OPERATIONALIZING OT THREAT INTELLIGENCE

A Rockwell Automation ControlLogix Case Study

DRAGOS: Kimberly Graham
Jimmy Wylie
ROCKWELL AUTOMATION: Maggie Morganti

AGENDA

1. THE DRAGOS ECOSYSTEM
2. BACKGROUND - WHAT HAPPENED?
3. VULNERABILITY ANALYSIS
4. INTELLIGENCE SHARING PARTNERS
5. NEIGHBORHOOD KEEPER & OT WATCH
6. MITIGATIONS & TAKEAWAYS

DRAGOS

Safeguarding Civilization

The Most Effective OT Security Tech Platform
Visibility into OT assets, vulnerabilities, traffic, and threats to reduce OT risk.

A Community-Focused Mission
Skills, communications, & resources to strengthen the collective defense

Expert OT Intelligence & Service Resources
OT expert analysts, threat hunters, & responders to help you win the fight.

DRAGOS PLATFORM Use Cases

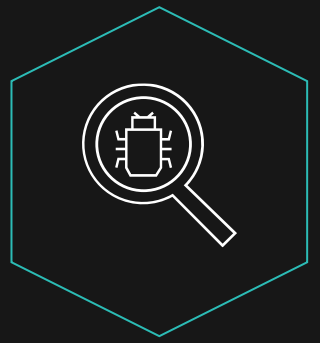
Comprehensive ICS/OT Cyber Security Technology

ASSET VISIBILITY

- Identify crown jewel assets
- Create asset inventory
- Evaluate unusual changes

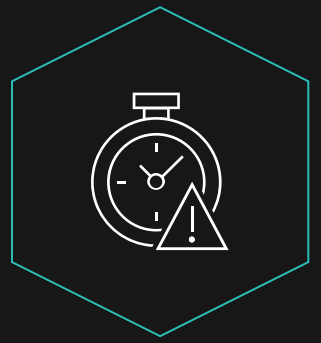
VULNERABILITY MANAGEMENT

- Simplify compliance
- Prioritize vulnerabilities
- Maximize remediation resources



THREAT DETECTION

- See unauthorized IT-OT traffic
- Analyze file downloads
- Detect adversary behaviors



INCIDENT INVESTIGATION

- Analyze changes & forensic records
- Efficiently manage response & recovery
- Leverage prescriptive playbooks

The DRAGOS PLATFORM Difference

OT Threat Intelligence & Expertise at Machine Speed and Scale

Research & Analysis

Threat groups & attack campaigns

Vulnerabilities, CVE enhancement, & alternative mitigation

Adversary research, IOC's, TTPs, threat behaviors

INTEGRATED

Applied In-field at Customers

Incident response plans & services

Threat hunting & vulnerability analysis

Architecture Assessments & Capability Maturity Assessments

DRAGOS PLATFORM KNOWLEDGE PACKS

Regular enhancements through content updates including:

Detections - for new or evolving threats

- Activity Groups (e.g. XENOTIME, KOSTOVITE, DYMALLOY)
- Ransomware and malware (e.g. Lockbit, Doppelpaymer, RYUK)
- Targeted exploits (e.g. Log4j, CRASHOVERRIDE, TeamViewer)

Characterizations - to expand protocol dissection

- ICS protocols (e.g. DNP3,FTE, Modbus, OPC-UA)
- Equipment (e.g. Oasys, DeltaV, Cimplicity, Experion, Triconex)
- Vendors (e.g. Emerson, Honeywell, Rockwell, Siemens, Yokogawa)

Playbooks - to guide cyber analysts and responders

- Protocol related (e.g. RDP RCE, IEC 104 violation)
- Behavior related (e.g. Authentication Success/Failure, scan activity)
- Hunt related (e.g. SolarWinds SUNBURST, Rockwell CIP, DeltaV)

OT Watch – Continuous Threat Hunting

Accelerate OT Security Operationalization

OUR TEAM IS YOUR TEAM

INDUSTRIAL THREAT HUNTING

DRAGOS PLATFORM

VISIBILITY	DETECTION	RESPONSE
OF YOUR OT ENVIRONMENT	PROACTIVE THREAT HUNTING	ALERT TRIAGE & REPORTING

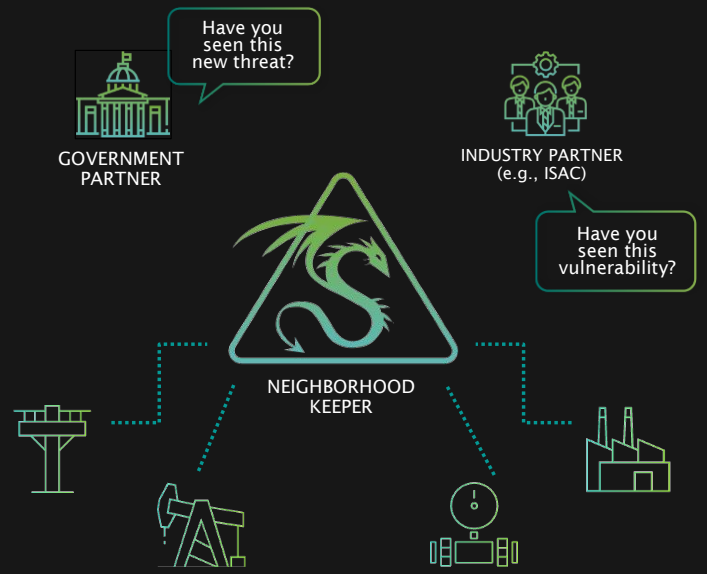
COMMUNITY DEFENSE - Neighborhood Keeper

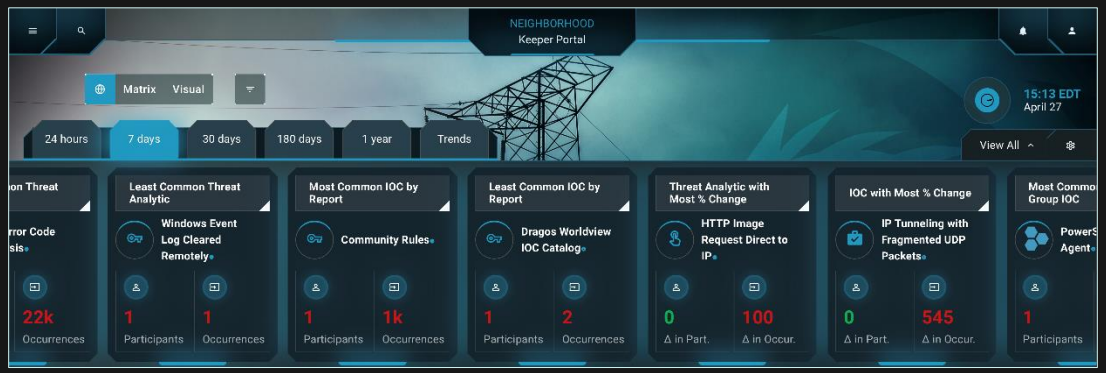
Community Wide Visibility & Collective Defense For OT Threats

A free, opt-in program for Dragos Platform customers

Collective ICS threat, asset, & vulnerability intelligence across Dragos Platform

Industry, regional, & system-wide view shared between asset owners & community defenders



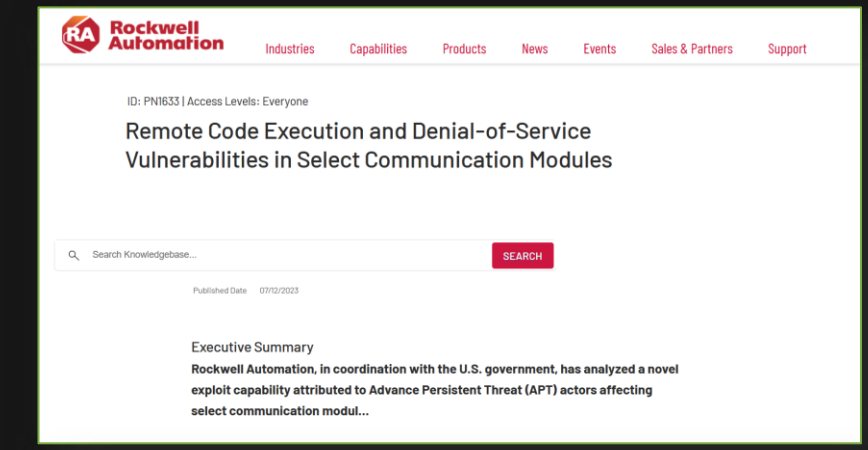


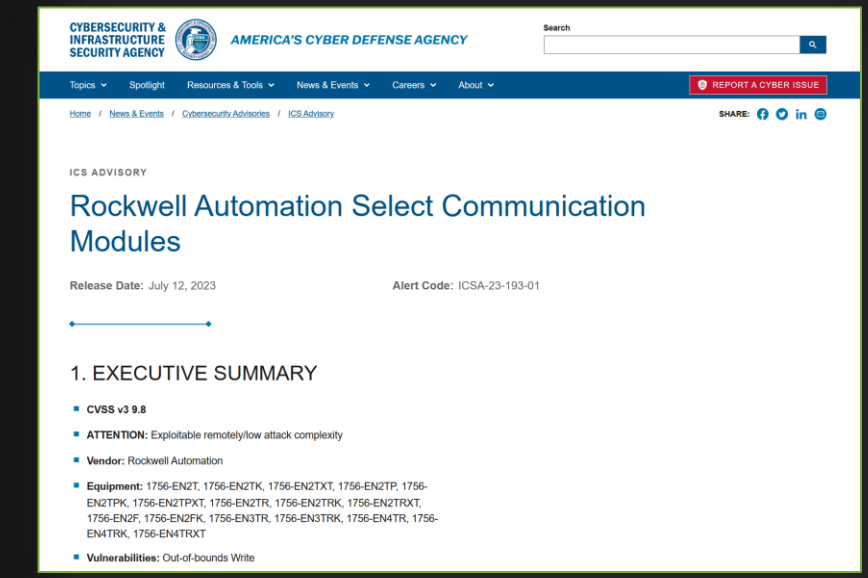
BACKGROUND

Rockwell Automation, in coordination with the U.S. government, released two vulnerabilities on 12 July 2023:

- CVE-2023-3595: RCE with persistence affecting 1756-EN2* and 1756-EN3* models of ControlLogix ENIP comms modules
- CVE-2023-3596: DOS affecting 1756 EN4* models of ControlLogix ENIP comms modules

These vulnerabilities are important because the USG identified a state actor developing exploits against these unknown vulnerabilities for use in attacks; this collective response was PRIOR to the attack leading to a massive success.





WHY ARE THESE VULNERABILITIES IMPORTANT?

The impacts are serious:

- Denial/Loss of View
- Manipulation/Denial of Control
- Theft of Operational Information
- Loss of Productivity and Revenue

They are associated with an unknown APT group.

No evidence of exploitation in the wild.

IMPACTED EN2* & EN3* DEVICES

EN2* and EN3* modules have three firmware lines

5.00X	5.028	10.X and 11.X
unsigned firmware	once installed only signed firmware may be installed	firmware signature verification
5.009 is patched	5.029 is patched	11.004 is patched
5.008 and earlier are vulnerable	5.028 is vulnerable	
	If 5.028 is installed, you cannot install 5.009	

VULNERABLE EN4 DEVICES

- Update to version 5.002
- 5.001and earlier are vulnerable to CVE-2023-3596 (DOS Vuln)

References:

- Rockwell Product Finder
- Product Notification on Rockwell Automation’s KnowledgeBase
- Dragos WorldView Report: AA-2023-20.1
- CISA Release: ICSA-23-193-01

COLLABORATIVE WORK & COLLECTIVE DEFENSE

BIG CROSS-INDUSTRY LIFT

- US Government
- Rockwell Automation
- Dragos
- Other security vendors

COLLECTIVELY:

- Analyze vulnerabilities
- Test/Develop signatures
- Look for potential activity using respective telemetry

SECURITY VENDOR COLLABORATION

First time for this level of collaboration between: security vendors, an OEM, and government agencies.

Led to rapid improvement of industry-wide detections and rules.

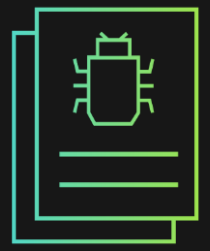
Perception of Security Vendors

How We Want To Work

BEHIND THE SCENES AT DRAGOS

Analyze vulnerabilities

Intel Research: device analysis, firmware reverse engineering, pcap analysis



Test/develop signatures

In-house testing, insights from Neighborhood Keeper & OT Watch, finding new detection methods

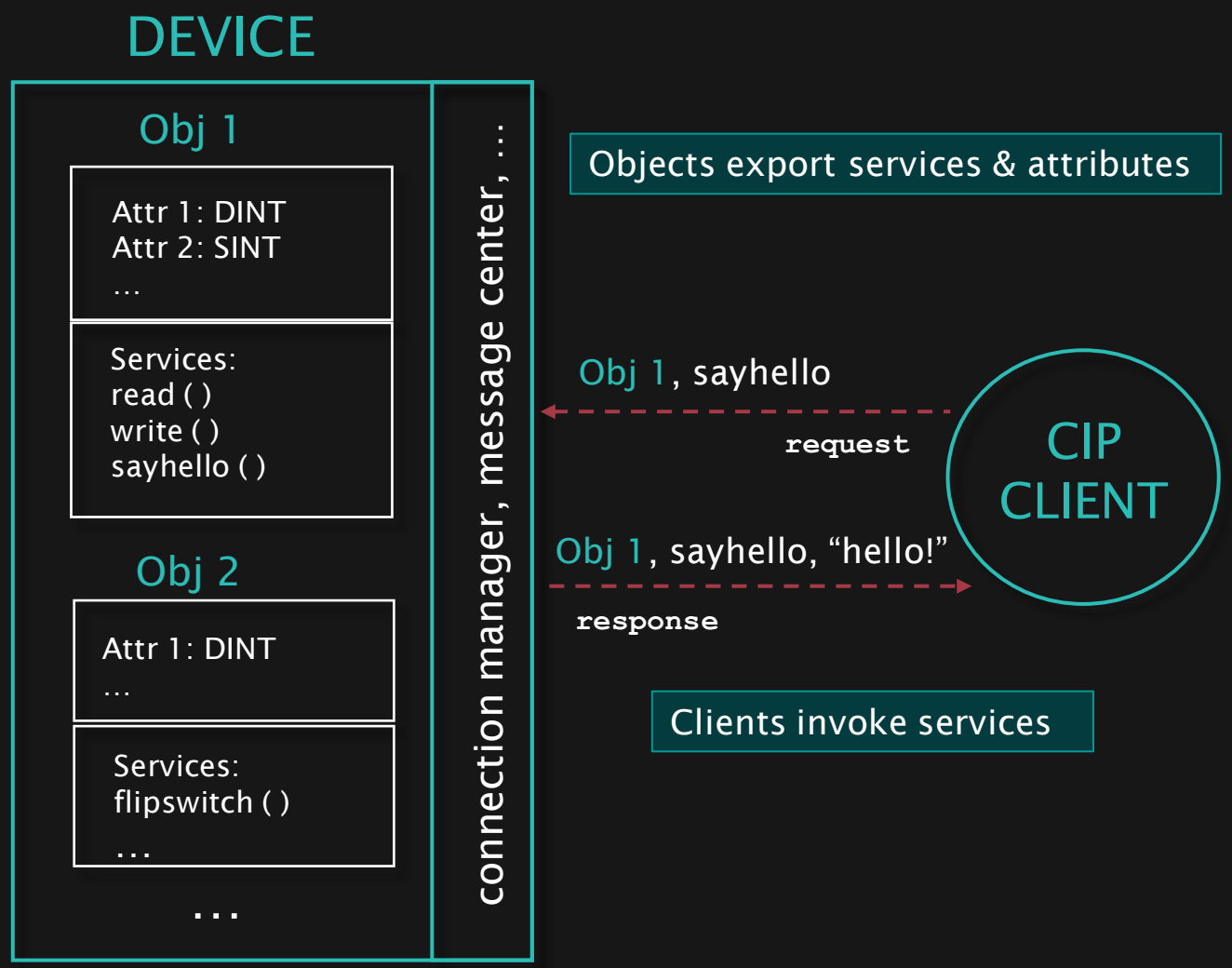
Look for potential activity

Use exclusive telemetry, deploy to Neighborhood Keeper, OT Watch, and the Dragos Platform

Findings are shared to benefit all Dragos customers and wider industry via collaboration

UNDERSTANDING CIP

- Common Industrial Protocol (CIP) is used to monitor and administers industrial controllers
- CIP is commonly seen in Rockwell Automation devices but is used by many industrial vendors
- The exploitation of both vulnerabilities targets the CIP
- These vulnerabilities affect Ethernet/IP devices with TCP/44818 and UDP/2222 implementation



CIP OBJECT IDS

The CIP protocol defines standard objects

- Identity, Connection Manager, AC/DC drives

Each object has standard attributes and services

- Identity Attributes: Vendor ID, Device Type, etc.
- Identity Services: Get_Attribute_All, Reset

Each standard object has a pre-defined ID

- 0x01, 0x06, 0x2A

Vendors can implement their own objects

- Example: 0x300-0x4FF are for Vendor Specific Objects

Conceptually, a device is a collection of standard (general use, application) & vendor specific objects.

FINDING - VULNERABLE CIP OBJECTS

The devices affected by the disclosure contain vulnerable CIP object implementations.

Exploitation occurs via maliciously crafted parameters to services exposed by those vulnerable objects.

- It's in the realm of Web API exploit/vulnerabilities. Pass weird input, get weird behavior.

For CVE-2023-3595: remote code execution and arbitrary access to firmware memory.

- Any firmware code or data can be potentially manipulated or overwritten by exploitation of this vulnerability.

CVE-2023-3596: Denial of Service on the comms module

- Possible loss of control scenario/loss of view scenario

CVE-2023-3595 – SIMILARITIES TO TRISIS 0-DAY

Comparison for context, these vulns are not related to TRISIS

Both allow for arbitrary firmware memory manipulation

- TRISIS the network command handler
- These vulns target a communication module responsible for handling network commands.
- (Targeting the entryway)

Repercussions of exploitation are similar

- Both are essentially all access exploits

Incident response is possibly affected

- Interfaces exposed to a user to collect incident response or forensics information could be intercepted

MITRE ATT&CK SUMMARY

CVE-2023-3595

- Loss of View
- Denial of View
- Manipulation of View
- Manipulation of Control
- Denial of Control
- Theft of Operational Information
- Loss of Productivity and Revenue

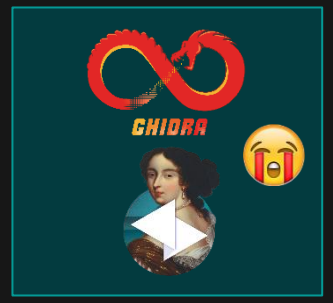
CVE-2023-3596

- Loss of View
- Denial of View
- Denial of Control
- Loss of Productivity and Revenue

NEIGHBORHOOD KEEPER & OT WATCH

PCAP ANALYSIS

FIRMWARE RE



informs

informs

informs

SIGNATURE/
ANALYTIC
CREATION

BYPASS
DISCOVERY

TEST
IN HOUSE

**DEPLOY TO
Neighborhood
Keeper &
OT Watch**

NEIGHBORHOOD KEEPER & OT WATCH RESULTS

- ✓ Some rule ideas we discarded as too FP prone and others we just needed to tune and fix.
- ✓ 9 hits in OTW and 7 in NK across water, food and bev, and manufacturing.
  - Not really what we were expecting
    "wait why are we seeing a beer brewery?"
  - EWS -> PanelView Terminal (HMI) comms.
    Rockwell Automation (Yes!), Equipment (No!).

In each of these situations, we passed information back to Rockwell Automation and the larger group.

NEIGHBORHOOD KEEPER & OT WATCH – ANY ACTIVITY?

We found no evidence that these vulnerabilities were being actively exploited.

What if we had?

- This would be a different conversation.
- Notify Rockwell, USG partners, and get all the relevant parties together.
- For Neighborhood Keeper, use Trusted Insight Response to engage the participant where anonymized activity was observed.
- For OT Watch, we would contact the customer directly.

MITIGATIONS – An Overview

1. Update firmware for affected devices as operations allow.
2. Backup devices to allow for reversion to a clean copy of firmware or working project
3. Restrict access to TCP/44818 and UPD/2222
4. Block all traffic to CIP-enabled devices from outside the ICS/OT network, and segment your networks
5. Disable unused CIP objects on comms modules like unused Socket Objects.
6. Monitor for CIP traffic from unknown/untrusted sources

TAKEAWAYS FOR DRAGOS CUSTOMERS

1

KP-2023-004 has detections for exploitation of vulnerabilities in AA-2023-20.

WorldView

2

Dragos Platform customers have access to a dashboard to assist in identifying vulnerable devices.

Platform

3

Your account team is here to assist with any deployment questions specific to your environment.

Services

QUESTIONS AND ANSWERS

THANK YOU