DRAGOS

# PIPEDREAM Malware and the CHERNOVITE Threat Group


**Speakers**

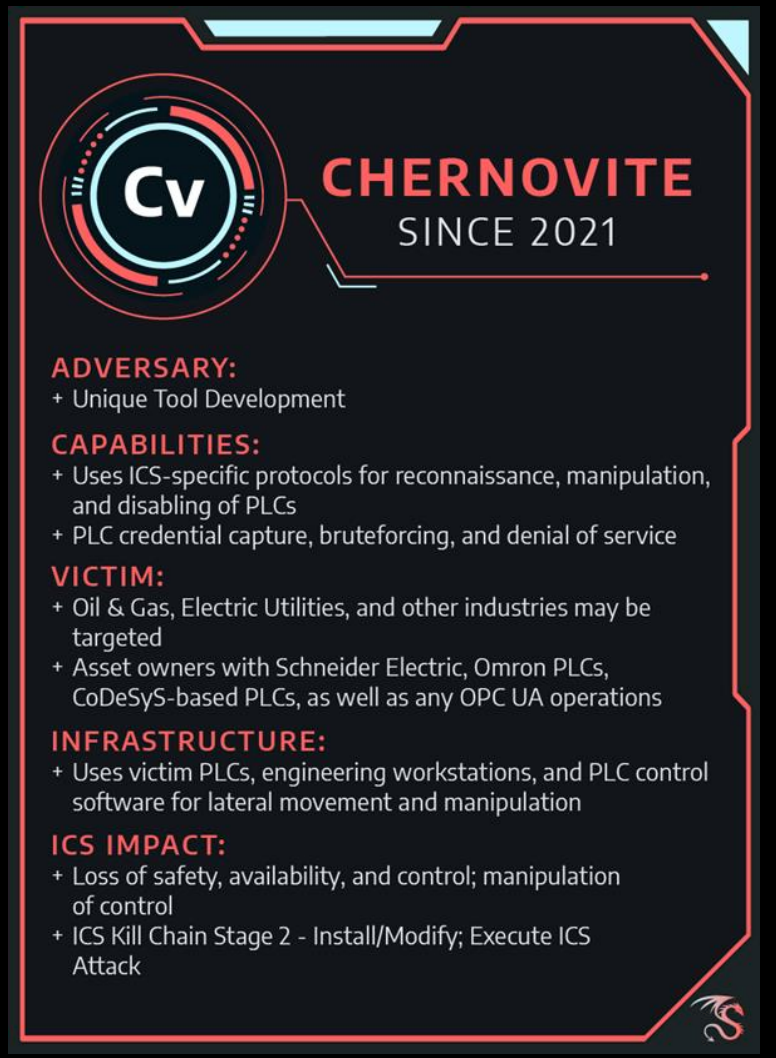
| | |
|---|---|
| Jimmy Wylie | Principal Malware Analyst II, @mayahustle |
| Reid Wightman | Principal Vulnerability Analyst, @ReverseICS |
| Sam Hanson | Vulnerability Analyst II, @secureloon |

# Agenda

- Introduction
- History of ICS
- Impacted hardware
- PIPEDREAM Capabilities
- Mitigation
- Q & A

# PIPEDREAM - CHERNOVITE

- Developed to manipulate and disrupt industrial processes.
- Has not yet been employed for disruptive or destructive effects.
- Dragos designates the group behind PIPEDREAM as CHERNOVITE.



# CHERNOVITE Capabilities


**CHERNOVITE** has the capability to operate in both IT and OT networks. It has been developed for use against OT technology.

## Capability Capacity:

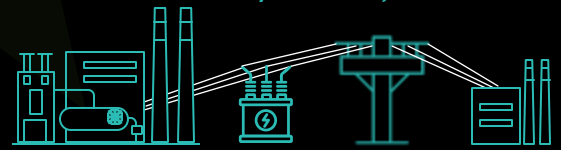
- CHERNOVITE's capability capacity can impact multiple key PLC types used across multiple sectors.
- The expansion of CHERNOVITE capabilities could impact more PLC vendors than Schneider Electric and Omron if development continues.

# History of ICS Malware

## CRASHOVERRIDE

Effective techniques with little knowledge of protocols used.

IEC101, IEC104, IEC61850/MMS, OPC-DA



## PIPEDREAM

Combines aspects of CRASHOVERRIDE and TRISIS.

Significant breadth and depth of protocol and controller knowledge.

## HAVEX

2010 | 2013 | 2015 | 2016 | 2017 | 2022

## STUXNET

## BLACKENERGY

## TRISIS

Much more in-depth attack.

Understanding of the protocols for reconnaissance and attack.

TRISTATION, TCM, Triconex OS

## INDUSTROYER2

# Impacted Devices, Abused Protocols and Vulns

**OMRON**

NX1P2 Compact Machine Controller
NX-SL3300 Safety Controller
NJ501-1300 Automation Controller
NX-ECC EtherCAT Coupler
NX-EIC202 EtherCAT Coupler
NX-ECC203 EtherCAT Coupler
S8VK Power Supply
R88D-1SN10F-ECT Servo Drive

**Schneider Electric**

TM251 PLC
TM241 PLC
TM221 PLC
TM258 PLC
TM238 PLC
LMC058 Motion Controller
LMC078 Motion Controller

**ICS Protocols**

CODESYS
Schneider Discovery (NetManage)
Modbus
Omron FINS
OPC-UA

**Vulnerabilities, Exposures, and Susceptibilities**

CVE-2020-15368 – LAZYCARGO utilizes this CVE to load an unsigned driver.

Undisclosed Vulnerabilities in Schneider Electric.

Undisclosed vulnerabilities in Omron devices.

Due to CODESYS and OPC-UA, potentially 100s of other devices affected across industry verticals.

# PIPEDREAM Components

**EVILSCHOLAR**

Designed to discover, access, manipulate, and disable Schneider Electric PLCs. Can target additional hardware through CODESYS library.

**BADOMEN**

Designed to scan, identify, and interact with Omrom software and PLCs.

**MOUSEHOLE**

Tool for interacting with OPC-UA servers. Designed to read and write node attribute data, enumerate the Server Namespace and associated NodeIds, and brute force credentials.

## Windows Components

**DUSTTUNNEL**

Remote operational implant to perform host reconnaissance and command-and-control.

**LAZYCARGO**

User-mode Windows executable that drops and exploits a vulnerable ASRock driver to load an unsigned driver.

| INITIAL ACCESS | EXECUTION | PERSISTENCE | PRIVILEGE ESCALATION | EVASION | DISCOVERY | LATERAL MOVEMENT | COLLECTION | COMMAND & CONTROL | INHIBIT RESPONSE FUNCTION | IMPAIR PROCESS CONTROL | IMPACT |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Data Historian Compromise | Change Operating System | Modify Program | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credentials | Automated Collection | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Drive-by Compromise | Command Line Interface | Module Firmware | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Data from Information Repositories | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Engineering Workstation Compromise | Execution Through API | Project File Infection | | Indicator Removal on Host | Remote System Discovery | Lateral Tool Transfer | Detect Operating System | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| Exploit Public-Facing Application | Graphical User Interface | System Firmware | | Masquerading | Remote System Information Discovery | Program Download | I/O Image | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Exploitation of Remote Services | Hooking | Valid Accounts | | Rootkit | Wireless Sniffing | Remote Services | Man in the Middle | | Block Serial COM | Unauthorized Command Message | Loss of Control |
| Internet Accessible Device | Modify Controller Tasking | | | Spoof Reporting Message | | Valid Accounts | Monitor Process State | | Data Destruction | | Loss of Productivity & Revenue |
| Remote Services | Native API | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Protection |
| Replication Through Removable Media | Scripting | | | | | | Program Upload | | Detect Restart/ Shutdown | | Loss of Safety |
| Rogue Master | User Execution | | | | | | Screen Capture | | Manipulate I/O Image | | Loss of View |
| Spearfishing Attachment | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of Control |
| Supply Chain Compromise | | | | | | | | | Rootkit | | Manipulation of View |
| Wireless Compromise | | | | | | | | | Service Stop | | Theft of Operational System |
| | | | | | | | | | System Firmware | | |

# PIPEDREAM Design & Development

**EVILSCHOLAR** and **BADOMEN** are extensible and modular.

**MOUSEHOLE** provides an interactive capability for manipulating OPC-UA server nodes and associated devices.


**DUSTTUNNEL** and **LAZYCARGO** show that CHERNOVITE isn't simply interested in OT but also how it can achieve an end-to-end attack.

# Implications of PIPEDREAM on CHERNOVITE

## The breadth of knowledge required to develop these tools indicates that CHERNOVITE:

Understands how to apply this knowledge to achieve an effect.

Is highly knowledgeable of ICS protocols.


Likely has a budget for acquiring devices.

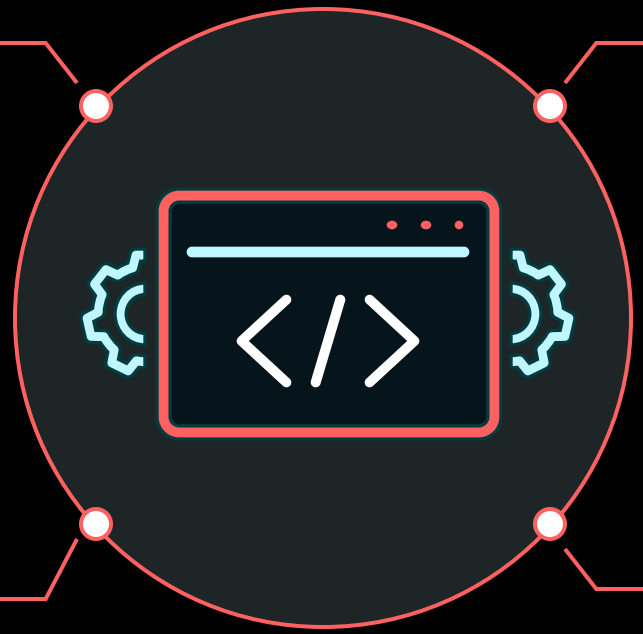
Is well versed in various PLCs.

# Assessment of CHERNOVITE Developers

Given these indicators, Dragos assesses with high confidence that CHERNOVITE is:

Highly motivated.

Well versed in ICS protocols and intrusion techniques.



Skilled in software development methods.

Well-funded.

# PIPEDREAM
# Malware Capabilities

EVILSCHOLAR

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

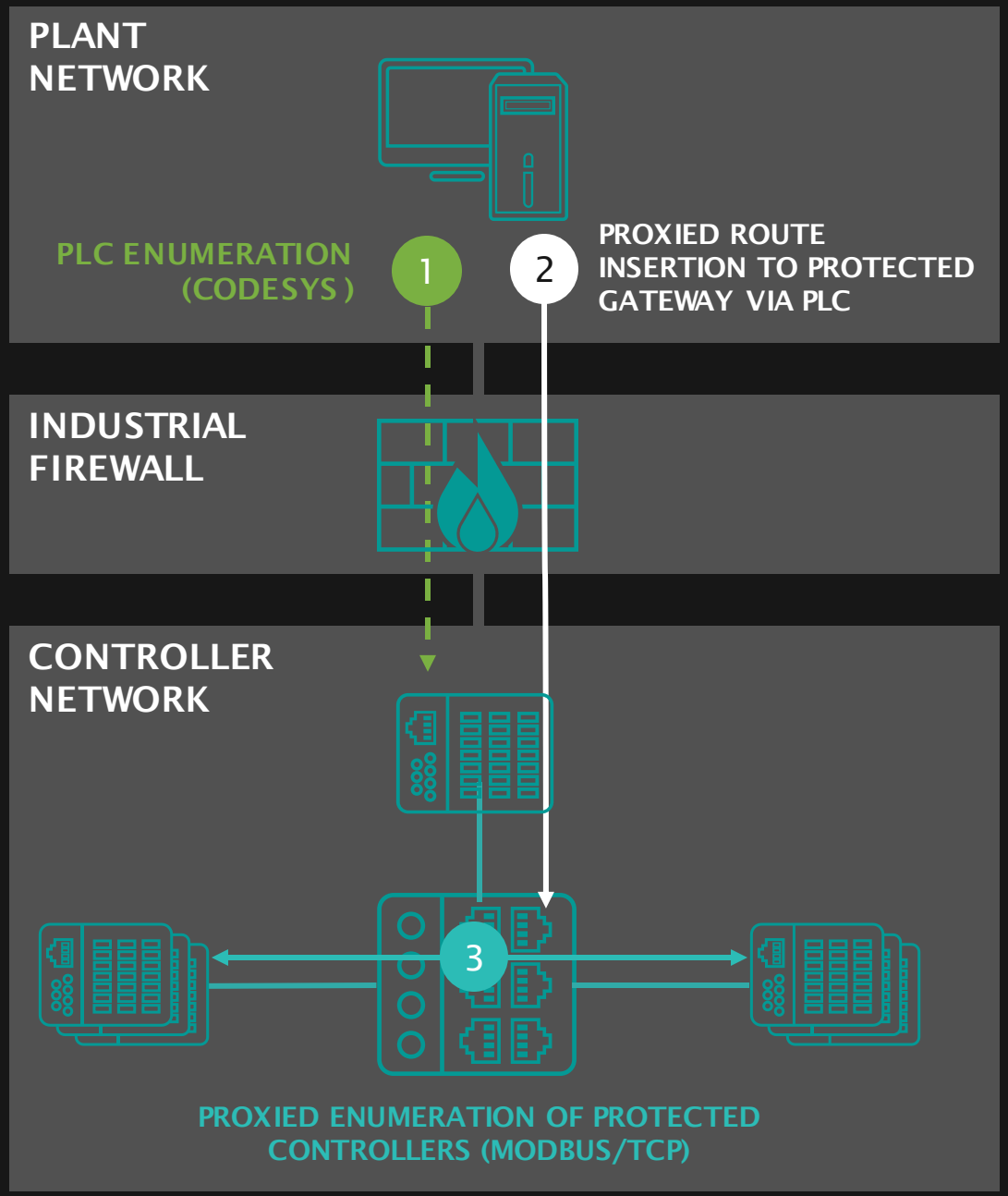
**FORMAT:**
Python + Linux ELF Library

**TARGETS:**
Schneider Electric Controllers

## Designed to discover, access, manipulate, and disable PLCs:

- Run a rapid scan that identifies all Schneider PLCs on the local network from a device that has already been compromised via User Datagram Protocol (UDP) multicast with a destination port of 27127.
- Brute force Schneider Electric PLC passwords using UDP port 1740.
- Conduct a CODESYS denial-of-service attack to prevent network communications from reaching the PLC.
- Sever CODESYS connections, likely to facilitate either credential capture or to prep for DOS
- Conduct a ‘packet of death’ attack.
- Proxy Modbus traffic through a target PLC
- ”Maintenance” actions like logging in/out, uploading/downloading files, etc.


# 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.

BADOMEN

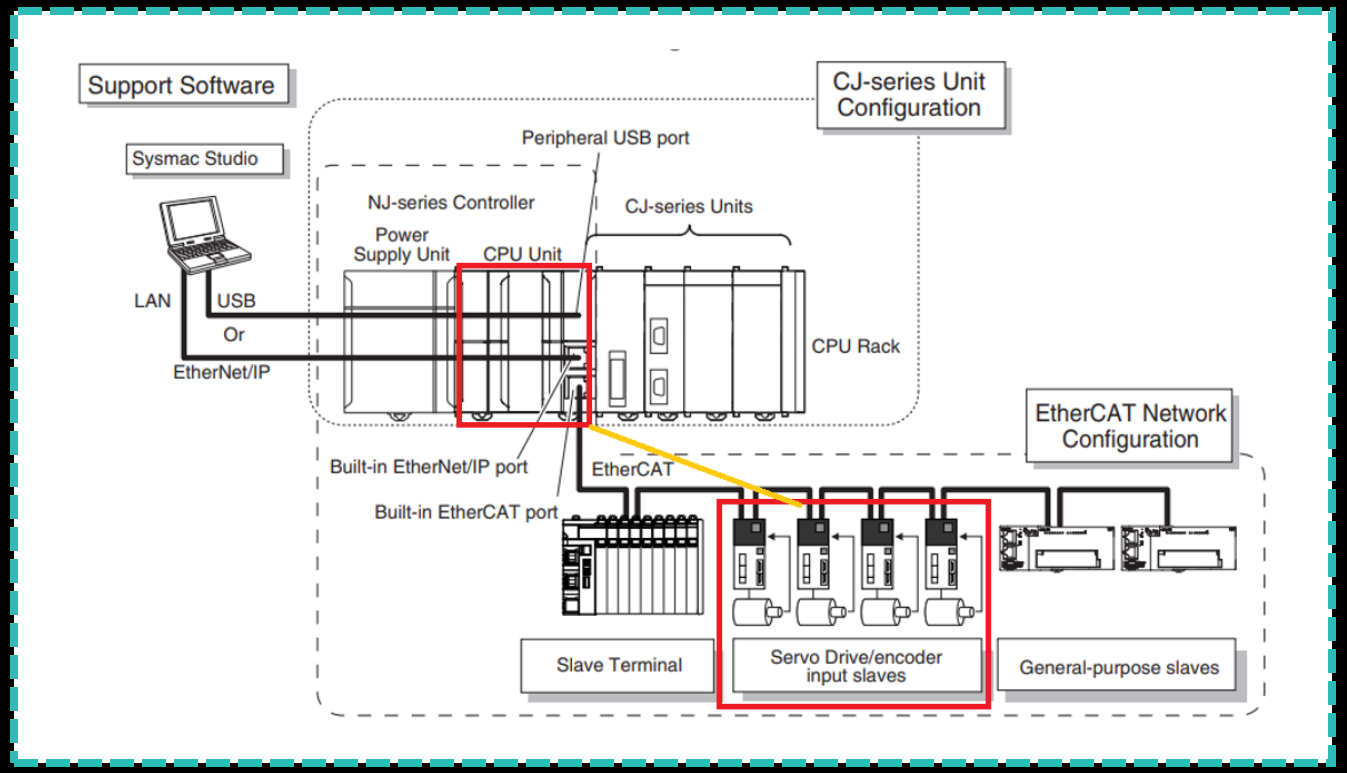
*Framework to interact with Omron controllers via Omron HTTP API and FINS protocol*

**FORMAT:**
Python framework

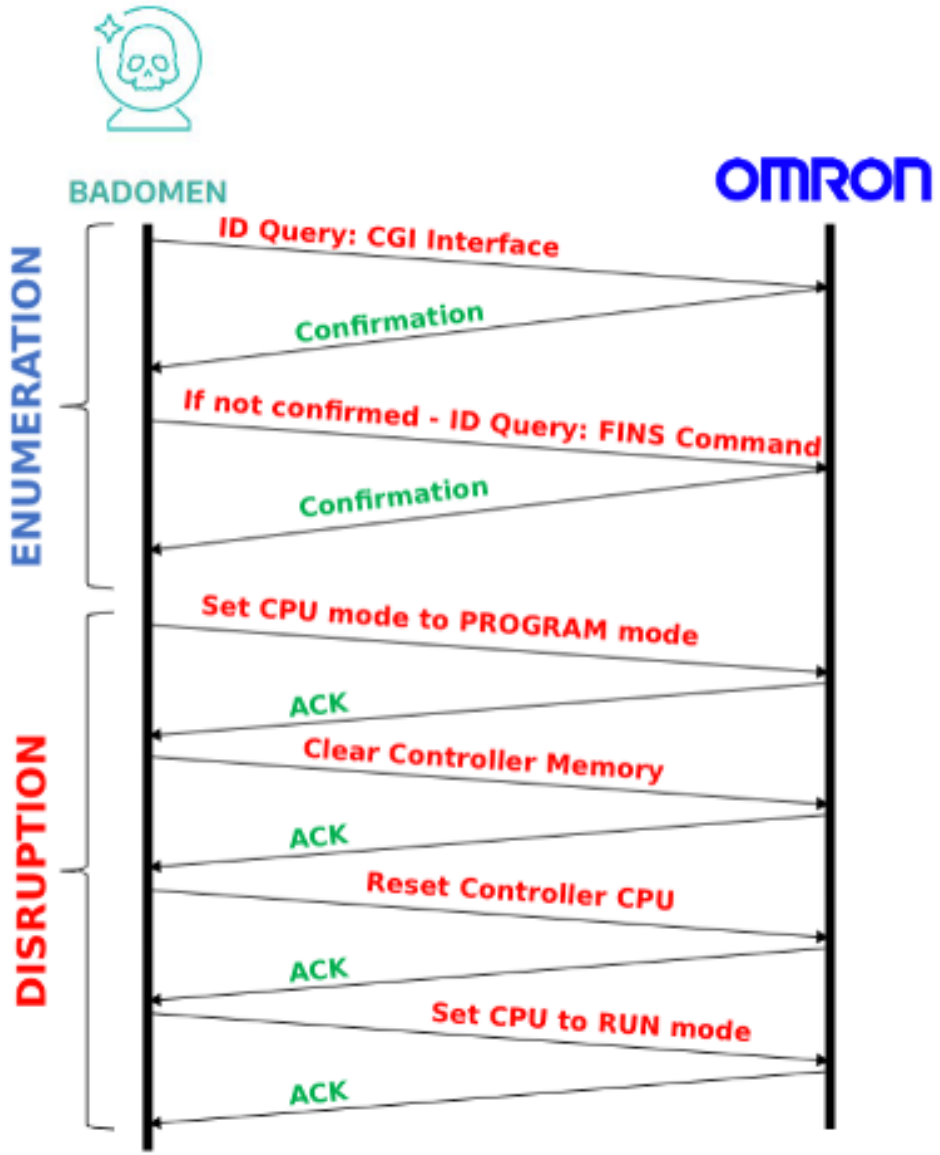
**TARGETS:**
Omron equipment

## Remote shell containing the following capabilities:

- Log into a PLC with a variety of methods.
- Exploit telnet connections to the PLC to load a malware implant.
- List directories of the PLC.
- Upload, download, delete and execute files on the PLC.
- Perform a denial-of-service (DoS) attack against a PLC.
- Terminate active PLC connections.
- Scan and identify Omron devices using FINS (Factory Interface Network Service) protocol.
- Interpret Omron device responses.
- Collect PCAP on the OT network via uploaded TCPDUMP.
- Manipulate Servos via EtherCat.
- Creating, restoring, and decoding of system process and configuration files (possible ladder logic theft).
- Change Operating Mode (Program -> Run).
- Wipe the controller's memory.




DIRECT ETHERCAT CONTROL




PLC WIPER

DRAGOS


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

**FORMAT:**
Python framework

**TARGETS:**
OPC-UA servers

*ANALYST NOTE: This is an example of an adversary evolving an attack methodology deployed by another adversary group.*

## MOUSEHOLE

Used to scan for OPC UA Servers on a local network (by default uses TCP/4840).

- Port can be changed so can scan for OPC UA Servers anywhere.

Has ability to brute force OPC UA server password based on password list supplied by user of the script.

- Can use a default password or compromised passwords.

Can read OPC UA structure from the server and change specific attributes.

- Better implementation of CRASHOVERRIDE OPC-DA attack methodology.


*Microsoft Windows implant to facilitate remote interactive operations.*

---

**FORMAT:**
C++ Compiled binary

---

**TARGETS:**
Microsoft Windows Devices

## DUSTTUNNEL configuration information commands to execute install or delete modules.

The DUSTTUNNEL implant has the following host-based capabilities:

- Enumerate victim host machine
- Enumerate network connections
- Run commands received from the command-and-control server
- Upload/download files
- Edit registry keys
- VM-awareness techniques
- Anti-debugging/anti-analysis techniques.


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

---

**FORMAT:**
C++ Compiled binary

---

**TARGETS:**
Microsoft Windows Devices

---

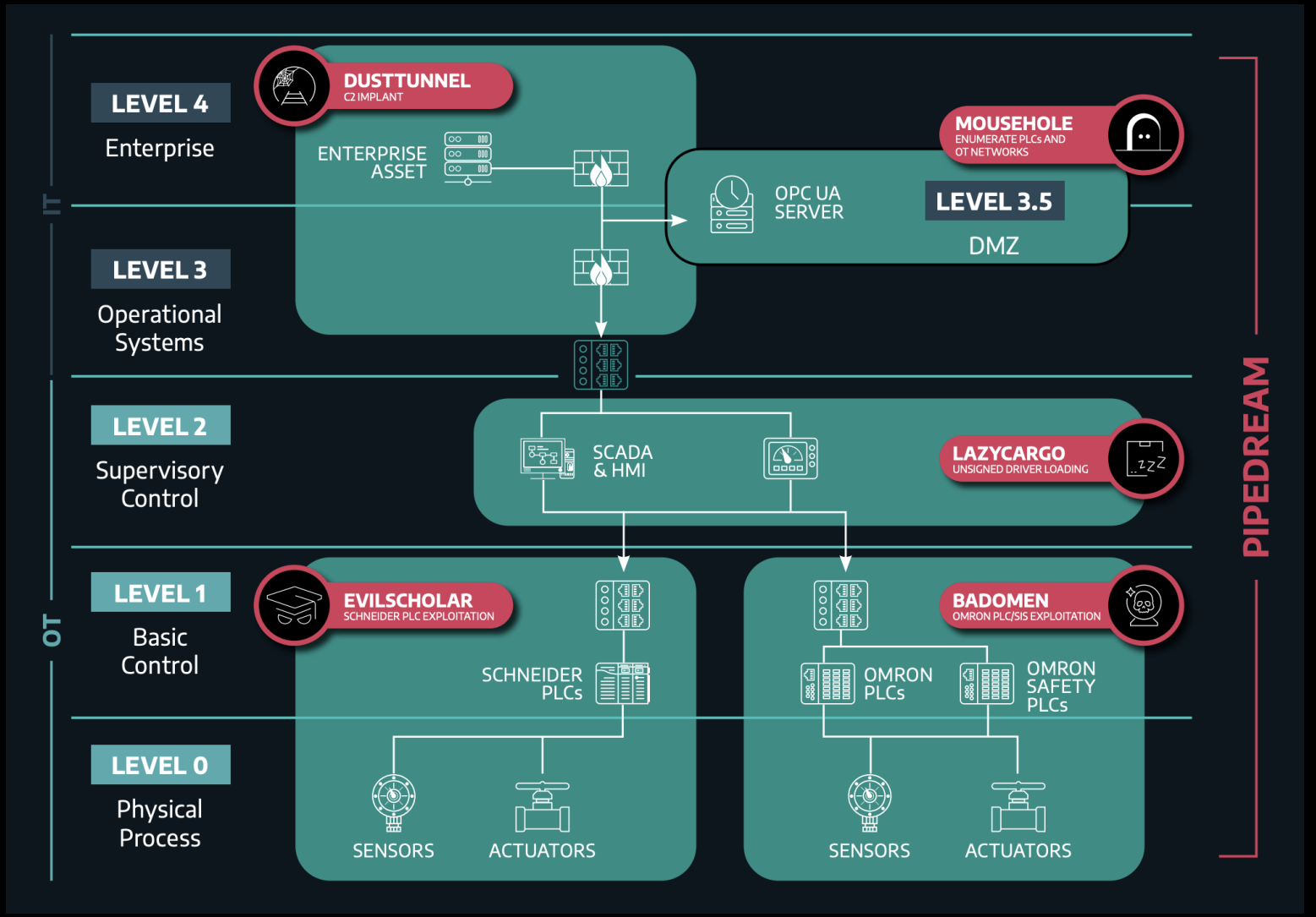
**Works against all motherboard manufacturers and VMs**

## LAZYCARGO is a user-mode executable that drops and exploits an ASRock RGB configuration driver.

Exploits a known vulnerability: CVE-2020-15368. A CVE write-up and Proof of Concept can be found on the internet.

- Exploit requires administrator access to install the ASRock driver as a service as well as to access the ASRock driver once loaded.
- Could load an unsigned driver. Dragos does not currently have access to that capability.
- Likely a rootkit designed to protect or hide their implant but might also be used to hide communications from PLCs.

# An Example Deployment Scenario



# Impact

- Denial of Control, View
- Loss of Availability, Control, Safety and View
- Manipulation of Control
- Program Download/Upload

# Mitigation &
# OT Best Practices

# RECOMMENDATIONS

Schneider Electric

| Action | Target |
|---|---|
| **Change default credentials** | Where feasible and in conjunction with operations and site personnel on Schneider Electric TM2xx series PLCs. Beginning with firmware 5.0, the devices use default credentials: ”Administrator”/”Administrator”, 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 known to communicate with this port from the engineering workstation. |
| **Disable the Schneider NetManage discovery service** | Used by CHERNOVITE to discover PLCs |
| **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, TCP/502 |
| **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. |

# RECOMMENDATIONS

OMRON

| Action | Target |
| --- | --- |
| **Restrict access to TCP/80, TCP/9600, and UDP/9600** | For all Omron PLCs. Only allow EWS systems to communicate on these ports. |
| **Validate the engineering workstation software - Omron Sysmac/CX-One/NX IO Configurator** | 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. |

# RECOMMENDATIONS


| Action | Target |
| --- | --- |
| **Enable OPC-UA security** | • Ensure OPC UA security is correctly configured with application authentication enabled and explicit trust lists.<br>• Ensure the certificate private keys and user passwords are stored securely.<br>• Ensure mDNS (which actively broadcasts the location of OPC UA servers) is disabled on all machines.<br>• ICS operators can manage the security configuration for their OPC UA devices using their engineering workstation software (in most cases).<br>• Using "sign-only" security mode with OPC UA is optimal for ICS environments that leverage network monitoring solutions (like the Dragos Platform). Sign-only security mode sends messages unencrypted but with an authentication code that allows receivers to be sure the message came from a trusted sender. This protects against tools like MOUSEHOLE that send unauthorized messages to OPC UA clients and servers while allowing the packets to be inspected by network security devices.<br>• Specific recommendations for OPC UA security best practices can be found on the OPC UA foundation's website @ https://opcfoundation.org/UA/Security/BestPractices.pdf |

# OT BEST PRACTICES

## Monitor East-West ICS networks with ICS protocol aware technologies

- Perform network traffic monitoring on East-West communications in addition to North-South (ingress/egress) communications. Look for modifications to PLCs occurring outside of maintenance periods such as changing the logic using native ICS protocols.

## Conduct network telemetry analysis

- Look for non-standard workstations or accounts to identify unusual interactions with PLCs.

## Network isolation of safety systems

- Monitor safety system networks for new connections or devices and verify all configuration changes comply with change management procedures.

## Isolate mission critical skid systems

- Consider implementing hardwired I/O between critical skid systems and distributed control systems I/O in place of direct communications if feasible.

# LONG-TERM READINESS


Create and update an ICS-focused Incident Response Plan with accompanying SOPs and EOPs for operating with a hampered or degraded control system.


Create and update a spare parts inventory for critical control system components, including hardware, software, firmware, configuration backups, and licensing information. Develop plans and procedures for sourcing and procurement of critical control system components. Consider the implementation of cold backups for rapid replacement of ICS level on devices.


QUESTIONS AND ANSWERS

# Thank You!