Detecting CHERNOVITE's PIPEDREAM with the Dragos Platform

By Dragos, Inc.

Published: 2022-04-28 · Archived: 2026-04-02 11:12:24 UTC

As referenced in the original blog post, "CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems," and the detailed whitepaper, PIPEDREAM is the seventh known ICS-specific malware. Developed by the Activity Group (AG) which Dragos has designated as CHERNOVITE, PIPEDREAM malware can disrupt, degrade, and potentially destroy industrial environments and processes.

PIPEDREAM can manipulate a wide variety of programmable logic controllers (PLCs) and other industrial equipment including Omron and Schneider Electric hardware. It can also execute attacks against the ubiquitous industrial technologies CODESYS, Modbus, and OPC UA. It is believed to have the potential to execute at least 38 percent of known ICS attack techniques and 83 percent of known ICS attack tactics.[1] PIPEDREAM impacts its targets by way of five integrated utilities Dragos has labeled: EVILSCHOLAR, BADOMEN, MOUSEHOLE, DUSTTUNNEL, and LAZYCARGO.

> [PIPEDREAM] is believed to have the potential to enable at least 38 percent of known ICS attack techniques and 83 percent of known ICS attack tactics.

In addition to the Dragos Intel blog and whitepaper referenced above, further technical details on PIPEDREAM are available to customers with a Dragos WorldView Threat Intelligence Subscription. A companion blog from the Dragos Global Services team provides guidance for review of incident response plans, activating components of those plans to proactively address impacted assets, manual search methods to look for potential malicious behaviors for customers without the Dragos Platform, as well as a reminder for "best practices" for building an effective ICS/OT cybersecurity program.

This blog post provides Dragos Platform customers with summary guidance for how to leverage the Platform to quickly identify and mitigate risk from PIPEDREAM. A more detailed version and instructions about the new dashboard is available in the Dragos customer portal.

Dragos Platform Detections

General Detections: These are general detections that would fire in the Dragos Platform, covering most related threats. They will fire but are not specific to CHERNOVITE:

- Compiled Python Executable Yara Rules, Compiled Python Transfer, Compiled Python Transfer to OT Asset
- Windows Python Compiled Executable
- Command and Control after Exploitable File Download; Windows cmd.exe file download; File Downloads, File Download then New Comms

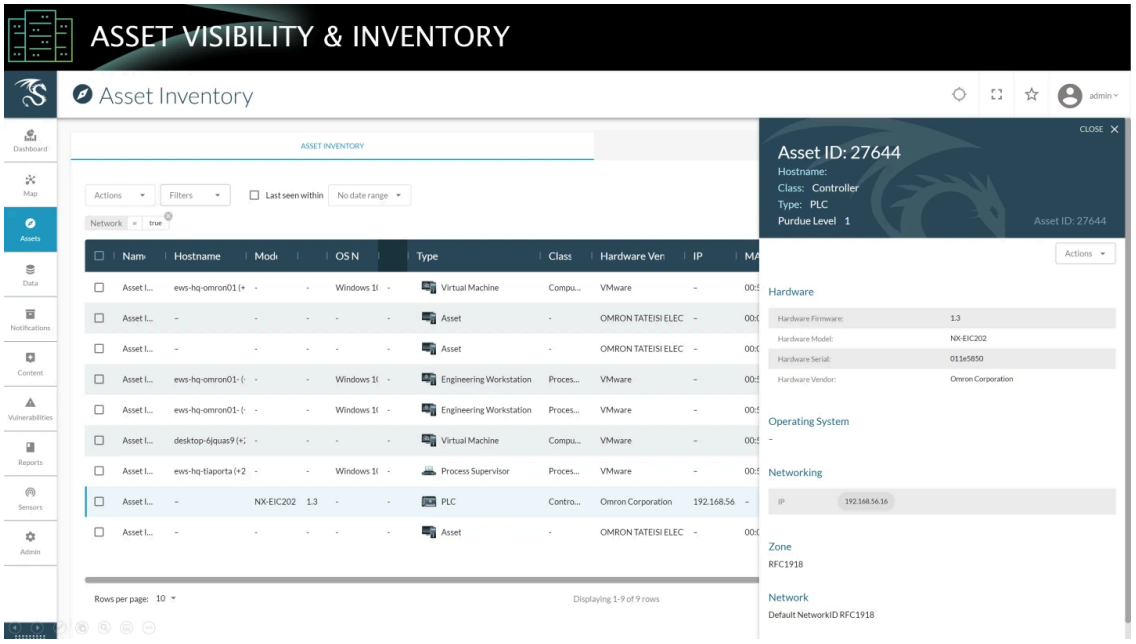
- Command and Control after Exploitable File Download; Windows cmd.exe file download; File Downloads, File Download then New Comms
- Windows Python Execution with Network Connection
- C2 Backdoor via SSL

Specific Detections Related to CHERNOVITE

Dragos Platform Detection(s)	MITRE ATT&CK for ICS Technique
Compiled Python Transfer, C2 After File Download	T1544 Remote File Copy; T1105 Ingress Tool Transfer
Windows Python Execution with Network Connection	T1059 Command and Scripting Interpreter
WinRM Enable, Windows Lateral Movement	T1047 Windows Management Instrumentation
Omron PLC Hardcoded Telnet Username and Password Used	T1552.001 Unsecured Credentials: Credentials in Files
Omron PLC Hardcoded HTTP Username Used	T1552.001 Unsecured Credentials: Credentials in Files
Omron Shell Unauthorized PLC Manipulation	T0868 Detect Operating Mode
Omron Shell Unauthorized PLC Manipulation	T0888 Remote System Information Discovery
Omron Shell Unauthorized PLC Manipulation	T1573 Encrypted Channel
Omron Shell Unauthorized PLC Manipulation	T1021 Remote Services
Omron Shell Unauthorized PLC Manipulation	T1544 Remote File Copy
Authentication Brute Force Attempts	T1110 Brute Force
Schneider Modicon Modbus Denial of Service	T0814 Denial of Service
Schneider Electric PLC Corruption Framework	T0869 Standard Application Layer Protocol
Schneider Electric PLC Corruption Framework	T1078 Valid Accounts
AsRock SignSploit, File Downloads	T1544 Remote File Copy
Scan Sequential, Port Sweep ICS Ports	T1046 Network Service Scanning
OPC UA Python Library Initial Connection	T0869 Standard Application Layer Protocol

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		

Mapping CHERNOVITE PIPEDREAM Behaviors to MITRE ATT&CK for ICS Matrix



Dragos Platform Search for Omron PLCs

Retrospective Search for Potential Malware Activity

If they haven't yet applied KP-2022-004, Dragos Platform customers can start manual hunts for potential malicious activity in their environments using the information included in Dragos Worldview Threat Report TR-2022-10. Identifiers for potential target devices including manufacturers, models, ports, and URI strings are included along with information contained in AA-2022-25.

Dragos continues to perform analysis of PIPEDREAM and several additional detections are under development for future Dragos Platform Knowledge Pack (KP) releases. These will be announced when available and included

in release update communications.

Summary Guidance for Dragos Platform Customers

1. Deploy the latest Knowledge Pack: Knowledge Pack KP-2022-004 and above contains detections for EVILSCHOLAR, BADOMEN, MOUSEHOLE, and LAZYCARGO
2. Identify impacted assets: Access your Asset Inventory and search for Schneider PLCs, Omron PLCs, and OPC UA Servers
3. Look for current potential malicious behavior: Review your dashboards to determine if any general detections have been triggered (see above for both general and specific detections that could be triggered)
4. Perform a retrospective search for potential malicious behavior: across your SiteStore forensics for signs of past activity involving this malware. See above for “Retrospective Search for Potential Malware Activity”

Get the complete analysis Read the complete analysis on CHERNOVITE and the PIPEDREAM malware targeting ICS, with defensive recommendations on what to do to protect against possible cyber attack.

Download Whitepaper

References

[1] As measured against the MITRE ATT&CK for ICS malicious behavior matrix.
