

Free Whitepaper - PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Environments | Dragos

Archived: 2026-04-05 17:29:04 UTC

Read our complete analysis on CHERNOVITE and the PIPEDREAM malware, and get actionable guidance on what you can do to mitigate risk from cyber attack.

PIPEDREAM is the seventh known ICS-specific malware. The CHERNOVITE Activity Group (AG) developed PIPEDREAM. PIPEDREAM is a modular ICS attack framework that an adversary could leverage to cause disruption, degradation, and possibly even destruction depending on targets and the environment.

Dragos assesses with high confidence that PIPEDREAM has not yet been employed in the wild for destructive effects. This is a rare case of accessing and analyzing malicious capabilities developed by adversaries before their deployment and gives defenders a unique opportunity to prepare in advance.

PIPEDREAM can manipulate a wide variety of programmable logic controllers (PLC) and industrial software, including Omron and Schneider Electric controllers. It can also execute attacks against the ubiquitous industrial technologies CODESYS, Modbus, and OPC UA. Together, a significant percentage of industrial assets worldwide are vulnerable to PIPEDREAM.

Source: <https://hub.dragos.com/whitepaper/chernovite-pipedream>