SANS
INDUSTRIAL CONTROL
SYSTEMS SECURITY

The Story of KurtLar_SCADA

From Malware Discovery to Victim Notification

Sam Hanson

Website: sam-hanson.space | X: @__samhanson__ | BlueSky: @sam-hans0n.bsky.social

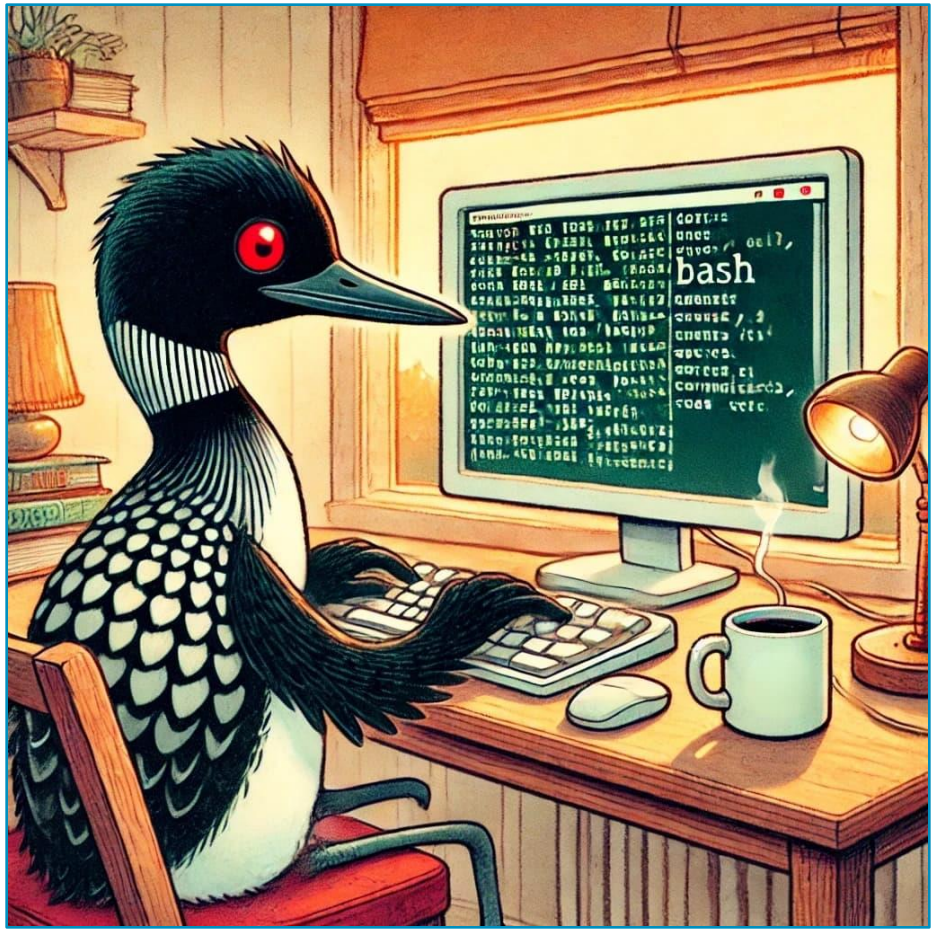
>> whoami

Associate Principal Vulnerability Analyst at Dragos

I dabble in:

- Vulnerability analysis and research
- Malware analysis
- Threat hunting

All specifically focused on identifying cyber threats/risks to industrial systems.



We’ve All Heard About Hacktivism Recently…

It’s been in the news quite a bit this past year.

NBC News

Treasury says Iranian hackers posed as anti-Israel activists

The Treasury Department named and sanctioned six Iranian military hackers Friday, accusing them of cyberattacks against U.S. water...

Feb 2, 2024

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia’s Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin’s Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn’t dare to.

CNN Politics SCOTUS Congress Facts First 2024 Elections Watch Liste

Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says

By Sean Lyngaas, CNN

5 minute read · Published 6:07 AM EDT, Wed April 17, 2024

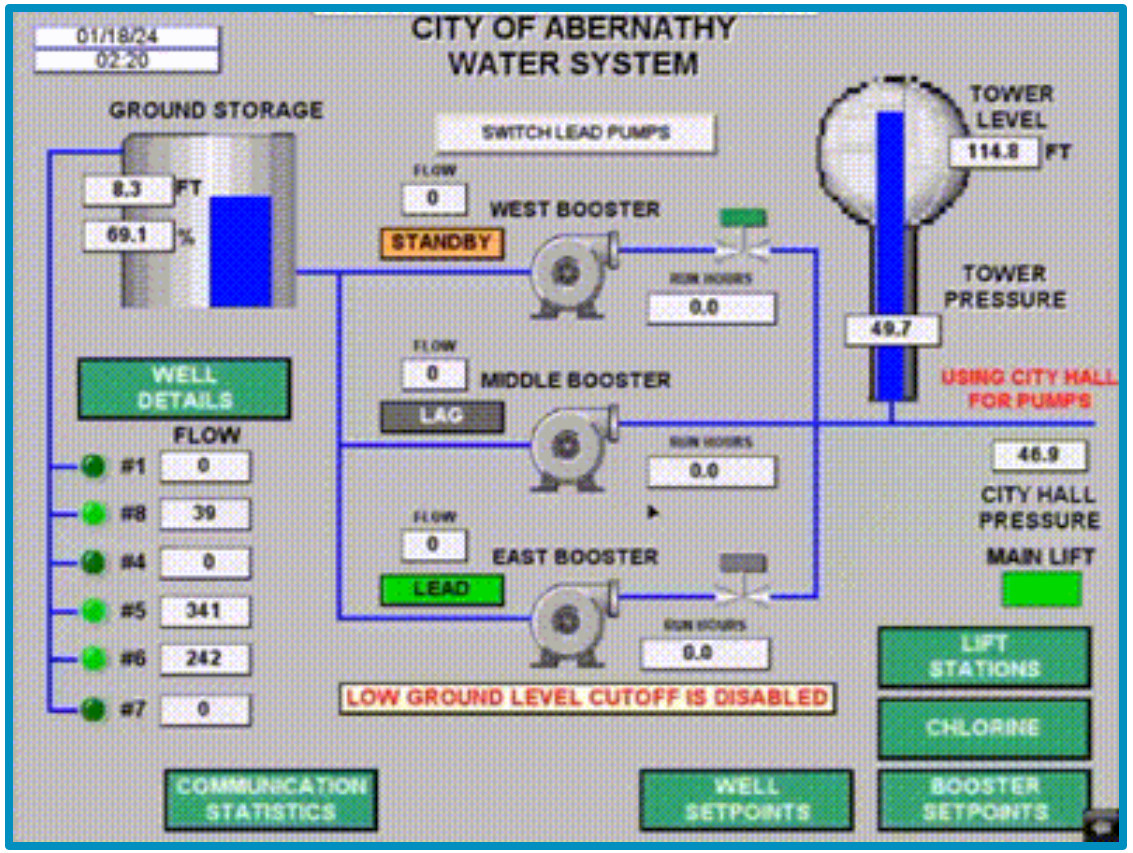
Cyber Army of Russia Reborn

Compromised Internet-exposed, poorly secured devices over VNC.

- Impacted sectors include water and wastewater, oil and natural gas in California, Florida, Texas, and Pennsylvania.
- Regional targeting based on geopolitical events
- Achieved Stage 2 of the ICS cyber kill chain by modifying HMI values

"Despite CARR briefly gaining control of these industrial control system, instances of major damage to victims have thus far been avoided due to CARR's lack of technical sophistication."

-- U.S. Dept. of the Treasury



CARR poking around a compromised HMI

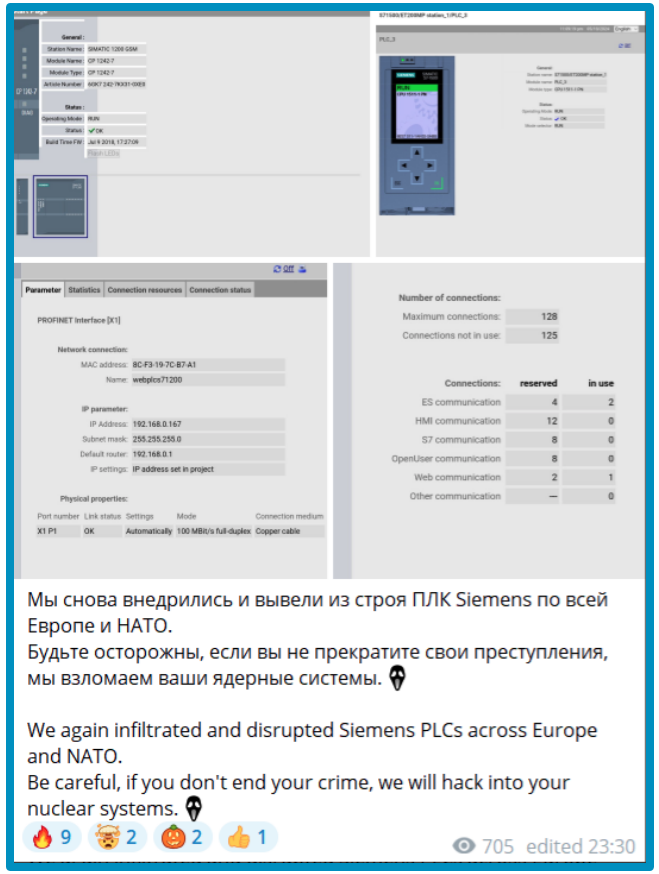
Hunt3r Kill3rs

Claimed compromise of exposed Siemens and Unitronics PLCs.

Another opportunistic hacktivist group

- Use Telegram to advertise their activity
- Leverage default credentials

Appear to have reached Stage 2 of ICS Cyber Kill Chain 3 times by modifying fields and resetting device passwords.



CyberAv3ngers

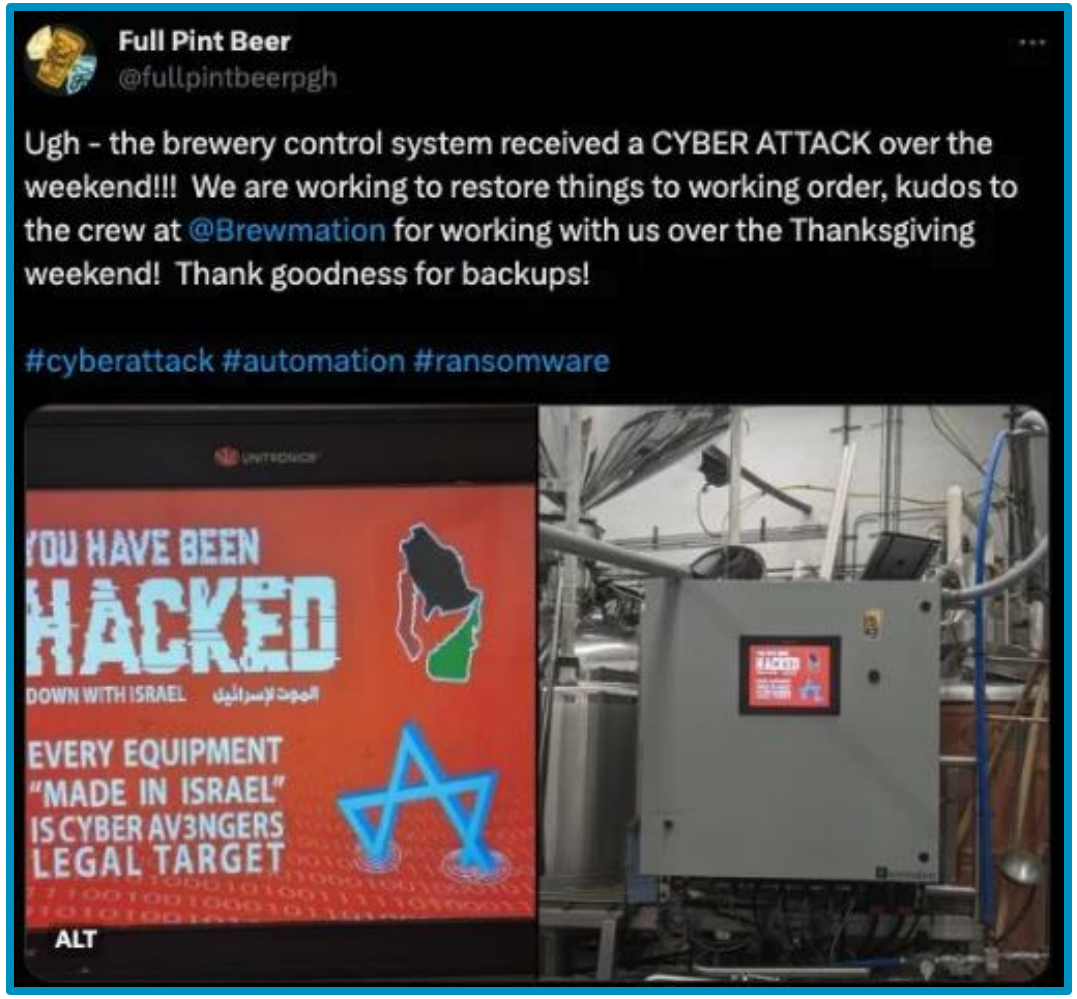
Compromised Israeli-made Unitronics PLCs/HMIs, spanning multiple countries.

IOCONTROL publicly attributed to CyberAv3ngers

Pro-Iranian hacktivist persona, CISA affiliates with IRGC

CYBERSECURITY ADVISORY

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities



The List Goes On and On

There are plenty more that haven't been covered in the media.

- Most exaggerate their claim to sensationalize.

They care more about the attention received than the actual impact of the attack.

So, What Does 'Hacktivism' Look Like?

There are a few patterns:

- Geopolitically motivated
- Utilizes encrypted messaging services (e.g. Telegram)
- TTPs
  - Internet-exposed devices
  - Default credentials
  - Open-source tools
- Primarily opportunistic

Stage 2 ICS Kill Chain - Do they know what they're doing? Debatable.

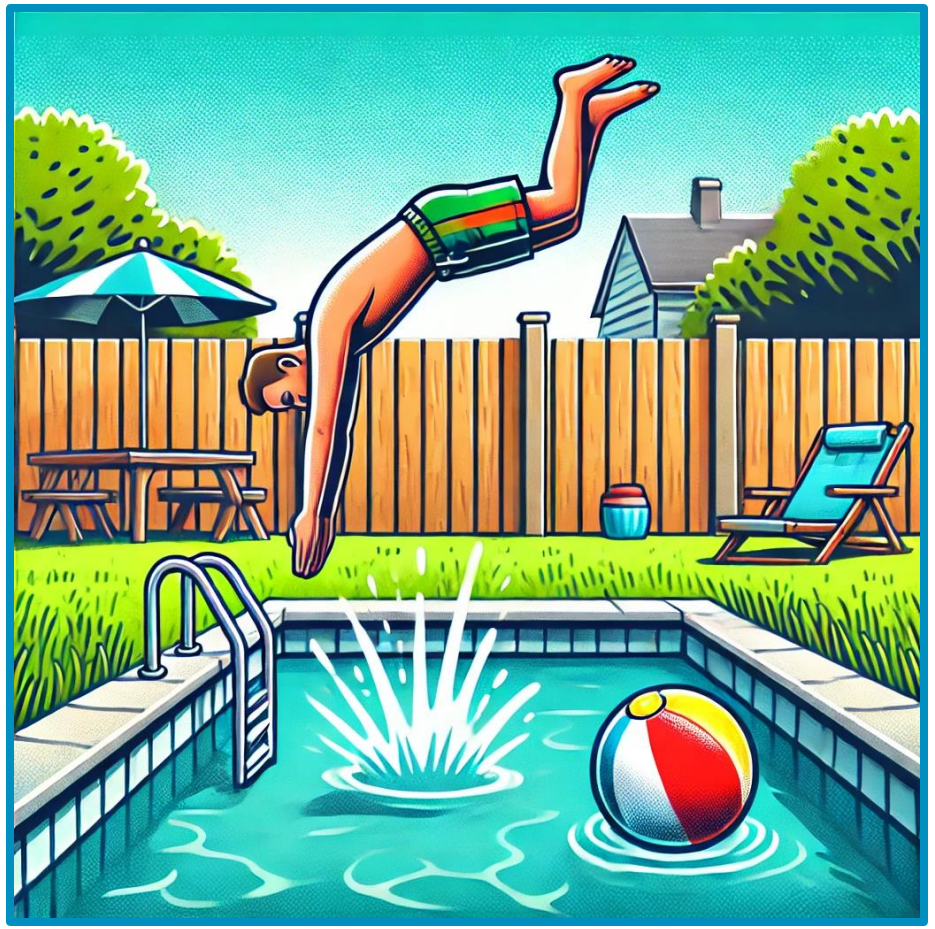
This Presentation will Introduce Another

We will cover:

- Discovery
- Analysis
- Victim Notifications

And along the way learn about:

- Malware analysis
- Threat hunting



VirusTotal

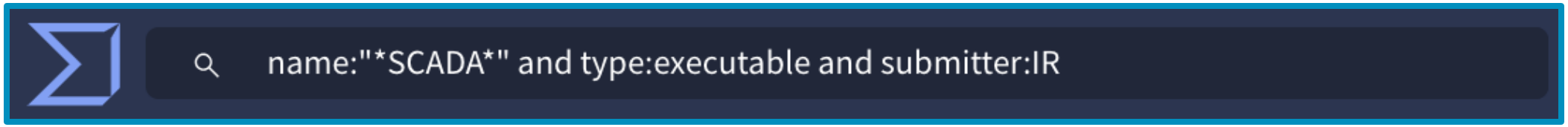
...a massive repository of files that users upload to when they suspect a file is malicious.

- Free comprehensive antivirus scan!

VT Enterprise users can hunt through files for malicious activity.

Threat Hunting in VirusTotal

VirusTotal queries can be quite powerful for narrowing down the search space.

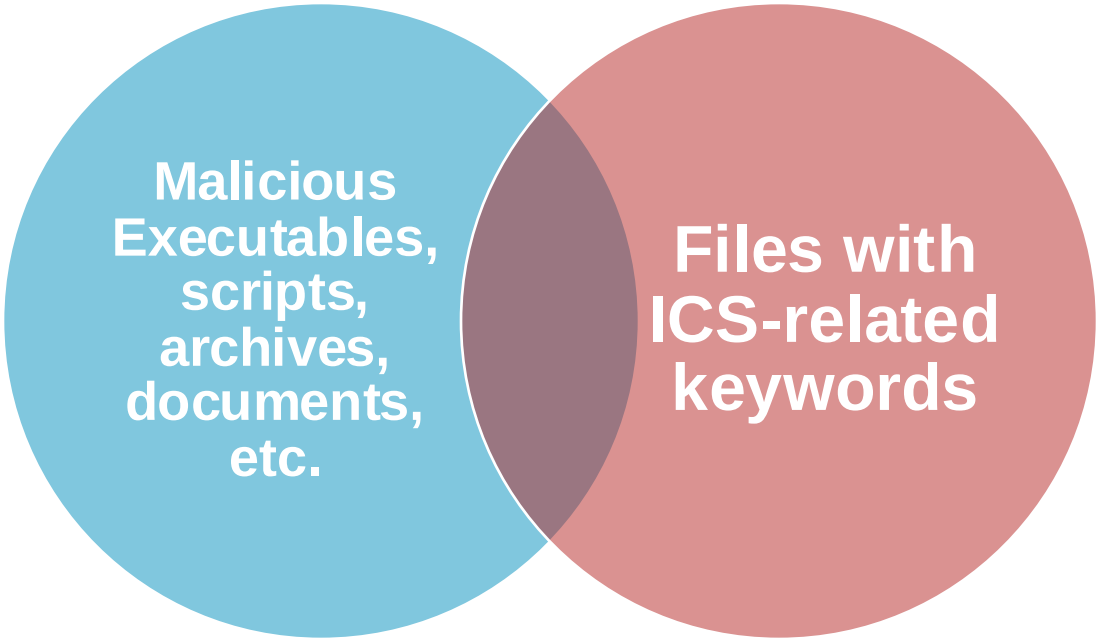


Try dozens of query combinations, it can be a game of numbers!

More Advanced Searching Mechanisms

Yara: a rule-based language to identify malware.

- Highly efficient way to comb through massive amounts of data




```
rule detect_ics_compiled_python {
    strings:
        $ics1 = "BACnet"
        $ics2 = "modbus"
        $ics3 = "OPCUA"
        $ics4 = "ControlNet"
        $ics5 = "s7comm"
        $ics6 = "Rockwell Automation"
        $ics7 = "Schneider Electric"
        // ...
    condition:
        is_compiled_python and 3 of ics_keywords
}
```

More Advanced Searching Mechanisms

RetroHunts: mechanism to search files collected on VT from the past year

LiveHunts: enables continuous monitoring, running provided rule against all future uploads.

Finding KurtLar_SCADA

name:"*SCADA*" AND type:python AND submitter:IR

Summary - 1/1 Files	Associations	Detections	First seen	Last seen	Submitters	
1df6ea128bc9866f6564cfb3d01d3065469e3ca304b4a47a… kurtlar_scada (1).py python idle	-	0 / 64	2024-09-09 20:03:26	2024-11-11 20:02:10	2	108.62 KB

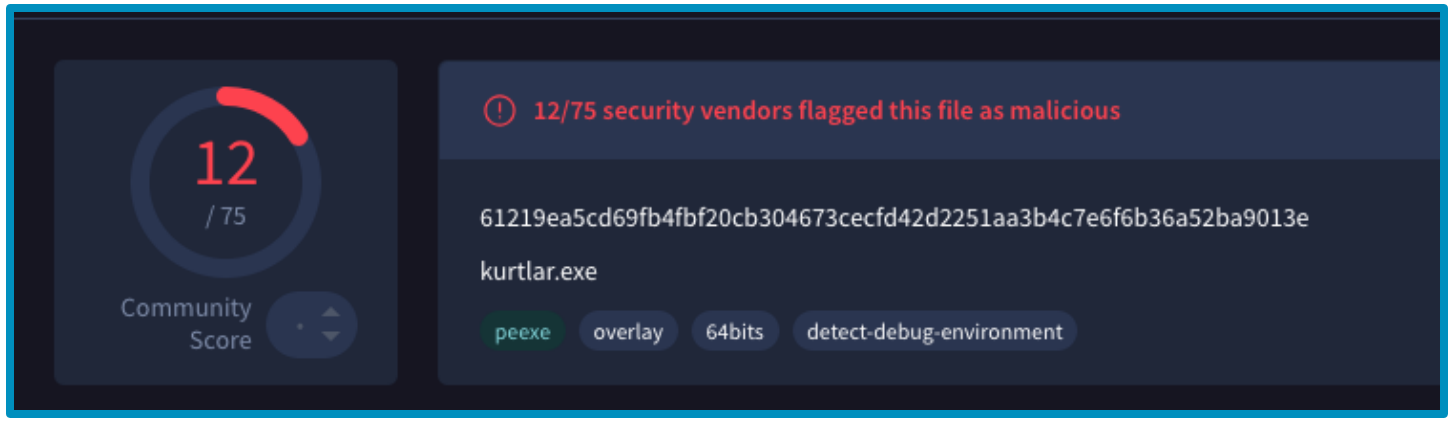
What Made it Look Suspicious?

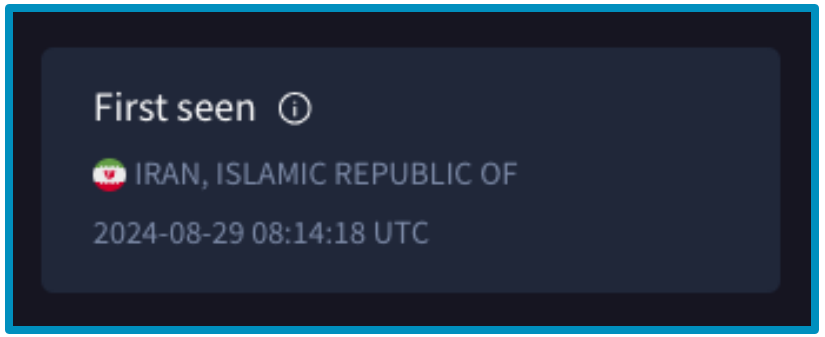
VirusTotal has a nifty “Preview file” feature!

Strings Hex Preview

```
import marshal
min =
b'\xe3\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x07\x00\x00\x00\x00\x00\x
\x02\x00\x00\x00\x00\x00\x00Z\x00\x02\x00G\x00d\x02\x84\x00d\x03\xab\x02\x00\x0
08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00j\n\x
j\r\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xab
\x01\x00\x00\x00\x00\x00\x00\x01\x00\x02\x00e\x03j\x10\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x01\x00d\x04d\x05l\tZ\td\x04d\x05l\nZ\nd\x04d\x05l\x0bZ\x0b\t\x0
\x02g\x00c\x02]0\x00\x00}\x00\x02\x00e\tj"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xab\x00\x00\x00\x00\x00\x00\x00\xab
00\x00\x00\x00\x00\x00\x00\x00\x00\xab\x00\x00\x00\x00\x00\x00\x00\x91\x02\x8c2
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00e\x14d\x0b\xac\x0c\xab\x02
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xab\x0
\x00\x00\x00\x00\x00\x00Z\x17\x02\x00G\x00d\x0f\x84\x00d\x10\xab\x02\x00\x00\x0
```

KurtLar.exe

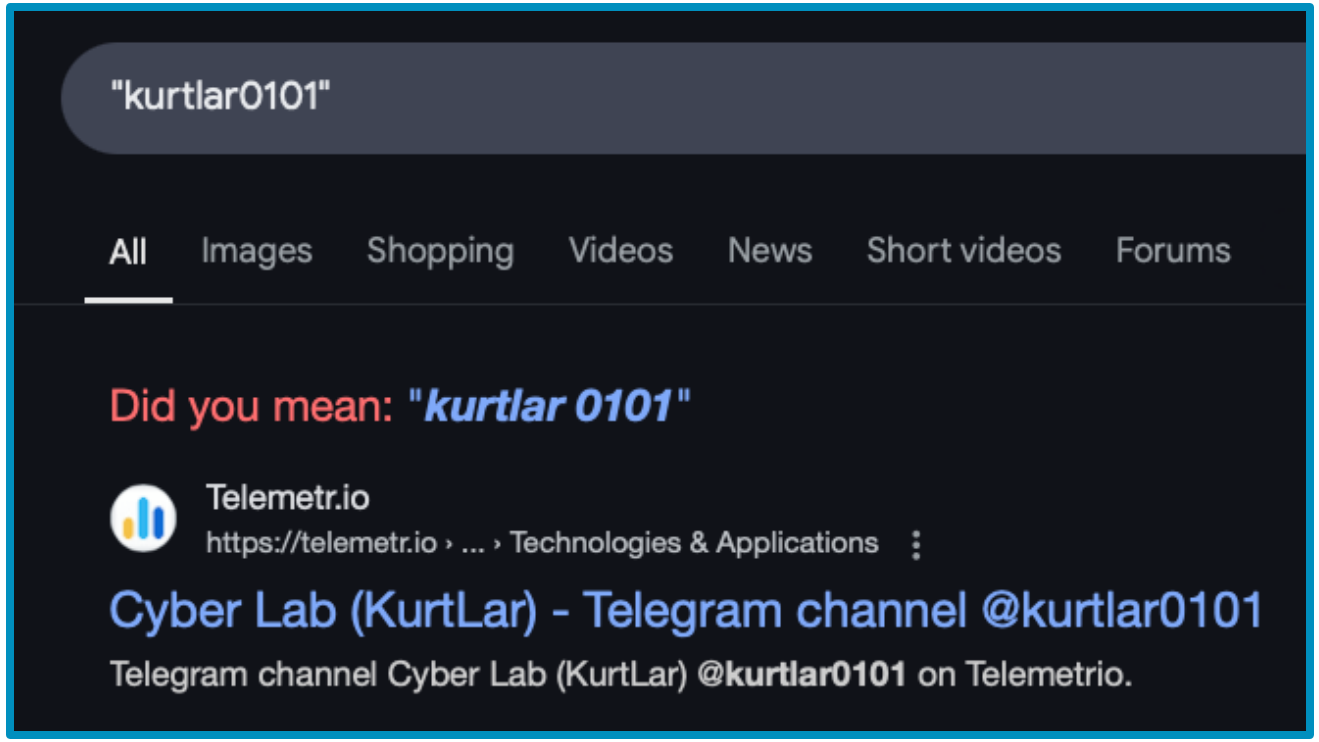

12
/ 75
Community Score
12/75 security vendors flagged this file as malicious
61219ea5cd69fb4fbf20cb304673cecfd42d2251aa3b4c7e6f6b36a52ba9013e
kurtlar.exe
peexe
overlay
64bits
detect-debug-environment


First seen
IRAN, ISLAMIC REPUBLIC OF
2024-08-29 08:14:18 UTC


@KURTLAR0101
USAGE : file IP-LIST.txt combo(y,n)

Discovering the Telegram Channel

You can discover a lot by googling unique artifacts!

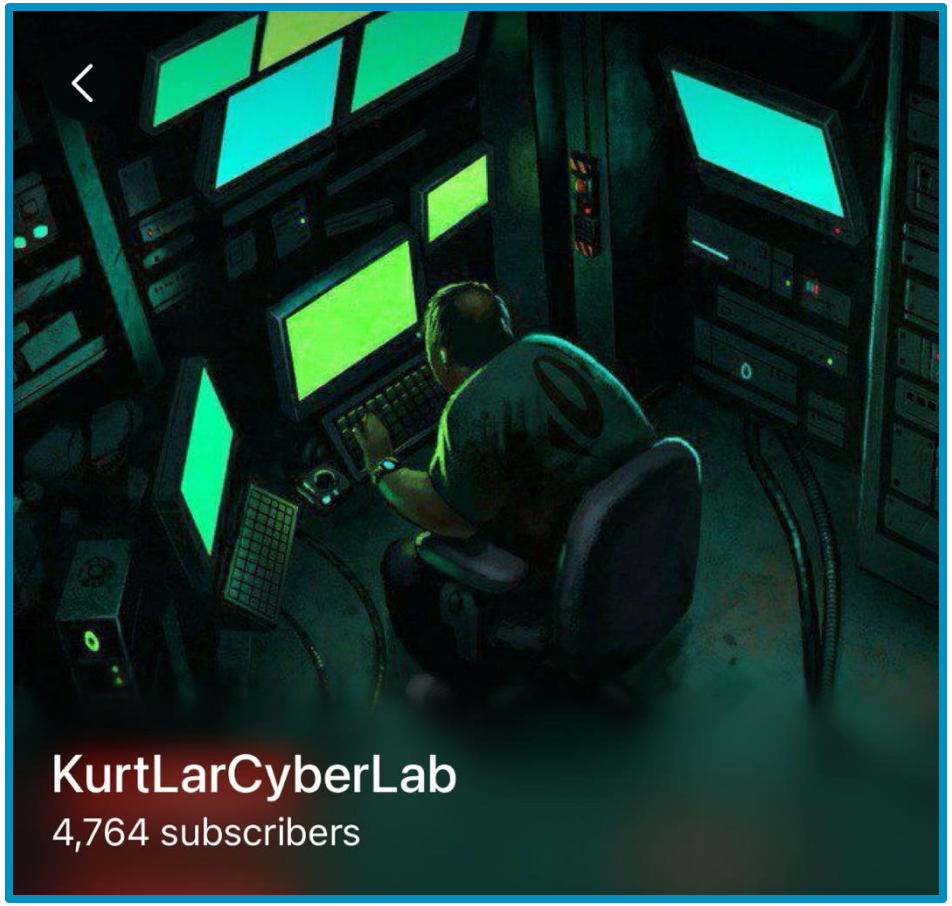


KurtLarCyberLab Telegram Channel

KurtLarCyberLab boasts over 4500 members

Administrator operates several back-up and VIP channels.

- After Durov's arrest, the administrator archived the old channel and created several new ones.



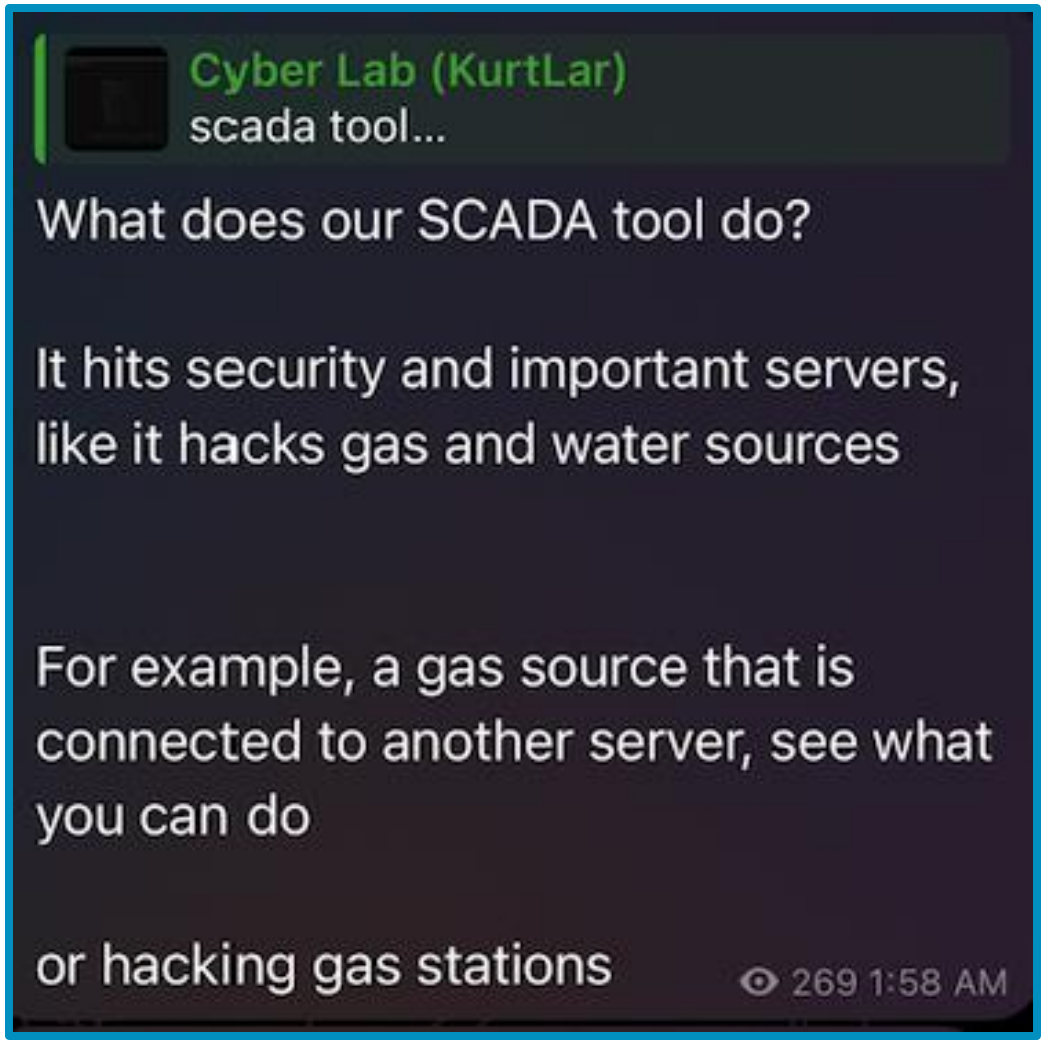
Pro-Iranian Ideology

The administrator makes their ideology very clear

- Pro-Iran
- Offers discounts to tools for those targeting USA or Israel

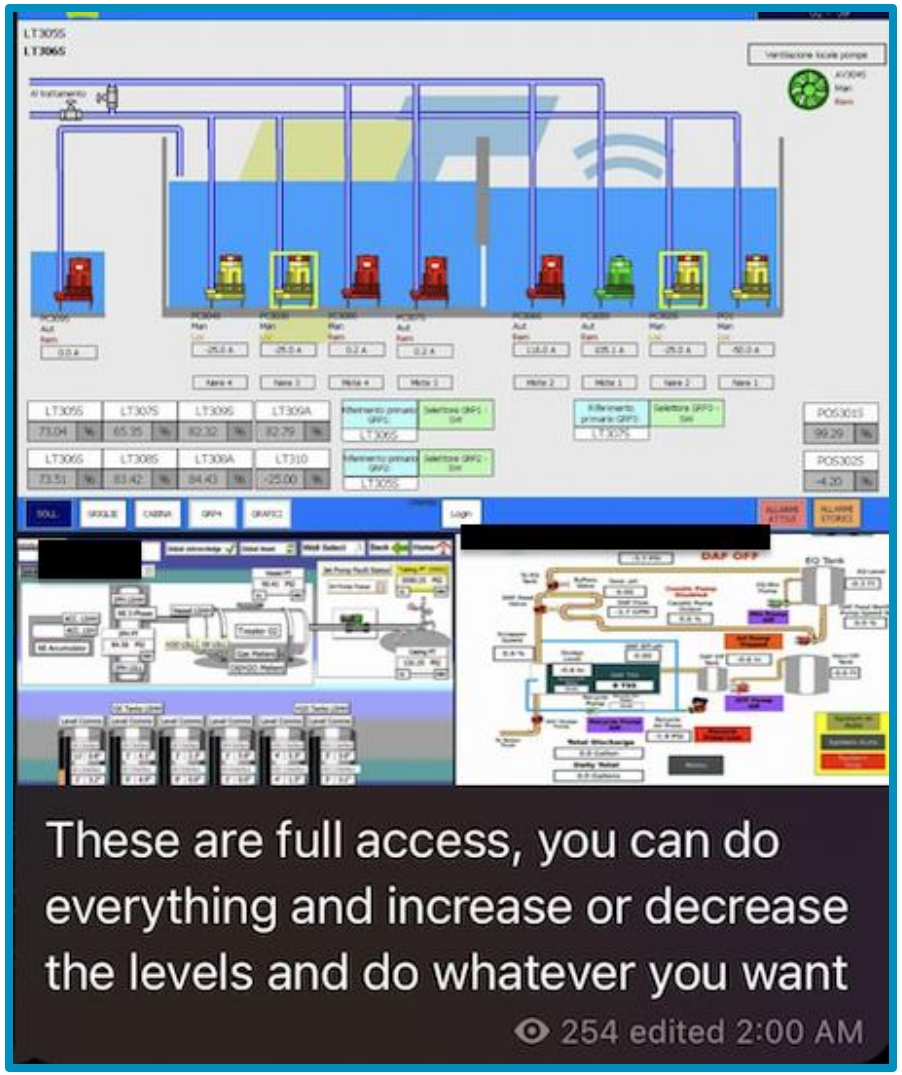
Telegram channel description claims they're an anti-terrorism channel.

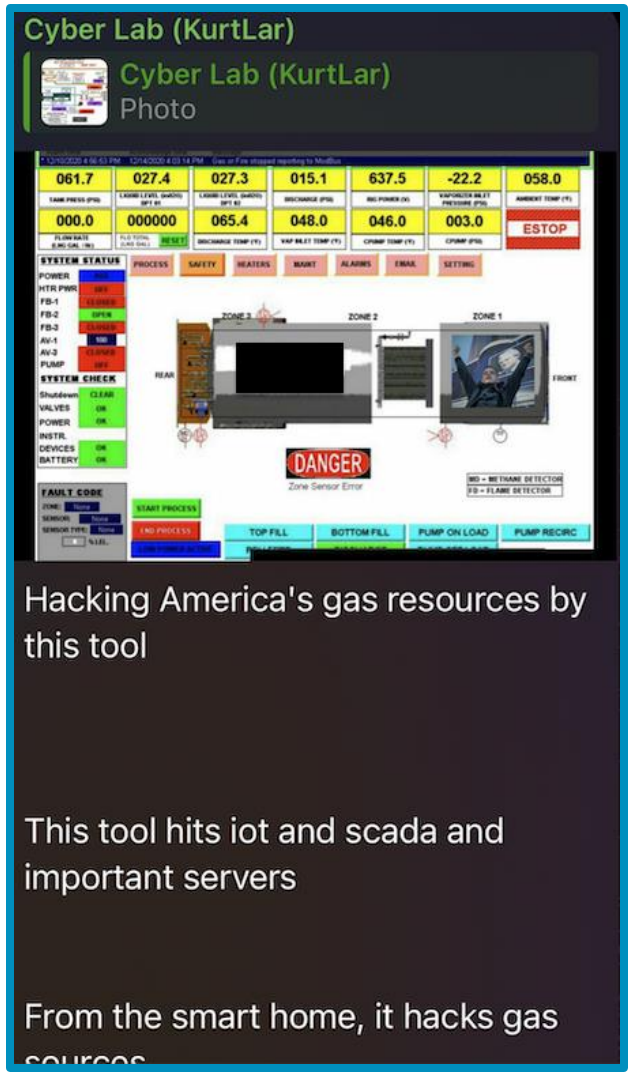
Telegram Channel Advertisements



Telegram Channel Advertisements

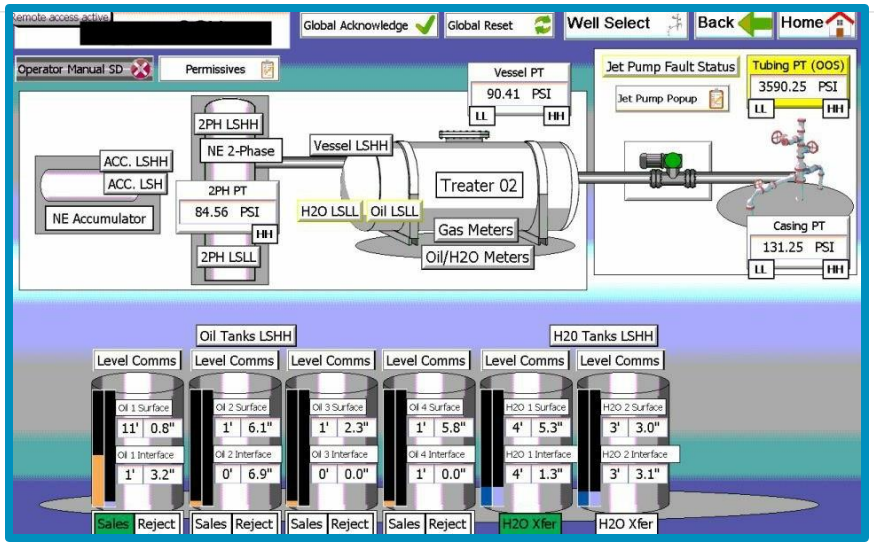
Very clearly motivated to hack American/Israeli industrial systems



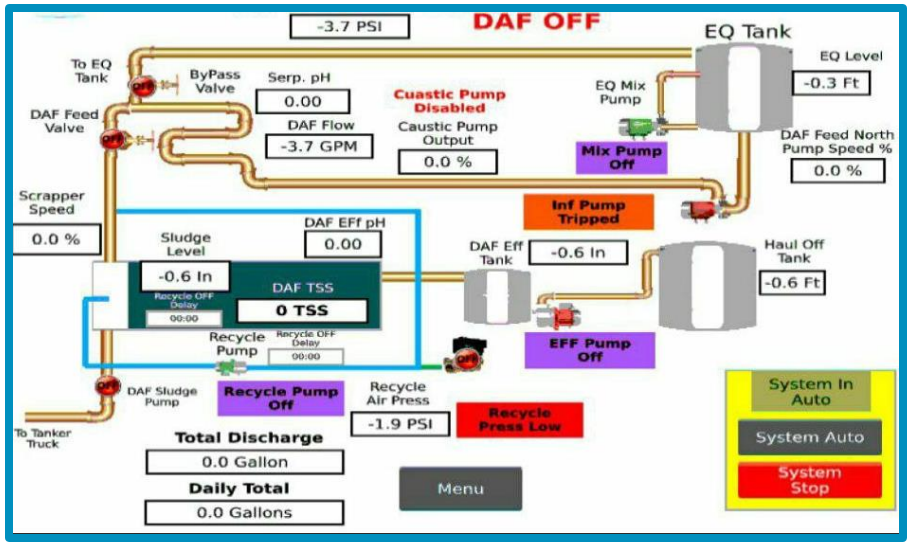


Telegram Channel Advertisements

Oil drilling operations.



Tanker truck washing water treatment site.



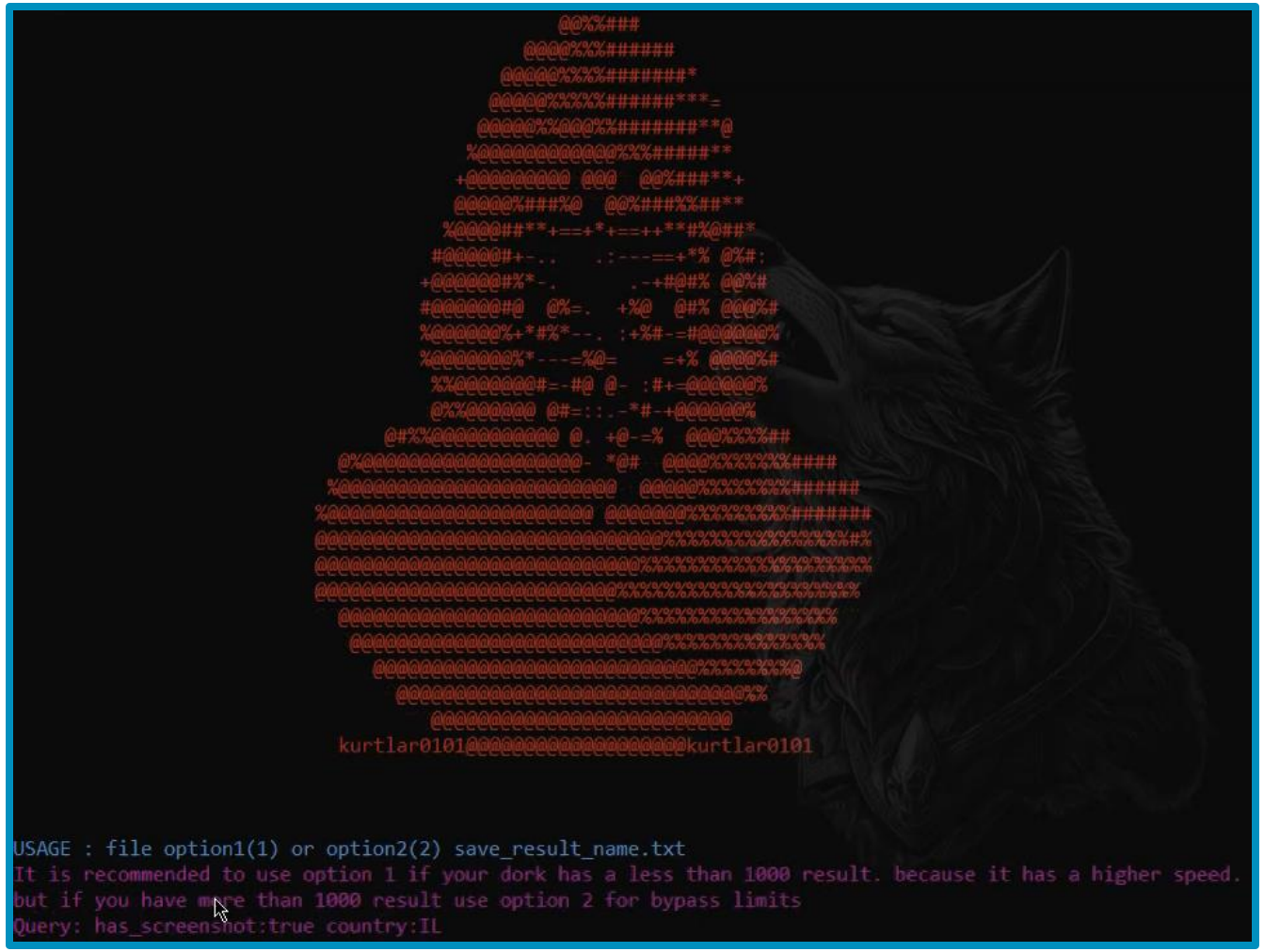
Full Product Offerings

SpyLens – access internet-exposed IP cameras

SMS Bomber – send mass texts, likely for scamming purposes.

Shodan Grabber – bypass monthly Shodan query credits

ShellFinder – exploit vulnerable web servers then uploads web shell



Timeline at Discovery

Tool advertised on Telegram

KurtLar_SCADA.py uploaded to VT

08/14/24

09/09/24

08/29/24

10/09/24

KurtLar.exe uploaded to VT

Discovery of the samples

Analysis Goals

What we know:

- Tool is *advertised* as SCADA/HMI remote access capability.

What we don't know:

- Are the claims in the Telegram channel legitimate?
- How does it work?

Goals:

- Understand how it works!
- Can we identify the victims?

Kurtlar.exe

Crowdsourced YARA rules

⚠ Matches rule PyInstaller from ruleset PyInstaller at https://github.com/bartblaze/Yara-rules by @bartblaze

↳ *Identifies executable converted using PyInstaller. This rule by itself does NOT necessarily mean the detec*

```
Error loading Python DLL '%s'.
Failed to pre-initialize embedded python interpreter!
Failed to allocate PyConfig structure! Unsupported python version?
Failed to set python home path!
Failed to start embedded python interpreter!
bpython312.dll
8python312.dll
```

Compiled Python

A mechanism to bundle Python bytecode and the Python interpreter into one executable.

pyinstaller

python : py2exe

Why is this desirable?

- All dependencies are bundled; no version worries!
- Python has lots of open-source library support.

JoelBender / bacpypes Public

pymodbus-dev / pymodbus Public

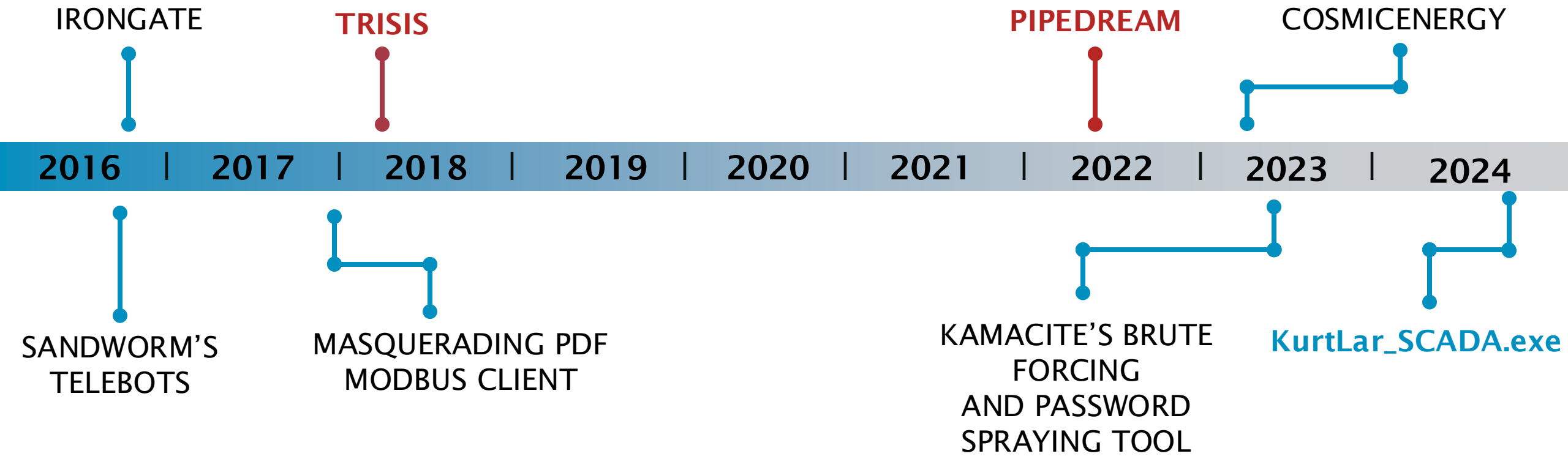
FreeOpcUa / python-opcua Public

dmroeder / pylogix Public

...

ICS "Threats" Have Often Used Compiled Python

Lots of nuance to discuss here!



Decompiling is Usually Easy

Source code is represented as Python bytecode contained in the executable.

- Extract bytecode and turn it back to Python!

The typical process (PyInstaller):

```
./python3.12 pyinstxtractor.py kurtlar.exe
```

↓

```
pycdc kurtlar_scada.pyc
```

↓

```
kurtlar_scada.py
```

However, KurtLar_SCADA Does Not Decompile

However, reliable tools fail for Python v3.10 and later!

Thankfully, new tools exist!

The typical process:

```
./python3.12 pyinstxtractor.py kurtlar.exe
```

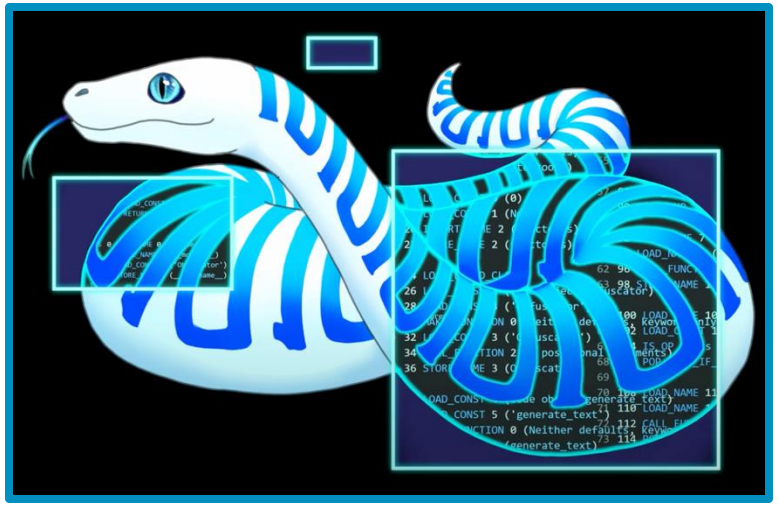
↓

```
pycdc kurtlar_scada.pyc
```

↓

~~kurtlar_scada.py~~

Transformer AI Models Can Help



PyLingual can turn PYC files → Python source

PYC Disassembly

Static analysis is quite doable with PYC file.

- Why not then read the assembly?

One word: obfuscation

```
...
LOAD_CONST
STORE_FAST

SETUP_LOOP
LOAD_NAME
LOAD_CONST
...
```

KurtLar_SCADA.exe Obfuscation Techniques

A couple of obfuscation layers are utilized across the samples:

- Marshalling python bytecode
- Hex-encoded strings
- Symbol obfuscation

Mostly easy to defeat; variable/function renaming is a PITA for static analysis.

```
[Code]
    File Name: r.py
    Object Name: __OOOOOOOOOOOOOOOO
    Qualified Name: OOOOOOOOOOOOOOOO.__OOOOOOOOOOOOOOOO
    Arg Count: 8
    Pos Only Arg Count: 0
    KW Only Arg Count: 0
    Stack Size: 2
    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
    [Names]
        ' OOOOOOOOOOOOOOOO  OOOOOOOOOOOOOOOO'
    [Locals+Names]
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
        'OOOOOOOOOOOOOOOO'
```

Defeating Marshalled Python Bytecode

This is a Python script that contains another Python script

- Inner-most script is represented via byte string
- Leverages internal library to deserialize, load, and execute payload.

```
import marshal

min = b'\xe3\x00\x00\x00<PYTHON_BYTECODE>\xde\x01\x00\x00'
ob = marshal.loads(min)
exec(ob)
```

Defeating Marshalled Python Bytecode

Easily defeated by modifying wrapper script

```
import marshal

min = b'\xe3\x00\x00\x00<PYTHON_BYTECODE>\xde\x01\x00\x00'
ob = marshal.loads(min)
exec(ob)

```

```
import marshal
import importlib

min = b'\xe3\x00\x00\x00<PYTHON_BYTECODE>\xde\x01\x00\x00'
ob = marshal.loads(min)
# exec(ob) # IT IS IMPERATIVE THIS LINE IS COMMENTED OUT
bytecode = importlib._bootstrap_external._code_to_timestamp_pyc(ob)
with open("./kurtlar_scada.pyc", "wb") as pyc_file:
    f.write(bytecode)


```

Hex-encoded Strings

ASCII values are hex-encoded.

Useful for avoiding detections like Yara

```
'53757370656e64'
'50726f6772657373732054656c6572696b20466964646c657220576562
'466964646c6572'
'576972657736861726b'
'64756d70636170'
'646e537079'
'646e5370792d783836'
'6368656174656e67696e652d7838365f3634'
'485454504465627567676572549'
'50726f636d6f6e'
'50726f636d6f6e3634'
'50726f636d6f6e363461'
'50726f636573734861636b6572'
'783332646267'
'783634646267'
'446f744e657444617461436f6c6c6563746f723332'
'446f744e657444617461436f6c6c6563746f723634'
'485454504465627567676572537663'
'485454502044656275676765726'
'696461'
'6964613634'x
'69646167'
'696461673634'
'69646177'
'696461773634'
'69646171'
'696461713634'
'69646175'
```

Decoding Hex to ASCII with CyberChef

Recipe

Find / Replace

Find: ... REGEX | Replace | ☑ Global match | ☐ Case insensitive

☑ Multiline matching | ☐ Dot matches all

Find / Replace

Find: ' REGEX | Replace | ☑ Global match | ☐ Case insensitive

☑ Multiline matching | ☐ Dot matches all

Pad lines

Position: End | Length: 2 | Character: 0a

From Hex

Delimiter: Auto

Output

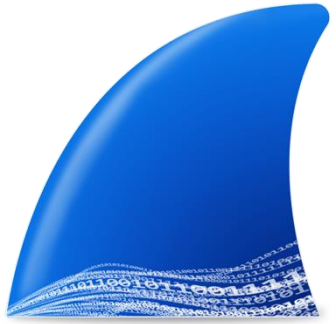
```
Suspend
Progress Telerik Fiddler Web Debugger
Fiddler
Wireshark
dumpcap
dnSpy
dnSpy-x86
cheatengine-x86_64
HTTPDebuggerUI
Procmon
Procmon64
Procmon64a
ProcessHacker
x32dbg
x64dbg
DotNetDataCollector32
DotNetDataCollector64
HTTPDebuggerSvc
HTTP Debugger
ida
ida64
idag
idag64
idaw
idaw64
```

...

Anti-analysis Checks

Hex-encoded strings are process names for common malware analysis tools

- If found during execution, the program terminates.

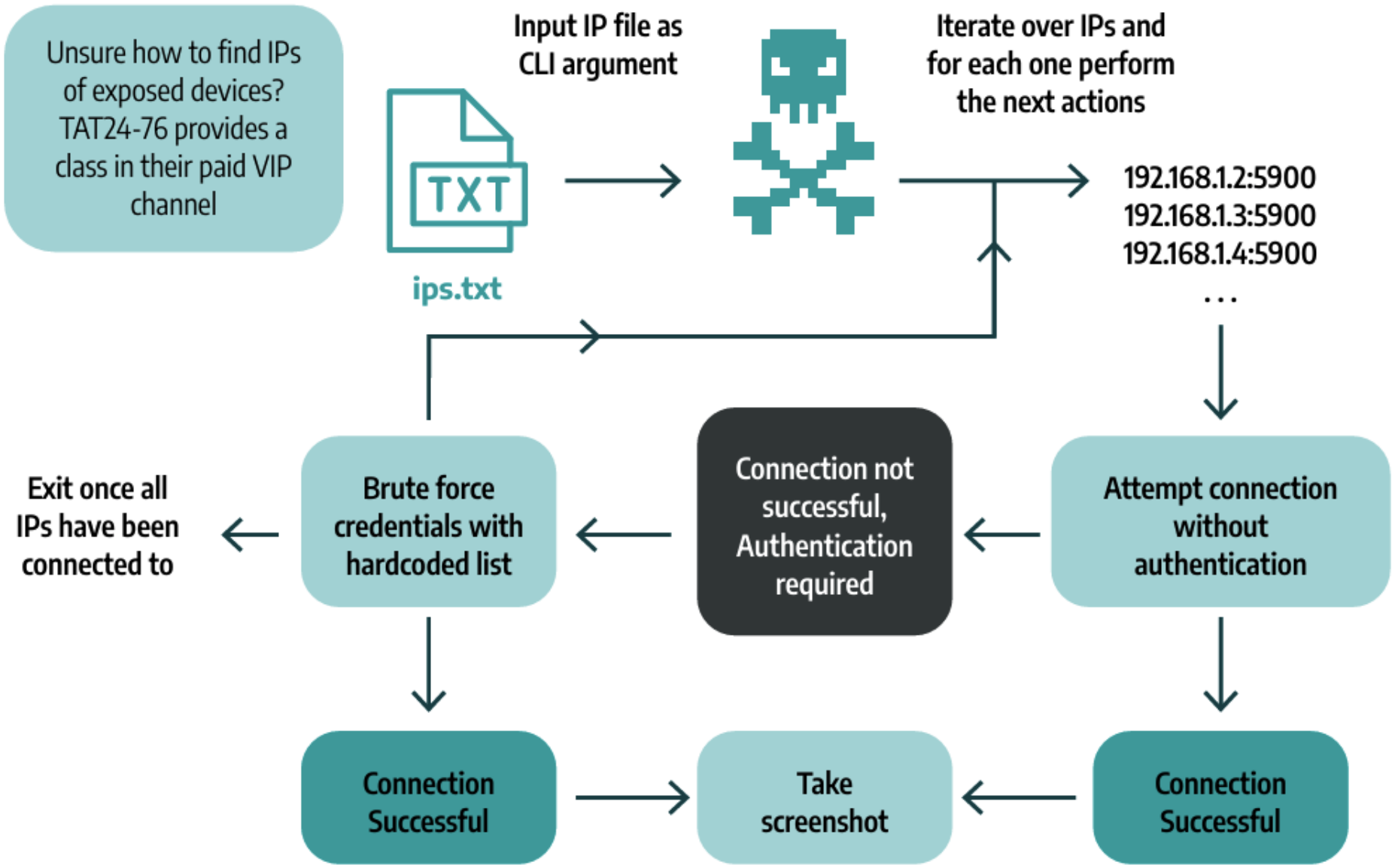


Uncovering KurtLar_SCADA.exe

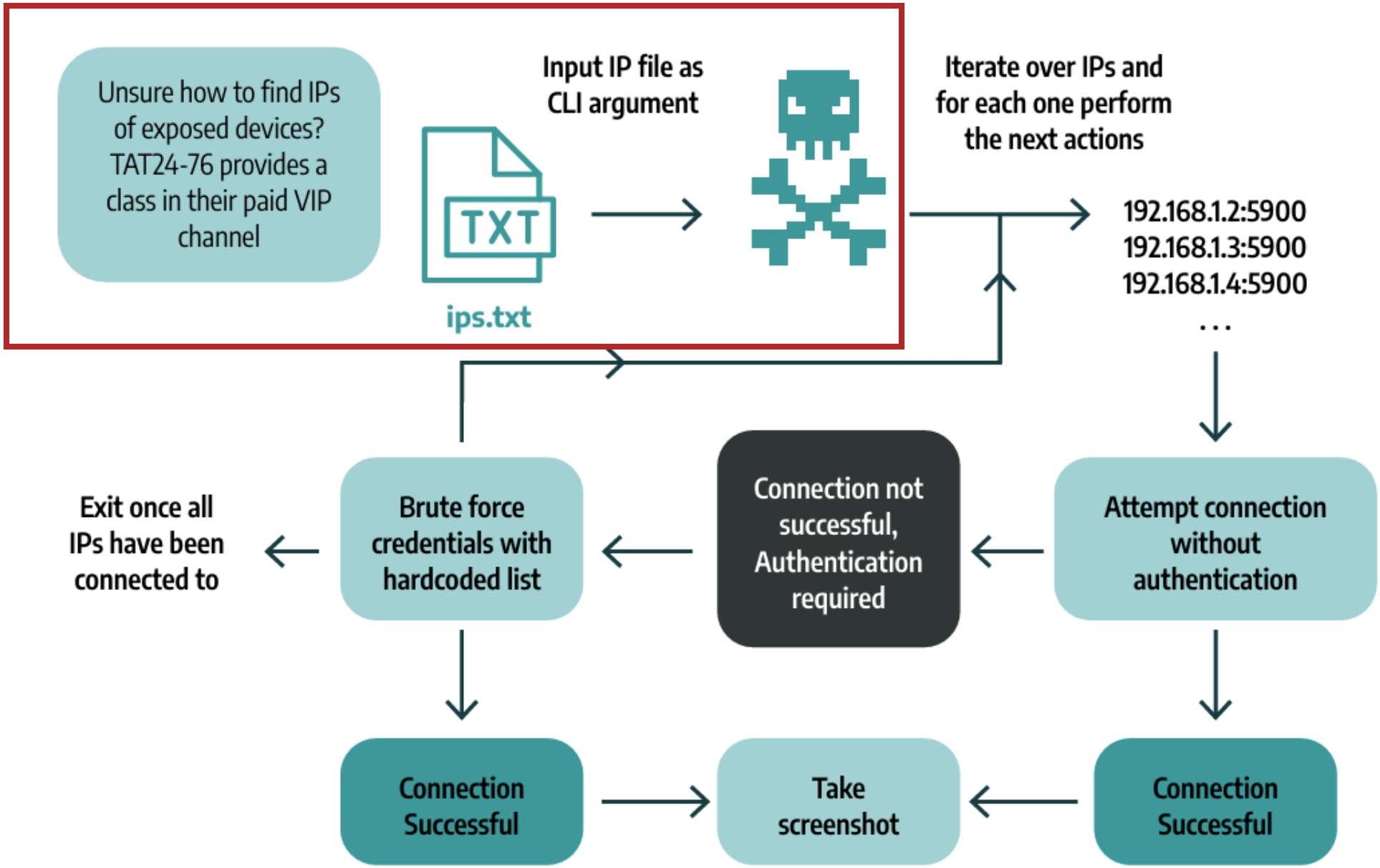
In the end, the winning combo was AI models + static analysis of PYC disassembly

KurtLar_SCADA.exe brute forces VNC authentication with a small list of credentials.

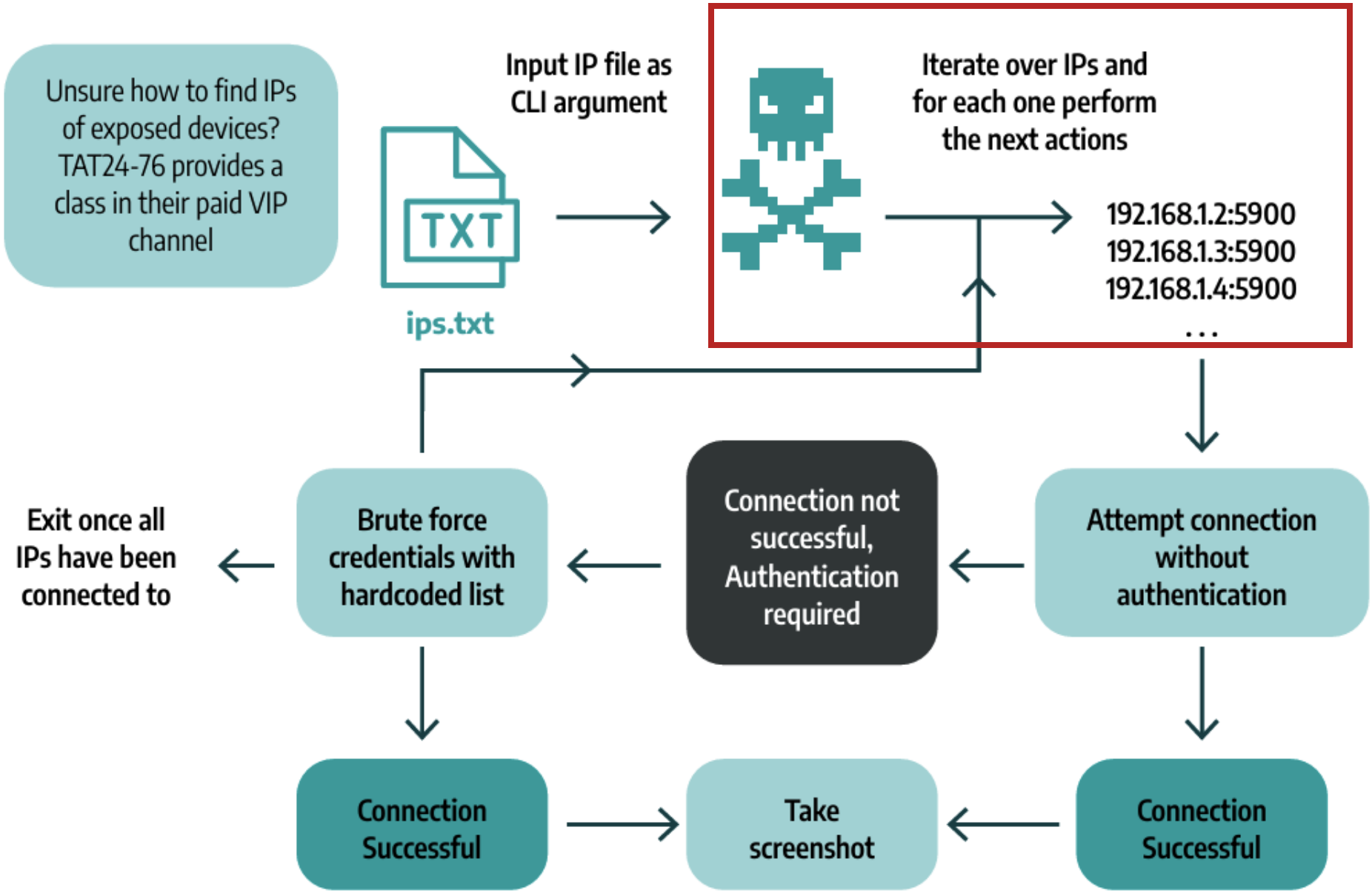
Execution Flow of kurtlar.exe and kurtlar_scada.exe



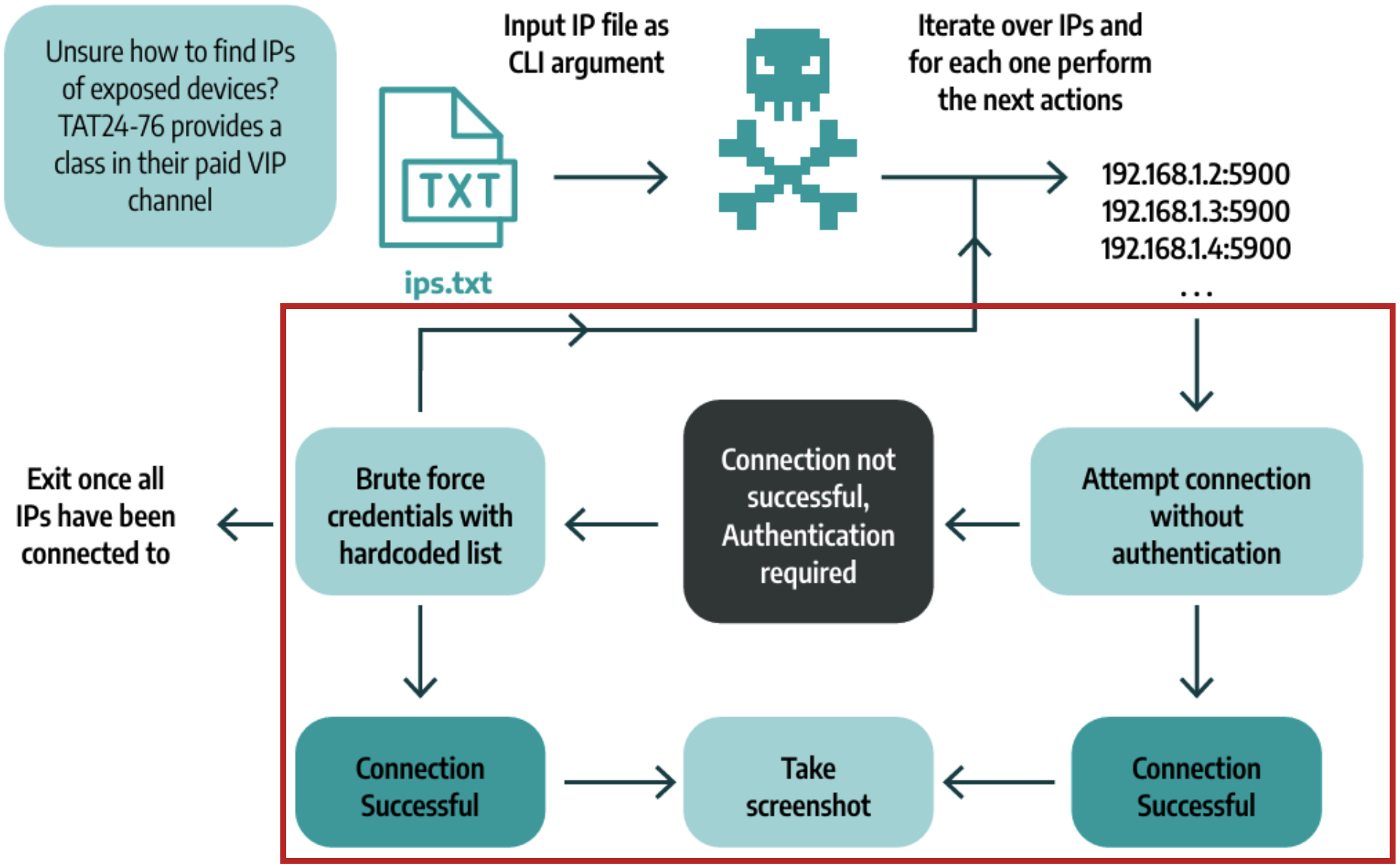
Execution Flow of kurtlar.exe and kurtlar_scada.exe



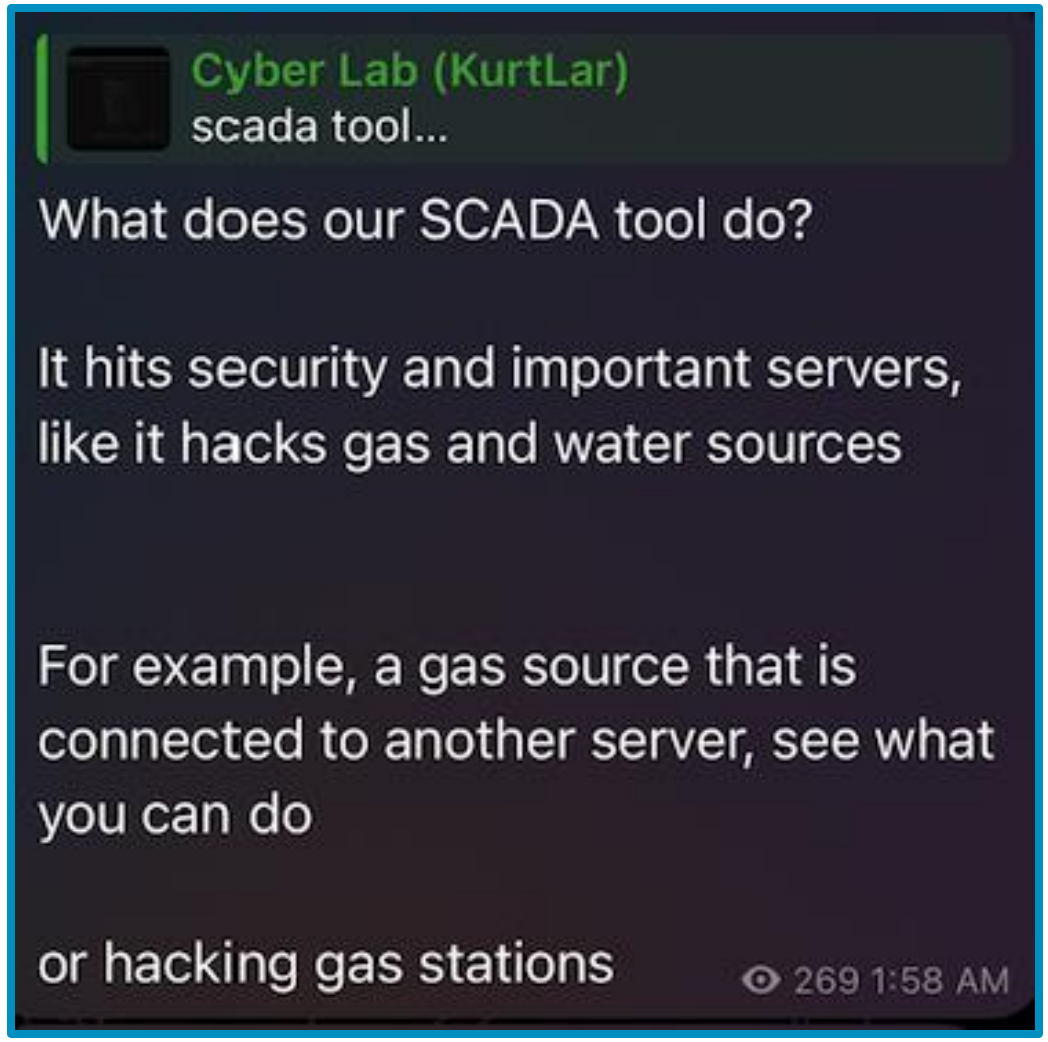
Execution Flow of kurtlar.exe and kurtlar_scada.exe



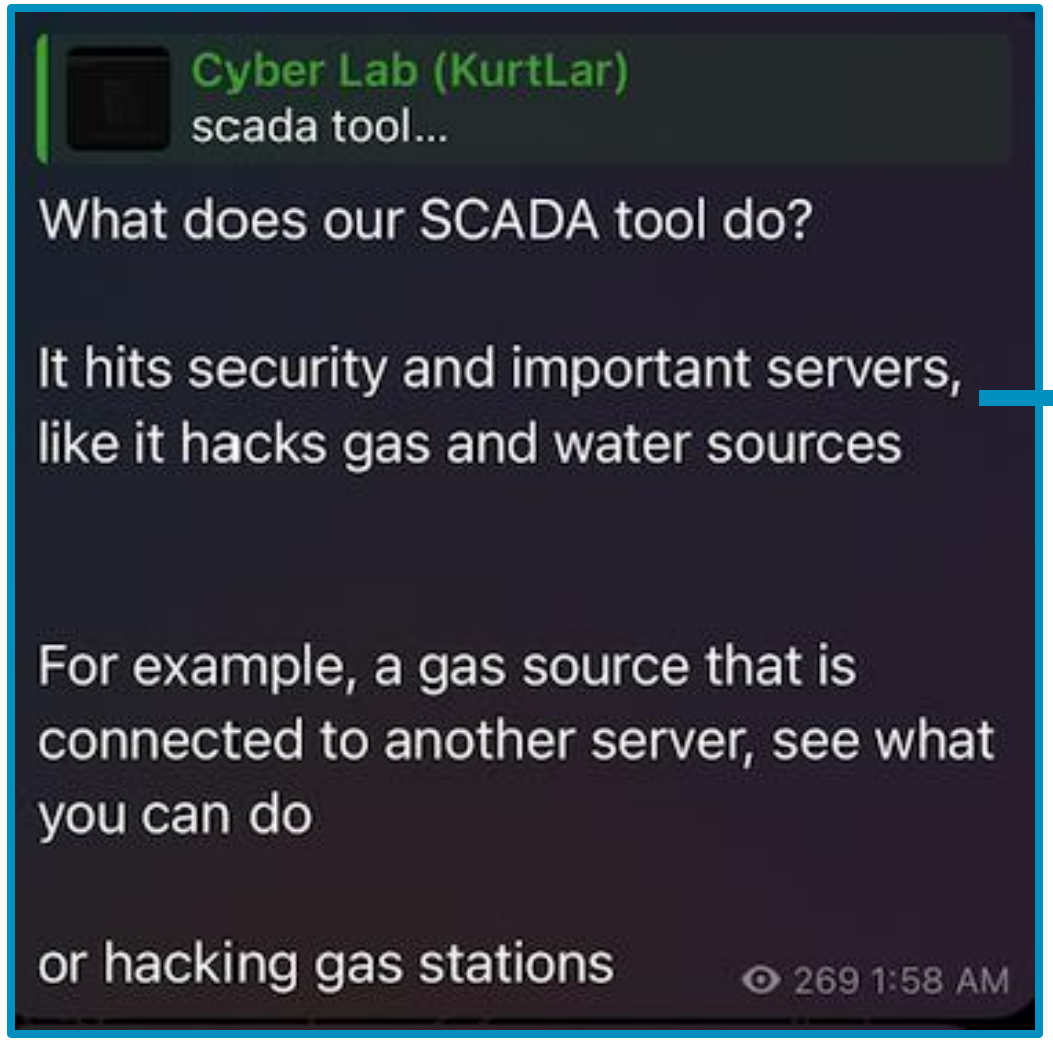
Execution Flow of kurtlar.exe and kurtlar_scada.exe

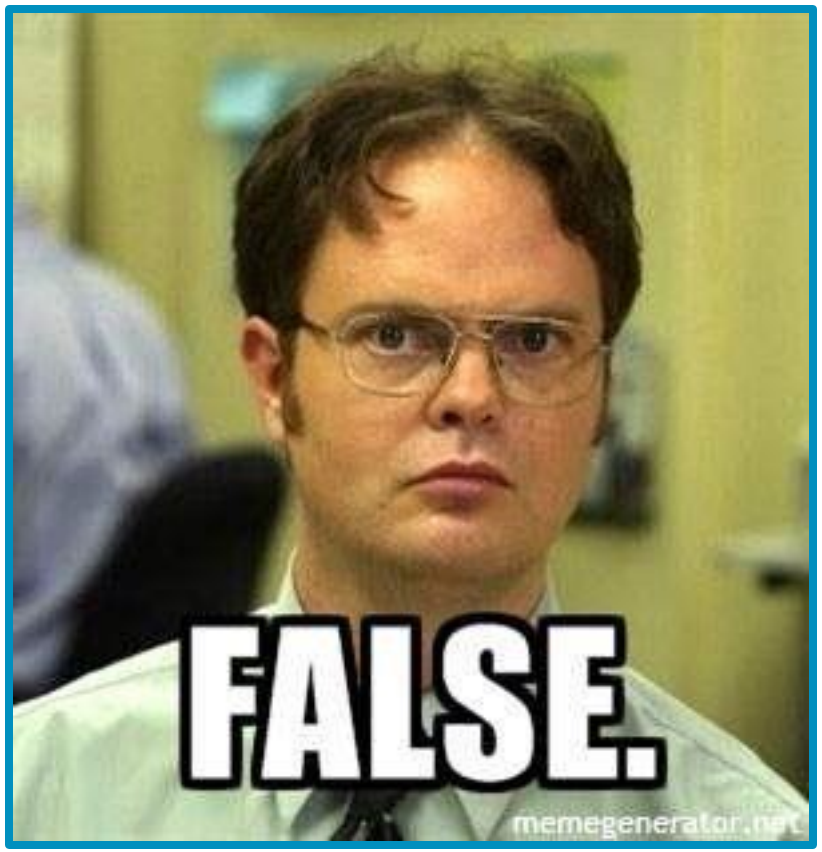


Telegram Channel Advertisements



Telegram Channel Advertisements





Telegram Channel Advertisements

We provide our own support and no one is going to have a problem running this tool

And that this tool is super private, nobody has this tool anywhere, it is coded by the team itself and you can download it only from us.

Telegram Channel Advertisements

We provide our own support and no one is going to have a problem running this tool

And that this tool is super private, nobody has this tool anywhere, it is coded by the team itself and you can download it only from us.

Telegram Channel Advertisements

We provide our own support and no one is going to have a problem running this tool

And that this tool is super private, nobody has this tool anywhere, it is coded by the team itself and you can download it only from us.

Is KurtLar_SCADA.exe ICS Malware?

ICS malware is defined as:

"ICS-capable software intentionally designed for adverse effects on operational technology environments."

and must meet the following properties:

1. *Must be ICS-capable*
2. *Must be designed with malicious intent*
3. *Must have the ability for adverse effects on OT environments.*

No, KurtLar_SCADA is not ICS Malware

ICS malware is defined as:

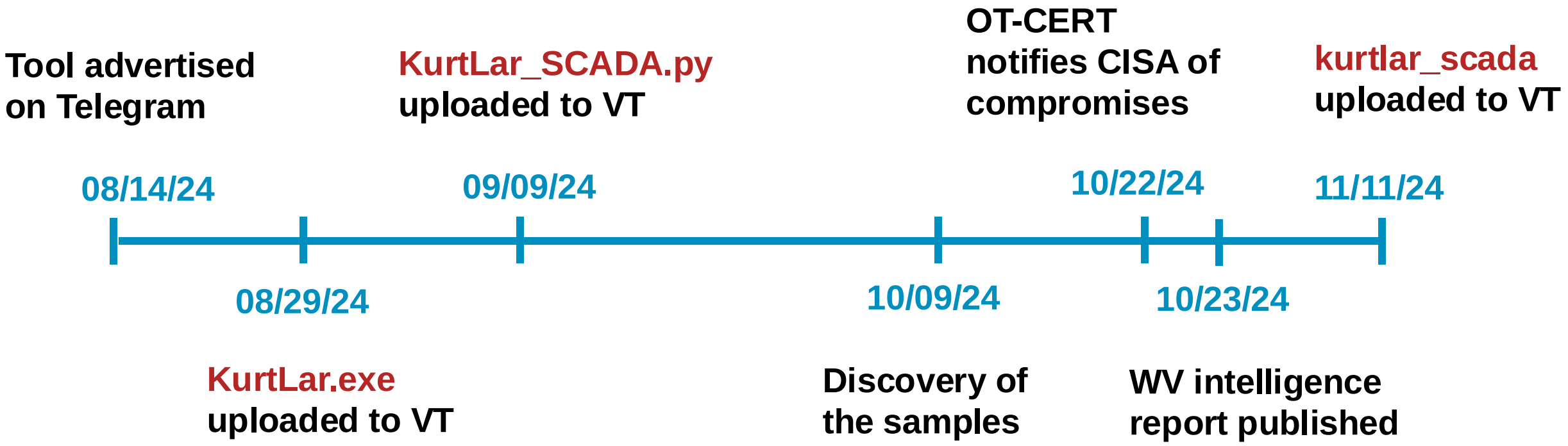
"ICS-capable software intentionally designed for adverse effects on operational technology environments."

and must meet the following properties:

1. *Must be ICS-capable* ✗
2. *Must be designed with malicious intent* ✓
3. *Must have the ability for adverse effects on OT environments.* ✗

…but it's nuanced. No new initial access method created here, just using known remote access protocols!

Timeline after Victims Notified



Dragos OT-CERT: A Community Approach

OT-CERT is a community of members from small to large businesses, and partners like ISACs.

- Completely free!
- OT-CERT has over 2400+ members.

OT-CERT
OPERATIONAL TECHNOLOGY
CYBER EMERGENCY READINESS TEAM

Dragos OT-CERT: A Community Approach

FREE CYBERSECURITY RESOURCES

OPEN TO GLOBAL ICS/OT COMMUNITY

ONGOING CONTENT

WORKING SESSIONS

VULNERABILITY DISCLOSURES

VICTIM NOTIFICATIONS

Alerting the Victims

3 screenshots contained enough information to identify victims:

- Norwegian fishing ship
- Washing station for tanker trucks (wastewater treatment) in U.S.
- Oil drilling company in U.S.

"…we were able to make contact and share the info. It 'rattled' them a bit. They have also engaged CISA for their services as a result of the notification."

"…he was rather uninterested in doing anything about the incident."

Low-Hanging Fruit is Effective!

KurtLar_SCADA.exe is a glorified VNC client with brute-forcing capabilities.

A capability does not have to be impressive to pose a risk.

If you expose your devices directly to the Internet, they are sitting ducks.

Vendors, We Need Your Help!

Vendors aren't incentivized to design secure systems.

Security

One may be concerned about rogue actors connecting through VNC to spy on secret data or remotely operate the system.

VNC can have several layers of security: the VNC client must give a password before connecting; blacklists may exempt certain machines from connecting; nonstandard port numbers may be used etc.

We have currently chosen not to implement these means, in order to avoid too much complexity. We think the fact that the [redacted] will only activate VNC when he want to, and that his address is neither static nor easily found, gives a reasonable degree of security. This policy may be changed if so demanded.

Conclusion – Defense is Doable!

Good news: defense is doable!

Bad news: hacktivists will continue to abuse poorly secured/exposed systems to gain attention and notoriety.

Conclusion – Defense is Doable!

In this case, proactive threat hunting yielded success:

- Identified hacktivist activity and capabilities
- Notified victim
- Informed community

Collaboration with OT-CERT and CISA was key!

Doing the Basics

- Ensure industrial devices are not directly exposed on the Internet, use a VPN!
- Use allow lists and restrict access to remote access services (such as VNC, RDP, etc.)
- Ensure default or weak credentials are changed.
- Deactivate remote access solutions if not being used.

Thank You

Sam Hanson | shanson@dragos.com

X: @__samhanson__ | Bluesky: @sam-hans0n.bsky.social

Website: sam-hanson.space


Q&A


SANS
ICS SECURITY
Summit & Training 2025
Summit: June 15–17 (NEW | 3 DAYS!)
Training: June 18–23
Join us at Disney's Contemporary Resort
Orlando, FL
ICS
20TH ANNIVERSARY