



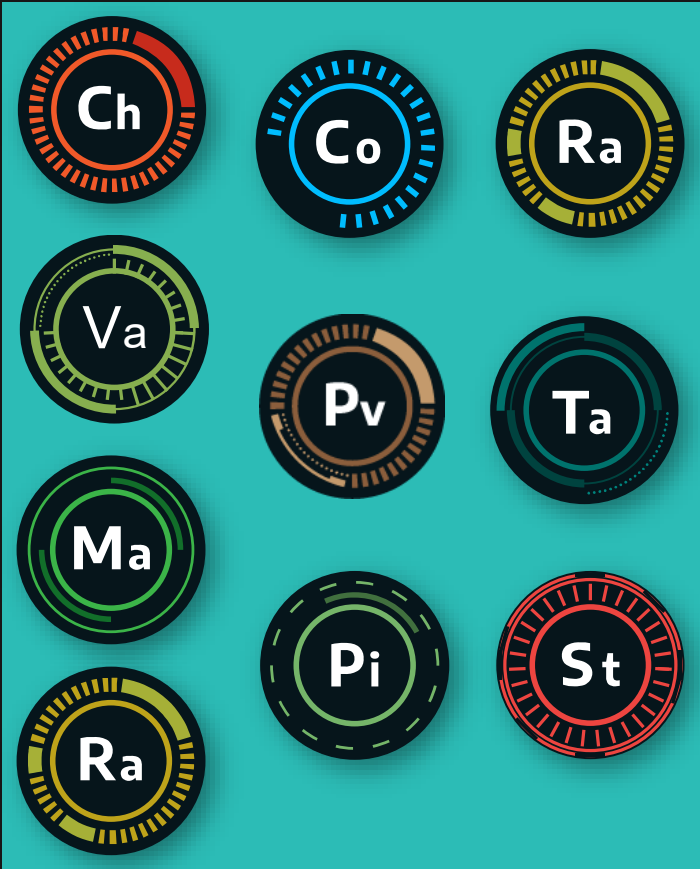
CHERNOVITE's PIPEDREAM

The Seventh ICS-Tailored Malware

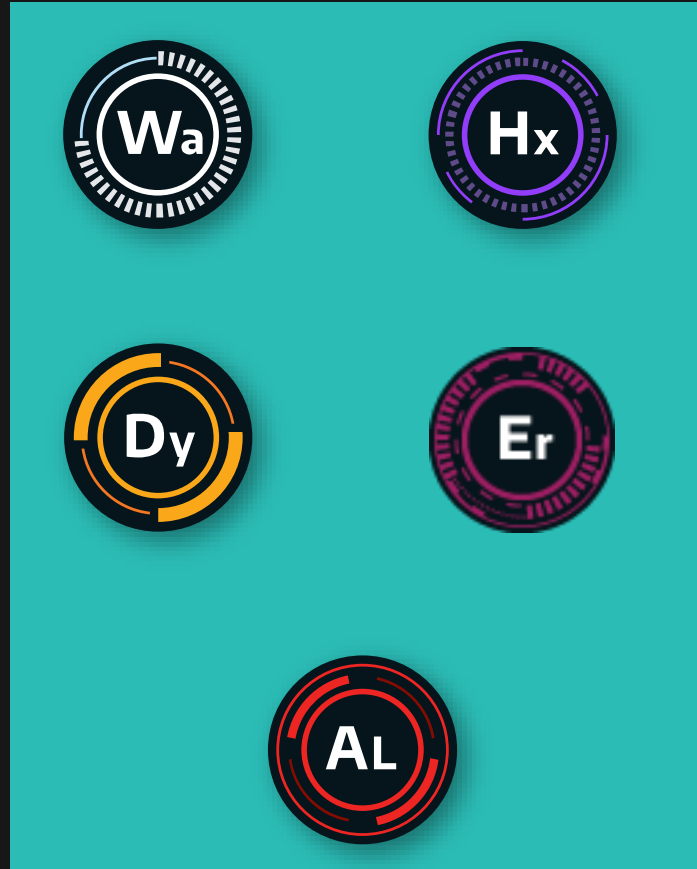
Ben Miller
@electricfork

The ICS Cyber Threat Landscape

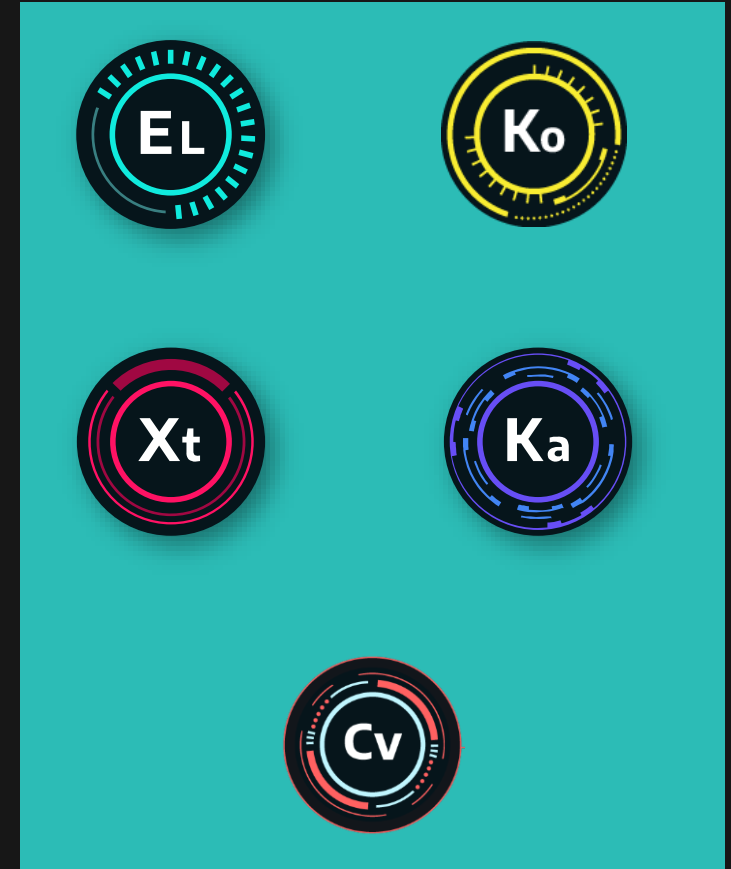
ICS Curious (ICS CKC Stage 1)



ICS Capable (ICS CKC Stage 2)



ICS Clowns (ICS CKC Stage 2 - Act)



CHERNOVITE



CHERNOVITE
SINCE 2021

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



PROFILE

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

FORMAT:
C++ 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



PROFILE

*Microsoft Windows implant
to facilitate remote
interactive operations.*

FORMAT:

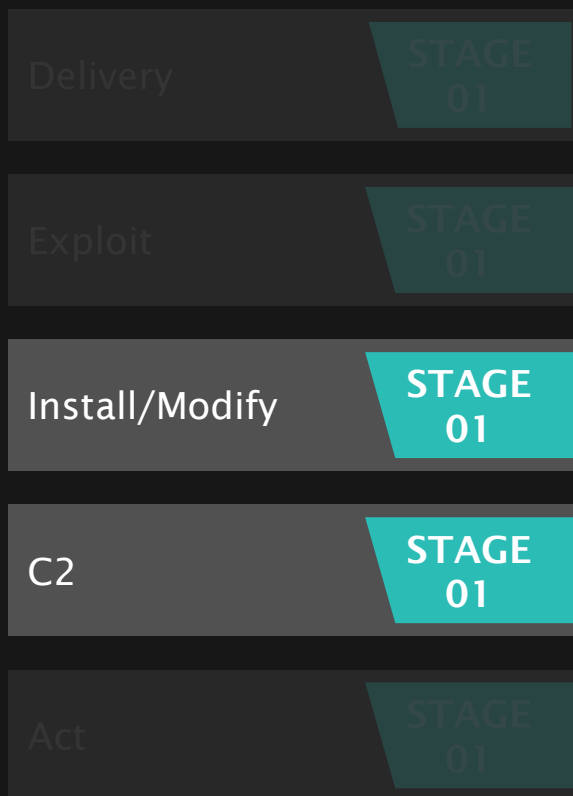
C++ Compiled binary

TARGETS:

Microsoft Windows Devices



KILLCHAIN ANALYSIS



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)



PROFILE

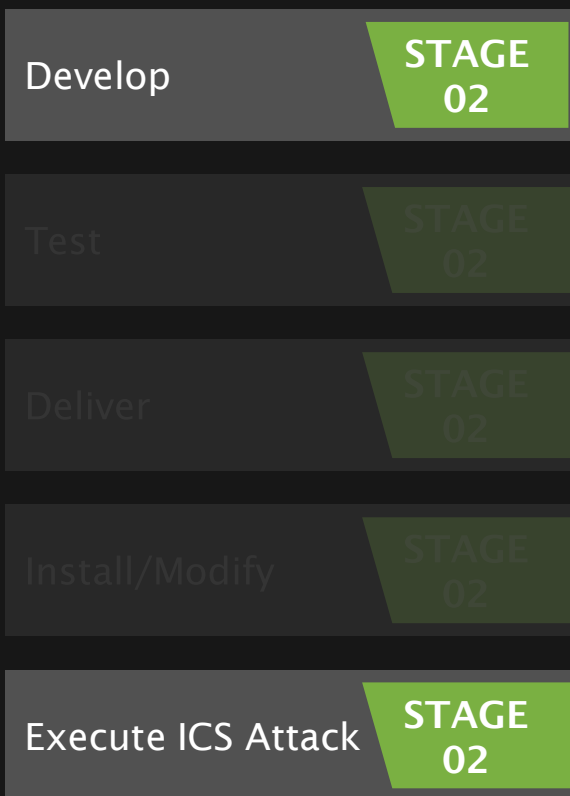
*Multiplatform toolkit
to interact with
OPC-UA servers.*

FORMAT:
Python framework

TARGETS:
OPC-UA servers

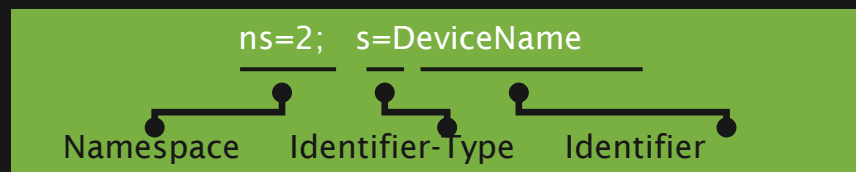


KILLCHAIN ANALYSIS

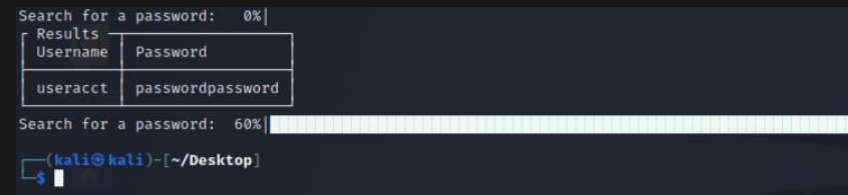


CAPABILITIES

- OPC-UA server identification / network enumeration
- Dictionary / brute-force authentication attacks
- OPC-UA server structure enumeration



Reading and Writing to OPC-nodes





PROFILE

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

FORMAT:

Python + Linux ELF Library

TARGETS:

Schneider Electric Controllers



KILLCHAIN ANALYSIS

Develop

STAGE
02

Test

STAGE
02

Deliver

STAGE
02

Install/Modify

STAGE
02

Execute ICS Attack

STAGE
02

CAPABILITIES

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

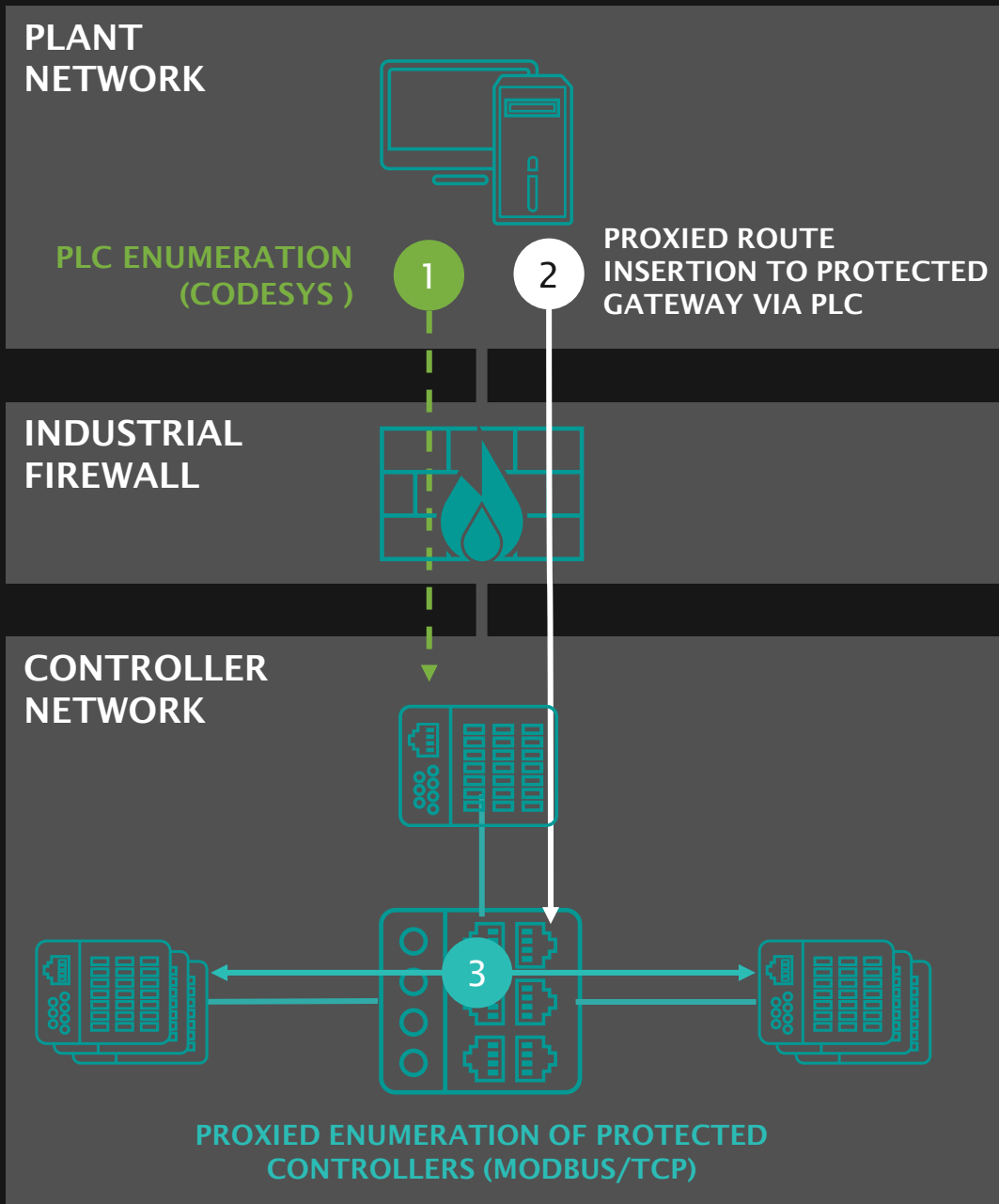
PLC disruption (DoS and Crash functions)

Traffic proxying via target controller(s)

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



PLC PROXY



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.



PROFILE

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

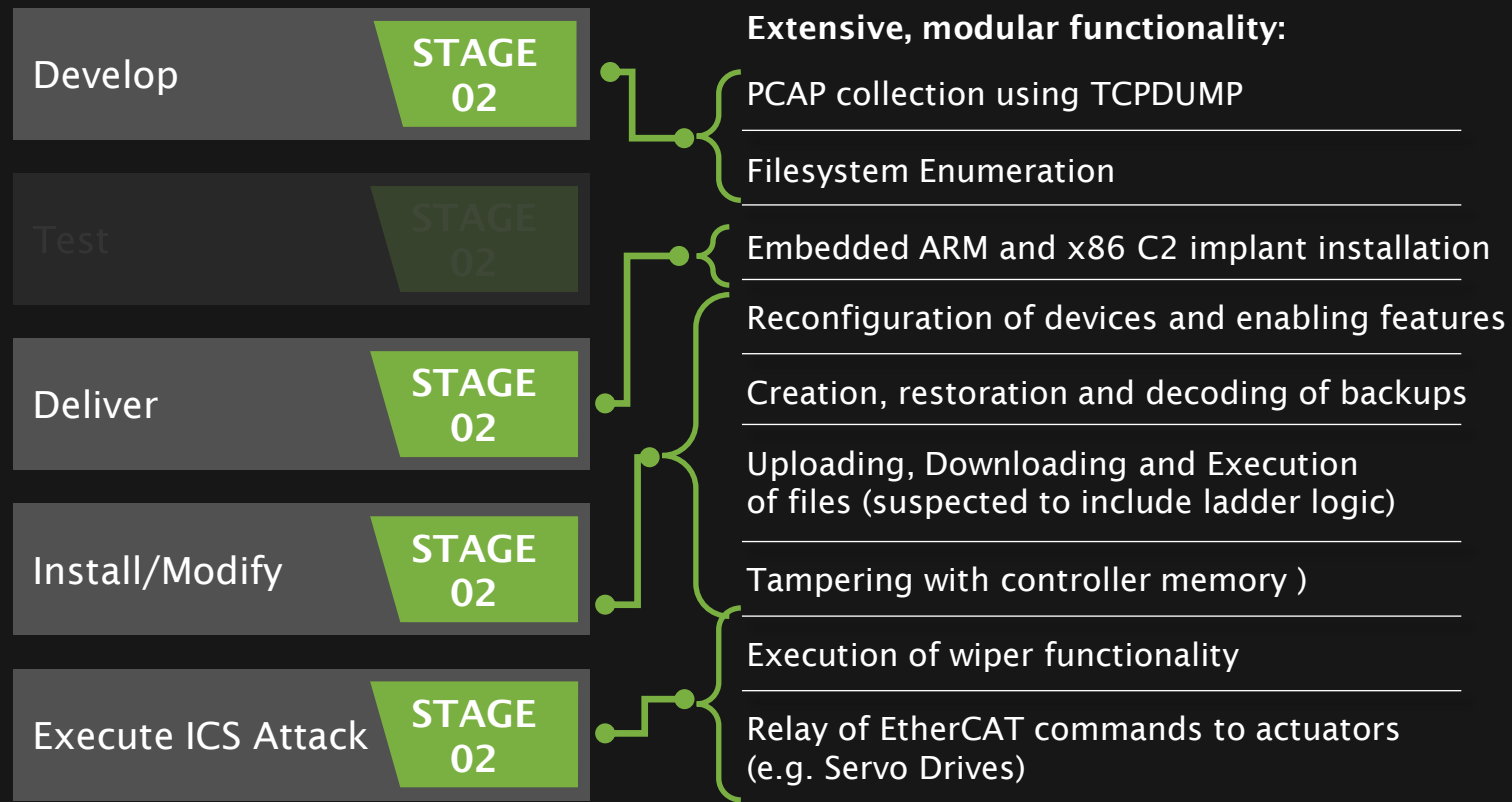
FORMAT:
Python framework

TARGETS:
Omron equipment

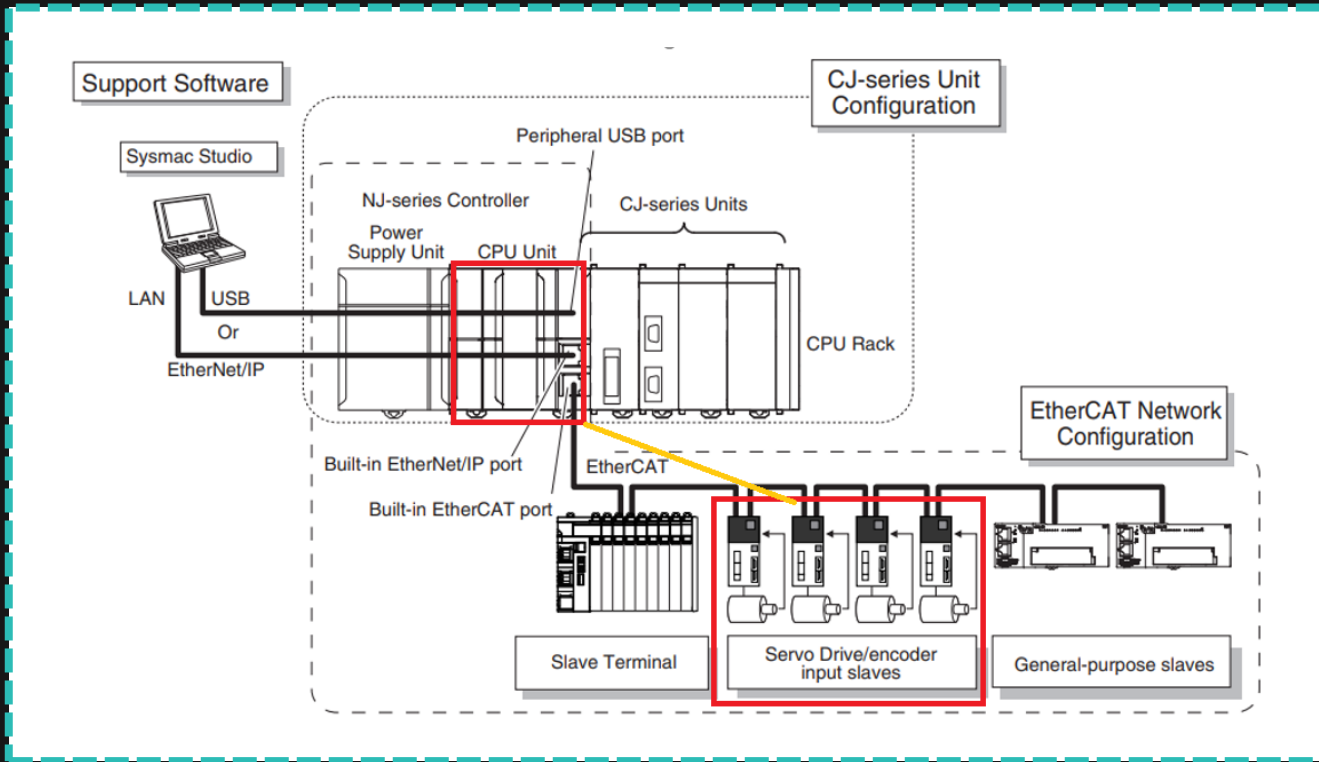


OMRON

KILLCHAIN ANALYSIS



CAPABILITIES



DIRECT ETHERCAT CONTROL

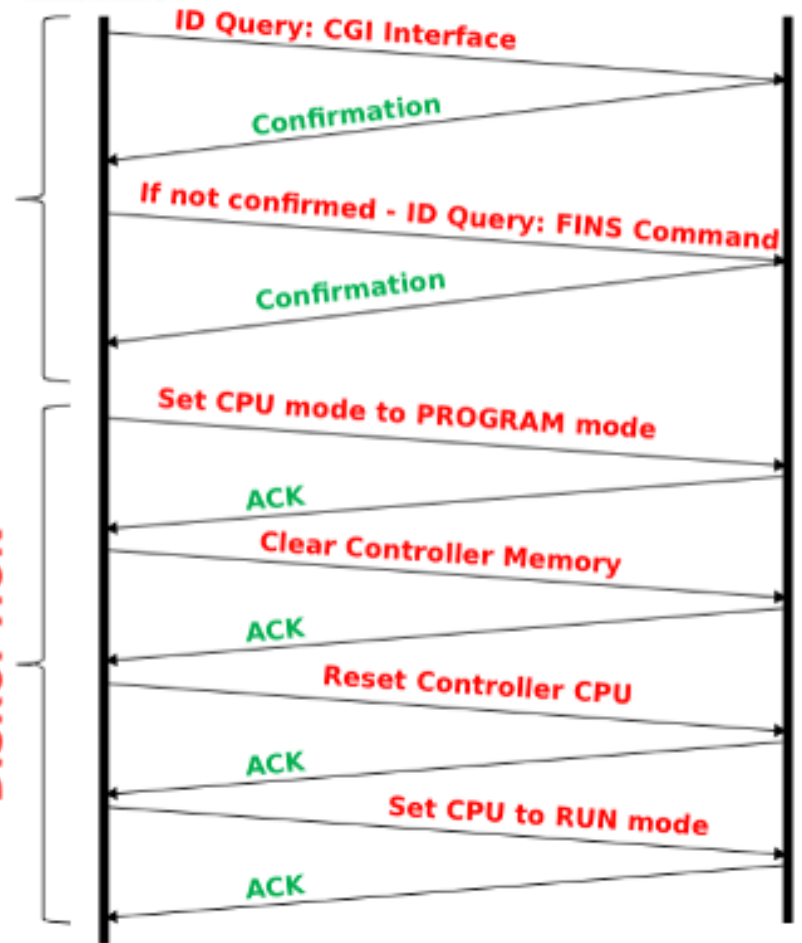


BADOMEN

OMRON

ENUMERATION

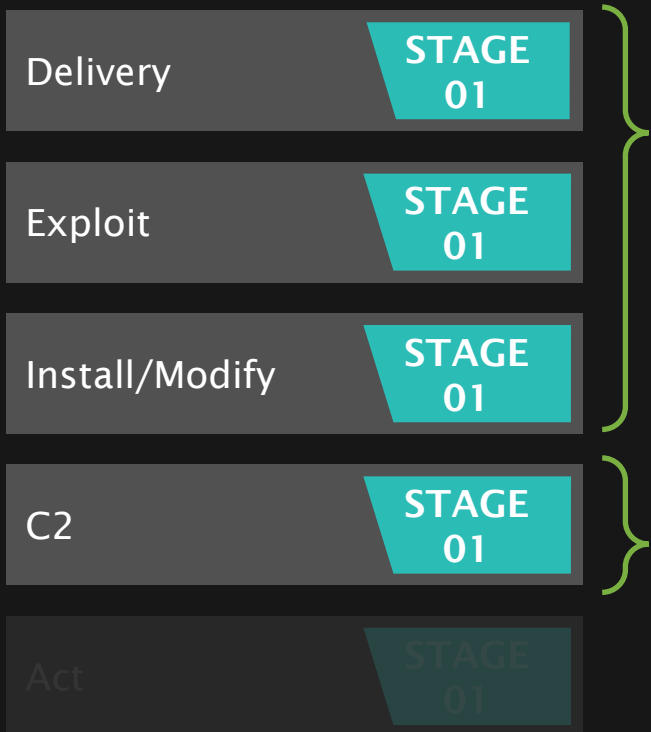
DISRUPTION



PLC WIPER

Potential Attack Scenarios: STAGE 1

Recon | Weaponization | Targeting



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 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 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 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**

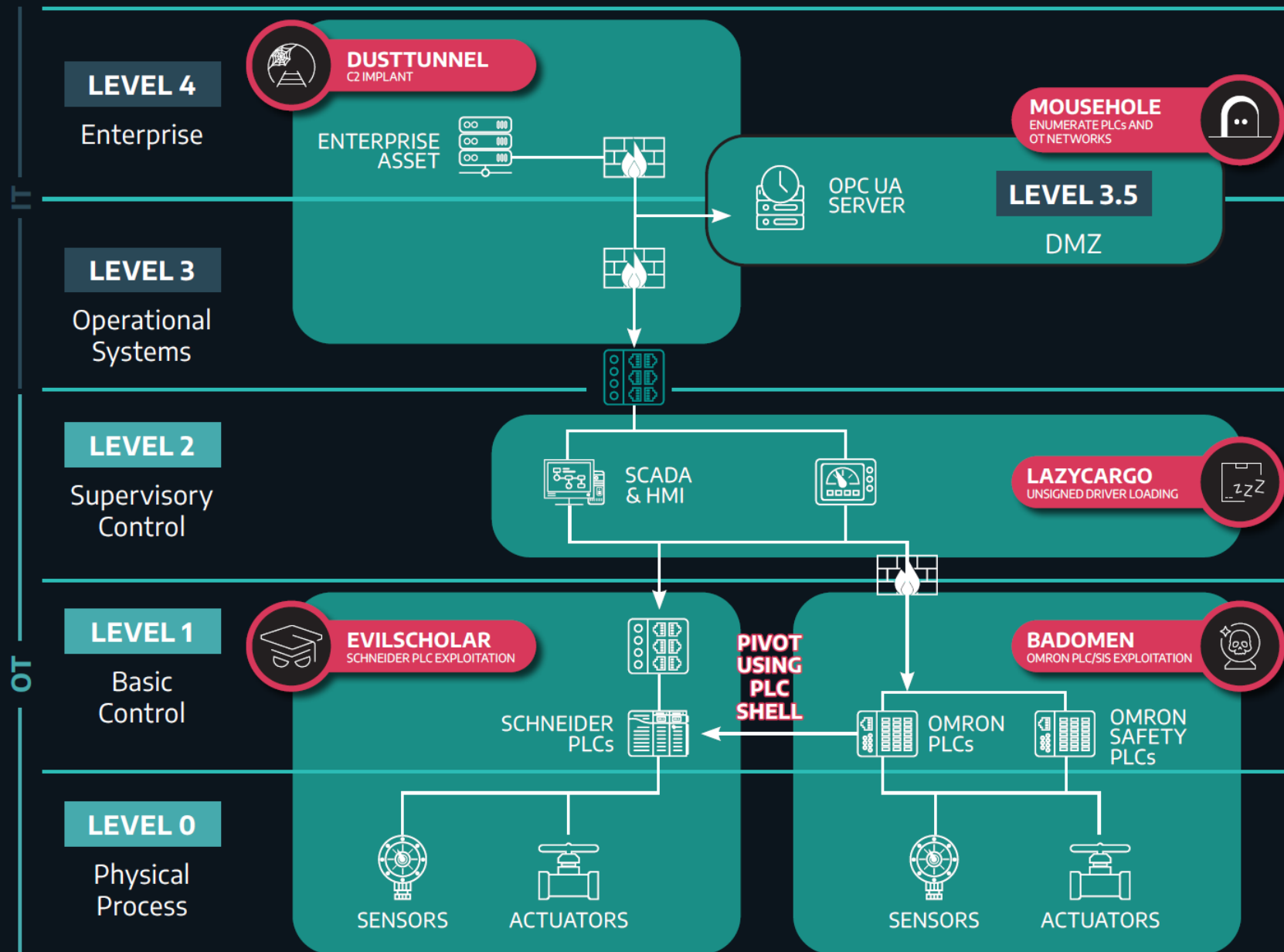
Install/Modify **STAGE 02**

Execute ICS Attack **STAGE 02**



BADOMEN 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



CHERNOVITE MITIGATION RECOMMENDATIONS

Action	Target
Change default credentials	Schneider Electric TM2xx series PLCs <ul style="list-style-type: none">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		

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/>



Thank You