DRAGOS

Whitepaper

PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS

Dragos, Inc.

info@dragos.com

@DragosInc

CONTENTS

EXECUTIVE SUMMARY

PIPEDREAM is the seventh-known Industrial Control Systems (ICS)-specific malware and the fifth malware specifically developed to disrupt industrial processes. PIPEDREAM demonstrates significant adversary research and development focused on the disruption, degradation, and potentially, the destruction of industrial environments and physical processes.

The Dragos-designated threat group CHERNOVITE developed PIPEDREAM, which consists of a collection of components. PIPEDREAM can impact a wide variety of Programmable Logic Controllers (PLC) and industrial software, including specific Omron and Schneider Electric PLCs, and poorly configured Open Platform Communications Unified Architecture (OPC-UA) servers.

One of the Schneider Electric PLCs that PIPEDREAM targets, leverages CODESYS as its underlying system architecture. PIPEDREAM uses CODESYS as a key component to abuse due to its lack of security. CODESYS is a third-party software component used by hundreds of industrial equipment vendors. While PIPEDREAM can currently identify and target PLCs from Omron and Schneider Electric, its tooling may be used to target and attack controllers from hundreds of other vendors. In sum, PIPEDREAM can target a variety of PLCs in multiple verticals due to its versatility.

Dragos assesses with high confidence that PIPEDREAM has not yet been employed for disruptive or destructive effects. This is a rare case of analyzing malicious capabilities before employment of effects against victim infrastructure, giving defenders a unique opportunity to prepare in advance. Dragos assesses with high confidence that this capability was developed by a state-sponsored adversary with the intention to leverage PIPEDREAM in future operations.

CHERNOVITE - THE THREAT GROUP BEHIND PIPEDREAM

Based on current observations, CHERNOVITE focuses on manipulating industrial control systems and can achieve Stage 2 of the ICS Cyber Kill Chain. As an impact-focused team, CHERNOVITE would need access facilitated by other teams to ingress into target environments.

CHERNOVITE's observable infrastructure consists of compromised, adversary-controlled command-and-control infrastructure. Their activity is expected to shift to a malicious adversary-controlled domain or webserver. CHERNOVITE is likely to use service provider infrastructure; however, there are no indications of current active infrastructure. CHERNOVITE can use target infrastructure to facilitate interactive operations and lateral movement, access enablement in an operational technology (OT) environment, and the manipulation of processes to achieve adversary intent.

WHY ARE WE PUBLISHING THIS?

Threats to industrial infrastructure security are an extremely sensitive matter. Given the unique realities of industrial operations, it is often harder for defenders to react than for adversaries to leverage public information. The more time the community has to implement mitigations before new malicious capabilities become public, the better the chance the adverse effects from any attempted attacks will be reduced.

Dragos identified and analyzed PIPEDREAM's capabilities through our normal business, independent research, and collaboration with various partners in early 2022. Our primary focus is informing industrial asset owners and operators with as much information as possible. It is the team's stance never to be first to communicate detailed technical insights on ICS threats and capabilities until the information is already going to become public; this is done as the information can often be weaponized and industrial control system (ICS) defenders need as much time as possible. Once information about threats and new capabilities are made public, Dragos's approach is to follow up with detailed analysis and advice to the security community. This report was proactively written and readied for release as the information became public through other avenues.

KEY FINDINGS

Summary of Key Findings:

- PIPEDREAM is a clear and present threat to the availability, control, and safety of industrial control systems and processes. PIPEDREAM can be used to endanger operations and lives.
- PIPEDREAM's industrial-related components expose a command-line interface for manipulating target controllers and OPC-UA servers.
- PIPEDREAM can execute 36 MITRE ICS-ATT&CK techniques.
- CHERVONITE can manipulate the speed and torque of Omron servo motors used in many industrial applications. This manipulation can cause disruption or destruction of industrial processes, leading to potential loss-of-life scenarios.
- PIPEDREAM's Windows-related components facilitate host reconnaissance, command and control (C2), lateral tool transfer, and the deployment of unsigned rootkits.
- CHERNOVITE can leverage PIPEDREAM's multiple components to perform rapid reconnaissance of ICS networks by using a variety of mechanisms, including:
  - Identifying known MAC addresses
  - Port numbers
  - HTTP banners
  - Omron's proprietary Factory Interface Network Service Protocol (FINS)
  - Modbus
  - Schneider's custom Discovery broadcast protocol (NetManage).
- CHERNOVITE can achieve Develop, Deliver, Install/Modify, and Execute ICS Attack portions of the ICS Cyber Kill Chain Stage 2 in several ways. These are some examples:
  - Remotely interacting with PLCs using CODESYS to support numerous attacks like brute-force passwords, performing denial-of-service (DoS) attacks against the controller, and severing connections.
  - Remotely interacting with Omron PLCs through HTTP and Telnet to load a native implant to support further command execution.
  - Remotely interacting with Omron PLCs through exposed HTTP endpoints to change the operating mode (program, run, etc.), backing up and restoring configurations, and wiping the PLC's memory, among other capabilities.
  - Writing arbitrary node attributes on an OPC-UA server.
- CHERNOVITE can trigger Denial of Control and Denial of View for operators using multiple methods.
- CHERNOVITE disrupts operational technology by subverting and masquerading within trusted processes.
- CHERNOVITE can significantly extend time-to-recovery after an industrial incident by disabling process controllers, potentially requiring them to be returned to the manufacturer before reuse.
- CHERNOVITE can operate across process and security zones by using PLCs as network proxies across an OT environment, potentially bypassing firewalls, DMZs, and perimeter-based threat detection.
- CHERNOVITE can undermine authentication and encryption inside OT environments by collecting network traffic from PLCs and weakening PLC authentication.

IMPACTED TECHNOLOGY

PIPEDREAM has been designed to interact with and exploit the following devices. These devices are used in many vertical industries. However, Dragos assesses that the likely targets of the malware are equipment in liquefied natural gas (LNG) and electric power environments. Table 1 contains a summary of the potentially impacted technology.

Table 1: Summary of the potentially impacted technology (continued next page)

Product	Manufacturer	Description	PIPEDREAM Attack Module
	Omron NX1P2 PLC	**Compact Machine Controller** Built in EtherCAT to simplify the wiring of up to eight servo systems including for single-axis position control.	BADOMEN
	Omron NX-SL3300	**Safety Controller** SIL-3 rated safety controller. Integrated safety over EtherCAT.	BADOMEN
	Omron NJ501-1300 PLC	**Machine Automation Controller** Native OPC-UA, EtherCAT, Ethernet/IP.	BADOMEN
	Omron NX-ECC, NX-EIC202, NX-ECC203	**EtherCAT Couplers** Provides an interface between a controller and connected EtherCAT Terminals.	BADOMEN
	Omron R88D-1SN10F-ECT	**1S Servo Drive** 1 kW, , 3-400 VAC EtherCAT type servo drive.	BADOMEN
	Omron S8VK	**Power Supply** DC 24V 5.0A DIN Rail Power Supply.	BADOMEN

Table 1: Summary of the potentially impacted technology

Product	Manufacturer	Description	PIPEDREAM Attack Module
	Schneider Modicon M241 (TM241)	**IIoT Native Edge Logic Controller** EtherNet/IP; RS 232/RS 485 serial link; USB mini-B programming port	EVILSCHOLAR
	Schneider Modicon M251 (TM251)	**Programmable Logic Controller** EtherNet/IP; CANopen (master) and SAE J1939; Serial link; USB mini-B programming port	EVILSCHOLAR
	Schneider Modicon M221 (TM221)	**Logic Controller/IO Relay** PLC for hardwired architectures. EtherNet/IP; RS 232/RS 485 serial link; USB mini-B programming port	EVILSCHOLAR
	Schneider Modicon (TM238)	**Logic Controller** Standalone / “all-in-one” solution in a compact unit. Ethernet Modbus/TCP, Profibus DP, DeviceNet, etc.	EVILSCHOLAR
	Schneider Modicon M258 (TM258)	**Logic Controller** 42 or 66 digital I/O; Embedded serial link and Ethernet port; 4 analog inputs	EVILSCHOLAR
	Schneider LMC058	**Motion Controller** Solution for axis control and positioning, including automation functions	EVILSCHOLAR
	Schneider LMC078	**Motion Controller** Designed for compact machines that require a high level of performance in motion control applications. Velocity and torque control, etc.	EVILSCHOLAR

PIPEDREAM can also be used to execute attacks against the ubiquitous industrial technologies listed below.

Modbus TCP

Modbus is a serial communication protocol developed and published by Modicon® in 1979 for use with its PLCs. In simple terms, it is a method used for transmitting information over serial lines between electronic devices. Modbus later adopted the Open Systems Interconnect (OSI) TCP/IP communications protocols to expand communications over interconnected networks. The resulting protocol is now commonly referred to as Modbus TCP and is one of the most common ICS protocols.[1]

OPC-UA

The OPC Unified Architecture (UA), released in 2008, is a platform-independent service-oriented architecture that integrates all the functionality of the individual Open Platform Communications (OPC) Classic specifications into one extensible framework.[2]

CODESYS

With the adaptable CODESYS Control runtime system, any intelligent device is transformed into a complete IEC 61131-3 controller. PLC manufacturers use a toolkit to port the CODESYS runtime system on their device and turn it into a CODESYS-compatible IEC 61131-3 PLC.[3]

Windows

ASRock Motherboard Utility is an all-in-one utility designed for system updates and software downloading. It is integrated with a variety of applications and support software. ASRock Motherboard Utility provides the latest BIOS updates and system upgrade software for users to download. ASRock Inc. is the world's third-largest motherboard brand and manufactures both industrial and consumer computers and hardware.[4]

PIPEDREAM SUMMARY ANALYSIS

PIPEDREAM is a collection of utilities that includes tools for reconnaissance, manipulation, and disruption of PLCs, as well as tools for intrusion operations against Windows devices. At the highest level, the PLC-related components of PIPEDREAM provide the adversary with an interface for manipulating the targeted devices. Tools in PIPEDREAM can scan for new devices, brute force passwords and sever connections, and crash the target device. To accomplish these goals, PIPEDREAM uses several different protocols, including Omron's proprietary FINS, Modbus, and Schneider Electric's implementation of CODESYS. Given the variety of protocols that PIPEDREAM abuses, CHERNOVITE possesses a breadth of ICS knowledge beyond any of Dragos's previously discovered threat groups.

[1] *https://www.modbus.org/specs.php;* [2] *https://opcfoundation.org/about/opc-technologies/opc-ua/;* [3] *https://www.codesys.com;* [4] *https://en.wikipedia.org/wiki/ASRock*

CHERNOVITE's PIPEDREAM is a highly capable offensive ICS attack framework. It can execute 36 known ICS attack techniques (which is 46 percent of known ICS attack tactics) as measured against the MITRE ATT&CK for the ICS behavior matrix, shown in Figure 1.

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 Mode	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 Information		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Modify Formware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Blockk 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 and Revenue
Remote Services	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Replication via Removable Media	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Rogue Master	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Spearphishing Attachment							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Supply Chain Compromise									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 1 - Mapping for CHERNOVITE/PIPEDREAM MITRE ATT&CK for ICS Techniques

PIPEDREAM utilizes PLC implants to execute untrusted code on the PLC devices themselves beyond the view of the host-based monitoring found on Windows and Linux assets. Implants could live on PLCs for years before they are discovered, as only a firmware forensic analysis of a PLC would reveal the existence of the implant.

PIPEDREAM Utilities Explained

There are a few key design decisions about PIPEDREAM that indicate CHERNOVITE's development team characteristics.

Both EVILSCHOLAR and BADOMEN are extensible and modular. This fact suggests that developers intend to support the tool long term. They are aware that the toolsets need to adapt to new operational requirements. In other words, they may need to be extended for new target devices. The design is comparable to common red team tools such as Metasploit and Powershell Empire. Furthermore, the tools are easy to use, which means the developers are likely aware they may need to be used by operators less knowledgeable than the developers.

MOUSEHOLE provides an interactive capability for manipulating OPC-UA server nodes and the associated devices. MOUSEHOLE is akin to an upgraded CRASHOVERRIDE and is the first time Dragos has witnessed a threat group learning from another threat group, in this case, ELECTRUM's attack. This indicates that the adversary is aware of successful attacks and is actively seeking to develop a mature capability to achieve a similar impact.

The addition of DUSTTUNNEL and LAZYCARGO to PIPEDREAM indicates that CHERNOVITE is not only thinking about OT. They are also thinking about how it can achieve an end-to-end attack, starting with an IT intrusion, pivoting into OT, and executing an attack that covers ICS Kill Chain Stages 1 and 2.

The breadth of knowledge required to develop these tools indicates that CHERNOVITE is highly knowledgeable of ICS protocols, devices, and how to apply this knowledge to achieve an effect. They likely have a budget for acquiring devices to test their toolset.

Given these indicators, Dragos assesses with high confidence that CHERNOVITE is highly motivated, skilled in software development methods, well versed in ICS protocols and intrusion techniques, and well-funded.

The following is a list of the utilities with their capabilities. It is important to note that while the adversary could use these tools together, they are not required to be deployed together. PIPEDREAM should be viewed as a toolkit rather than a holistic attack suite.

EVILSCHOLAR
A capability designed to discover, access, manipulate, and disable Schneider Electric PLCs.

BADOMEN
A remote shell capability designed to interact with Omron software and PLCs.

MOUSEHOLE
A tool for interacting with OPC-UA servers. It is designed to read and write node attribute data, enumerate the Server Namespace and associated NodeIds, and brute force credentials.

DUSTTUNNEL
A custom remote operational implant capability to perform host reconnaissance and command-and-control.

LAZYCARGO
A capability that drops and exploits a vulnerable ASRock driver to load an unsigned driver.

Figure 2 - PIPEDREAM Utility Capabilities

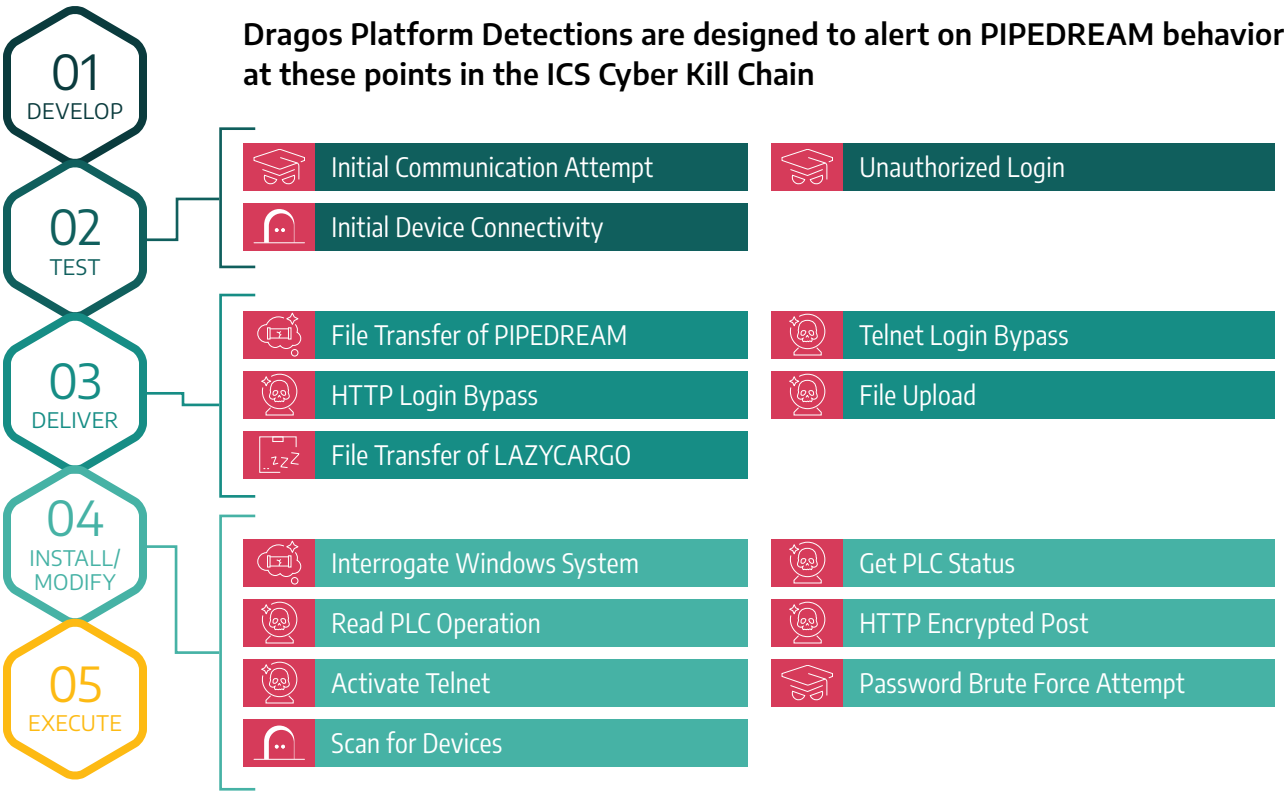

Figure 3: ICS Cyber Kill Chain

Suspected Deployment Scenarios

The following provides an example scenario of the deployment of PIPEDREAM components, along with the possible impact based on Dragos' analysis of PIPEDREAM malware to date.

PHASE 1: IT NETWORK INTRUSION

CHERNOVITE could deploy DUSTTUNNEL within an enterprise network through phishing or compromised remote access. Using DUSTTUNNEL's command-and-control functions, CHERNOVITE could drop additional tools such as Mimikatz to gather credentials to access a legitimate account and gain a persistent foothold in the enterprise network. From there, DUSTTUNNEL can allow the adversary to enumerate the network to locate IT-OT DMZ and then move laterally using captured credentials. At this stage, CHERNOVITE may deploy LAZYCARGO to install a rootkit to protect the established foothold within the corporate network.

PHASE 2: OT ENUMERATION

DUSTTUNNEL can allow CHERNOVITE to traverse to operational technology (OT) networks or jump boxes in the IT-OT demilitarized zone (DMZ). LAZYCARGO could also be deployed at this stage on operator stations/Human-Machine Interface (HMI) to install unsigned device drivers to manipulate traffic being sent between HMIs and field devices.

PHASE 3: CONTROLLER COMPROMISE

Once in the OT network, CHERNOVITE can leverage MOUSEHOLE to identify and brute force authentication to an OPC-UA server. CHERNOVITE can then enumerate devices on the OT network and see configurations, with the potential to manipulate tags and control points. Depending on the identified plant infrastructure, CHERNOVITE could deploy EVILSCHOLAR and/or BADOMEN to interact with Schneider Electric PLCs and Omron PLCs.

PHASE 4: FURTHER COMPROMISE OF CONTROL NETWORKS

EVILSCHOLAR proxy functionality could then be used to pivot into protected network segments by abusing Schneider Electric controller routing behavior. This functionality would allow further enumeration of controllers to be targeted in Modbus enumeration and exploitation.

PHASE 5: CROWN-JEWEL OBJECTIVES

Capabilities to reprogram and potentially disable safety controllers and other machine automation controllers could then be leveraged to disable emergency shutdown systems, and subsequently manipulate the operational environment to unsafe conditions.

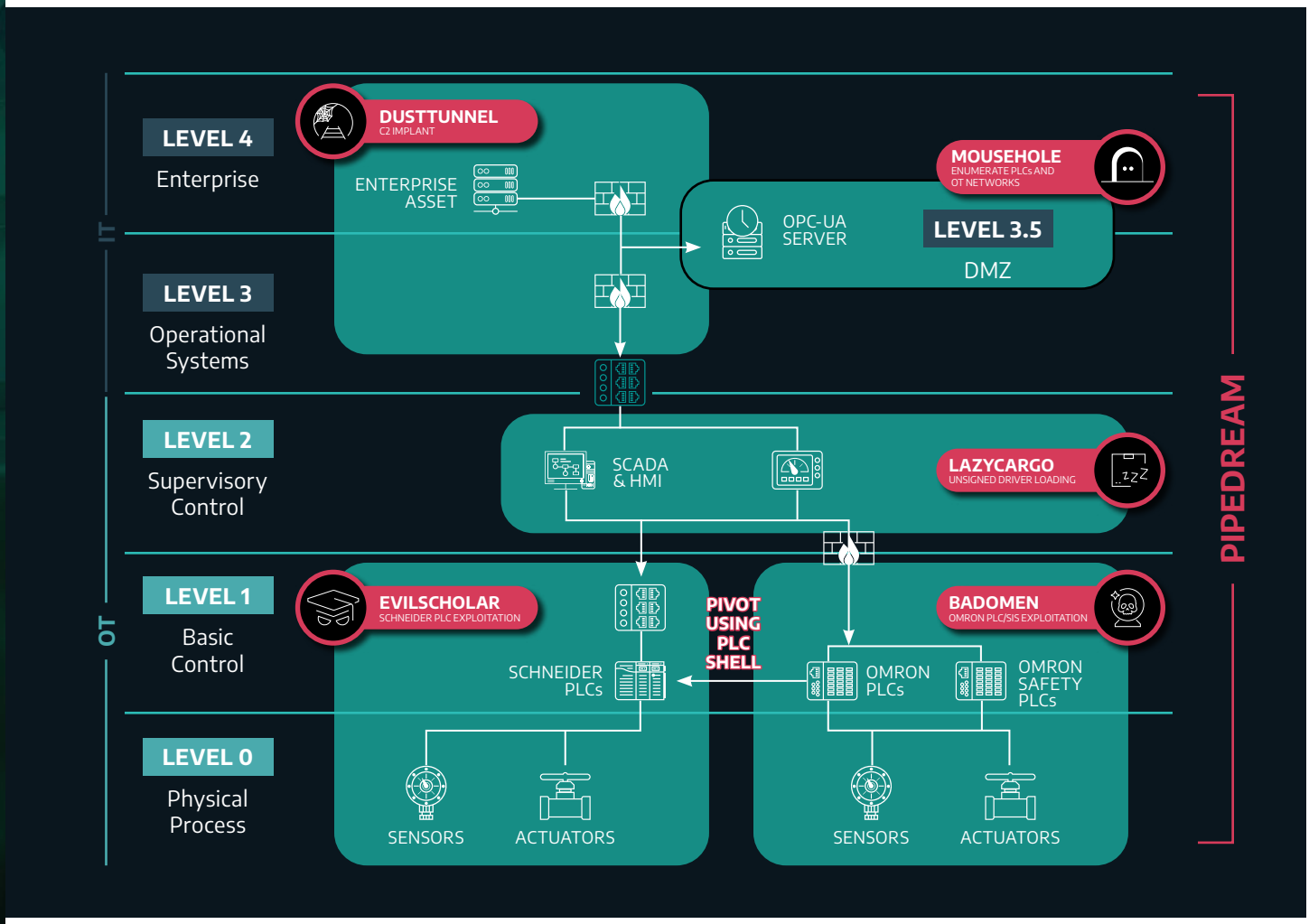

Figure 4: CHERNOVITE scenario example

DEFENDING AGAINST PIPEDREAM – WHAT YOU CAN DO NOW

The Dragos Platform contains several detections for PIPEDREAM activity. Dragos customers employing the most recent Knowledge Packs can find these detections in the Dragos platform under the Content tab. Managed service customers can go through OT Watch. Dragos has already searched through Neighborhood Keeper participants for activity. Asset owners who are not Dragos platform customers should focus on identifying the Tactics, Techniques, and Procedures (TTP) detailed in this report and follow the recommended actions to mitigate impacts to your environment in Table 2. Much of the guidance to the community in the form of standards, frameworks, and regulations heavily focuses on preventing cyber attacks. This means the community often puts very limited focus on detection and response. Given the type of threat, it is imperative to be able to detect and respond instead of simply attempting to prevent access.

Schneider Electric Technology Mitigations

Table 2: Schneider Electric Technology Mitigations

Action	Target
Change default credentials	Where feasible, in conjunction with operations and site personnel for 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 known to communicate with this port from the engineering workstation
Disable the Schneider NetManage discovery service.	In conjunction with operations and site personnel, disable Schneider NetManage discovery service, as it is used by CHERNOVITE to discover PLCs (see VA-2019-02).
Monitor affected PLCs for new outbound connections.	Look for communications to other PLCs on the network, on: UDP/1740-1743, TCP/1105, and TCP/11740.
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.

Omron Technology Mitigations

Table 3: Omron Technology Mitigations

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.

OPC-UA Mitigations

Table 4: OPC-UA Mitigations

Action	Target
Enable OPC-UA security	Ensure OPC-UA security is correctly configured with application authentication enabled and explicit trust lists. Ensure the certificate private keys and user passwords are stored securely. Ensure mDNS (which actively broadcasts the location of OPC-UA servers) is disabled on all machines. ICS operators can manage the security configuration for their OPC-UA devices using their engineering workstation software (in most cases). 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. 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

MITRE ATT&CK for ICS Techniques

In addition, focus detection and monitoring efforts on the TTPs outlined in this document, including the following:

Table 5: MITRE ATT&CK for ICS Technologies

Activity	MITRE ATT&CK for ICS Technique
File Transfer of PIPEDREAM	T1544 Remote File Copy; T1105 Ingress Tool Transfer
PIPEDREAM Execution	T1059 Command and Scripting Interpreter
PIPEDREAM Interrogate Windows System	T1047 Windows Management Instrumentation
BADOMEN Telnet Login Bypass	T1552.001 Unsecured Credentials: Credentials in Files
BADOMEN HTTP Login Bypass	T1552.001 Unsecured Credentials: Credentials in Files
BADOMEN Get PLC Status	T0868 Detect Operating Mode
BADOMEN PLC Read Operation	T0888 Remote System Information Discovery
BADOMEN HTTP Encrypted Post	T1573 Encrypted Channel
BADOMEN Activate Telnet	T1021 Remote Services
BADOMEN File Upload	T1544 Remote File Copy
EVILSCHOLAR Password Brute Force Attempt	T1110 Brute Force
EVILSCHOLAR Denial of Service Attempt	T0814 Denial of Service
EVILSCHOLAR Initial Communication Attempt	T0869 Standard Application Layer Protocol
EVILSCHOLAR Unauthorized Login	T1078 Valid Accounts
File Transfer of LAZYCARGO	T1544 Remote File Copy
MOUSEHOLE Scan for Devices	T1046 Network Service Scanning
MOUSEHOLE Initial Device Connectivity	T0869 Standard Application Layer Protocol

OT Best Practices

MONITOR EAST-WEST ICS NETWORKS WITH ICS PROTOCOL AWARE TECHNOLOGIES

Perform network traffic monitoring with a focus on East-West communications instead of simply North-South (ingress/egress) communications. PIPEDREAM's ability to move from Engineering Workstation to PLC and then PLC to PLC means that simply monitoring North-South communications or putting emphasis on segregation will be insufficient. Specifically look for modifications to PLCs occurring outside of maintenance periods such as the changing of logic using native ICS protocols.

PLC NETWORK TELEMETRY ANALYSIS

Monitor for unusual interactions with PLCs from non-standard workstations or accounts.

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.

NETWORK ISOLATION OF SAFETY SYSTEMS

Ensure network isolation for safety system components, monitor safety system networks for new connections or devices, and verify all configuration changes are compliant with change management procedures.

Long-Term Readiness

ICS-FOCUSED INCIDENT RESPONSE PLAN

Create and update an ICS-focused Incident Response (IR) plan with accompanying Standard Operating Procedures (SOP) and Emergency Operating Procedures (EOP) for operating with a hampered or degraded control system. Conduct a table top exercise focused on CHERNOVITE's ICS Cyber Kill Chain with an emphasis on PIPEDREAM; use this opportunity to identify process and collection gaps that could hinder the detection and response efforts.

SPARE PARTS INVENTORY

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 one devices.

FREQUENTLY ASKED QUESTIONS

How significant is PIPEDREAM to ICS/OT environments?

PIPEDREAM is the seventh-known ICS-specific malware, following STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE/INDUSTROYER, TRISIS/TRITON, and INDUSTROYER2. It is the first-ever known ICS-tailored malware assessed to be developed by a state actor to be identified before use for its intended purpose. New tactics, techniques, and procedures (TTP) based on detections and awareness will increase the overall security posture of OT environments, regardless of whether CHERNOVITE will deploy PIPEDREAM.

What questions should executives ask?

Executives should ask their security teams:

- Do we have Omron, Schneider Electric, or OPC-UA in our environment(s)? If so, where and what type(s)?
- If we needed to collect data from the environment, or validate that the system has not been modified, could we?
- If the processes that use these devices or protocols are disrupted, is there a cybersecurity component in place to determine root cause analysis and if an attack has occurred?
- Do we have an incident response plan that factors in the loss of any of these devices? What monitoring do we have in place to ensure it is not impacted?

Could this malware lead to loss of life?

When discussing safety impacts, there must be a thorough understanding of the specific environments and how they are configured and implemented. It is possible to leverage PIPEDREAM in a wide range of industrial controllers and environments, meaning that it could also be leveraged in attacks on safety instrumented systems (SIS). Should CHERNOVITE reprogram the safety controller without appropriate outputs, the safety integrity of the plant would be compromised and could rely on mechanical fail-safes. However, PIPEDREAM was found before the adversary could employ it for their desired effects, so there are no known targeted environments currently, and the adversary's goal may or may not be safety focused.

What are the Indicators of Compromise (IOC)?

Dragos recommends that defenders focus on the TTPs of PIPEDREAM components versus simple IOCs. Please refer to the mitigations in this paper.

If I do not have Schneider Electric or Omron in my network, should I care about PIPEDREAM?

Yes, the capabilities are further reaching than Schneider Electric or Omron vendors. CODESYS protocol is used in hundreds of controllers far beyond Schneider Electric and Omron.

Additionally, MOUSEHOLE targets and compromises OPC-UA servers.

OPC is an interoperability standard for the secure exchange of industrial automation data. It is designed to be platform-agnostic so devices from different vendors can exchange information.

[2] *https://www.motioncontroltips.com/what-is-opc-ua-and-how-does-it-compare-with-industrial-ethernet/*

Multiple Industrial Ethernet (IE) protocols in manufacturing processes and plants — such as EtherNet/IP, PROFINET, or EtherCAT — are used across different networks to meet specific topology requirements and communication speeds or latency guarantees. Although these communication protocols are open, they are often incompatible, resulting in fragmented networks that cannot "speak" to each other.

OPC-UA was developed to solve this problem by allowing industrial devices operating with different protocols and on different platforms (Windows, Mac, or Linux, for example) to communicate with each other. OPC-UA goes beyond Industrial Ethernet in reach, including devices from the lowest level of the automation pyramid — such as field devices that deal with real-world data, such as sensors, actuators, and motors — to the highest levels, such as Supervisory Control and Data Acquisition (SCADA), Manufacturing Execution Systems (MES), and Enterprise Resource Planning (ERP) systems, as well as to the cloud.[1]

What's the attribution?

Dragos does not make assessments about attribution. It is Dragos's position that what is valuable to a significant majority of defenders is understanding the "what and how, not who." Additionally, given the unique geopolitical nature of malicious capabilities and operations targeting critical national infrastructure, it could be disruptive to security efforts to focus on attribution.

What could have the original equipment manufacturers done differently?

The original equipment manufacturers (OEM)— Schneider Electric and Omron— were targets but did not do anything wrong. Each time malware families target ICS, conversations emerge about the OEM. However, product security is not the same thing as ICS security. CHERNOVITE takes advantage of the native functionality available in the industrial environment and does not rely on vulnerabilities in the ICS equipment to achieve its operations. Any focus on the OEMs is misplaced; based on the Dragos analysis, it is likely that the adversary will develop modules against numerous equipment vendors.

[1] Source: *https://www.motioncontroltips.com/what-is-opc-ua-and-how-does-it-compare-with-industrial-ethernet/*

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT

www.dragos.com.