Responding to CHERNOVITE's PIPEDREAM with Dragos Global Services

By Dragos, Inc.

Published: 2022-04-28 · Archived: 2026-04-02 10:34:14 UTC

PIPEDREAM is the seventh known ICS-specific malware. Developed by the Threat Group that Dragos has designated CHERNOVITE, PIPEDREAM malware can disrupt, degrade, and potentially destroy industrial environments and processes. This blog post is intended to provide guidance for the impacted ICS/OT environments of Dragos customers and draws on the experience of our Global Services team providing architecture reviews, maturity assessments, and incident response services.

For details on the Threat Group and Malware, refer to the original blog post, "CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)," and the in-depth whitepaper, "PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems." Additional technical details on PIPEDREAM are available with a Dragos WorldView Threat Intelligence subscription.

Dragos Platform customers can get summary guidance for how to leverage the Platform in this recent blog to quickly identify and mitigate risks from PIPEDREAM – including deploying the latest knowledge pack, identifying impacted assets with Asset Inventory, looking for current malicious behaviors, performing retrospective search for past malicious behaviors, and using the Platform vulnerability management plan to manage this event.

Review Incident Response Plans – Get Moving Now, Not Later

Incident Response Plans (IRPs) and Collection Management Framework (CMF) are the starting point for incident response preparation and response. Dragos recommends asset owners have an OT-specific IRP. If you do not have one in place, use this as an impetus to construct one. While the IRP is being developed, defenders should gather insights from those responsible for the process environment and those who will be working on automation systems during restoration.

CMF is a process that documents and institutionalizes data sources that are available to defenders including what information is available and how long that data is retained. The CMF will provide the baseline for identifying impacted assets and searching for potential threat behaviors. If you do not have a CMF, start building one. Identify data sources that contain asset information and OT network traffic logs.

Find & Address Impacted Systems

Incident Response (IR) begins with evidence collection. Therefore, defenders need to ensure quality collection capability is in place for the identified targeted systems:

- Schneider PLCs

- Omron PLCs
- OPC-UA Endpoints
- CODESYS-based devices
- Engineering workstations controlling the affected devices
- Systems with firewall rules allowing communication to these devices

Teams should understand their roles and responsibilities and communicate with corresponding teams. Educate OT operations staff on the potential for cyber impacts to their environments, and ensure they are aware that they should report any concerns for investigation. Operations and automation staff should consider cybersecurity into their decisions concerning odd behaviors observed.

Establish a Solid Baseline of Known "Good" Configurations

For Schneider and Omron PLCs specifically, having a full set of known "good" project files for the systems potentially affected by PIPEDREAM can help reduce the time for analysis of potentially malicious logic files found on Engineering Workstations (EWS). Compare the digital fingerprints, the MD5 or SHA256 hashes of known good project files, to those of project files found on EWSes suspected of having been compromised. The same applies to configuration data and especially Python scripts found on EWSes.

Operators should ensure personnel are open to considering that a cybersecurity incident is a potential root cause during a fault analysis. This requires the OT operations team to quickly loop in the incident response (IR) team during a fault analysis, with the IR team collecting forensic host and network data during any incident analysis to verify or rule out any malicious cyber activity that might have led to the malfunction.

This is true for systems running the OPC-UA protocol – any unusual network activity from HMIs or data historians using the OPC-UA protocol should be investigated. OPC scanning is always a highly suspicious activity and does not commonly occur on operational systems. Malfunctioning HMIs leveraging the OPC-UA protocol should follow the same fault analysis approach as mentioned above for PLCs: forensic data should be collected and analyzed for a potential compromise of these systems.

Finally, unusual failures in segments that are not connected via Ethernet but have serial Modbus connections terminating on PLCs that are network connected, should also be investigated with the assumption that malicious cyber activity is a potential root cause. In this case, the segment that requires forensic collection is the one that is network connected and terminates the serial connection.

Brief Your Operations Team to Be on the Lookout

Operations teams are often the first line of detection during abnormal process changes or conditions. Dragos recommends OT security teams talk to operations employees to understand how to manage the environment under emergent operational conditions, especially under a loss of view condition.

Teams should know when and how to safely shutdown critical processes when HMI information is tampered with or simply unavailable.

- Historians and process visualization applications, which leverage OPC-UA, may cross IT/OT security boundaries.

- Losing these connections can create the potential for loss of process trends, custody transfer information, or environmental data, for example. Additionally, IT/OT interconnections provide adversarial pathways to pivot into the ICS/OT environment from the enterprise.

Update and Mature Your Incident Response Plan

If you haven't tested your disaster recovery or OT Incident Response Plans recently, you should consider facilitating a discussion-based scenario, such as a Tabletop Exercise (TTX) to ensure that team members are well versed on the IRP, their roles, and overall preparedness for a potential incident. If you have limited internal incident response capabilities or lack an incident response plan tailored to ICS/OT, then Dragos recommends reaching out to a trusted ICS incident response provider for a retainer.

Take Steps to Mitigate Risk of Impacted Assets

The detailed whitepaper, "PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems," contains specific recommendations for mitigating impacts of PIPEDREAM.

Additionally, operators should look for quick wins like the ability to deny vulnerable drivers, such as the ASRock driver that PIPELINE utility LazyCargo requires. This has a potentially high probability for OT vendor approval for deployment and a large net gain for detection/mitigation capabilities. It is important to also understand that this vulnerability has multiple public examples of exploitation and POC code so it should be considered a high priority for mitigation.

Microsoft recently announced a driver blocklist feature to Windows Defender, however the current recommended blocklist already contains ASRock driver. Because this is such a new capability, it may not apply to most ICS/OT environments but is something to consider in planning.

It is good to remember that this vulnerability requires prior access, and an adversary must interact with the system to exploit it. This creates additional opportunities for detection across the network or on the host. The "CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)" blog provides additional prospective details to inform detection activities.

Finally, operators should explore other areas within the OT environment where they can fortify and enhance defenses, such as monitoring for telnet use or enablement. If owners can segment or harden many of the targeted technologies, they can break the adversaries' collection of tools.

What's Next?

As Dragos continues to perform analysis of PIPEDREAM, several additional detections are in development for future Dragos Platform Knowledge Pack (KP) releases. For more insight on streamlining PIPEDREAM/CHERNOVITE detection, see the blog, "Detecting CHERNOVITE's PIPEDREAM with the Dragos Platform."

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
