RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-W08**

CHERNOVITE and PIPEDREAM: Understanding the Latest Evolution of ICS Malware

Ben Miller

Dragos
@electricfork

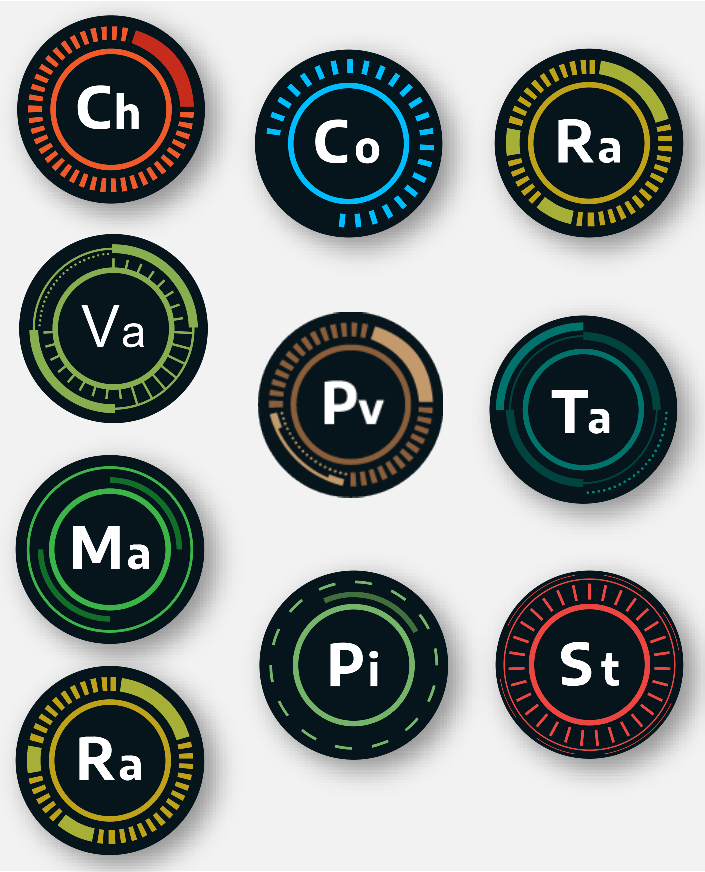
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

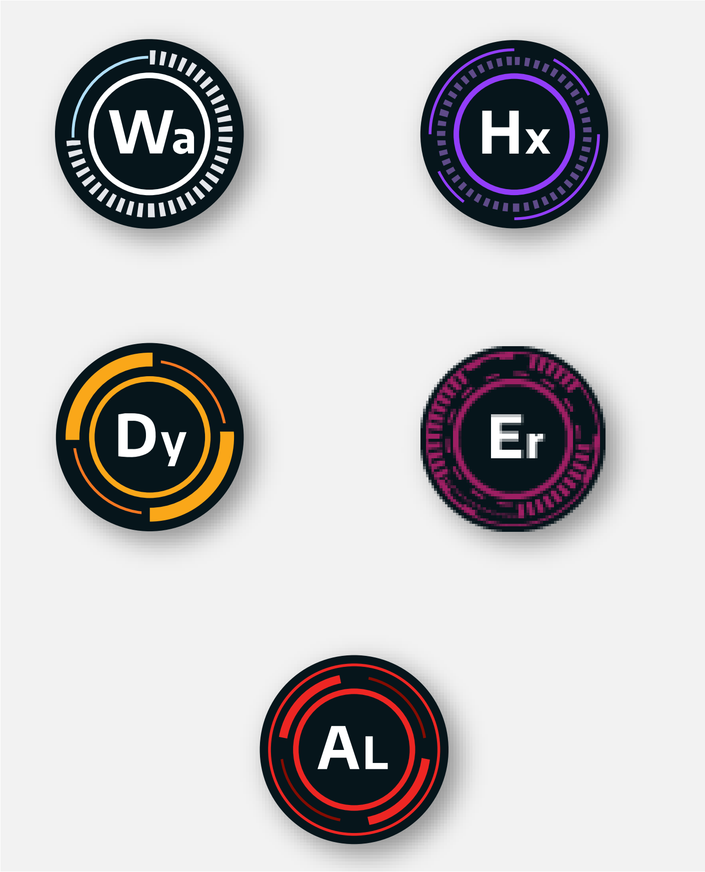
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The ICS Cyber Threat Landscape

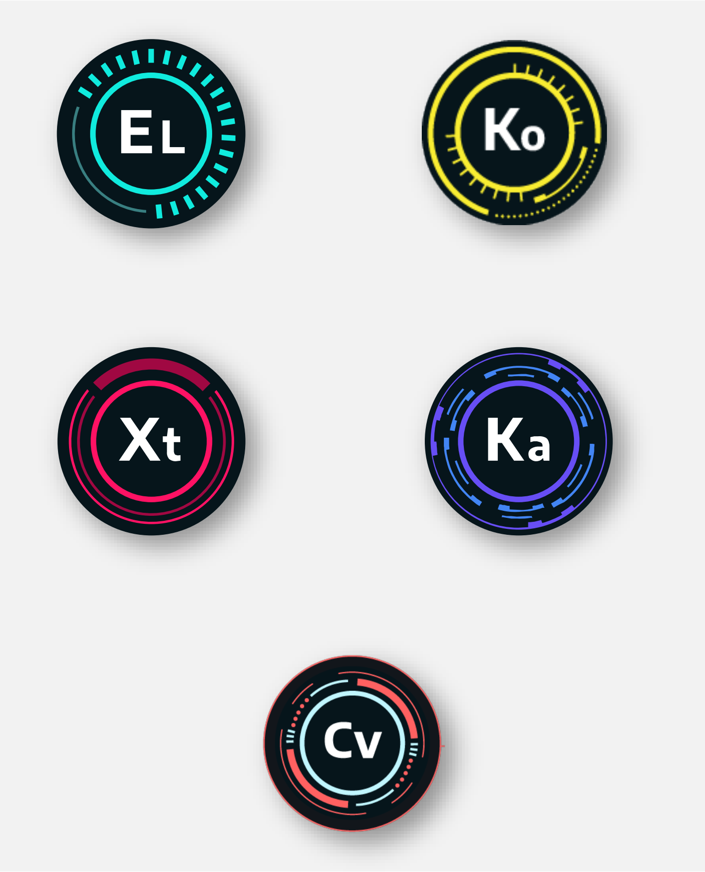
ICS Curious (ICS CKC Stage 1)



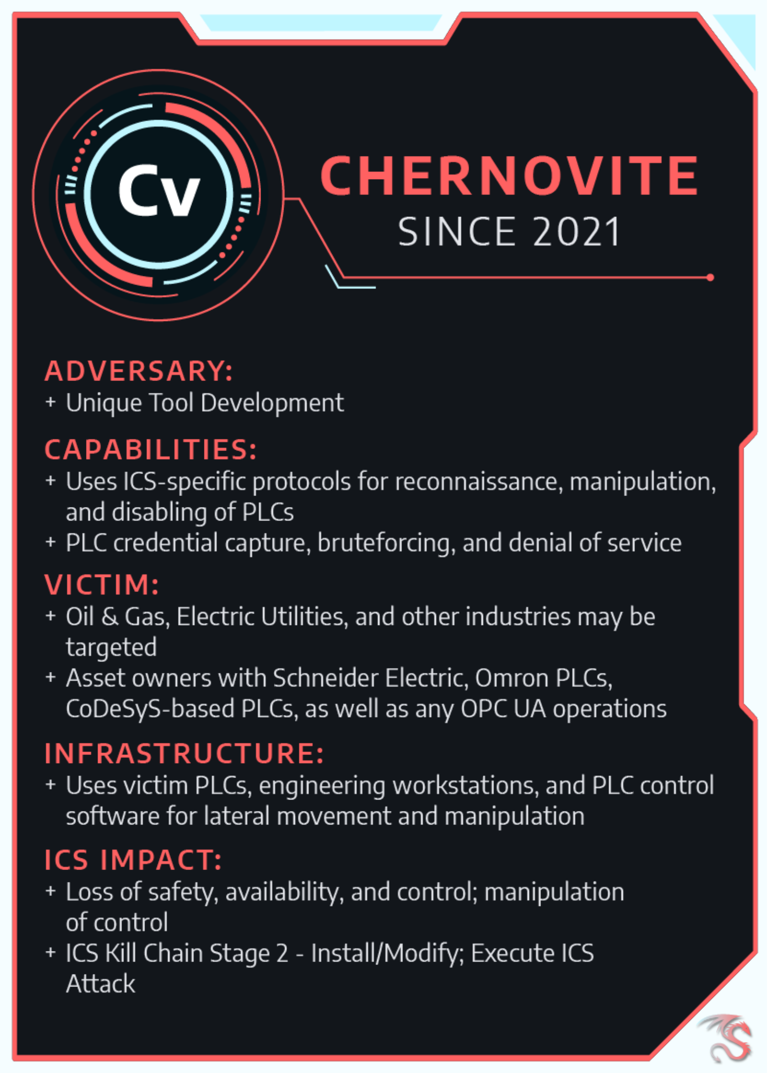
ICS Capable (ICS CKC Stage 2)



ICS ~~Clowns~~ (ICS CKC Stage 2 – Act)



Chernovite



CHERNOVITE
SINCE 2021

Cv

ADVERSARY:
- Unique Tool Development

CAPABILITIES:
- Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
- PLC credential capture, bruteforcing, and denial of service

VICTIM:
- Oil & Gas, Electric Utilities, and other industries may be targeted
- Asset owners with Schneider Electric, Omron PLCs, CoDeSyS-based PLCs, as well as any OPC UA operations

INFRASTRUCTURE:
- Uses victim PLCs, engineering workstations, and PLC control software for lateral movement and manipulation

ICS IMPACT:
- Loss of safety, availability, and control; manipulation of control
- ICS Kill Chain Stage 2 - Install/Modify; Execute ICS Attack

- Discovered in early 2022 by a partner
- Partner shared the insights with Dragos to help identify/analyze the malware PIPEDREAM
- CHERNOVITE is a threat group that has not yet employed their capability, PIPEDREAM, for its intended (disruptive/destructive) effects – their assessed intent is disruptive in nature
- CHERNOVITE's initial target set appears to be U.S. Liquid Natural Gas and key Electric Power sites
- CHERNOVITE's capability is in no way limited to those industries and is the most flexible ICS attack framework to date

Chernovite Victimology

- Target Environments – CHERNOVITE built a highly flexible attack framework; PIPEDREAM should be viewed as a collection of tools and not specific to the current target assets
- Target Assets –

Omron PLCs including:

- NX1P2
- NX-ECC
- NX-EIC202
- NX-SL3300
- NX-ECC203
- NJ501-1300
- S8VK
- R88D-1SN10F-ECT (Servo)

Schneider Electric PLCs including:

- TM251
- TM241
- TM221
- TM258
- TM238
- LMC058
- LMC078

Omron PLC Control Software including:

- CX-One
- CX-Supervisor
- NX-IO Configurator

- Vulnerabilities, Exposures, and Susceptibilities
  - CVE-2020-15368 – LAZYCARGO utilizes this CVE for arbitrary code execution.
  - CVE-2018-7823

LAZYCARGO

PROFILE

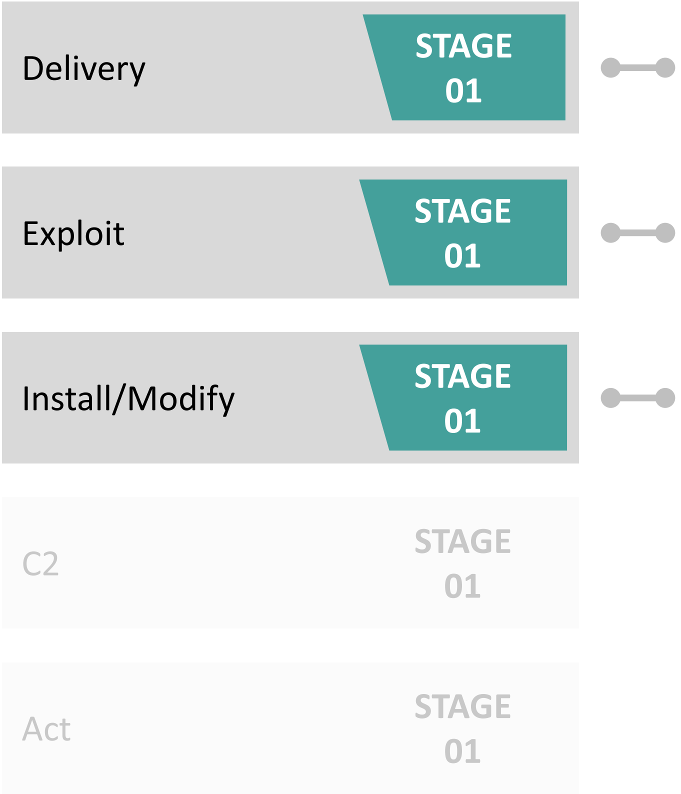
CVE-2020-15368
ASRock driver arbitrary code execution) exploit / dropper

FORMAT:
++ Compiled binary

TARGETS:
Microsoft Windows Devices

Works against all motherboard manufactures and VMs

KILLCHAIN ANALYSIS



Delivery
STAGE 01

Exploit
STAGE 01

Install/Modify
STAGE 01

C2
STAGE 01

Act
STAGE 01

CAPABILITIES

Drops and loads vulnerable ASRock driver on a victim machine (requires administrator privileges)

Identifies and overwrites the ASRock driver memory region containing its IOCTL handler function with shellcode

Reflectively loads unsigned driver specified by user as command line parameter

Restores ASRock IOCTL handler function

Windows

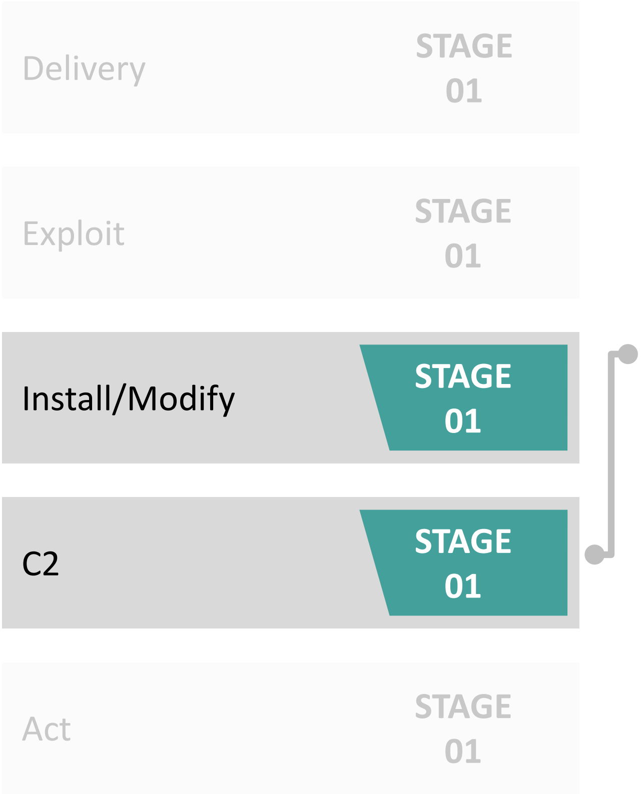
PROFILE

Microsoft Windows implant to facilitate remote interactive operations.

FORMAT:
C++ Compiled binary

TARGETS:
Microsoft Windows Devices

KILLCHAIN ANALYSIS


Delivery STAGE 01

Exploit STAGE 01

Install/Modify STAGE 01

C2 STAGE 01

Act STAGE 01

CAPABILITIES

Enumeration of victim infrastructure:

- Hardware and Operating System information
- Network connections, drives, shares
- Patch / HotFix status

Execution of commands from C2 server

Upload (exfiltration) and Download of files to victim

Filesystem modification (files, registry, etc.)

Anti-forensics (e.g. VM detection, anti-debugging)

MOUSEHOLE

PROFILE

Multiplatform toolkit to interact with OPC-UA servers.

FORMAT:
Python framework

TARGETS:
OPC-UA servers

KILLCHAIN ANALYSIS

Develop — STAGE 02

Test — STAGE 02

Deliver — STAGE 02

Install/Modify — STAGE 02

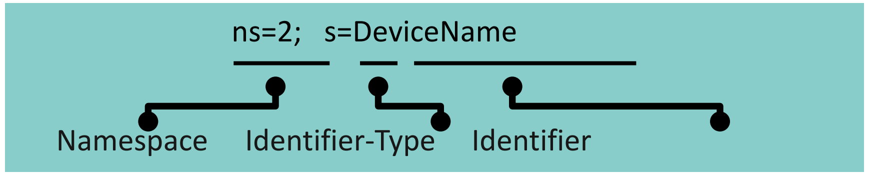
Execute ICS Attack — STAGE 02

CAPABILITIES

OPC-UA server identification / network enumeration

Dictionary / brute-force authentication attacks

OPC-UA server structure enumeration

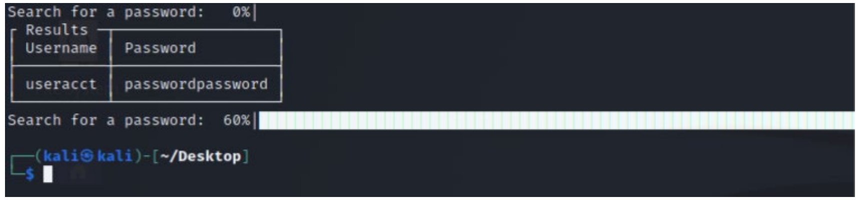

ns=2; s=DeviceName

Namespace

Identifier-Type

Identifier

Reading and Writing to OPC-nodes


```
Search for a password:   0%|
┌ Results ─────────────────────┐
│ Username  │ Password         │
│           │                  │
│ useracct  │ passwordpassword │
Search for a password:  60%|
┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

EVILSCHOLAR

Schneider Electric

PROFILE

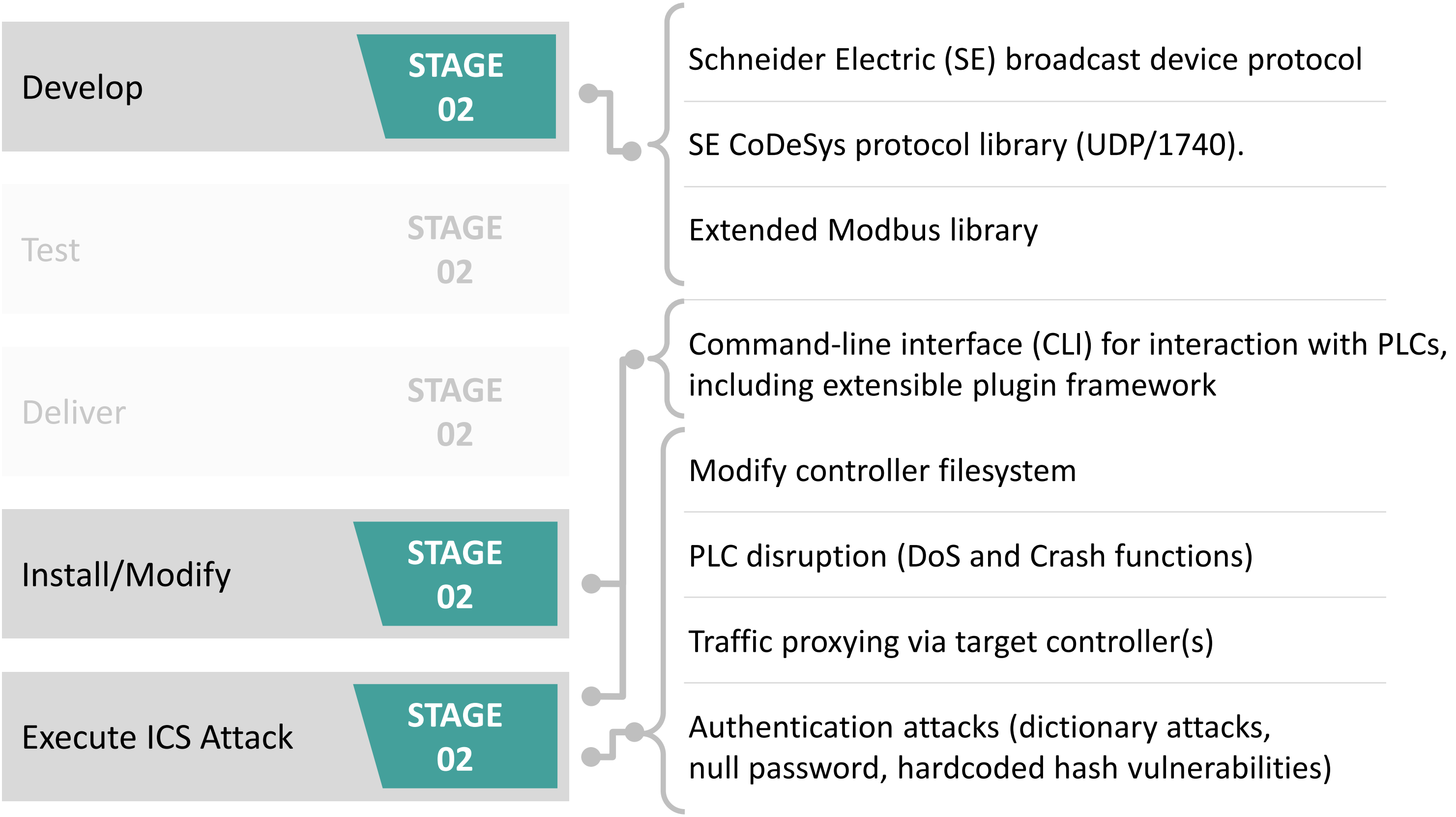
Framework to interact with Schneider Electric controllers via CoDeSys and Modbus libraries

FORMAT:
Python + Linux ELF Library

TARGETS:
Schneider Electric Controllers

KILLCHAIN ANALYSIS

CAPABILITIES



Develop — STAGE 02

Test — STAGE 02

Deliver — STAGE 02

Install/Modify — STAGE 02

Execute ICS Attack — STAGE 02

Schneider Electric (SE) broadcast device protocol

SE CoDeSys protocol library (UDP/1740).

Extended Modbus library

Command-line interface (CLI) for interaction with PLCs, including extensible plugin framework

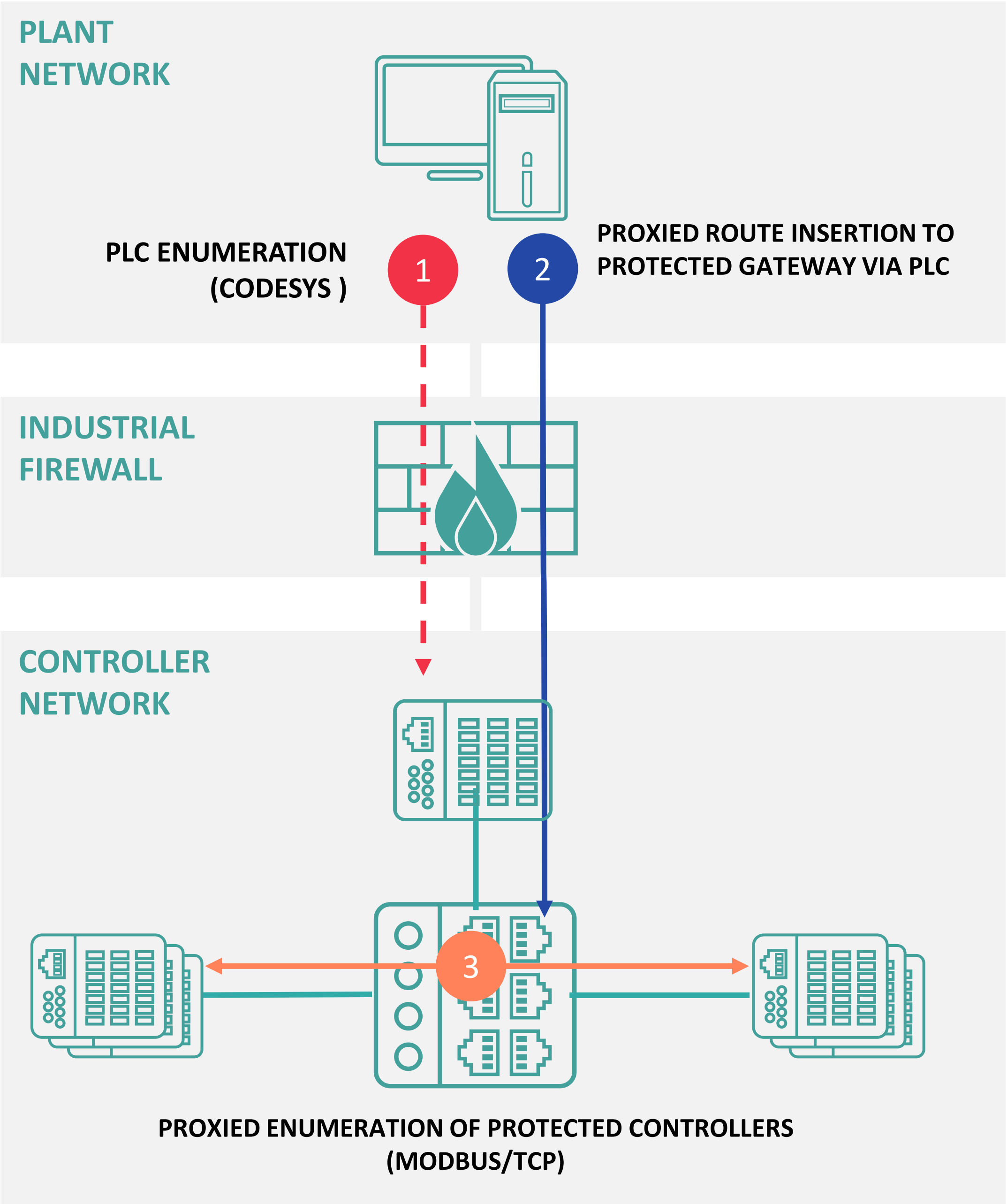
Modify controller filesystem

PLC disruption (DoS and Crash functions)

Traffic proxying via target controller(s)

Authentication attacks (dictionary attacks, null password, hardcoded hash vulnerabilities)

EVILSCHOLAR


PLANT NETWORK
PLC ENUMERATION (CODESYS)
1
2
PROXIED ROUTE INSERTION TO PROTECTED GATEWAY VIA PLC
INDUSTRIAL FIREWALL
CONTROLLER NETWORK
3
PROXIED ENUMERATION OF PROTECTED CONTROLLERS (MODBUS/TCP)

STEP 1

- EVILSCHOLAR CodeSys module used to identify accessible PLC(s) from compromised workstation.
- Password attack functionality leveraged to gain access to PLC(s).
- Configuration enumeration used to identify victim PLC's configured gateway in protected network.

STEP 2

- Route added to compromised workstation to enable proxied communication via exposed PLC:
- *$ ip route add **<gateway_ip>**/ 24 dev **<nic>** via **<plc_ip>***
- Allows adversary to route commands to controllers not otherwise exposed to the plant network.

STEP 3

- Using established proxied route, EVILSCHOLAR sends Modbus commands to protected controllers.
- Leverages pyModbus library to establish client communications.
- Enumerates devices responding to Modbus/TCP requests in the gateway's subnet and records for further action.

BADOMEN

OMRON

PROFILE

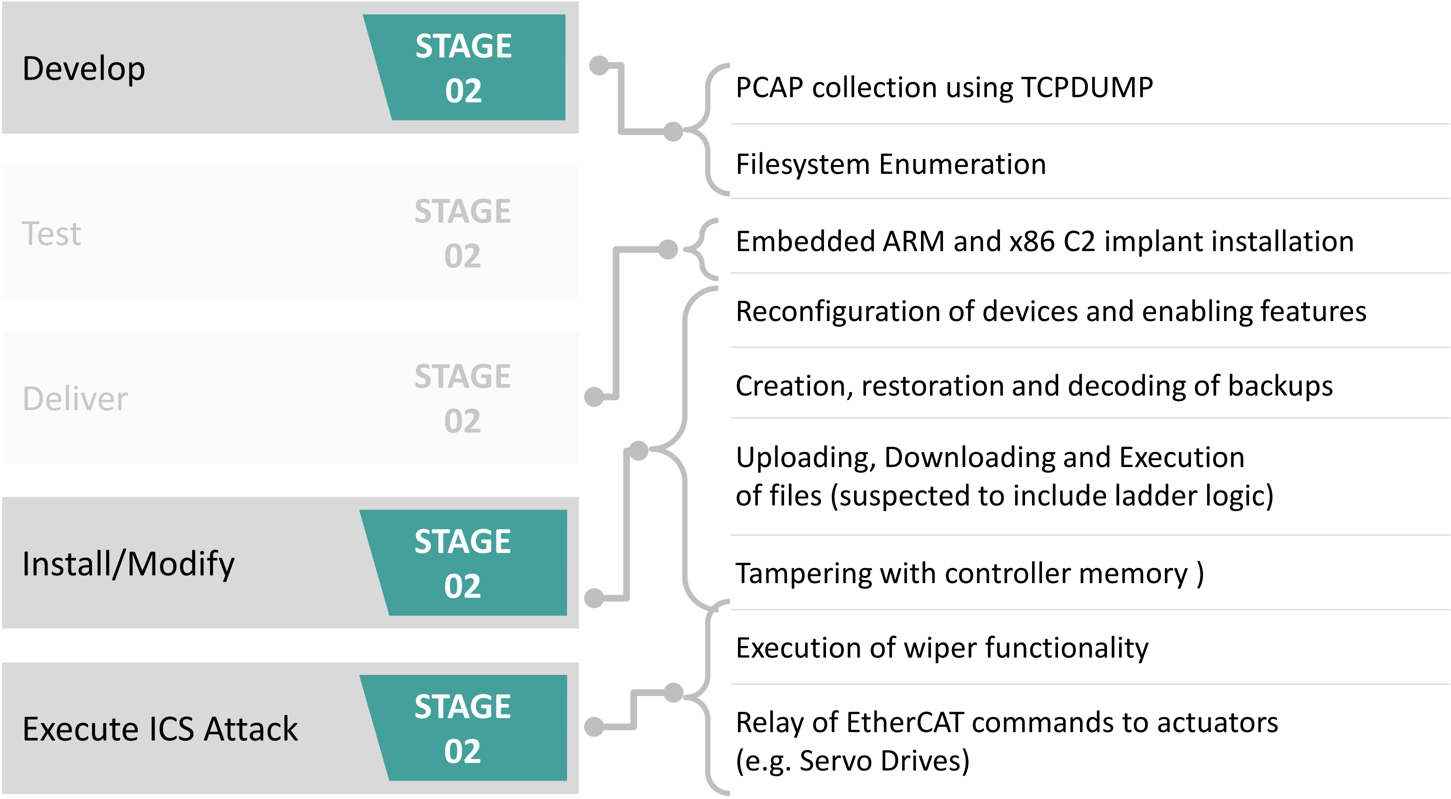
Framework to interact with Omron controllers via Omron HTTP API and FINS protocol

FORMAT:
Python framework

TARGETS:
Omron equipment

KILLCHAIN ANALYSIS

CAPABILITIES



Develop — STAGE 02

Test — STAGE 02

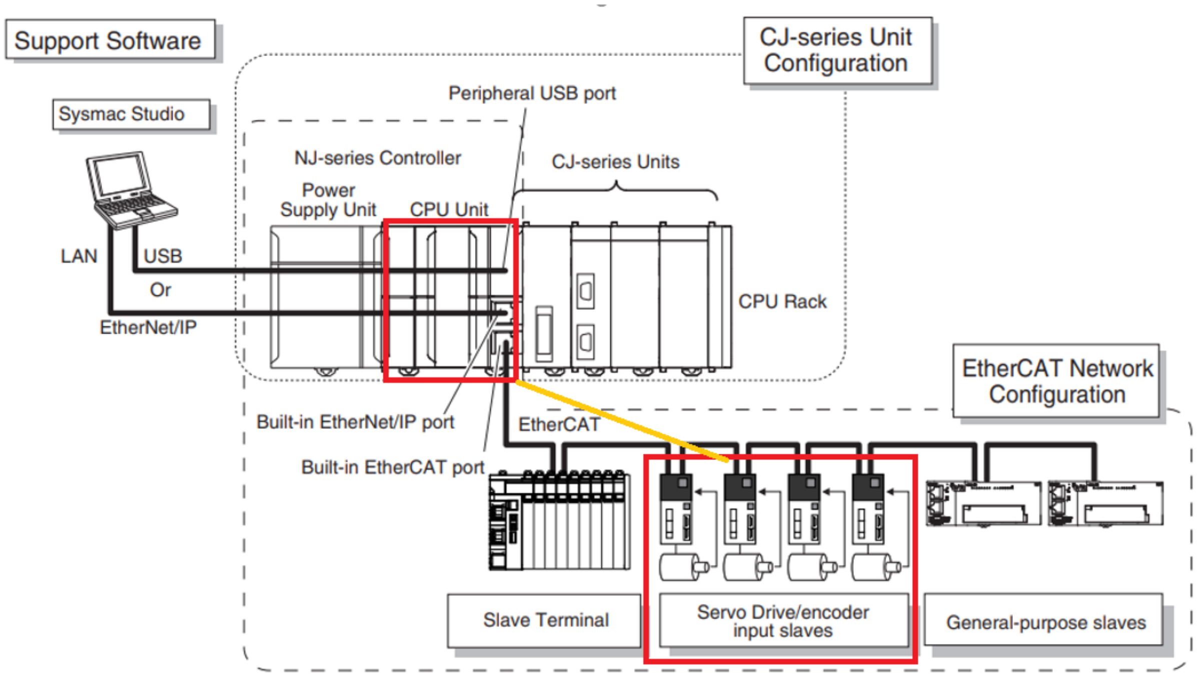
Deliver — STAGE 02

Install/Modify — STAGE 02

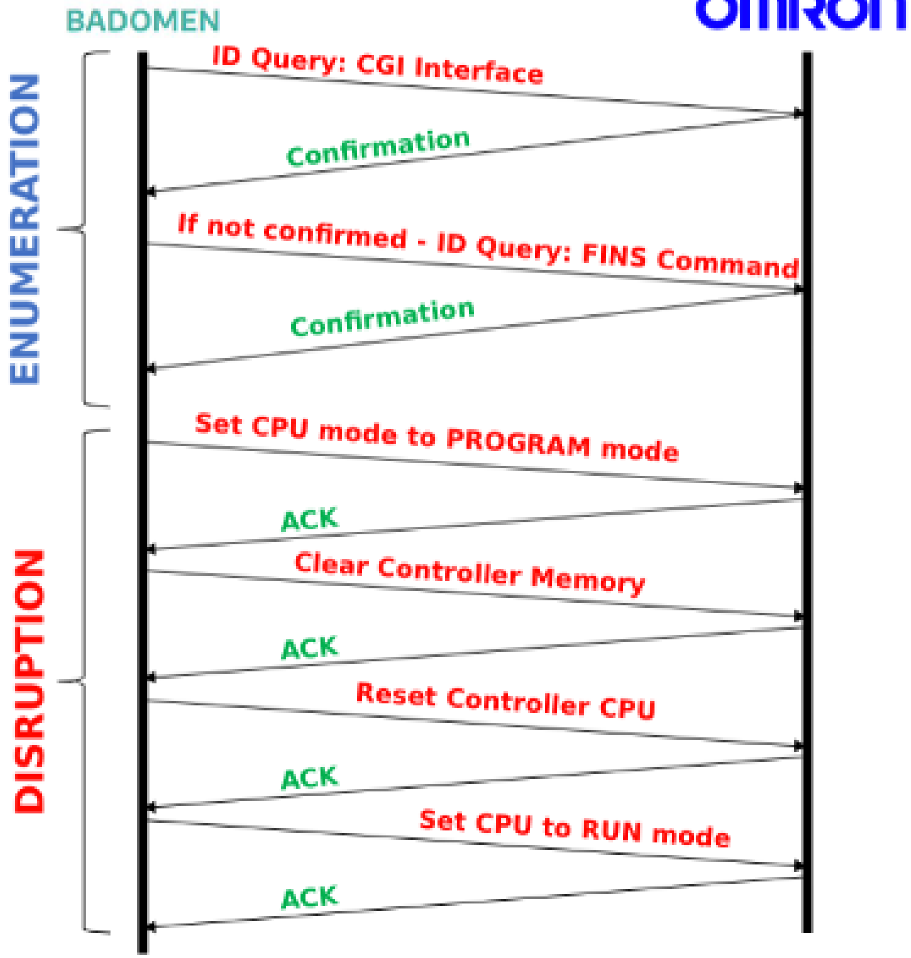
Execute ICS Attack — STAGE 02

- PCAP collection using TCPDUMP
- Filesystem Enumeration
- Embedded ARM and x86 C2 implant installation
- Reconfiguration of devices and enabling features
- Creation, restoration and decoding of backups
- Uploading, Downloading and Execution of files (suspected to include ladder logic)
- Tampering with controller memory)
- Execution of wiper functionality
- Relay of EtherCAT commands to actuators (e.g. Servo Drives)

BADOMEN



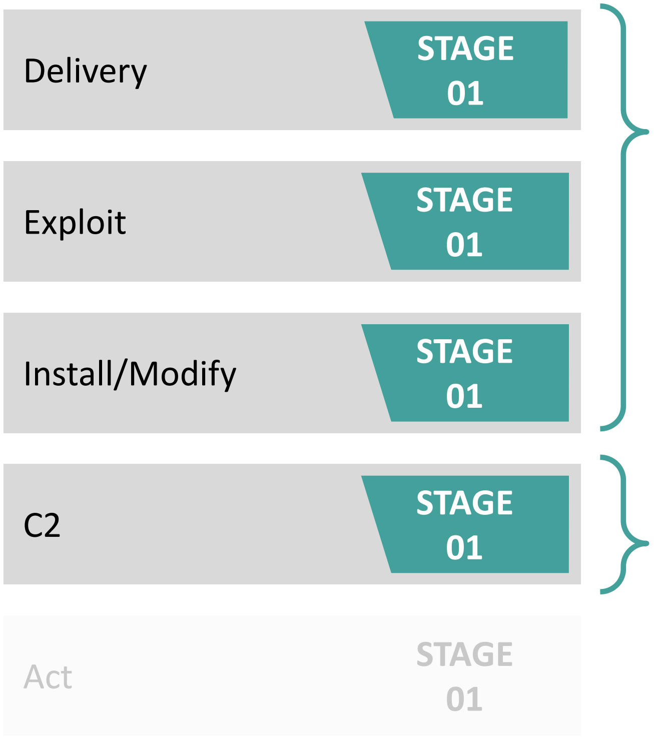
DIRECT ETHERCAT CONTROL



PLC WIPER

Potential Attack Scenarios: STAGE 1

Recon | Weaponization | Targeting



Delivery STAGE 01

Exploit STAGE 01

Install/Modify STAGE 01

C2 STAGE 01

Act STAGE 01

LAZYCARGO

LAZYCARGO installs a vulnerable ASRock driver on a victim machine, then exploits an arbitrary code execution vulnerability (CVE-2020-15368) to reflectively load an unsigned device driver specified by the adversary.

This could be used for persistence on a compromised host, or to impact the integrity of other software.

DUSTTUNNEL

DUSTTUNNEL serves as a Windows implant to enable adversary actions on a victim machine, including enumeration of underlying infrastructure, command execution, Upload (exfiltration) and Download of files.

Potential Attack Scenarios – STAGE 2

Deliver	STAGE 02
Execute ICS Attack	STAGE 02

MOUSEHOLE

MOUSEHOLE provides a framework for the identification and enumeration of OPC-UA servers. The tool provides functionality to attack authentication, enumerate the OPC node structure, then interact with specified nodes.

Deliver	STAGE 02
Install/Modify	STAGE 02
Execute ICS Attack	STAGE 02

EVILSCHOLAR

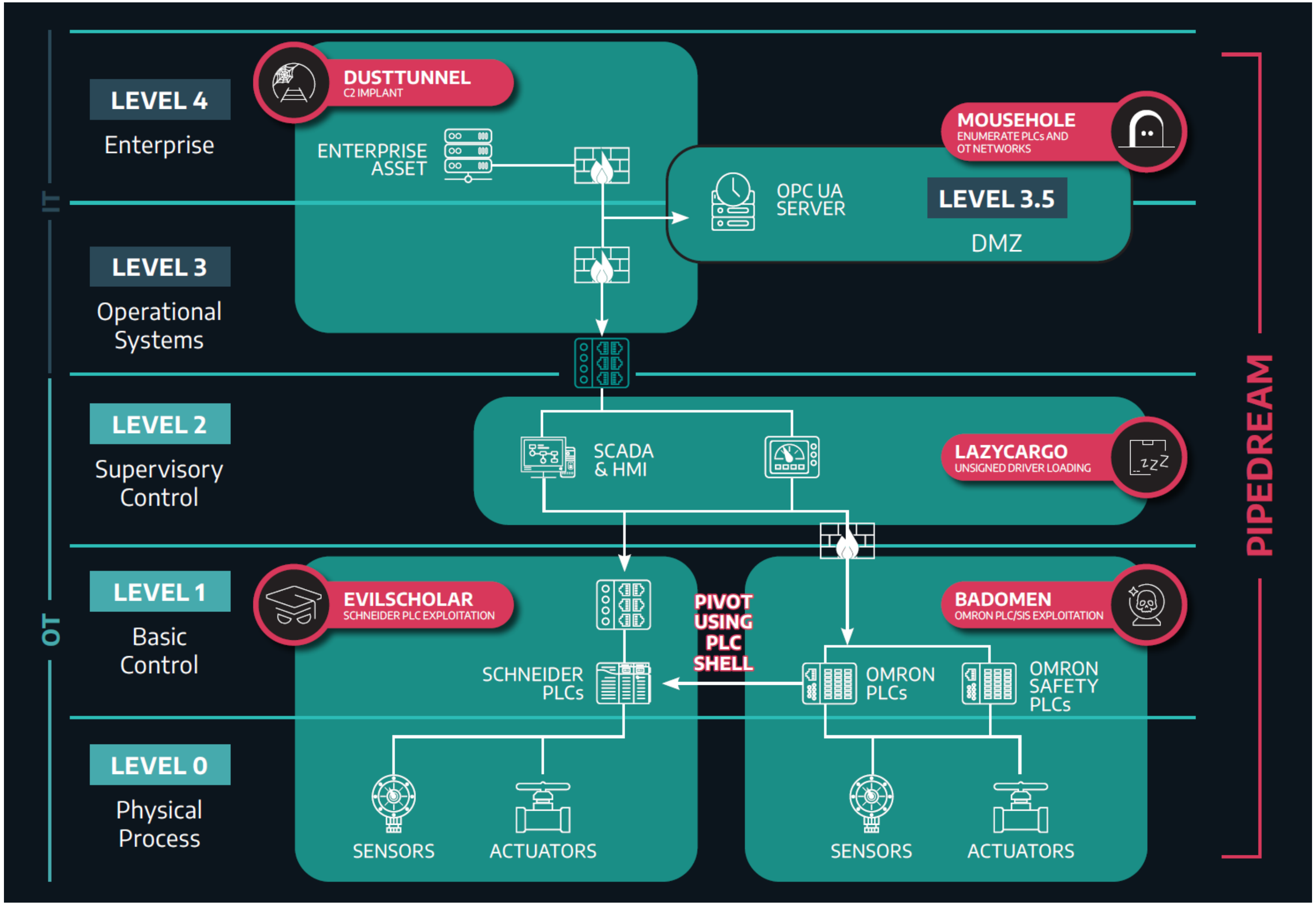
EVILSCHOLAR is an extensible framework implementing various protocols with extended functionality observed in Schneider Electric devices (e.g. CoDeSys and Modbus/TCP). The framework enables device discovery, manipulation and disruption, as well as capabilities to proxy commands via a victim controller.

Develop	STAGE 02
Deliver	STAGE 02
Install/Modify	STAGE 02
Execute ICS Attack	STAGE 02

BADOMEN

BADOMEN provides a similarly extensible framework for interacting with Omron controllers. The tool implements a HTTP API normally used by Omron engineering tools and provides functionality to:

- manipulate Omron controllers and connected actuators
- tamper with device memory and filesystems
- disrupt operation with wiper functionality


IT
OT
LEVEL 4
Enterprise
LEVEL 3
Operational Systems
LEVEL 2
Supervisory Control
LEVEL 1
Basic Control
LEVEL 0
Physical Process
DUSTTUNNEL
C2 IMPLANT
ENTERPRISE ASSET
MOUSEHOLE
ENUMERATE PLCs AND OT NETWORKS
OPC UA SERVER
LEVEL 3.5
DMZ
SCADA & HMI
LAZYCARGO
UNSIGNED DRIVER LOADING
EVILSCHOLAR
SCHNEIDER PLC EXPLOITATION
PIVOT USING PLC SHELL
BADOMEN
OMRON PLC/SIS EXPLOITATION
SCHNEIDER PLCs
OMRON PLCs
OMRON SAFETY PLCs
SENSORS
ACTUATORS
SENSORS
ACTUATORS
PIPEDREAM

Chernovite Mitigation Recommendations

Action	Target
Change default credentials	Schneider Electric TM2xx series PLCs • Beginning with firmware 5.0 the devices use default credentials' Administrator’/’Administrator', and these should be changed to a complex password using the EcoStruxure software
Restrict access to UDP/1740-1743, TCP/1105, and TCP/11740	For all Schneider Electric TM2xx series PLCs
Restrict access to TCP/11740	For non-Schneider PLCs are known to communicate with this port from the Engineering Workstation.
Validate the engineering workstation software - EcoStruxure Machine Expert	Remove unnecessary software. If possible, apply application allow listing software on the workstation. Restrict the workstation from making outbound network connections, especially to Internet services
Conduct network telemetry analysis for unusual interactions with PLCs	Look for non-standard workstations or accounts
Monitor affected PLCs for new outbound connections	Look for comms to other PLCs on the network, on UDP/1740-1743, TCP/1105, and TCP/11740
Disable the Schneider NetManage discovery service	Used by Chernovite to discover PLCs (see VA-2019-02[1])
Network isolation of safety systems	
ICS Focused Incident Response Plan	SOPs for operating with a hampered or degraded control system
Spare Parts inventory and Plans	for re-supply/cold backups for easy replacement of ICS level one devices

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
			Exploitation for Privilege Escalation			Default Credentials		Commonly Used Port			
	Command Line Interface				Network Sniffing			Connection Proxy		Modify Parameter	Denial of Control
					Remote System Discovery	Lateral Tool Transfer	Detect Operating System	Standard Application Layer Protocol			Denial of View
		System Firmware			Remote System Information Discovery	Program Download					Loss of Availability
		Valid Accounts		Rootkit		Remote Services				Unauthorized Command Message	Loss of Control
						Valid Accounts					Loss of Productivity & Revenue
	Scripting						Point & Tag Identification		Denial of Service		
	User Execution						Program Upload		Detect Restart/ Shutdown		Loss of Safety
									Manipulate I/O Image		Loss of View
											Manipulation of Control
											Theft of Operational System
									System Firmware		

Apply What You Have Learned Today

- Utilize MITRE ATT&CK for ICS to understand new unique threat behaviors (TTPs)
  - EVILSCHOLAR especially offers new capabilities for enumeration and lateral movement
- Threat capabilities dictate a need for OT specific visibility into East/West traffic (not just perimeter traffic)
- Prioritize system of system analysis to understand how your industrial process can fail as the threats continue to grow

Resources:

ICS Cyber Kill Chain: https://www.sans.org/white-papers/36297

Dragos’s Year in Review: dragos.com/yir

PIPEDREAM report:
https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/