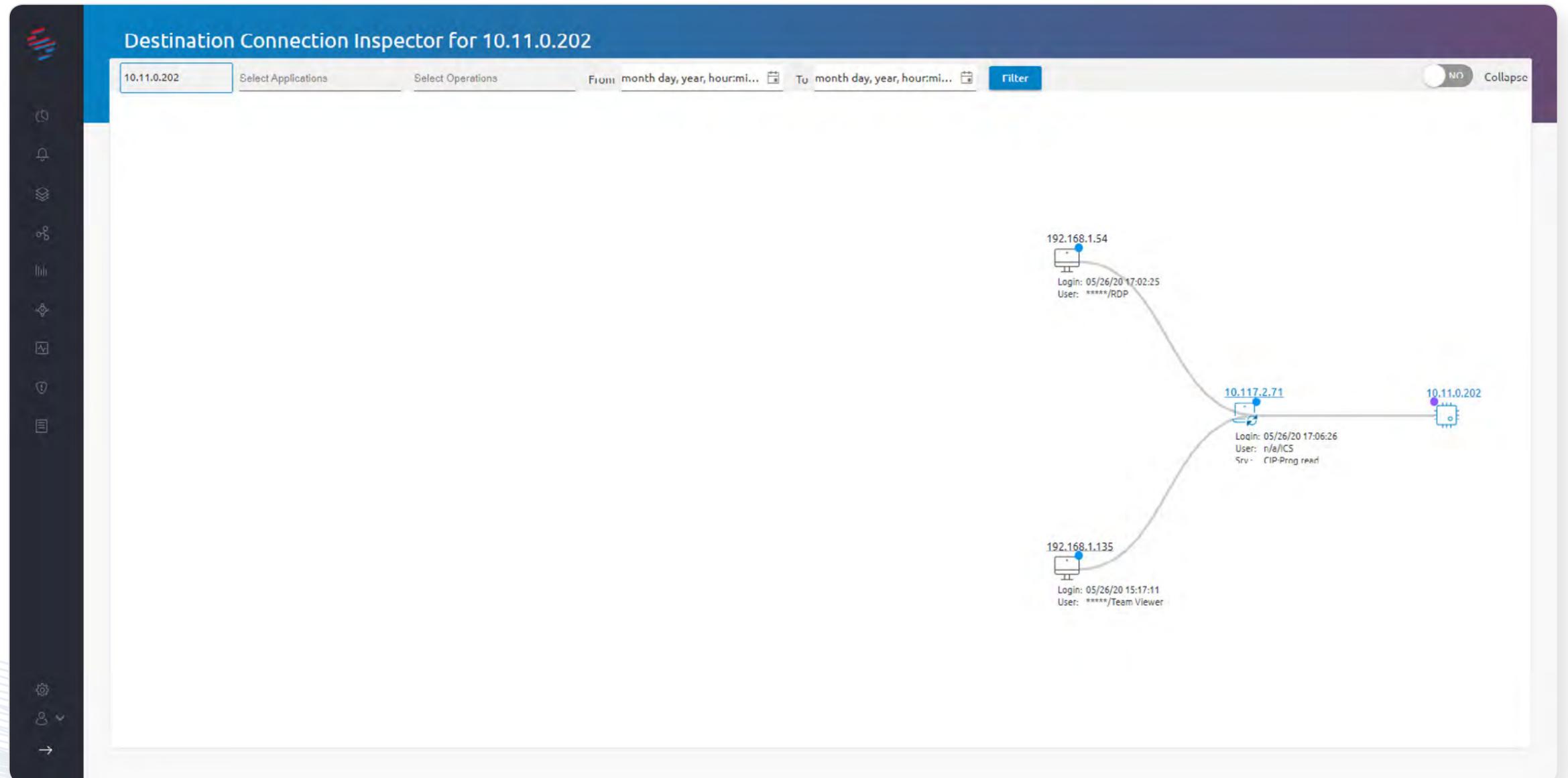
User Activity Analyzer

Select Applications | All Operations | All Data

Source IP ↑	Src Hostname	VPN	Dest. IP	Dest Hostname	Application	Operation	Service	Username	Time
10.117.2.71	Eng_STA_1	<input type="checkbox"/>	10.11.0.202		ICS	Prog.read	cip	n/a	05/26/2020 17:06:26
192.168.0.107	Eng_STA_4	<input type="checkbox"/>	192.168.0.140		ICS	PLCstop	umas	n/a	03/17/2019 17:04:27
10.77.1.60	win-k4tva753kkg	<input type="checkbox"/>	10.77.0.140		ICS	PLC prog write	umas	n/a	03/07/2019 15:16:47
192.168.0.107	Eng_SIA_4	<input type="checkbox"/>	192.168.0.140		ICS	PLCstart	umas	n/a	03/17/2019 17:04:34
10.77.1.60	win-k4tva753kkg	<input type="checkbox"/>	10.77.0.140		ICS	PLC stop	umas	n/a	01/16/2019 15:30:38
10.77.1.60	win-k4tva753kkg	<input type="checkbox"/>	10.77.0.140		ICS	PLC start	umas	n/a	01/16/2019 15:30:53
192.168.0.123	Eng_STA_1	<input type="checkbox"/>	192.168.0.136		ICS	PLCstart	s7comm_plus	n/a	03/17/2019 14:29:42
192.168.0.123	Eng_STA_1	<input type="checkbox"/>	192.168.0.136		ICS	PLCstop	s7comm_plus	n/a	03/17/2019 14:29:36
192.168.0.123	Eng_STA_1	<input type="checkbox"/>	192.168.0.135		ICS	PLCstop	s7comm	n/a	03/17/2019 14:28:20
192.168.0.123	Eng_SIA_1	<input type="checkbox"/>	192.168.0.130		ICS	PLCstart	s7comm_plus	n/a	03/17/2019 14:31:34
192.168.0.123	Eng_STA_1	<input type="checkbox"/>	192.168.0.130		ICS	PLCstop	s7comm_plus	n/a	03/17/2019 14:31:29
192.168.0.125	Eng_STA_6	<input type="checkbox"/>	192.168.0.170		ICS	PLCstop	slmp	n/a	03/17/2019 16:02:57
192.168.0.125	Eng_STA_6	<input type="checkbox"/>	192.168.0.170		ICS	PLCstart	clmp	n/a	03/17/2019 16:06:47
192.168.0.135		<input type="checkbox"/>	192.168.0.123	Eng_STA_1	ICS	PushStateStop	s7comm	n/a	03/17/2019 14:20:20
192.168.0.135		<input type="checkbox"/>	192.168.0.123	Eng_STA_1	ICS	PushStateRun	s7comm	n/a	03/17/2019 14:25:52

1 - 15 of 20 items

2.B.1.3 - Connection Inspector:
Adversary to engineering-station to PLC



2.B.1.4 - Assets Manager:

PLC asset management page including device information and alerts

The screenshot displays the 'Assets Manager' interface for the IP address 10.11.0.202. The interface is divided into several sections:

- Header:** 'Assets Manager > 10.11.0.202'
- Summary:** 1 Information, 2 Threat, Connections: 1 Internal, 3 Exposure Groups
- Device Information:**
 - Device types: PLC
 - OS:
 - Hostname:
 - Vendor: Rockwell Automation
 - MAC: F4:54:33:AD:39:7A
 - First seen: May 26th 2020, 16:56:38
 - Last Seen: May 26th 2020, 17:27:04
 - NIC Type: Ethernet
- Additional Details:**
 - Asset name: 1769-I 16FR/B LOGIX5316FR
 - Serial number: 60D5ED50
 - Firmware version: 32.11
 - Vendor: Rockwell Automation/Allen-Bradley
 - Device Type: PLC
- Organization Details:**
 - Criticality:
 - OU:
 - Owner:
 - Physical Location:
 - Comment:
 - Product for CVE:
 - Version for CVE:
- Open Alerts:**

ID	Severity ↓	Description	Status	Details	MITRE ATT&CK	Last Event Time
51867	High	Programming read command detected	In Progress	10.117.2.71 (Eng_STA_1) sent a programming read sequence to PLC on 10.11.0.202 ...	Collection > Automated ...	05/26/2020 17:07:34
50102	High	New Source IP Connecting to industrial d...	In Progress	Unexpected conversation detected between IP address 10.11.0.154 (Engineering Sta...	Initial Access > Drive B...	05/22/2020 10:22:29
51807	Low	New host detected	Created	New host detected: 10.11.0.202 from source: communication from this IP.		05/26/2020 16:56:38

Attack method:

Adversaries may use the protocol associated with the port, or a completely different protocol to bypass firewalls or network detection systems and to blend in with normal network activity.

Tactic:

Command and Control (TA0101)

Technique:

Commonly Used Port (T0885)

Criteria:

Evidence of an established network connection over TCP port 445 from the control machine to the adversary machine as an outbound SSH tunnel request in the current running configuration.

4.B.2.1 - Traffic Analyzer - TCP/UDP Conversations:

Port 445 connection between engineering-station and adversary

Conv...	Source IP	Dest. IP	Dest. Port	Trans...	A to B Bytes	B to A Bytes	First seen	Last Seen	Total	Tir	In...
12234	10.117.2.71	10.117.6.6	generic (dynamic)	TCP	1.13 KB	658 B	10/19/2020 16:32:04	10/27/2020 14:13:40	1.79 KB		
12139	10.117.2.71	192.168.1.57	445 (SMB)	TCP	5.47 MB	4.29 MB	10/19/2020 16:32:27	10/27/2020 17:21:56	9.76 MB		
12026	10.117.0.51	255.255.255.255	1947 (SentinelSRM)	UDP	1.55 KB	0 B	10/19/2020 16:32:24	10/27/2020 17:22:00	1.55 KB		
12014	10.117.0.51	10.117.31.255	1947 (SentinelSRM)	UDP	1.55 KB	0 B	10/19/2020 16:32:28	10/27/2020 17:22:04	1.55 KB		
11031	10.117.3.17	10.117.2.17	2911 (Honeywell Discovery)	UDP	903 B	0 B	10/19/2020 16:33:03	10/27/2020 17:22:14	903 B		
11701	10.117.2.73	10.117.6.5	135 (EPMAP)	TCP	4.23 MB	1.03 MB	10/19/2020 16:32:25	10/27/2020 17:22:02	5.26 MB		
11652	10.117.2.71	10.117.6.5	135 (EPMAP)	TCP	4.55 MB	804.09 KB	10/19/2020 16:32:38	10/27/2020 17:22:09	5.35 MB		
11383	10.117.3.17	10.117.2.15	2911 (Honeywell Discovery)	UDP	746 B	0 B	10/19/2020 16:32:08	10/27/2020 17:22:14	746 B		
11298	10.117.2.41	10.117.2.15	123 (NTP)	UDP	2.09 MB	2.09 MB	10/19/2020 16:32:21	10/27/2020 17:21:34	4.18 MB		
11298	10.117.2.41	10.117.2.15	123 (NTP)	UDP	2.09 MB	2.09 MB	10/19/2020 16:32:21	10/27/2020 17:21:34	4.18 MB		
11228	10.117.2.15	10.117.3.15	2911 (Honeywell Discovery)	UDP	753 B	0 B	10/19/2020 16:32:24	10/27/2020 17:22:16	753 B		
11203	10.117.2.73	10.117.6.6	generic (dynamic)	TCP	1.14 KB	601 B	10/19/2020 16:32:07	10/27/2020 16:10:44	1.74 KB		
11057	10.117.2.15	10.117.3.17	2911 (Honeywell Discovery)	UDP	751 B	0 B	10/19/2020 16:32:04	10/27/2020 17:22:16	751 B		
10955	10.117.2.15	10.117.6.3	53 (DNS)	UDP	2.13 MB	3.84 MB	10/19/2020 16:32:14	10/27/2020 17:21:24	5.97 MB		
10843	10.117.1.11	10.117.0.51	135 (EPMAP)	TCP	708 B	6.86 MB	10/19/2020 16:32:24	10/27/2020 17:21:52	1.05 KB		

4.B.2.2 - Traffic Analyzer - Protocols:

Port 445 connections

The screenshot displays the 'Traffic Analyzer' interface with the 'Protocols' tab selected. The top navigation bar includes 'IP Conversations', 'TCP/UDP Conversations', 'Protocols', 'Industrial Protocols', and 'Industrial Layer 2'. The main table lists various protocols and their traffic statistics. Below this, a 'Conversations' table provides details for specific connections.

Protocol	Dest. Port	Trans...	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total
Honeywell CDA	55556	TCP	1.19K	1.19K	73.13 KB	73.39 KB	146.52 KB
Honeywell CDA	55557	TCP	1.58K	1.07K	96.61 KB	65.74 KB	162.36 KB
dynamic	generic	UDP	75.23K	1.42K	20.59 MB	307.53 KB	20.9 MB
dynamic	generic	TCP	956.54K	1.16M	24.46 MB	43.91 MB	48.75 MB
DNS	53	TCP	3.24K	2.84K	1.44 MB	368.93 KB	1.81 MB
DNS	53	UDP	159.06K	152.23K	13.69 MD	17.01 MD	31.5 MD
BOOTPS	67	UDP	178	165	61.39 KB	58.84 KB	120.23 KB
NetBIOS	139	TCP	551.42K	468.7K	45.45 MB	43.97 MB	18.54 MB
SMB	445	TCP	907.27K	1.05M	43.62 MB	68.95 MB	64.53 MB

Conv...	Source IP	Src. Port	Dest. IP	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total ↓	In...
12139	10.117.2.71	65536	192.168.1.57	66.62K	41.96K	5.47 MB	4.29 MB	9.76 MB	
653	10.117.0.142	65536	10.117.6.3	14.7K	14.34K	3.38 MB	1.82 MB	5.2 MB	
507	10.117.2.71	65536	10.117.6.3	11.73K	11.32K	3.41 MB	1.37 MB	4.78 MB	
381	10.117.2.15	65536	10.117.6.3	10.87K	10.53K	2.88 MB	1.33 MB	4.22 MB	
425	10.117.2.73	65536	10.117.6.3	10.24K	9.69K	2.97 MD	1.19 MD	4.16 MD	
389	10.117.2.17	65536	10.117.6.3	10.41K	10K	2.89 MB	1.24 MB	4.13 MB	
398	10.117.0.51	65536	10.117.6.3	9.49K	9.27K	2.76 MB	1.15 MB	3.91 MB	
3006	10.117.3.101	65536	10.117.0.51	11.74K	9.32K	1.2 MB	2.24 MB	3.43 MB	

 **Attack method:**

Adversaries attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for subsequent Lateral Movement or Discovery techniques.

 **Tactic:**

Discovery (TA0102)

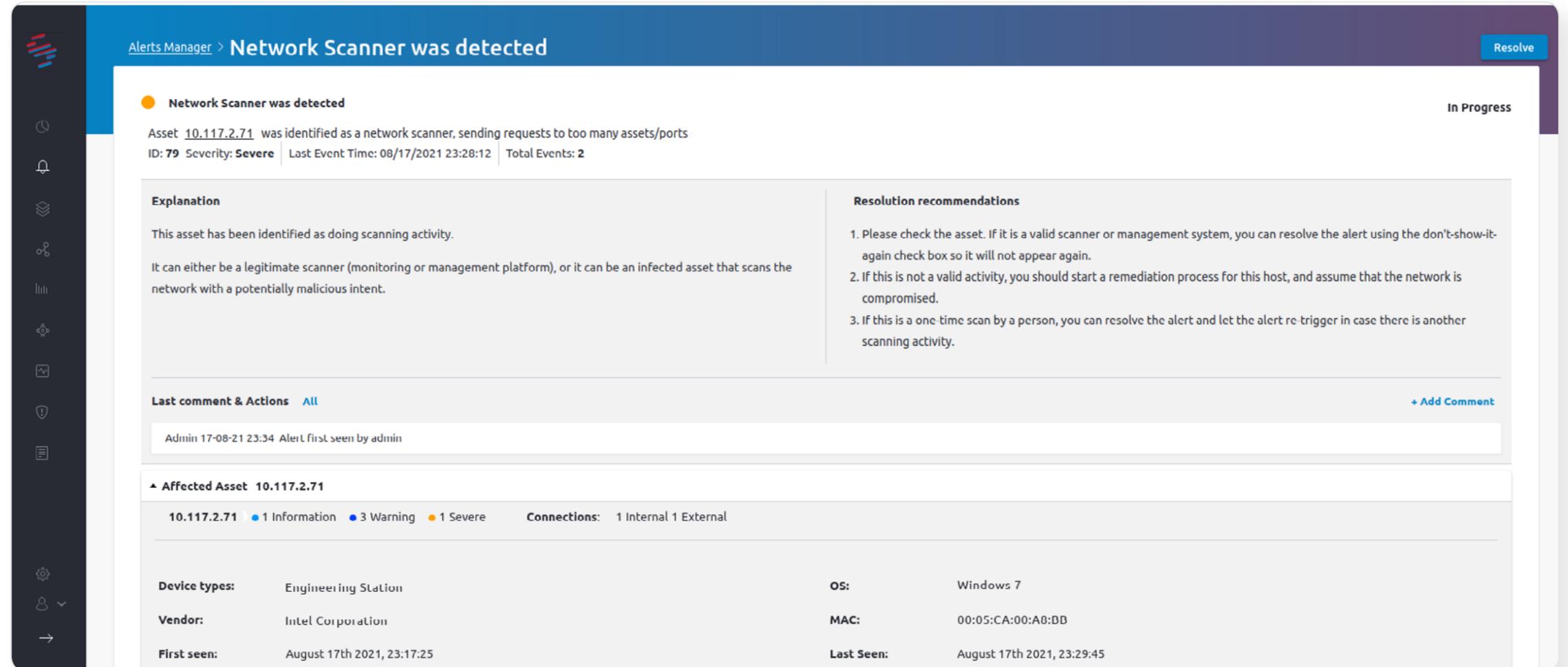
 **Technique:**

Remote System Discovery (T0846)

 **Criteria:**

Evidence that a network discovery scan for TCP port 44818 was initiated from the control machine on hosts across the whole subnet.

9.A.2 - Network Scanner detection alert



The screenshot displays the SCADAfence Alerts Manager interface. The main header shows 'Alerts Manager > Network Scanner was detected' with a 'Resolve' button. The alert details include:

- Alert Title:** Network Scanner was detected (In Progress)
- Asset:** 10.117.2.71 was identified as a network scanner, sending requests to too many assets/ports
- ID:** 79 | **Severity:** Severe | **Last Event Time:** 08/17/2021 23:28:12 | **Total Events:** 2

The alert content is divided into two columns:

- Explanation:** This asset has been identified as doing scanning activity. It can either be a legitimate scanner (monitoring or management platform), or it can be an infected asset that scans the network with a potentially malicious intent.
- Resolution recommendations:**
 - Please check the asset. If it is a valid scanner or management system, you can resolve the alert using the don't-show-it-again check box so it will not appear again.
 - If this is not a valid activity, you should start a remediation process for this host, and assume that the network is compromised.
 - If this is a one-time scan by a person, you can resolve the alert and let the alert re-trigger in case there is another scanning activity.

Below the explanation, there is a 'Last comment & Actions' section with a '+ Add Comment' link. A comment from 'Admin' at 17-08-21 23:34 states 'Alert first seen by admin'.

The 'Affected Asset' section for 10.117.2.71 shows:

- Alerts:** 1 Information, 3 Warning, 1 Severe
- Connections:** 1 Internal, 1 External

Asset details table:

Device types:	Engineering Station	OS:	Windows 7
Vendor:	Intel Corporation	MAC:	00:05:CA:00:A8:BB
First seen:	August 17th 2021, 23:17:25	Last Seen:	August 17th 2021, 23:29:45

Attack method:

Adversaries attempt to get a listing of other systems by IP address on a network that may be used for subsequent Lateral Movement.

Tactic:

Discovery (TA0102)

Technique:

Remote System Discovery (T0846) [Link](#)

Criteria:

Evidence of the network discovery broadcast request sent from the control EWS over TCP port 44818..

9.B.2.1 - Traffic Analyzer - Industrial Protocols:

EtherNet/IP broadcast scan (List Identity) commands visibility

The screenshot shows the Traffic Analyzer interface with the 'Industrial Protocols' tab selected. The main table displays traffic details:

Conv...	Source IP	Src Hostname	Dest. IP ↓	Dest Hostname	Protocol
- 1	10.117.2.71		255.255.255.255		EtherNet/IP I/O

Below this, a detailed view of a specific command is shown:

Conv...	Command description	Last Seen
6	List Identity (Request)	02/02/2021 20:43...

A secondary table shows a list of broadcast requests:

Conv...	Source IP	Dest. IP	Protocol
+ 1	192.168.0.140	192.168.1.20	EtherNet/IP I/O
+ 1	192.168.1.160	192.168.1.19	EtherNet/IP I/O
+ 1	192.168.1.198	192.168.1.25	EtherNet/IP I/O
+ 1	192.168.0.165	192.168.1.19	EtherNet/IP I/O
+ 1	192.168.1.199	192.168.1.19	EtherNet/IP I/O

9.B.2.2 - Link Inspector:
Control to broadcast

Link Inspector for 10.117.2.71 and 255.255.255.255

First seen: 02/02/2021 20:42:37 Last Seen: 02/02/2021 20:43:14

Device types:	Engineering Station	10.117.2.71	255.255.255.255
Vendor:	Intel Corporation		Last Seen: February 2nd 2021, 20:42:37
MAC:	68:05:CA:00:A8:BB		
Last Seen:	February 2nd 2021, 20:43:45		

SUMMARY TCP/UDP INDUSTRIAL

Conv...	Direction	Protocol
1	→	EtherNet/IP I/O

Conv...	Command description	Last Seen
6	List Identity (Request)	02/02/2021 20:43...

1 - 1 of 1 items

Attack method:

An adversary attempts to get detailed information about remote systems and their peripherals, such as make/model, role, and configuration.

Tactic:

Discovery (TA0102)

Technique:

Remote System Information Discovery (T0888)

Criteria:

Evidence of an adversary initiated Get Attribute Single CIP request for the "Device Type" attribute (instance 0x01, class 0x01) of the control PLC.

9.C.2 - Traffic Analyzer - Industrial Protocols:

CIP GetAttributeSingle 'Device Type' commands visibility

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostname	Protocol
+ 124	192.168.0.19		192.168.0.160		CIP
+ 69	192.168.1.19		192.168.1.160		CIP
+ 52	192.168.0.20		192.168.0.160		CIP
- 36	10.117.2.71		10.11.0.202		CIP

Conv...	Command description	Last Seen
38	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Vendor ID	02/02/2021 20:41...
21	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Product Code	02/02/2021 20:41...
21	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Device Type	02/02/2021 20:41...
17	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Revision	02/02/2021 20:41...
3	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attributes All (Request)	02/02/2021 20:42...

Attack method:

An adversary attempts to get detailed information about remote systems and their peripherals, such as make/model, role, and configuration.

Tactic:

Discovery (TA0102)

Technique:

Remote System Information Discovery (T0888)

Criteria:

Evidence of an adversary initiated Get Attribute Single CIP request for the "Status" attribute (instance 0x01, class 0x01) of the control PLC.

9.D.2 - Traffic Analyzer - Industrial Protocols:

CIP GetAttributeSingle 'Status' commands visibility

Traffic Analyzer

IP Conversations | TCP/UDP Conversations | Protocols | **Industrial Protocols** | Industrial Layer 2 >

Type exact IP

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostname	Protocol
+ 124	192.168.0.19		192.168.0.160		CIP
+ 69	192.168.1.19		192.168.1.160		CIP
+ 52	192.168.0.20		192.168.0.160		CIP
- 36	10.117.2.71		10.11.0.202		CIP

Conv...	Command description ↑	Last Seen
2	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Serial Number	02/02/2021 20:41...
2	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Status	02/02/2021 20:41...
38	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attribute Single (Request), Attribute: Vendor ID	02/02/2021 20:41...
3	ENIP: Unconnected Message; CIP Object: Identity, Service: Get Attributes All (Request)	02/02/2021 20:42...

6 - 9 of 9 items

Attack method:

Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:

Execution (TA0104)

Technique:

Execution through API (T0871)

Criteria:

Evidence that all controller and program tag names were requested over CIP from the control PLC to the control machine.

9.E.2.1 - Traffic Analyzer - Industrial Protocols:

CIP Read/Write Tags commands visibility

The screenshot displays the 'Traffic Analyzer' interface with the 'Industrial Protocols' tab selected. It features a table of network conversations and a detailed view of specific commands.

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostname	Protocol
+ 124	192.168.0.19		192.168.0.160		CIP
+ 69	192.168.1.45		192.168.1.160		CIP
+ 57	192.168.0.20		192.168.0.160		CIP
+ 36	192.168.1.19		192.168.1.198		CIP
+ 31	192.168.1.47		192.168.1.199		CIP
+ 28	192.168.0.160		192.168.0.19		CIP
- 23	10.117.2.71		10.11.0.202		CIP

# Co...	Command description	Last Seen
6	ENIP: Connected Message; CIP Object: Generic, Service: Write Tag Fragmented (Response:Success)	02/02/2021 20:41...
2	ENIP: Connected Message; CIP Object: Generic, Service: Read Tag (Response:Partial transfer)	02/02/2021 20:43...
7	ENIP: Connected Message; CIP Object: Generic, Service: Read Tag (Response:Success)	02/02/2021 20:43...

The SCADAfence OT Inspector helps maintain the integrity and availability of critical industrial processes by monitoring process values of PLCs, RTUs, and other field devices.

- Support in main industry protocols: Siemens-S7, EtherNet/IP-CIP, Modbus and Bacnet
- Enhanced visibility into the ENIP/CIP protocols where we determine and display the internal port structure and configuration of assets in the ENIP\CIP protocol.

- Supports the import of tag mapping files (from Engineering/HMI software) for variables of the Siemens S7 protocol.
- Detects and alerts upon packets that are not according to the BACnet protocol structure. Our system detects malformed packets based on non-standard opcodes, invalid values or packet length mismatch. Additionally, we can detect DoS trials, fuzzing, misconfigurations that endanger processes.
- Users can define thresholds and mark important data points and set up alerts on single data points



In the next 2 pages, you can see how the CIP Value Level Visibility and Value Level Data Point Views are displayed in the SCADAfence Platform

9.E.2.2 - Traffic Analyzer - OT Inspector:
CIP Value Level visibility

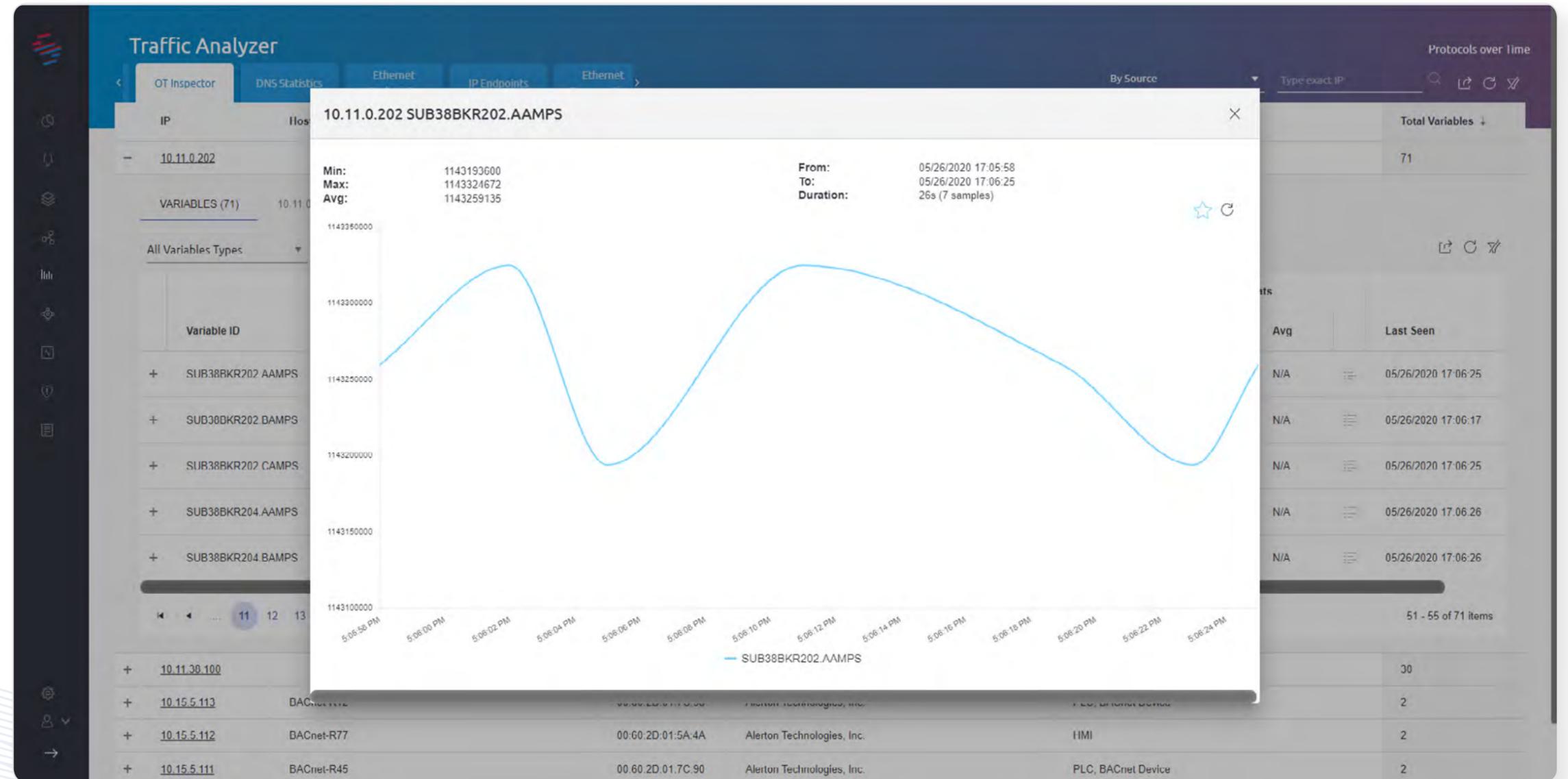
The screenshot displays the Traffic Analyzer interface with the OT Inspector tab selected. The main view shows details for IP 10.11.0.202, including its MAC address (F4:54:33:AD:39:7A), Vendor (Rockwell Automation), and Device type (PLC). Below this, a table lists 71 variables for this IP. The table columns include Variable ID, Device ID, Alias, Alert Mode, Last 500 Values (Min, Max, Avg), Last 5 Days Stats (Min, Max, Avg), and Last Seen. The first five variables shown are:

Variable ID	Device ID	Alias	Alert Mode	Last 500 Values			Last 5 Days Stats			Last Seen
				Min	Max	Avg	Min	Max	Avg	
+ SUB38BKR202.AAMPS			Off	1143193600	1143324672	1143259135	N/A	N/A	N/A	05/26/2020 17:06:25
+ SUB38BKR202.BAMPS			Off	1143324672	1143390208	1143357440	N/A	N/A	N/A	05/26/2020 17:06:17
+ SUB38BKR202.CAMPS			Off	1143259136	1143521280	1143399570	N/A	N/A	N/A	05/26/2020 17:06:25
+ SUB38BKR204.AAMPS			Off	1134985216	1135509504	1135247358	N/A	N/A	N/A	05/26/2020 17:06:26
+ SUB38BKR204.BAMPS			Off	1134985216	1135247360	1135097562	N/A	N/A	N/A	05/26/2020 17:06:26

Below the variable list, a summary table shows other IP addresses and their associated devices:

IP	Hostname	MAC	Vendor	Device types	Total Variables
+ 10.11.38.100		00:20:85:F1:5A:71	Eaton Corporation	PLC	30
+ 10.15.5.113	BACnet-R12	00:60:2D:01:7C:90	Alerton Technologies, Inc.	PLC, BACnet Device	2
+ 10.15.5.112	BACnet-R77	00:60:2D:01:5A:4A	Alerton Technologies, Inc.	HMI	2
+ 10.15.5.111	BACnet-R45	00:60:2D:01:7C:90	Alerton Technologies, Inc.	PLC, BACnet Device	2

9.E.2.3 - Traffic Analyzer - OT Inspector:
CIP Value Level data point view



 **Attack method:**

Adversaries change the operating mode of a controller to gain additional access to engineering functions such as Program Download.

 **Tactic:**

Evasion (TA0103)

 **Technique:**

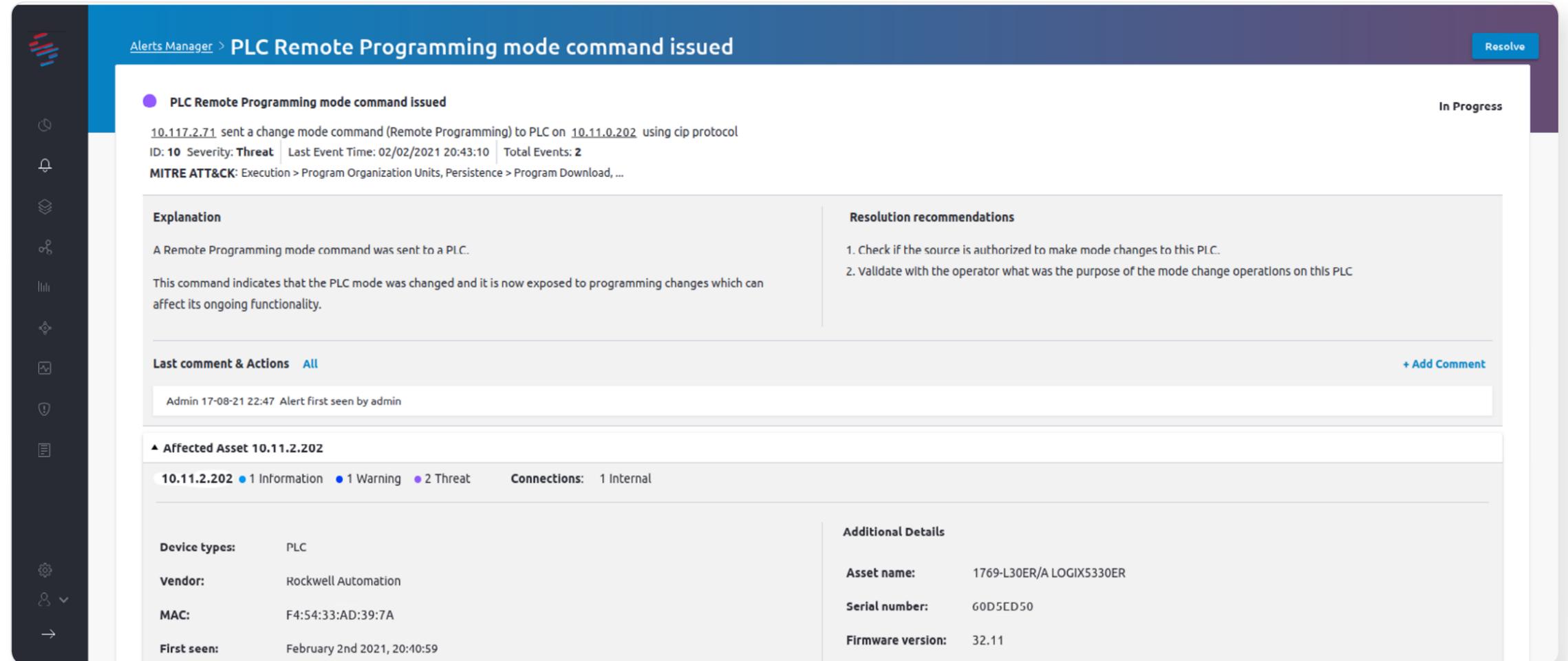
Change Operating Mode (T0858)

 **Criteria:**

Evidence of the safety PLC operating mode being switched to Program Mode following adversary CIP request to instance 0x01 of class 0x8E using service 0x07.

22.A.2 - Alerts Manager:

PLC Remote Programming Mode alert



The screenshot displays the Alerts Manager interface for a specific alert. The alert title is "PLC Remote Programming mode command issued" and its status is "In Progress". The alert details include the source IP (10.117.2.71), the target IP (10.11.0.202), the protocol used (CIP), and the severity (Threat). It also lists the last event time, total events, and the associated MITRE ATT&CK framework categories. The interface is divided into sections for Explanation, Resolution recommendations, Last comment & Actions, Affected Asset, and Additional Details.

Alerts Manager > PLC Remote Programming mode command issued Resolve

PLC Remote Programming mode command issued In Progress

10.117.2.71 sent a change mode command (Remote Programming) to PLC on 10.11.0.202 using cip protocol
ID: 10 Severity: Threat Last Event Time: 02/02/2021 20:43:10 Total Events: 2
MITRE ATT&CK: Execution > Program Organization Units, Persistence > Program Download, ...

Explanation
A Remote Programming mode command was sent to a PLC.
This command indicates that the PLC mode was changed and it is now exposed to programming changes which can affect its ongoing functionality.

Resolution recommendations

1. Check if the source is authorized to make mode changes to this PLC.
2. Validate with the operator what was the purpose of the mode change operations on this PLC.

Last comment & Actions All + Add Comment

Admin 17-08-21 22:47 Alert first seen by admin

Affected Asset 10.11.2.202

10.11.2.202 1 Information 1 Warning 2 Threat **Connections:** 1 Internal

Device types:	PLC	Additional Details	
Vendor:	Rockwell Automation	Asset name:	1769-L30ER/A LOGIX5330ER
MAC:	F4:54:33:AD:39:7A	Serial number:	60D5ED50
First seen:	February 2nd 2021, 20:40:59	Firmware version:	32.11

 **Attack method:**

Adversaries perform a program download to transfer a user program to a controller.

 **Tactic:**

Lateral Movement (TA0109)

 **Technique:**

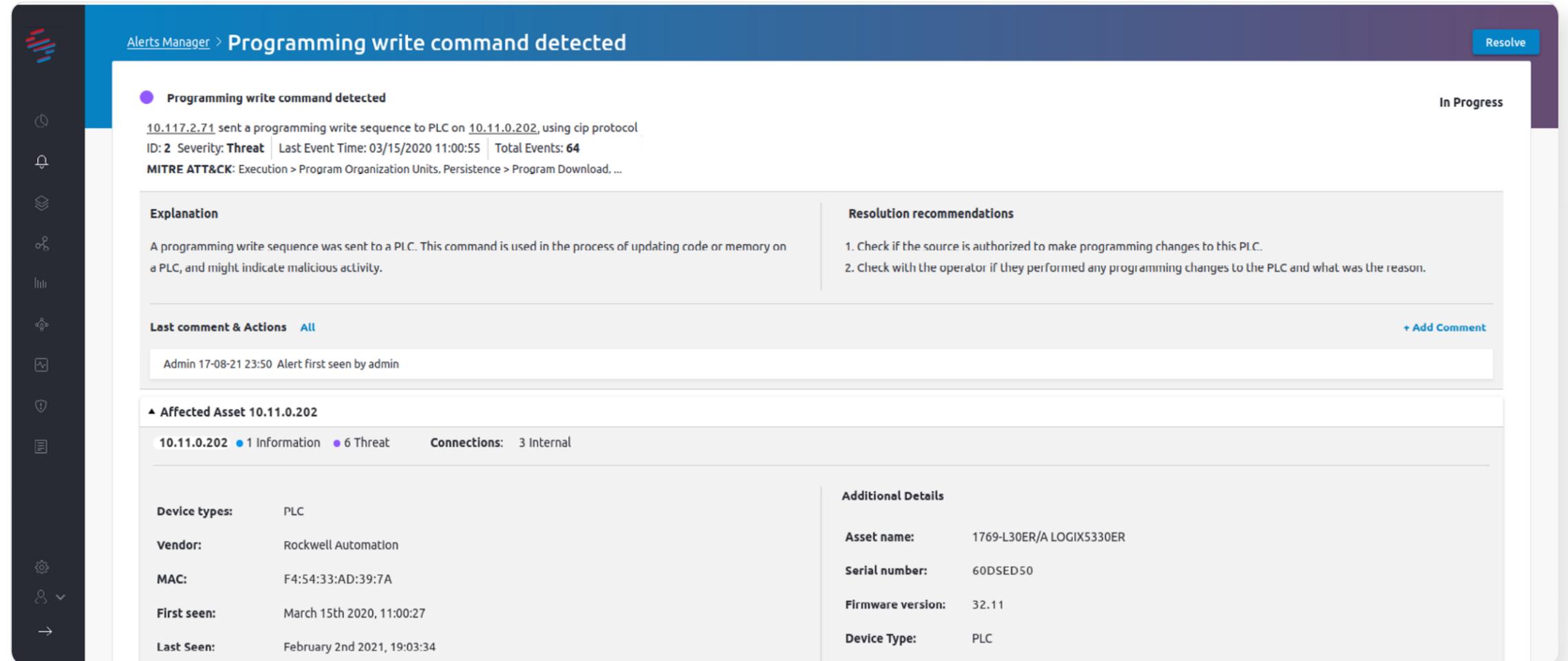
Program Download (T0843)

 **Criteria:**

Evidence of an adversary initiated online edit action on the safety PLC, requested from the safety machine.

20.B.3 - Alerts Manager:

PLC Program Download alert



The screenshot displays the Alerts Manager interface for a 'Programming write command detected' alert. The alert is currently in an 'In Progress' state. The main content area provides the following details:

- Alert Title:** Programming write command detected
- Description:** 10.117.2.71 sent a programming write sequence to PLC on 10.11.0.202, using cip protocol
- ID:** 2 | **Severity:** Threat | **Last Event Time:** 03/15/2020 11:00:55 | **Total Events:** 64
- MITRE ATT&CK:** Execution > Program Organization Units, Persistence > Program Download, ...

The interface is divided into several sections:

- Explanation:** A programming write sequence was sent to a PLC. This command is used in the process of updating code or memory on a PLC, and might indicate malicious activity.
- Resolution recommendations:**
 1. Check if the source is authorized to make programming changes to this PLC.
 2. Check with the operator if they performed any programming changes to the PLC and what was the reason.
- Last comment & Actions:** All (with an '+ Add Comment' link). A comment from 'Admin' dated 17-08-21 23:50 states 'Alert first seen by admin'.
- Affected Asset 10.11.0.202:** Shows 1 Information event and 6 Threat events. It has 3 Internal connections.
- Device Details:**

Device types:	PLC
Vendor:	Rockwell Automation
MAC:	F4:54:33:AD:39:7A
First seen:	March 15th 2020, 11:00:27
Last Seen:	February 2nd 2021, 19:03:34
- Additional Details:**

Asset name:	1769-L30ER/A LOGIX5330ER
Serial number:	60DSED50
Firmware version:	32.11
Device Type:	PLC

Attack method:

Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:

Execution (TA0104)

Technique:

Execution through API (T0871)

Criteria:

Evidence of an adversary initiated read/write action of the "CC" tag using the 0x4C/0x4D CIP service.

24.C.2 - Traffic Analyzer - Industrial Protocols:

CIP Read/Write Tags commands visibility

The screenshot shows the Traffic Analyzer interface with the 'Industrial Protocols' tab selected. The main table displays a list of conversations with columns for Conversation ID, Source IP, Src Hostname, Dest. IP, Dest Hostname, and Protocol. Below this, a detailed view shows command descriptions and their last seen timestamps.

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostname	Protocol
+ 124	192.168.0.45		192.168.0.160		CIP
+ 69	192.168.1.19		192.168.1.160		CIP
+ 57	192.168.0.20		192.168.0.160		CIP
+ 36	192.168.0.47		192.168.1.198		CIP
+ 31	192.168.1.19		192.168.1.199		CIP
+ 28	192.168.0.160		192.168.0.19		CIP
- 23	10.11.0.202		10.117.2.71		CIP

# Co...	Command description	Last Seen
6	ENIP: Connected Message; CIP Object: Generic, Service: Write Tag Fragmented (Response:Success)	02/02/2021 20:41...
2	ENIP: Connected Message; CIP Object: Generic, Service: Read Tag (Response:Partial transfer)	02/02/2021 20:43...
7	ENIP: Connected Message; CIP Object: Generic, Service: Read Tag (Response:Success)	02/02/2021 20:43...

Attack method:

Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:

Execution (TA0104)

Technique:

Execution through API (T0871)

Criteria:

Evidence of abuse of a CIP handshake between the engineering-station and control PLC resulting in an adversary privilege escalation (handshake sequence consisted of a service 0x4B class 0x64 initiation request and 0x4C class 0x64 challenge response).

The screenshot shows the 'Traffic Analyzer' interface with the 'Industrial Protocols' tab selected. It displays a table of network conversations and a detailed view of CIP handshake commands.

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostname	Protocol
124	10.117.2.71		10.11.0.202		CIP

# Co...	Command description	Last Seen
4	ENIP: Connected Message; CIP Object: Class [0x64], Service: Custom Service [0x4B] (Request)	04/12/2020 19:28...
4	ENIP: Connected Message; CIP Object: Class [0x64], Service: Custom Service [0x4C] (Request)	04/12/2020 19:28...
31	ENIP: Connected Message; CIP Object: Class [0x64], Service: Get Attribute List (Request)	04/12/2020 19:28...
2	ENIP: Connected Message; CIP Object: Class [0x64], Service: Set Attribute List (Request)	04/12/2020 19:30...

69	192.160.1.19	192.160.1.160	CIP
52	192.168.0.20	192.168.0.160	CIP
36	192.168.1.47	192.168.1.198	CIP
31	192.168.1.45	192.168.1.199	CIP
28	192.168.0.160	192.168.0.19	CIP

25.E.2 - Traffic Analyzer - Industrial Protocols:

CIP handshake commands visibility

Possible additional signatures and useful data:

- 1) https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/TRITON_Appendix_A.pdf
- 2) https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/TRITON_Appendix_B.pdf
- 3) <https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN>
- 4) <https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html>

About SCADAfence:

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner “Cool Vendor” in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, visit our [website](#), check out our [blog](#), or follow us on [LinkedIn](#).