INTELLIGENCE BRIEF

Impact of FrostyGoop ICS Malware on Connected OT Systems

MARK (MAGPIE) GRAHAM | INTEL CAPABILITY TECHNICAL DIRECTOR

CAROLYN AHLERS | PRINCIPAL MALWARE ANALYST

KYLE O'MEARA | PRINCIPAL ADVERSARY HUNTER

DRAGOS, INC

JULY 2024

TABLE OF CONTENTS

DRAGOS

Summary

FrostyGoop is the ninth industrial control systems (ICS) specific malware. It is the first ICS-specific malware that uses Modbus TCP communications to achieve an impact on Operational Technology (OT). PIPEDREAM, an ICS malware discovered in 2022, uses Modbus TCP communications in one of its components for enumeration.

Dragos discovered FrostyGoop in April 2024. It can interact directly with ICS using Modbus TCP, a standard ICS protocol 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. Dragos assesses that FrostyGoop was 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 with TCP port 502 open to the internet.

Given the widespread use of Modbus devices globally, the broad applicability of this threat underscores the urgent need for ICS network visibility and monitoring of Modbus TCP traffic. Detecting and flagging deviations from normal behavior and identifying attack patterns and behaviors that exploit the Modbus TCP protocol is crucial. This necessitates the development of detections from the latest threat intelligence on vulnerabilities, attack vectors, and malware targeting Modbus systems.

Key Findings

- FrostyGoop is the ninth industrial control system (ICS) specific malware. It is the first ICS-specific malware that uses Modbus TCP communications to achieve an impact on operational technology (OT).
- In April 2024, Dragos discovered multiple FrostyGoop binaries. FrostyGoop is ICS-specific malware written in Golang that directly interacts with industrial control systems (ICS) using Modbus TCP over port 502. It is compiled for Windows systems, and at the time of the discovery, antivirus vendors did not detect it as malicious.
- FrostyGoop can read and write to an ICS device holding registers containing inputs, outputs, and configuration data. It accepts optional command line execution arguments, uses separate configuration files to specify target IP addresses and Modbus commands, and logs output to a console and/or a JSON file.
- The Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine (Служба безпеки України), shared details with Dragos relating to a cyber attack that targeted a municipal district energy company in Ukraine. During sub-zero temperatures, the attack disrupted the power supply to heating services to over 600 apartment buildings. The adversaries sent Modbus commands to ENCO controllers, causing inaccurate measurements and system malfunctions. Remediation took almost two days.
- The investigation 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 attack.

- FrostyGoop's ability to communicate with ICS devices via Modbus TCP threatens critical infrastructure across multiple sectors. Given the ubiquity of the Modbus TCP protocol in industrial environments, this malware can potentially cause disruptions across all industrial sectors by interacting with legacy and modern systems.
- The Ukrainian 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.
- Dragos recommends that organizations implement the SANS 5 Critical Controls for World-Class OT Cybersecurity. These include ICS incident response, defensible architecture, ICS network visibility and monitoring, secure remote access, and risk-based vulnerability management.

Analyzing the FrostyGoop ICS Malware

In April 2024, Dragos discovered multiple FrostyGoop binaries during routine triage of suspicious files. FrostyGoop is an ICS-specific malware written in Golang that can interact directly with industrial control systems (ICS) using Modbus TCP over port 502. According to VirusTotal, antivirus vendors do not detect the FrostyGoop files as malicious. FrostyGoop binaries are compiled for Windows systems. The malware can read and write to the device holding registers. Holding registers are read/write registers containing inputs, outputs, and configuration data.[1]

At the time of discovery, Dragos assessed with low confidence that the FrostyGoop ICS malware discovered was used for testing purposes. However, this assessment changed when an attack was confirmed, as detailed later in this report. Dragos discovered an associated configuration file containing multiple Modbus commands to read data from a target ICS device and an IP address belonging to an ENCO control device. Dragos assessed with moderate confidence that FrostyGoop can impact other devices communicating over Modbus TCP; the malware's functionality is not specific to ENCO control devices. Analysis of FrostyGoop files is ongoing for Dragos WorldView Threat Intelligence subscribers.

What Is the Modbus Protocol?

Modbus is a client/server communication protocol initially designed for Modicon programmable logic controllers in 1979, but it is now widely used by other devices. It is an open protocol and is hardware agnostic, making it popular for communications between PLCs, DCS, controllers, sensors, actuators, field devices, and interfaces.

The Modbus protocol defines a message structure that controllers recognize and use, regardless of the type of networks over which they communicate. It describes the process a controller uses to request access to another device, how it responds to requests from other devices, and how errors are detected and reported. This protocol establishes a standard format for the layout and contents of message fields.

[1] Modbus Protocol Reference – Control Solutions Minnesota

The protocol outlines how each controller will identify its device address, recognize a message meant for it, decide on the necessary action, and extract any data or additional information from the message. The controller will create and transmit the reply message if a response is needed using the Modbus protocol.[2]

FrostyGoop ICS Malware Capabilities

- Accepts optional command line execution arguments.
- Uses separate configuration files to specify target IP addresses and Modbus commands.
- Communicates with ICS devices via Modbus TCP protocol.
- Sends Modbus commands to read or modify data on ICS devices.
- Logs output to a console or JSON file.

Optional Command Line Execution Arguments

FrostyGoop checks if the executable is running with any required command line arguments. The binaries exit execution if no command line arguments are provided. The specific arguments vary by sample, but functionality remains the same. Information required to initiate a TCP connection and send Modbus commands to a victim ICS device can be specified as command-line arguments or contained within a separate JSON configuration file. Arguments accepted by FrostyGoop would include data such as:

- IP addresses specifying the target device to communicate with
- A "mode" option that correlates to a Modbus command to execute on the ICS device (Read Holding Registers, Write to Single Holding Register, Write to Multiple Holding Registers)
- A Modbus register address on the target ICS device to send Modbus commands to
- A JSON configuration file name; there are two different configuration files accepted by FrostyGoop
  - A configuration file containing victim device information such as IP address, Modbus commands, and Modbus register addresses
  - A configuration file containing a specific time to begin Modbus TCP communications with the victim device and various lengths to delay the execution of Modbus commands.
- Specify a file name to save logging output

Configuration File

FrostyGoop accepts a JSON-formatted configuration file containing information used to execute Modbus commands on a target device. The malware reads the file, parses the JSON data, connects to the IP address from the file, and sends Modbus TCP commands to holding register addresses specified in the configuration file.

Dragos discovered a sample of the configuration file named 'task_test.json.' The IP address in the sample configuration file belongs to an ENCO control device. ENCO control devices are typically used "for process control in

[2] Modicon Mobus Protocol Reference Guide - Modbus

district heating, hot water, and ventilation systems" to monitor sensor parameters such as temperature, pressure, and insulation.[3]

The other fields in the configuration file are described below.

Field	Description
Code	Modbus Command Code (i.e. '3' for Read Holding Registers, '6' for Write Single Holding Register, and '16' for Write Multiple Holding Registers)
Address	Modbus register address
Count	Quantity of registers to read or write
Value	Integer used to modify the Holding Register (used for Modbus 'write holding register' commands)

CONFIGURATION FIELDS

Modbus TCP Network Traffic

FrostyGoop initiates communication with the target IP address over Modbus TCP port 502. The IP address can be specified either by using an argument during malware execution or by including it in the configuration JSON file. Once a connection is established, FrostyGoop sends Modbus commands to the device. After FrostyGoop sends commands and receives the target device's responses, the binaries close the connection and exit execution.

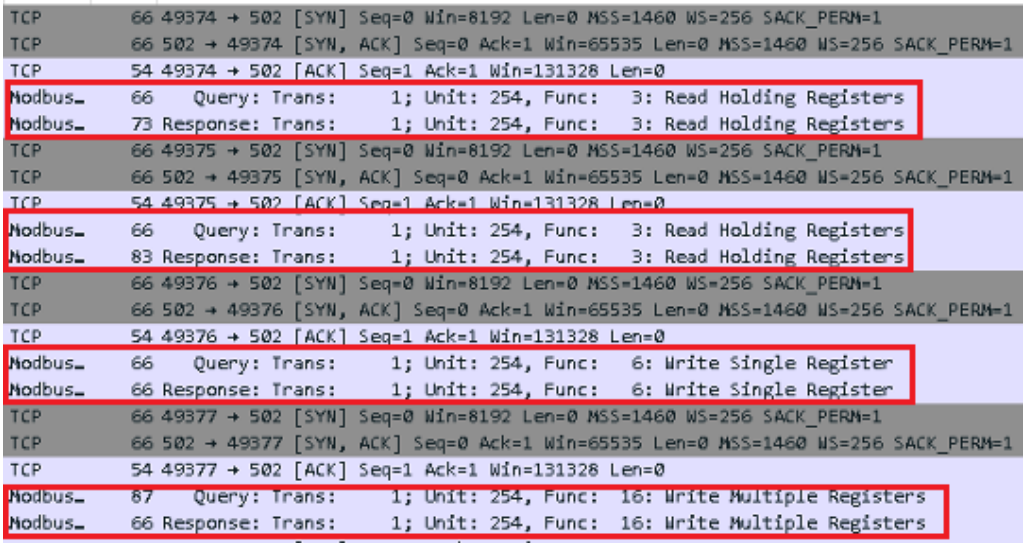
FrostyGoop binaries use a Go Modbus library retrieved from a publicly available Github repository.[4]

FrostyGoop implements three Modbus commands:

- **Command Code 3 'Read Holding Registers'** which is used to read the value currently in a Modbus holding register (or contiguous block of holding registers) [5]
- **Command Code 6 'Write Single Register'** which is used to write a value to a holding register[6]
- **Command Code 16 'Write Multiple Holding Registers'** which is used to write a value to a block of contiguous registers[7]

The figure below displays an example of Modbus TCP network traffic between FrostyGoop and a target device. In the example, FrostyGoop sends four commands to the device: Modbus function code 3 'Read Holding Registers' twice, function code 6 'Write Single Register', and function code 16 'Write Multiple Registers.'

[3] ENCO Control Configuration Instruction – Axis Industries
[4] Modbus Go Library – Github.com
[5] Modbus Application Protocol Specification – modbus.com
[6] Modbus Application Protocol Specification – modbus.com
[7] Modbus Application Protocol Specification – modbus.com



EXAMPLE OF FROSTYGOOP NETWORK TRAFFIC

Logging Capabilities

The FrostyGoop binaries log output from the Modbus TCP communications with the target IP address to a Windows console and a JSON file. FrostyGoop opens a console window upon execution. If the argument for logging is specified when executing the binary, then the output is logged to a JSON file. Below is an example of output to the console window during Modbus TCP communications with a device. Once the binaries are ready to begin communications with the target device, they log the local time and date, the target IP address when starting communications, and the string 'start' to the console window. Then, when FrostyGoop sends commands, it logs the holding register, the number of registers, a plus or minus depending on the response from the device for each command, and the time it took for a response. FrostyGoop logs a minus sign if the response from the device contains an exception. An example of when a device would send an exception to the malware would be if the holding register does not exist.

```
                    [runtime.goexit:asm_amd64.s:1598][INFO]                 ¦ (1/1)
¦ start
                    [main.TaskList.executeCommand:main.go:370][INFO]
 ¦ (1/1) ¦ address: 53370 count: 5 + ¦ 0s
                    [main.TaskList.executeCommand:main.go:370][INFO]
 ¦ (1/1) ¦ address: 53760 count: 10 + ¦ 15.625ms
                    [main.TaskList.executeCommand:main.go:370][INFO]
 ¦ (1/1) ¦ address: 53882 value: 0 + ¦ 0s
                    [main.TaskList.executeCommand:main.go:370][INFO]
 ¦ (1/1) ¦ address: 54272 count: 10 + ¦ 15.625ms
                    [runtime.main:proc.go:250][INFO] Time delta ¦ 2m3.5390625s
```

SAMPLE FROSTYGOOP CONSOLE LOG

2024 OT Cyber Attack Impacting Communities in Ukraine

The Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine (Служба безпеки України), shared details with Dragos of a cyber attack that took place in January 2024. Adversaries conducted a disruption attack against a municipal district energy company in Ukraine. At the time of the attack, this facility fed over 600 apartment buildings in a metropolitan area, supplying customers with central heating. Remediation of the incident took almost two days, during which time the civilian population had to endure sub-zero temperatures.

During the attack investigation, a discovery was made that adversaries possibly gained access to the victim network months earlier by exploiting an undetermined vulnerability in an externally facing router. Subsequently, the adversaries deployed a webshell with tunnel capabilities similar to ReGeorg[8], which was accessed predominantly via Tor IP addresses. The investigation revealed that the adversaries retrieved the contents of the Security Account Manager (SAM) registry hive, obtaining user credentials from the system. In January 2024, adversaries initiated L2TP (Layer Two Tunnelling Protocol) connections to Moscow-based IP addresses.

The victim network assets, which consisted of a router, management servers, and the district heating system controllers, were not adequately segmented within the network. A forensic examination during the investigation showed that the adversaries sent Modbus commands directly to the district heating system controllers from adversary hosts, facilitated by hardcoded network routes.

The affected heating system controllers were ENCO Controllers. The adversaries downgraded the firmware on the controllers, deploying a version that lacks monitoring capabilities employed at the victim facility, resulting in the Loss of View. The adversaries did not attempt to destroy the controllers. Instead, the adversaries caused the controllers to report inaccurate measurements, resulting in the incorrect operation of the system and the loss of heating to customers.

Dragos assesses that FrostyGoop, an ICS-related malware recently reported by Dragos, was used to facilitate this attack. FrostyGoop functionality uses the Modbus TCP protocol generically, meaning it could affect many devices. The associated FrostyGoop configuration file ("task_test.json") contained an IP address belonging to an ENCO control device exposed on the Internet, which leads Dragos to assess with medium confidence that before this attack, FrostyGoop was used to target one or more ENCO controllers where TCP port 502 was Internet accessible.

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 Ukraine.

[8] sensepost/reGeorg - Github

Assessing the Broader Impact on OT Cybersecurity

The discovery of the FrostyGoop ICS malware and its capabilities has raised significant concerns about the broader impact on OT cybersecurity. The specific targeting of ICS using Modbus TCP over port 502 and the potential to interact directly with various ICS devices pose a serious threat to critical infrastructure across multiple sectors.

The key findings suggest that FrostyGoop capabilities can be applied broadly. Modbus is embedded in legacy and modern systems and nearly all industrial sectors, indicating a wide-ranging potential for disrupting and compromising essential services and systems.

One of the major concerns is FrostyGoop's ability to communicate with ICS devices via the Modbus TCP protocol, enabling it to send commands to read or modify data on these devices. This represents a significant risk to the integrity and functionality of ICS devices, with potentially far-reaching consequences for industrial operations and public safety. The attack's involvement of internet-exposed controllers and insufficient network segmentation highlights the risks of not implementing basic cybersecurity controls and the importance of doing so. Currently, over 46,000 internet-exposed ICS devices communicate over Modbus TCP around the world.

Considering these developments, organizations, and defenders within critical infrastructure sectors must prioritize assessing and protecting their ICS networks. This includes restricting access to Modbus devices and conducting thorough network assessments to ensure they are not exposed to the Internet.

Dragos's ongoing analysis of FrostyGoop files and commitment to actively monitor the situation highlights the need for a coordinated response to a dynamic threat landscape. Vigilant network security monitoring, proactive defense measures, and collaborative information sharing will be crucial in mitigating the broad impact of ICS-specific malware, among other threats.

Guidance for Dragos Customers

FrostyGoop was first reported to Dragos WorldView[9] subscribers in late May 2024. Dragos Platform[10] detections were assessed against the threat, and indicators of compromise (IOCs) were deployed. Using the Dragos Platform, OT Watch has been hunting for FrostyGoop IOCs as part of regular sweeps across the fleet of subscribers since initial WorldView reporting to ensure coverage. OT Watch has also deployed a dashboard specific to FrostyGoop-related detections and IOCs for OT Watch customers, and an upcoming Knowledge Pack will deploy a FrostyGoop Playbook. Dragos continues to analyze FrostyGoop for future Dragos Platform Knowledge Pack releases to ensure appropriate detections are created and deployed.

The Dragos Platform detects FrostyGoop with threat detections already in place. Still, it is recommended that customers always deploy the latest Knowledge Pack (KP), including IOCs specific to this threat. For Dragos OT Watch[11] customers, our team has conducted searches for signs of this activity on your behalf – consider a lack of

[9] Dragos Worldview – Dragos.com
[10] Dragos Platform – Dragos.com
[11] Advanced Threat Hunting for Industrial Environments – Dragos.com

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[12] program, our collective defense platform. Any findings relating to this activity will be reported to you.

SID/Rule	Analytic Name	Description	Knowledge Pack
a0ddb920-0adc-4d01-9b3d-21414ef28607	Modbus Command Force Listen Only Mode	Modbus command to put device into Force Listen Only Mode, making the device unresponsive to commands. It will only respond after power up. This can be used maliciously to effectively disable devices.	KP_Plus-7.0.X
f7a0af6b-fa88-4382-9232-f56525befcde	Modbus Command Restart Communications Option	Modbus command to force a device to restart, making it unresponsive until it reboots. There is some chance this could be used maliciously to disable devices.	KP_Plus-7.0.X
f41c99e6-cabf-46b7-9576-d2ac4676baa9	Modbus Exception	Modbus servers send exception codes to Modbus clients when a requested operation cannot be carried out. This characterization summarizes exception codes sent from a Modbus server.	KP_Plus-6.0.X
e8cbde89-aa3a-4093-8064-3a8ca08fbf4c	Modbus External Comms	External device communicating with an internal asset using the Modbus protocol. This is a major security concern, as ICS devices should not be controlled outside of the OT network.	KP-2020-11
15c07ad4-5d03-4c3b-8d2d-613d5ec45217	Modbus External Write	External device writing to an internal asset using the Modbus protocol. This is a major security concern, as ICS devices should not be controlled outside of the OT network.	KP-2020-11
3cc434cd-5086-454c-bbd4-6142b01a4623	Modbus Write Observed for First Time	Modbus traffic with a write function code seen for the first time to a specific host.	KP-2022-009
d323014b-abee-461b-a12f-641b8796070f	New ModbusTCP Detection	Monitors for new devices using the ModbusTCP protocol and generates events when activity is seen	KP-2020-11

Summary Guidance

1. **Identify impacted assets:** Access your Asset Inventory and search for ENCO control servers and devices communicating over Modbus.

[12] Dragos Neighborhood Keeper - dragos.com

2. **Look for potential malicious behavior:** Review the FrostyGoop-specific dashboard to determine if related detections and IOCs have been triggered.
3. **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 mechanisms 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.

Dragos WorldView 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 situational awareness 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.

Recommendations – Implement 5 Critical Controls

The cyber threat characterized by deploying the FrostyGoop 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 5 Critical Controls for World-Class Cybersecurity, as recommended by SANS, 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. Here, we detail the necessity and application of these controls in the context of this threat.

1. ***ICS INCIDENT RESPONSE***
   Given the complexity and targeted nature of the FrostyGoop attack, a robust incident response plan is crucial. This plan should incorporate specialized responses for OT environments, as these systems often have operational continuity requirements that supersede traditional IT systems. For FrostyGoop, which directly interacts with ICS via Modbus commands, the response plan should include procedures for quickly isolating affected devices, analyzing network traffic for unauthorized Modbus commands, and restoring accurate system operations. Training and regular drills specific to Modbus and ICS-targeted attacks will also ensure preparedness and effective incident management.
2. ***DEFENSIBLE ARCHITECTURE***
   This attack highlights the lack of adequate network segmentation and the presence of internet-exposed controllers. To combat threats like FrostyGoop, a defensible architecture must be implemented, prioritizing the segmentation of network assets. This includes establishing industrial demilitarized zones (DMZs), enforcing strict access controls between the corporate IT network and OT environments, and using physical or virtual

barriers to prevent direct access from the internet to critical systems. Such measures would limit the spread of malware and restrict the blast radius of potential cyber attacks.

3. ***ICS NETWORK VISIBILITY & MONITORING***
   Continuous monitoring of the OT network traffic, like Modbus TCP communications, is essential to detect and respond to anomalies and threat behaviors. In the case of FrostyGoop, having a protocol-aware monitoring toolset could have identified unauthorized access or unusual Modbus TCP traffic patterns over port 502, enabling quicker detection and mitigation. Implementing a comprehensive monitoring solution, such as the Dragos Platform, that includes anomaly and behavioral detection will significantly enhance visibility into network operations and potential threats.
4. ***SECURE REMOTE ACCESS***
   The FrostyGoop incident exploited vulnerabilities associated with remote access points. Secure remote access protections must be strictly enforced to safeguard against similar threats. This includes deploying multi-factor authentication (MFA), ensuring all remote connections are logged and monitored, and using virtual private networks (VPNs) to encrypt data in transit. Furthermore, remote access should be granted on a need-to-use basis with regular audits to review access rights and privileges.
5. ***RISK-BASED VULNERABILITY MANAGEMENT***
   Effective vulnerability management tailored to the risk profile of ICS components would involve regular assessments to identify and address vulnerabilities that adversaries could exploit. Mitigating network exploitable vulnerabilities is vital, especially when evidence of active exploitation exists. Where patches are not feasible, compensating controls such as enhanced monitoring or restrictive access controls will mitigate the potential risks.

Conclusion

The discovery and analysis of the FrostyGoop ICS malware underscore the significant risks posed to OT environments. FrostyGoop's capabilities to interact with ICS devices via Modbus TCP and its undetected status by antivirus vendors highlight the critical need for robust OT cybersecurity measures. The cyber attack on the municipal district energy company in Ukraine, is a stark reminder of the potential real-world impacts of such vulnerabilities, emphasizing the necessity for adequate security controls and continuous OT network security monitoring. Organizations must prioritize the implementation of comprehensive cybersecurity frameworks to safeguard critical infrastructure from similar threats in the future.

ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. 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.

Dragos WorldView Threat Intelligence arms your organization with in-depth analysis and reporting into cyber threats targeting OT environments around the world. Request a demo at:

Request a Demo

info@dragos.com @DragosInc @Dragos, Inc.