How to Protect Against FrostyGoop: ICS Malware Targeting Operational Technology

By Dragos, Inc.

Published: 2024-07-23 · Archived: 2026-04-05 18:08:42 UTC

Information provided here is sourced from Dragos OT Cyber Threat Intelligence adversary hunters and analysts who conduct research on adversary operations and their tactics, techniques, and procedures (TTPs). Dragos OT cyber threat intelligence is fully reported in Dragos WorldView threat intelligence reports and is also compiled into the Dragos Platform for threat detection and vulnerability management.

Dragos discovered the FrostyGoop ICS Malware in April 2024. FrostyGoop is the ninth known ICS malware. This malware can interact directly with industrial control systems (ICS) in operational technology (OT) environments using the Modbus protocol, a standard ICS protocol used across all industrial sectors and organizations worldwide.

Additionally, the Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine (Служба безпеки України), shared details with Dragos about a disruptive cyber attack on a district energy company in Ukraine, which resulted in a two-day loss of heating to customers. The adversaries sent Modbus commands to ENCO controllers, causing inaccurate measurements and system malfunctions – taking almost two days to remediate the issues. Dragos assesses that FrostyGoop was likely used in this attack. An associated FrostyGoop configuration file contained the IP address of an ENCO control device, leading Dragos to assess with moderate confidence that FrostyGoop was used to target ENCO controllers through Modbus TCP port 502 open to the internet.

We want to express our gratitude to the Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine (Служба безпеки України), for its continued commitment to collaborative intelligence sharing and for allowing us to report on the disruptive OT incident impacting communities in Lviv, Ukraine.

What Is the FrostyGoop ICS Malware?

In April 2024, Dragos discovered multiple FrostyGoop binaries. The FrostyGoop ICS malware is written in Golang that directly interacts with industrial control systems (ICS) using Modbus TCP over port 502. It is compiled for Windows systems, and most antivirus vendors do not detect it as malicious.

FrostyGoop's ability to communicate with ICS devices via Modbus TCP threatens critical infrastructure across multiple sectors. Given the ubiquity of the Modbus protocol in industrial environments, this operational technology malware can potentially cause disruptions across all industrial sectors by interacting with legacy and modern systems.

The Ukraine cyber incident highlights the need for adequate security controls, including OT-native monitoring. Antivirus vendors' lack of detection underscores the urgency of implementing continuous OT network security

monitoring with ICS protocol-aware analytics to inform operations of potential risks.

The investigation of the Ukraine cyber incident revealed that the adversaries possibly gained access to the victim network through an undetermined vulnerability in an externally facing router. The network assets, including the router, management servers, and district heating system controllers, were not adequately segmented, facilitating the cyber attack.

Dragos recommends that organizations implement the SANS 5 Critical Controls for World-Class OT Cybersecurity, which include ICS incident response, defensible architecture, ICS network visibility and monitoring, secure remote access, and risk-based vulnerability management.

Key Protection Strategies for OT Systems

FrostyGoop was first reported to Dragos WorldView subscribers in late May 2024. Dragos Platform detections were assessed against the threat, and indicators of compromise (IOCs) were deployed. Using the Dragos Platform, OT Watch threat hunters have been hunting for FrostyGoop IOCs as part of regular sweeps across the fleet of subscribers since the initial WorldView reporting to ensure appropriate coverage. OT Watch has also deployed a dashboard specific to FrostyGoop-related detections and IOCs for OT Watch customers, and an upcoming Dragos Platform Knowledge Pack will include a FrostyGoop Playbook. Dragos continues to analyze FrostyGoop for future Knowledge Pack releases to ensure appropriate detections are created and deployed.

The Dragos Platform detects the FrostyGoop ICS malware with threat detections already in place. Still, it is recommended that customers always deploy the latest Knowledge Pack, including IOCs specific to this threat. For Dragos OT Watch customers, our team have conducted searches for signs of this activity on customers' behalf – consider a lack of communications on this subject as confirmation that there was no evidence of this activity found within your network. Dragos analysts also continue to proactively hunt on behalf of those in the Neighborhood Keeper program, our collective defense platform. Any findings relating to this activity will be reported to you.

What Dragos Customers Can Do

A summary of recommended guidance:

- **Identify impacted assets.** Access your Asset Inventory and search for ENCO control servers and devices communicating over Modbus.
- **Look for potential malicious behavior.** Review the FrostyGoop-specific dashboard to determine if related detections and IOCs have been triggered.
- **Perform a retrospective search for potential malicious behavior** across your SiteStore forensics for signs of past activity involving this malware.

The Dragos Platform has advanced OT-native threat detection capabilities to identify abnormal connections and communications over Modbus. It also incorporates threat-based behavioral analytics that are fine-tuned to recognize attack patterns and behaviors that exploit the Modbus protocol. By continuously analyzing network traffic and system interactions, the Dragos Platform can identify and enable a response to suspicious activities indicative of a Modbus-related attack, ensuring robust protection against both known and emerging threats.

Implementing Industrial Cybersecurity Controls

Dragos WorldView OT cyber threat intelligence further enhances situational awareness by providing in-the-moment insights into the threat landscape. This intelligence includes data on the latest vulnerabilities, attack vectors, and malware targeting Modbus systems, empowering security teams to proactively hunt for malicious activities and potential malware within the environment. This allows organizations to stay ahead of threats, rapidly identify indicators of compromise, and respond effectively to detected incidents. Dragos Platform customers can use the information in Dragos Worldview reports to start manual hunts for potential malicious activity in their environments.

The cyber threat characterized by deploying the FrostyGoop ICS malware underscores a significant vulnerability in operational technology infrastructure. The adversary exploited unsecured network points and inadequately protected systems, disrupting municipal services that resulted in considerable discomfort and potential danger to the affected population. Applying the SANS ICS 5 Critical Controls can mitigate such threats. Each control addresses specific aspects of cybersecurity readiness and resilience, each tailored to defend against the threats identified in this report.
