# Malware, Zero Days, and PLCs, Oh Boy!

Sam Hanson
Vulnerability Analyst II

# # whoami

Vulnerability Analyst on the Dragos Intelligence Research team.

- Dragos is an industrial cybersecurity company.
- Been with Dragos for nearly 3 years.

More generally, cybersecurity researcher focusing on OT.

- Vulnerability research and analysis.
- Malware reverse engineering and analysis.

# Goal of this Presentation

1. Showcase research findings of a strange threat to OT environments.

2. Demonstrate basic reverse engineering (RE) techniques in an accessible manner.

3. Explore the malware “ecosystem” and highlight areas that need further work and research.

# PLC? HMI? EWS?

Programmable Logic Controller – a ruggedized computer used to control an industrial process.

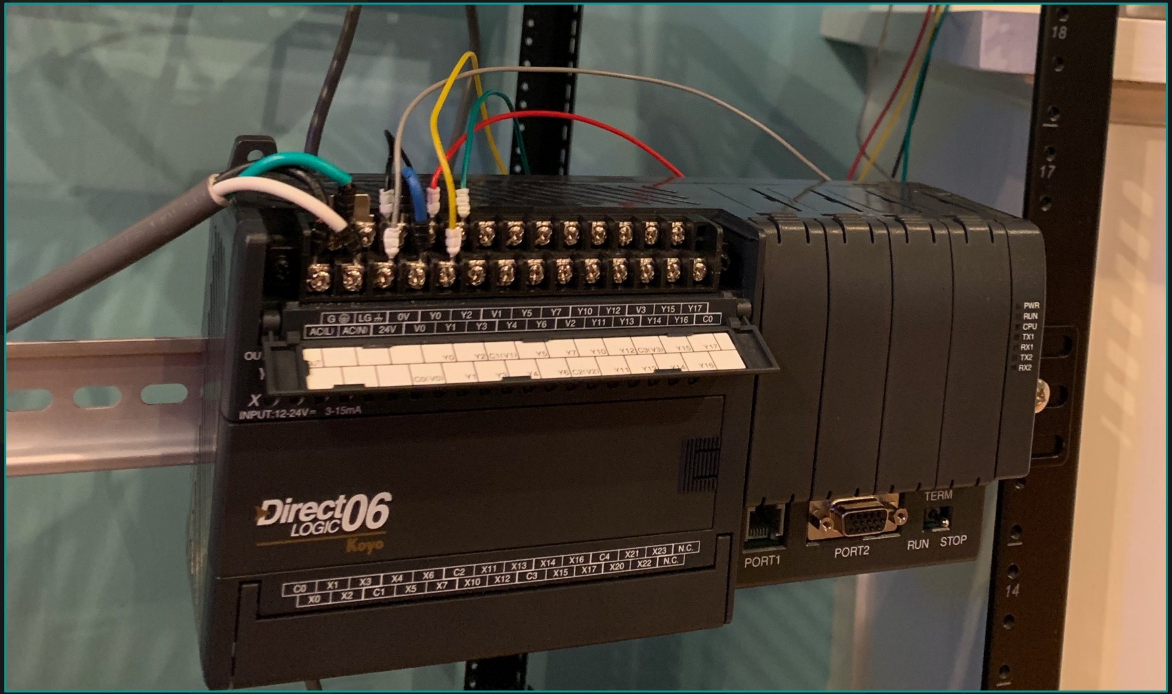
Human-Machine Interface – dashboard used to view and control an industrial process.

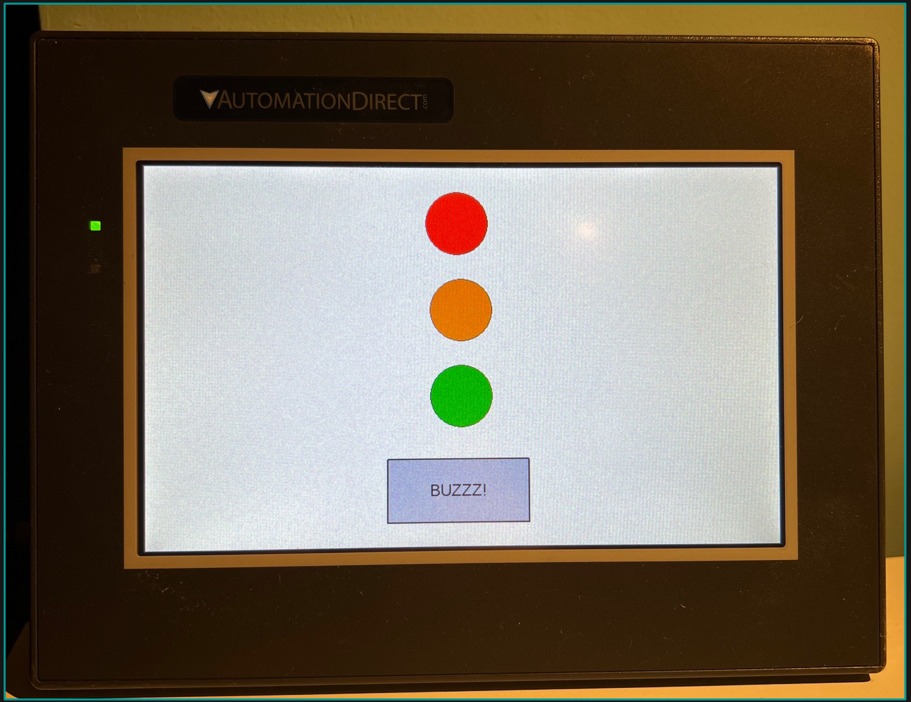
Engineering Workstation System – Windows machine with OT-related software (PLC/HMI programming, configuration, and monitoring software)

# How it Started

Vulnerability Assessment against:

- Automation Direct's DirectLogic 06 PLC
  - with ECOM Ethernet module
- Automation Direct's C-More EA9 HMI



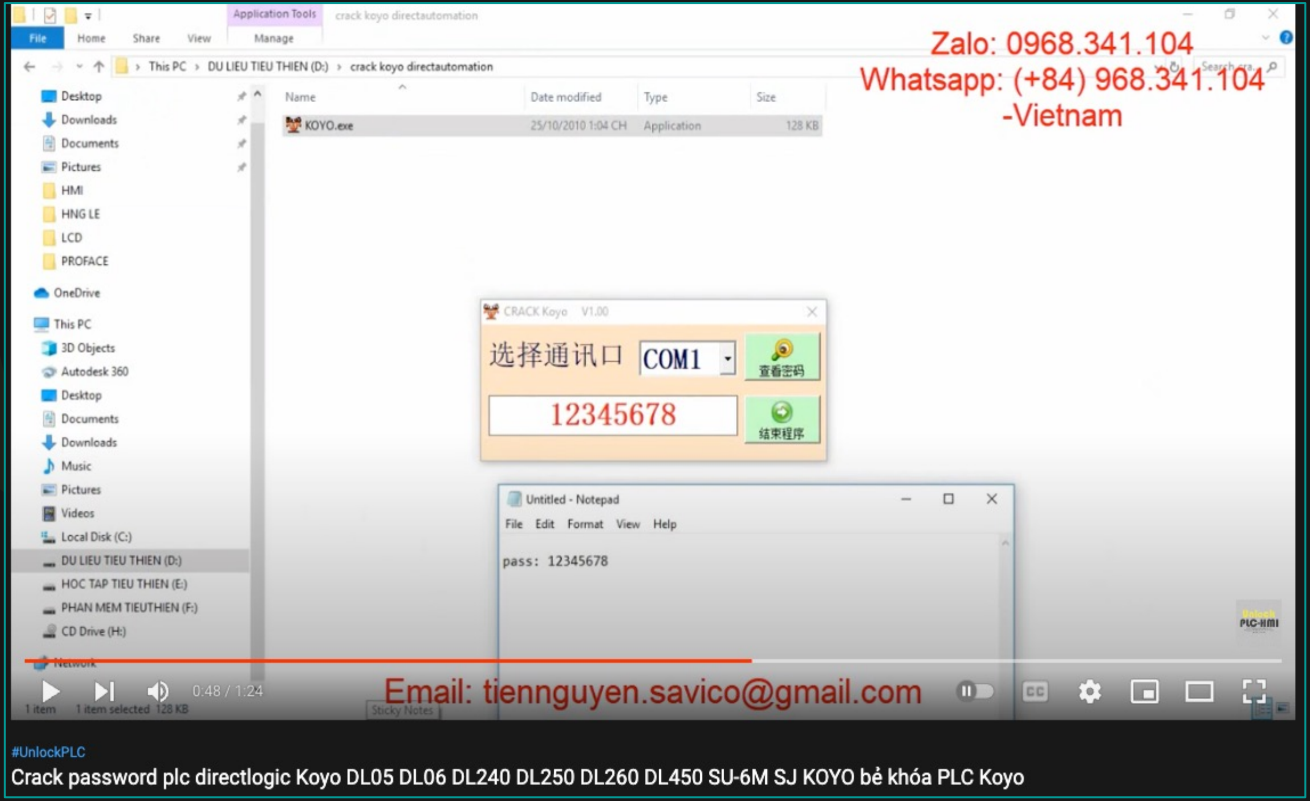


# Finding and Obtaining the Malware

First step in vulnerability assessment, understand the system and how it's supposed to work. Youtube is fantastic for this.

One video let to another and another and then finally…

Password cracking software advertisement! I was immediately suspicious.



| Name | Date modified | Type | Size |
|---|---|---|---|
| KOYO.exe | 25/10/2010 1:04 CH | Application | 128 KB |

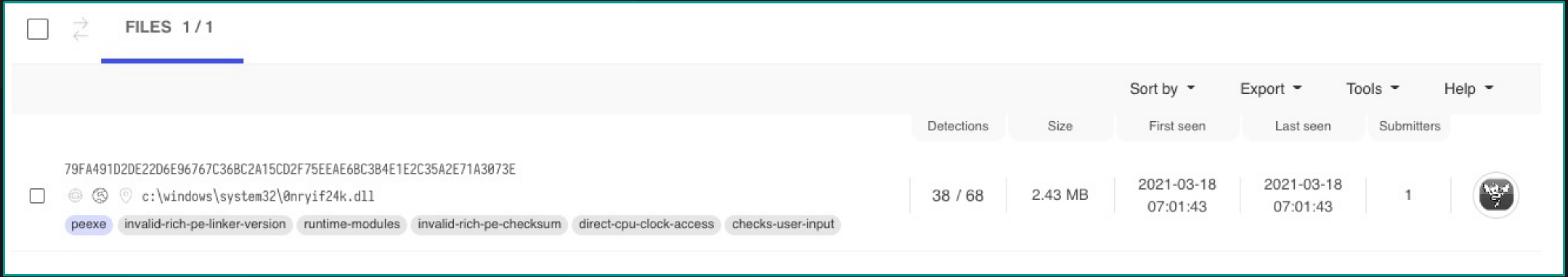
12345678

```
pass: 12345678
```

Zalo: 0968.341.104
Whatsapp: (+84) 968.341.104
-Vietnam

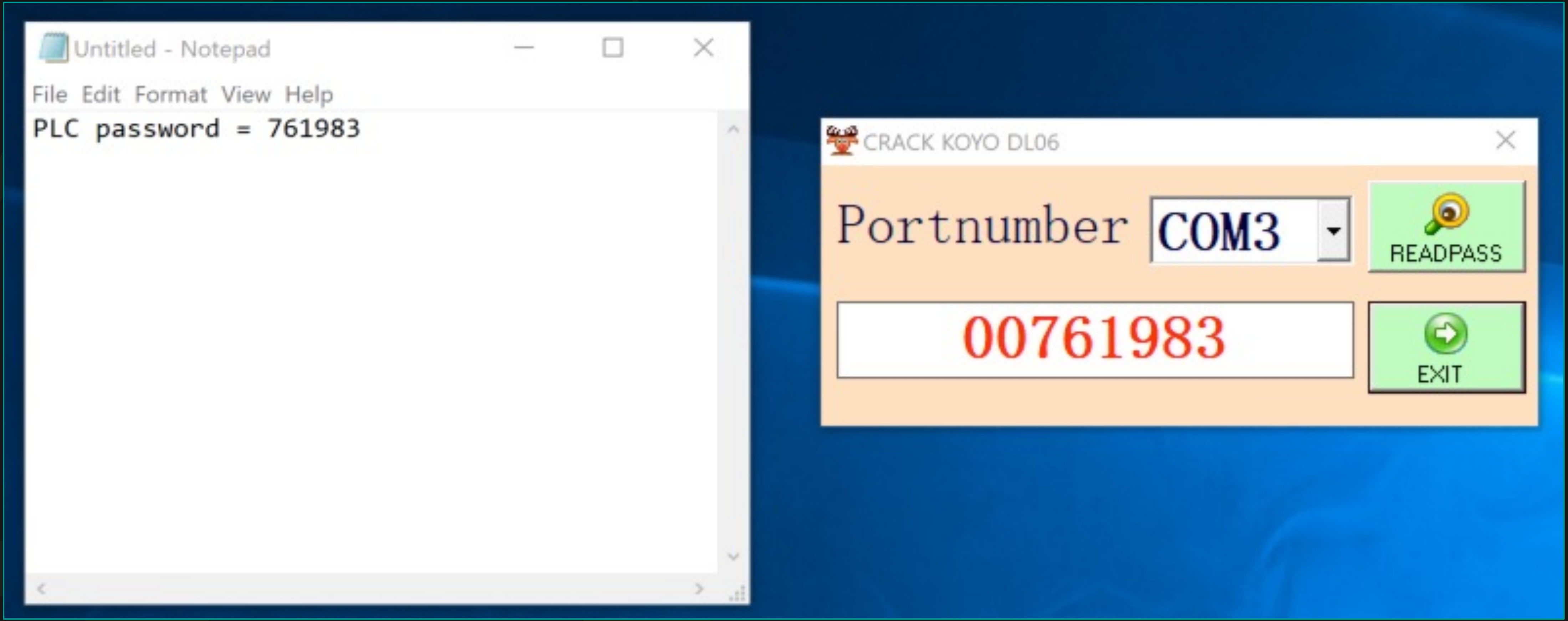
Email: tiennguyen.savico@gmail.com

#UnlockPLC
Crack password plc directlogic Koyo DL05 DL06 DL240 DL250 DL260 DL450 SU-6M SJ KOYO bẻ khóa PLC Koyo



| | Detections | Size | First seen | Last seen | Submitters |
|---|---|---|---|---|---|
| □ 79FA491D2DE22D6E96767C36BC2A15CD2F75EEAE6BC3B4E1E2C35A2E71A3073E<br>c:\windows\system32\0nryif24k.dll<br>peexe invalid-rich-pe-linker-version runtime-modules invalid-rich-pe-checksum direct-cpu-clock-access checks-user-input | 38 / 68 | 2.43 MB | 2021-03-18 07:01:43 | 2021-03-18 07:01:43 | 1 |

# Testing the Exploit



```
PLC password = 761983
```

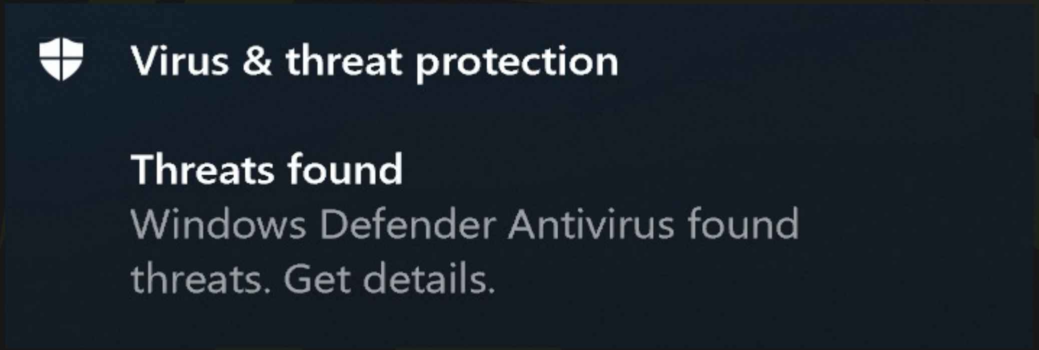
Portnumber COM3

00761983

PLC and EWS must be connected over serial!

Software obtained password within a second, so brute forcing seemed unlikely.

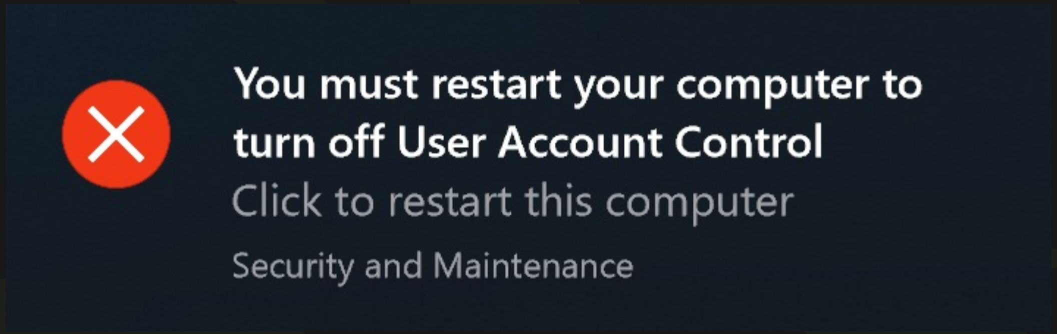
🚩🚩🚩



Virus & threat protection

Threats found

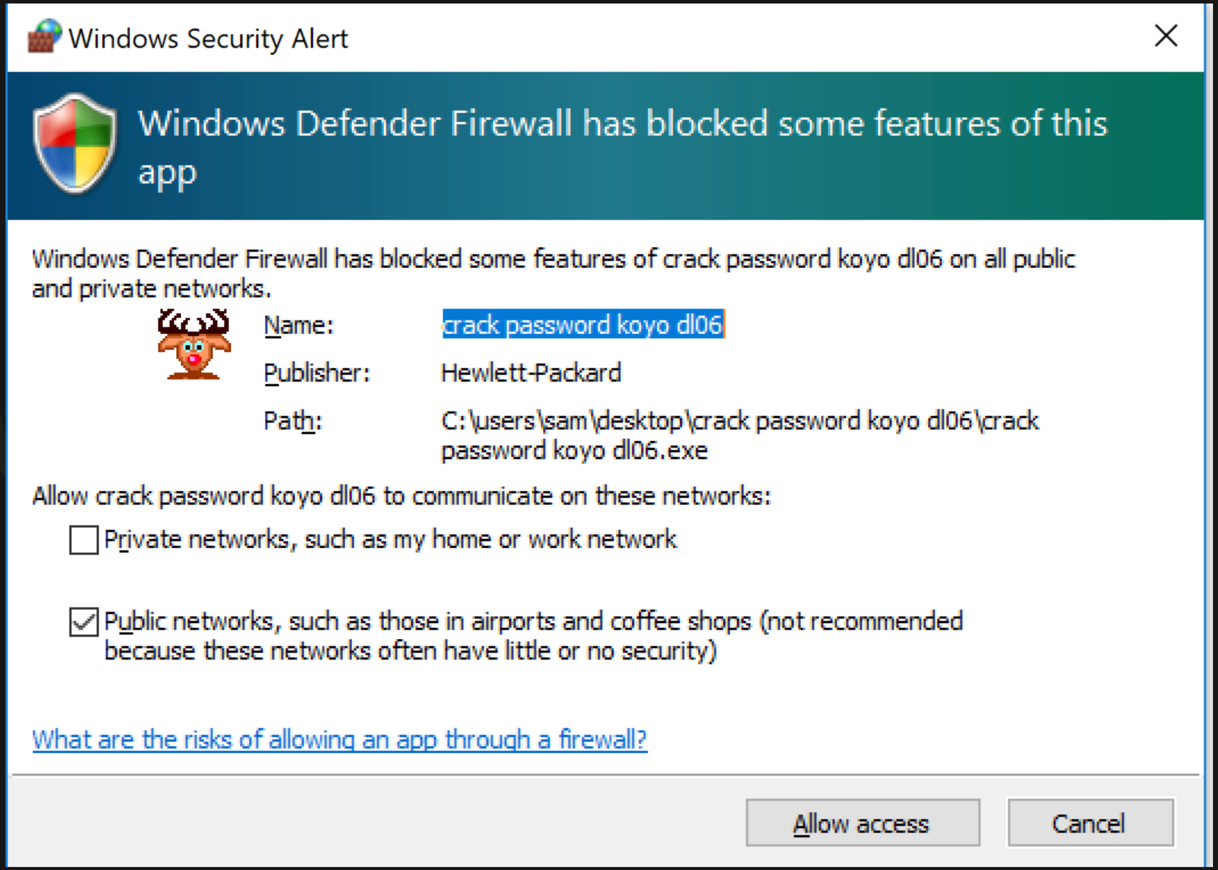
Windows Defender Antivirus found threats. Get details.



You must restart your computer to turn off User Account Control

Click to restart this computer

Security and Maintenance



Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of crack password koyo dl06 on all public and private networks.

Name: crack password koyo dl06

Publisher: Hewlett-Packard

Path: C:\users\sam\desktop\crack password koyo dl06\crack password koyo dl06.exe

Allow crack password koyo dl06 to communicate on these networks:

☐ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

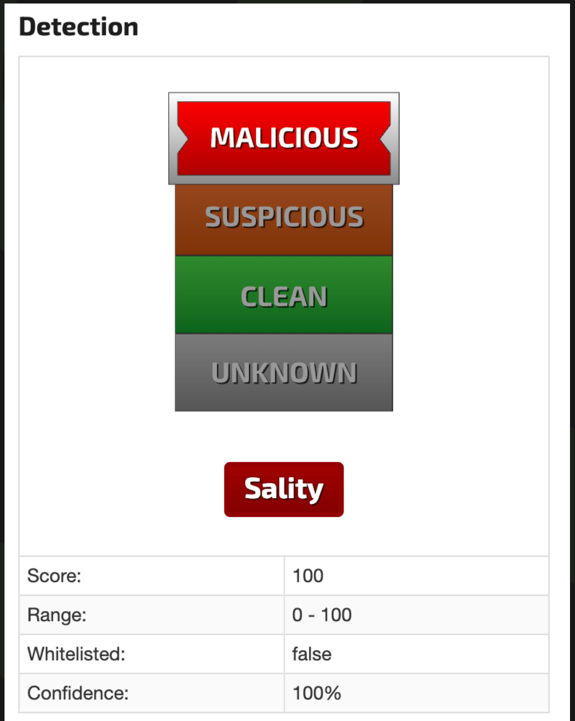
What are the risks of allowing an app through a firewall?

If on a somewhat recent machine, something is clearly off. Unfortunately, industrial systems often lack years behind.

# Dynamic Analysis Tools and Techniques

The easy (but expensive) methods:

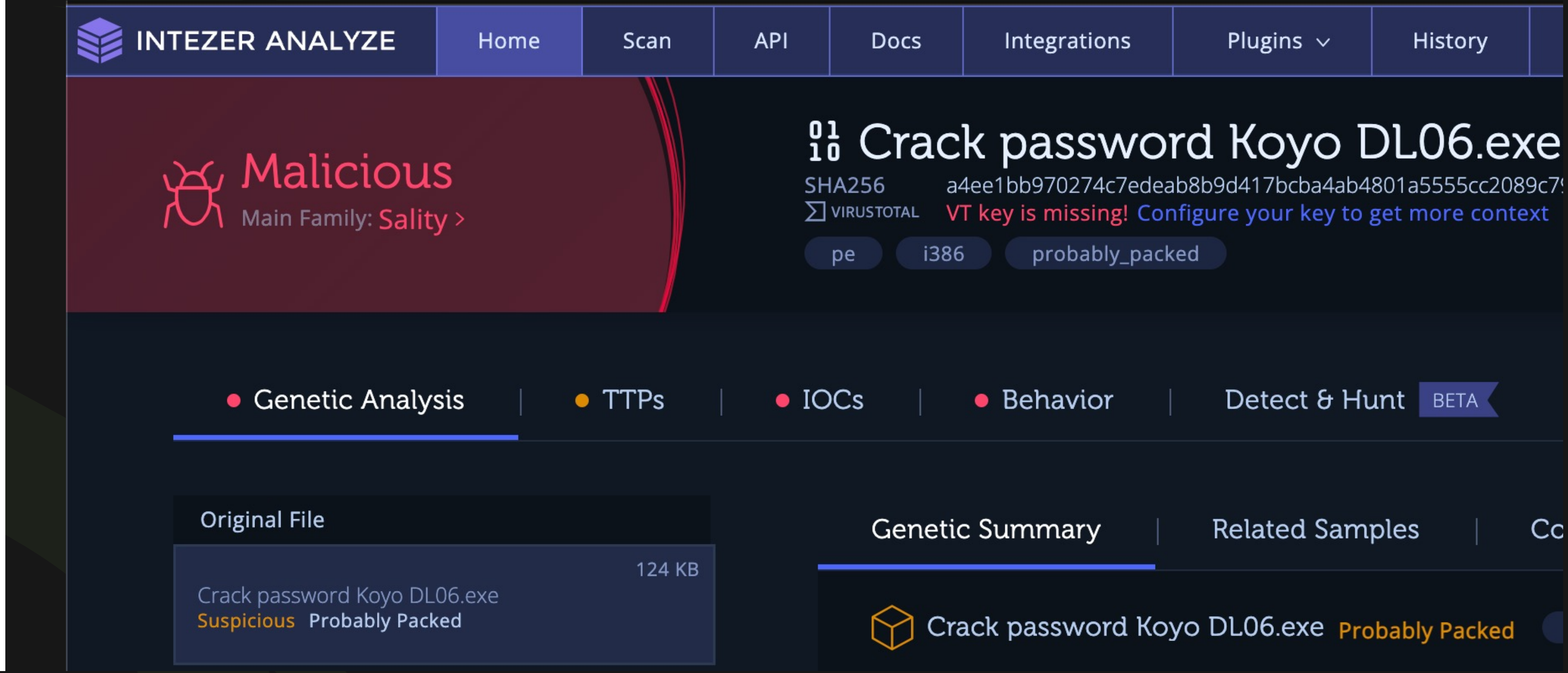
- Intezer
- JoeSandbox



**Detection**

Sality

| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |



Malicious

Main Family: Sality >

Crack password Koyo DL06.exe

SHA256 a4ee1bb970274c7edeab8b9d417bcba4ab4801a5555cc2089c7

VIRUSTOTAL VT key is missing! Configure your key to get more context

pe i386 probably_packed

Original File

Crack password Koyo DL06.exe 124 KB
Suspicious Probably Packed

Crack password Koyo DL06.exe Probably Packed

Useful for a quick, shallow understanding of what’s happening.

# The Sality Malware Family

Brief overview [1]:

- Botnet historically used for cryptocurrency mining, DDoS attacks, password spraying and password cracking.
- Been around for waaay too long (early 2000s!)
- Techniques include: file infection, process injection, antivirus disabling, IP filtering (reportedly), spread over USB, network shares, etc.

As a researcher, I want to see this functionality with my own eyes.

[1]: https://aroundcyber.files.wordpress.com/2012/11/sality_peer_to_peer_viral_network.pdf

# Core Research Questions

- Does this sample line up with previous Sality samples functionality wise?
  - File infection? Process injection? Cryptocurrency mining?

- How is the malware retrieving the PLC password? Is it done via the malware dropper or Sality?
  - Does this exploit solely work over serial?

- Are there more samples targeting other industrial systems and vendors?

# The First Problem – Packed Malware Payload

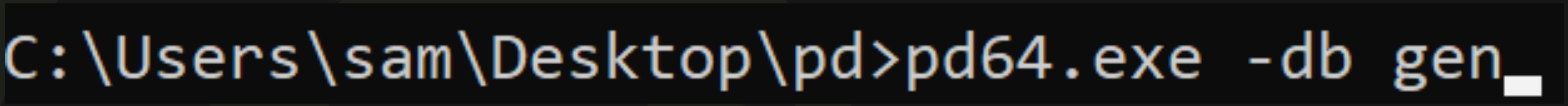
Sality is UPX packed in the dropper executable. We must find a way to obtain unpacked version.

- There are multiple methods to achieve this but I find the easiest is to use a dynamic analysis tool such as ProcessDump.

Download ProcessDump here: https://github.com/glmcdona/Process-Dump

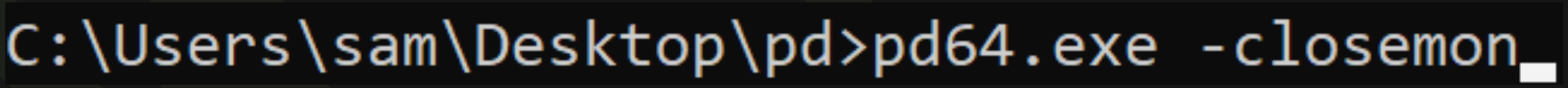
# ProcessDump: Instructions

**Step 1: Generate ”clean hash database”**



```
C:\Users\sam\Desktop\pd>pd64.exe -db gen
```

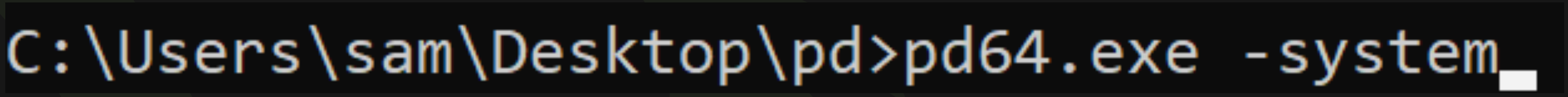
**Step 2: Start monitoring intermediate processes**



```
C:\Users\sam\Desktop\pd>pd64.exe -closemon
```

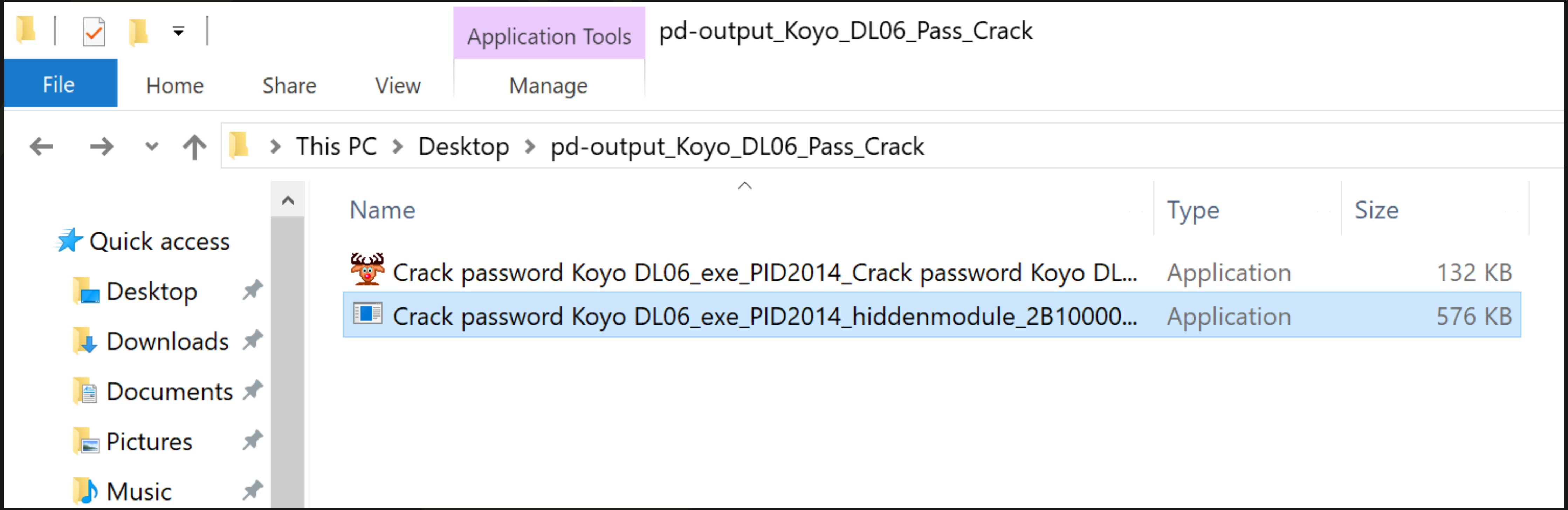
**Step 3: Run the malware dropper**

**Step 4: Dump the malware from memory:**



```
C:\Users\sam\Desktop\pd>pd64.exe -system
```

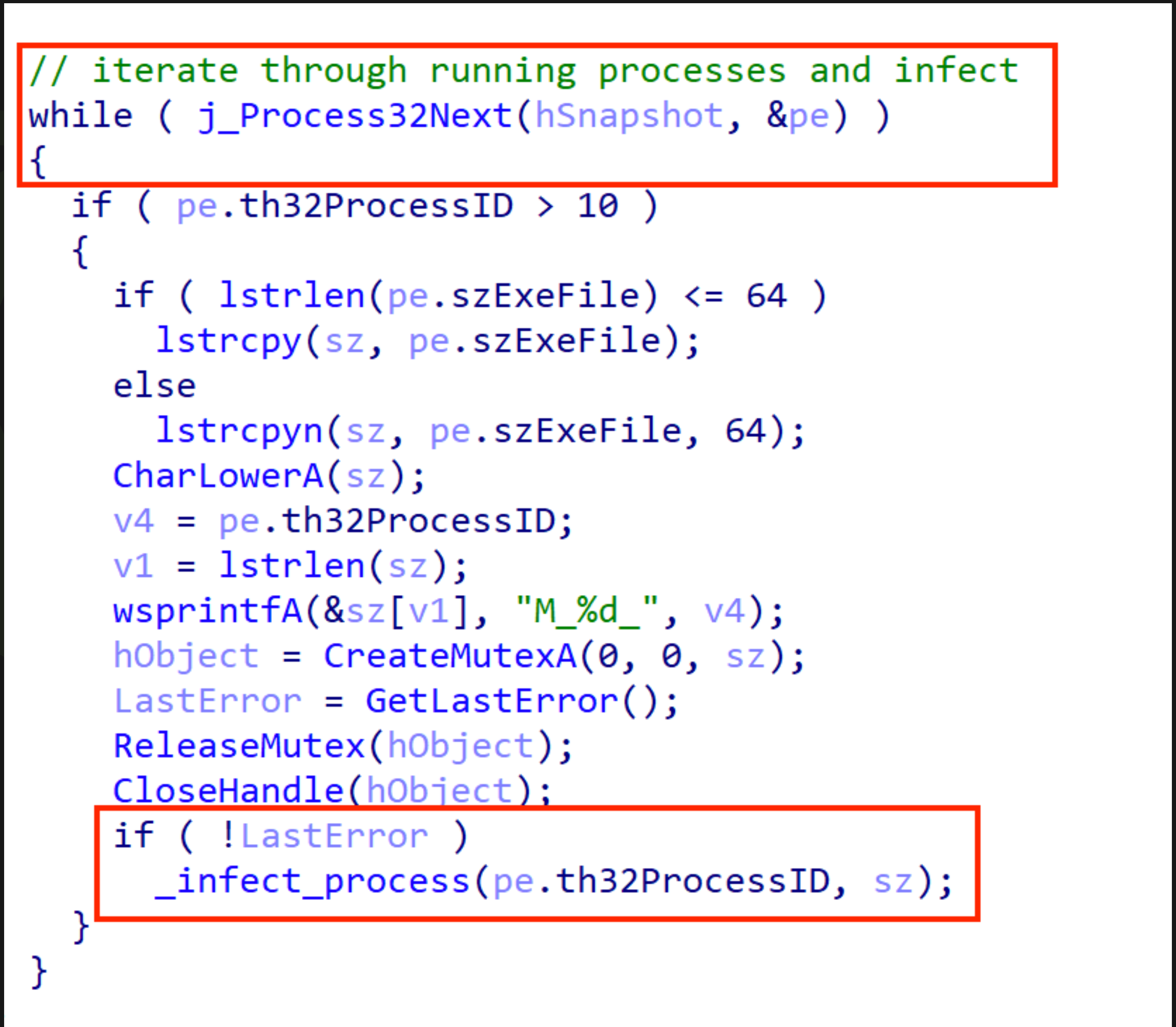
# ProcessDump: Output



| Name | Type | Size |
|---|---|---|
| Crack password Koyo DL06_exe_PID2014_Crack password Koyo DL... | Application | 132 KB |
| Crack password Koyo DL06_exe_PID2014_hiddenmodule_2B10000... | Application | 576 KB |

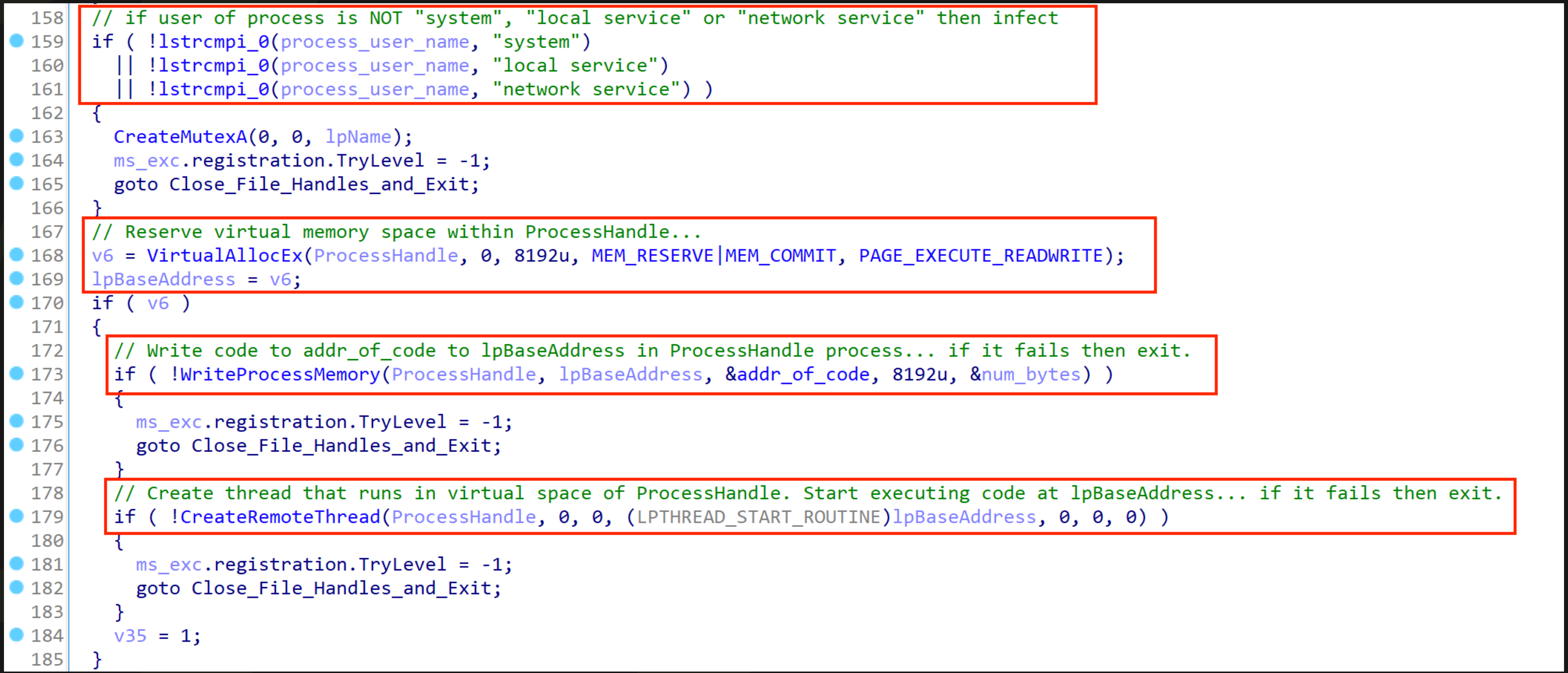
Sality executable highlighted in blue

# Sality Static Analysis – Iterating Processes



```
// iterate through running processes and infect
while ( j_Process32Next(hSnapshot, &pe) )
{
  if ( pe.th32ProcessID > 10 )
  {
    if ( lstrlen(pe.szExeFile) <= 64 )
      lstrcpy(sz, pe.szExeFile);
    else
      lstrcpyn(sz, pe.szExeFile, 64);
    CharLowerA(sz);
    v4 = pe.th32ProcessID;
    v1 = lstrlen(sz);
    wsprintfA(&sz[v1], "M_%d_", v4);
    hObject = CreateMutexA(0, 0, sz);
    LastError = GetLastError();
    ReleaseMutex(hObject);
    CloseHandle(hObject);
    if ( !LastError )
      _infect_process(pe.th32ProcessID, sz);
  }
}
```

# Sality Static Analysis – Injecting into Processes



```
// if user of process is NOT "system", "local service" or "network service" then infect
if ( !lstrcmpi_0(process_user_name, "system")
  || !lstrcmpi_0(process_user_name, "local service")
  || !lstrcmpi_0(process_user_name, "network service") )
{
  CreateMutexA(0, 0, lpName);
  ms_exc.registration.TryLevel = -1;
  goto Close_File_Handles_and_Exit;
}
// Reserve virtual memory space within ProcessHandle...
v6 = VirtualAllocEx(ProcessHandle, 0, 8192u, MEM_RESERVE|MEM_COMMIT, PAGE_EXECUTE_READWRITE);
lpBaseAddress = v6;
if ( v6 )
{
  // Write code to addr_of_code to lpBaseAddress in ProcessHandle process... if it fails then exit.
  if ( !WriteProcessMemory(ProcessHandle, lpBaseAddress, &addr_of_code, 8192u, &num_bytes) )
  {
    ms_exc.registration.TryLevel = -1;
    goto Close_File_Handles_and_Exit;
  }
  // Create thread that runs in virtual space of ProcessHandle. Start executing code at lpBaseAddress... if it fails then exit.
  if ( !CreateRemoteThread(ProcessHandle, 0, 0, (LPTHREAD_START_ROUTINE)lpBaseAddress, 0, 0, 0) )
  {
    ms_exc.registration.TryLevel = -1;
    goto Close_File_Handles_and_Exit;
  }
  v35 = 1;
}
```

This is precisely how prior versions of Sality work according to the Symantec report. I did this strategy for each major feature of Sality.

# Understanding Windows Internal APIs

The heavy lifting is accomplished by Windows Internal API calls. What do we do if we aren’t familiar with these APIs?

Two great resources:

- MalAPI.io – website tracking Windows APIs that are often abused.
- Microsoft documentation – the ultimate source for understanding Windows internals. Incredibly useful for static analysis as function parameters and return values are defined. This is the holy bible of Windows RE.

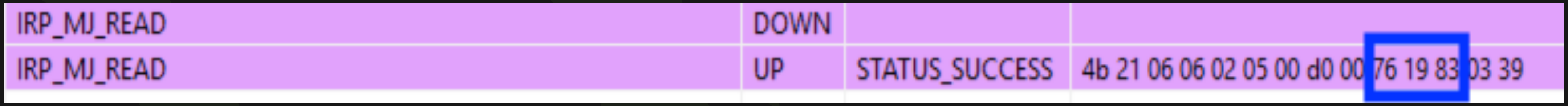
# Core Research Questions

- ✓ Does this sample line up with previous Sality samples functionality wise?
- How is the malware retrieving the PLC password? Is it done via the malware dropper or Sality?
    - Does this exploit solely work over serial?
- Are there more samples targeting other industrial systems and vendors?

# Sality Dropper and Exploit

Use Serial Port Monitor (free trial available) to capture serial traffic from EWS running the password cracker and the PLC.

- Serial equivalent of running tcpdump or Wireshark.
- Fair amount of traffic to dig through, but exploit is captured successfully.
- Specific, static byte sequence sent by dropper to PLC. PLC then immediately sends password back.
  - This hints at how the exploit works…
- Can’t show exploit bytes ☹ but I’ll leave this as an exercise for viewers and can demonstrate in the discussion room.



| | | | |
|---|---|---|---|
| IRP_MJ_READ | DOWN | | |
| IRP_MJ_READ | UP | STATUS_SUCCESS | 4b 21 06 06 02 05 00 d0 00 76 19 83 03 39 |

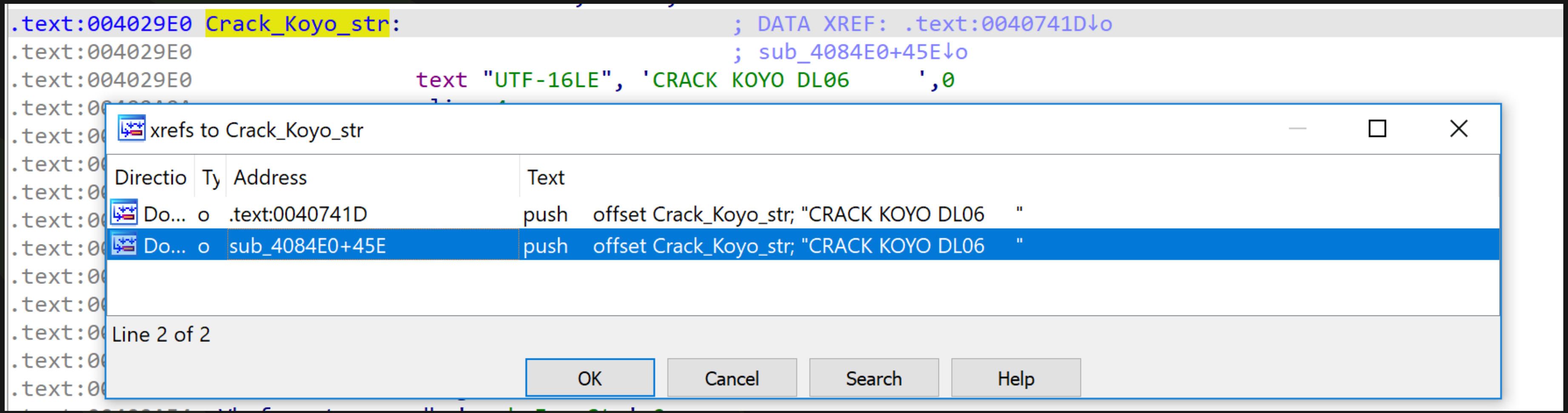
*Serial Response from PLC containing PLC password.*

# Static Analysis of Malware Dropper

Dropper is written in VB6, which *sucks* to RE.

I had to go back to the basics:

1. Using IDA Pro find a recognizable string, find the cross-references, and set a break point
2. Step through instructions until you reach desired function block.
3. Painful, but it worked! I was able to find the exploit byte sequence embedded in the malware.



```
.text:004029E0 Crack_Koyo_str:                                 ; DATA XREF: .text:0040741D↓o
.text:004029E0                                                 ; sub_4084E0+45E↓o
.text:004029E0                    text "UTF-16LE", 'CRACK KOYO DL06      ',0
```

xrefs to Crack_Koyo_str

| Directio | Ty | Address | Text |
|---|---|---|---|
| Do... | o | .text:0040741D | push offset Crack_Koyo_str; "CRACK KOYO DL06 " |
| Do... | o | sub_4084E0+45E | push offset Crack_Koyo_str; "CRACK KOYO DL06 " |

Line 2 of 2

# The Vulnerability and Exploit

The vulnerability: the PLC stores the password in an *unprotected memory region.*

- Confirmed this with the vendor.

The exploit: send a read memory command with the address at which the password is stored. PLC happily sends password back. This exploit ONLY works over serial.

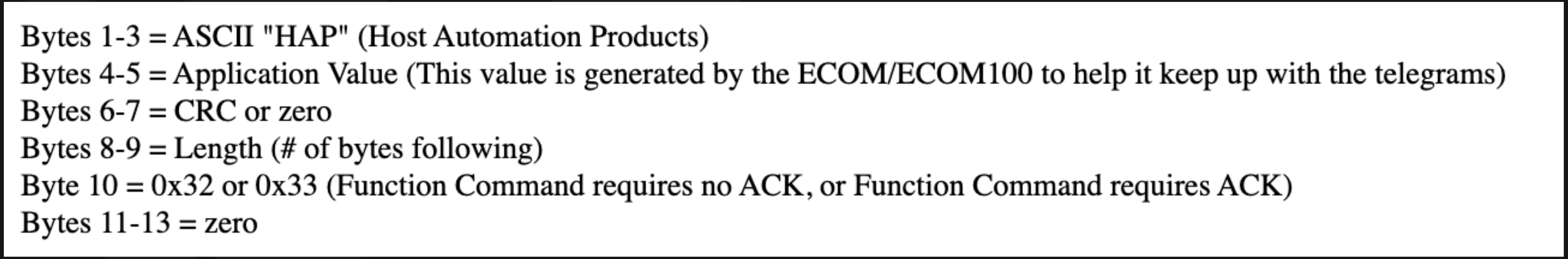
Theoretically, this same technique should also work over Ethernet…

- Time to start hacking!

🤔

# The Exploit Over Ethernet

Must first determine Automation Direct’s custom Ethernet protocol in order to create Ethernet exploit.



Bytes 1-3 = ASCII "HAP" (Host Automation Products)
Bytes 4-5 = Application Value (This value is generated by the ECOM/ECOM100 to help it keep up with the telegrams)
Bytes 6-7 = CRC or zero
Bytes 8-9 = Length (# of bytes following)
Byte 10 = 0x32 or 0x33 (Function Command requires no ACK, or Function Command requires ACK)
Bytes 11-13 = zero

However, their own documentation appeared slightly incorrect. Bytes 11-13 are the length of the command (serial exploit), and the command follows. We found this by incrementally fuzzing bytes 11-13.

Ethernet version of the exploit works! Hooray!

# Core Research Questions

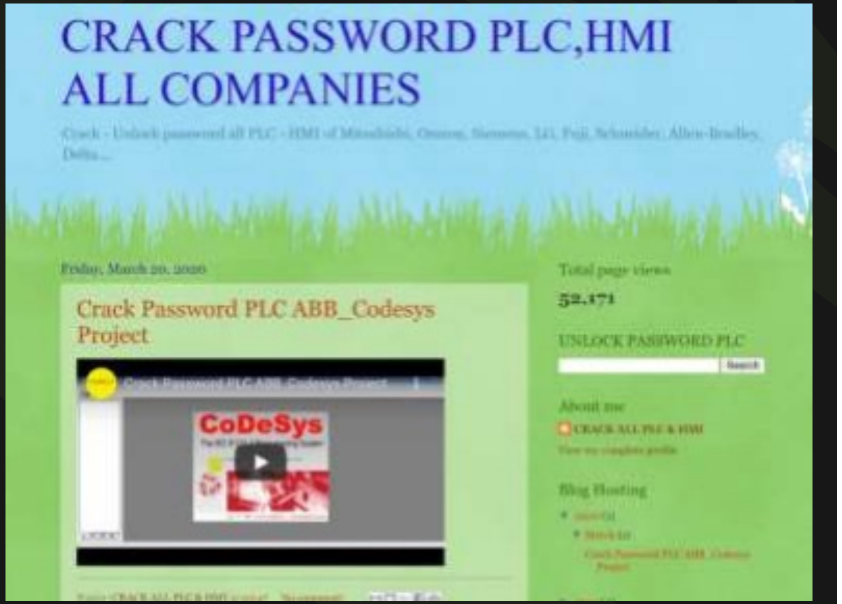
- ✓ Does this sample line up with previous Sality samples functionality wise?

- ✓ How is the malware retrieving the PLC password? Is it done via the malware dropper or Sality?
  - ✓ Does this exploit solely work over serial?

- Are there more samples targeting other industrial systems and vendors?

# Ecosystem of Password Cracking Software

Simple Google searches lead to multiple websites:



CRACK PASSWORD PLC,HMI ALL COMPANIES

Crack - Unlock password all PLC - HMI of Mitsubishi, Omron, Siemens, LG, Fuji, Schneider, Allen-Bradley, Delta...

Friday, March 20, 2020

Crack Password PLC ABB_Codesys Project

Total page views

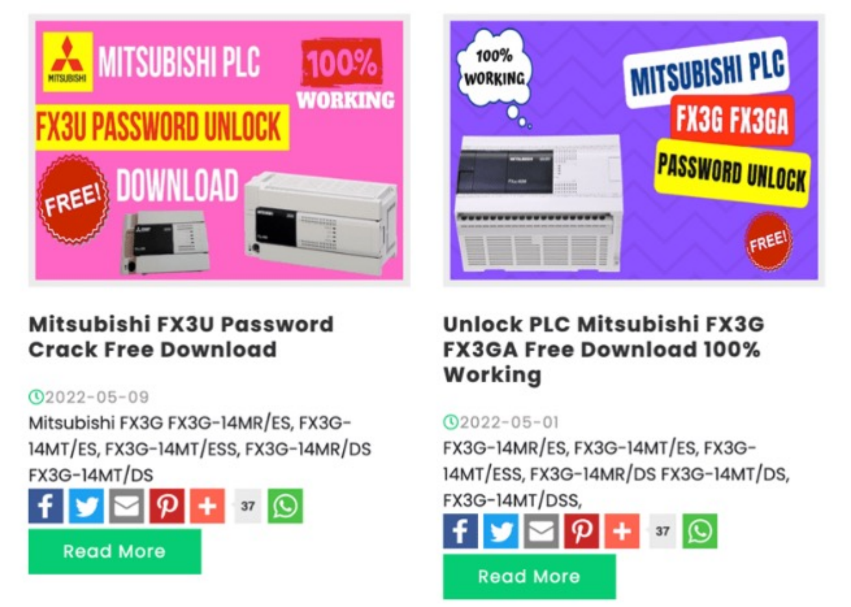
52,171

UNLOCK PASSWORD PLC

About me

CRACK ALL PLC & HMI

Blog Hosting



**Mitsubishi FX3U Password Crack Free Download**

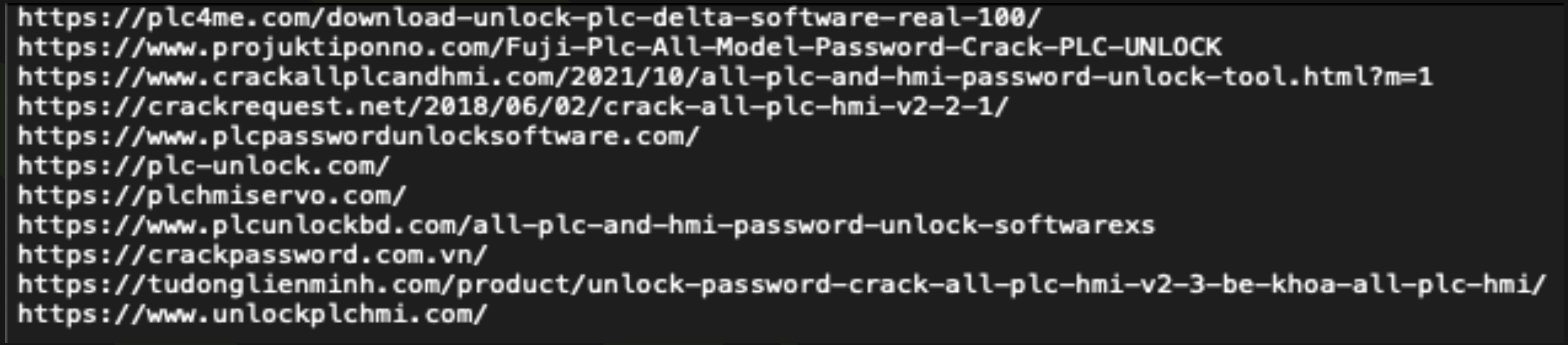
2022-05-09

Mitsubishi FX3G FX3G-14MR/ES, FX3G-14MT/ES, FX3G-14MT/ESS, FX3G-14MR/DS FX3G-14MT/DS

**Unlock PLC Mitsubishi FX3G FX3GA Free Download 100% Working**

2022-05-01

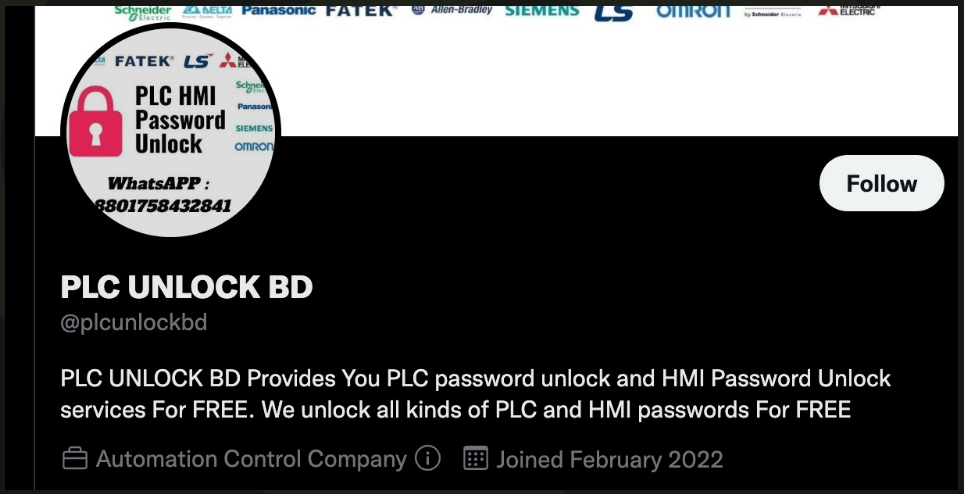
FX3G-14MR/ES, FX3G-14MT/ES, FX3G-14MT/ESS, FX3G-14MR/DS FX3G-14MT/DS, FX3G-14MT/DSS,



```
https://plc4me.com/download-unlock-plc-delta-software-real-100/
https://www.projuktiponno.com/Fuji-Plc-All-Model-Password-Crack-PLC-UNLOCK
https://www.crackallplcandhmi.com/2021/10/all-plc-and-hmi-password-unlock-tool.html?m=1
https://crackrequest.net/2018/06/02/crack-all-plc-hmi-v2-2-1/
https://www.plcpasswordunlocksoftware.com/
https://plc-unlock.com/
https://plchmiservo.com/
https://www.plcunlockbd.com/all-plc-and-hmi-password-unlock-softwarexs
https://crackpassword.com.vn/
https://tudonglienminh.com/product/unlock-password-crack-all-plc-hmi-v2-3-be-khoa-all-plc-hmi/
https://www.unlockplchmi.com/
```

# Ecosystem of Password Cracking Software

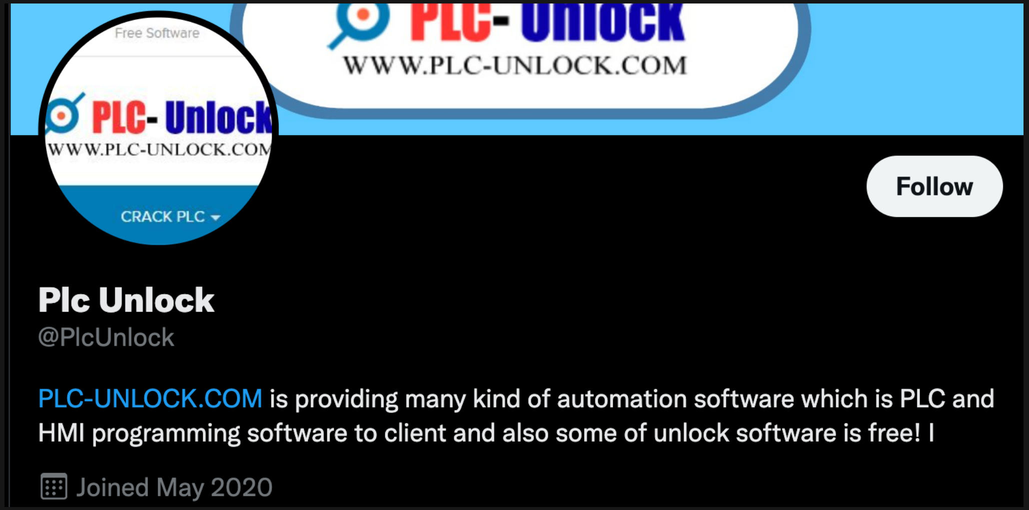
Simple Google searches lead to multiple Twitter accounts:



**PLC UNLOCK BD**
@plcunlockbd

PLC UNLOCK BD Provides You PLC password unlock and HMI Password Unlock services For FREE. We unlock all kinds of PLC and HMI passwords For FREE

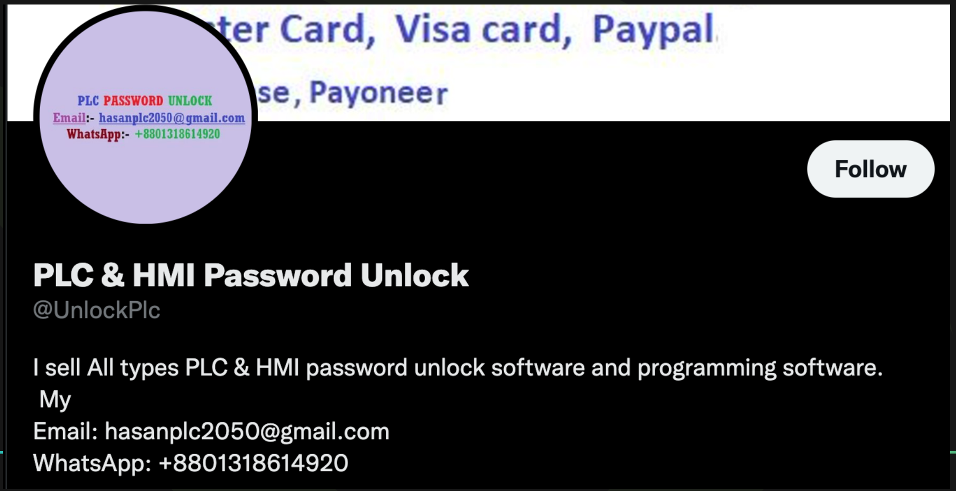
Automation Control Company ⓘ Joined February 2022



**Plc Unlock**
@PlcUnlock

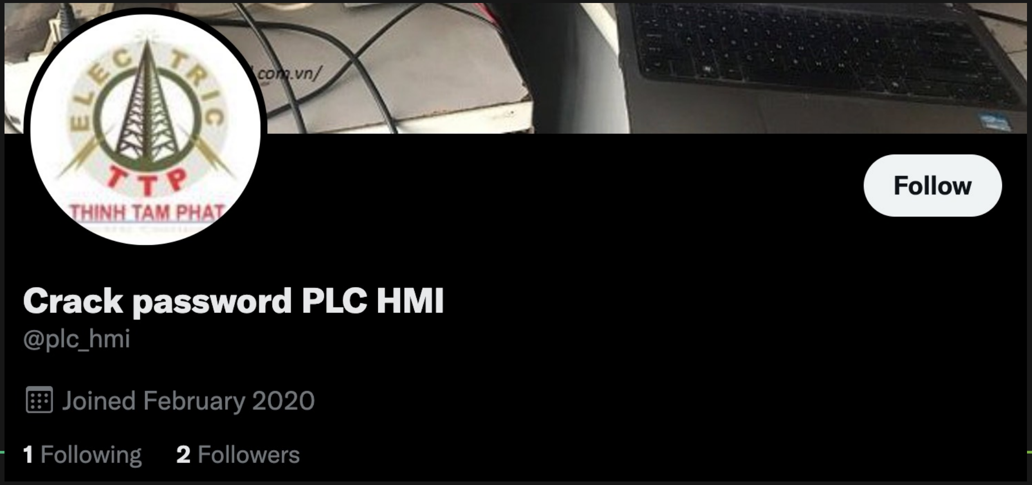
PLC-UNLOCK.COM is providing many kind of automation software which is PLC and HMI programming software to client and also some of unlock software is free! I

Joined May 2020


ter Card, Visa card, Paypal
se, Payoneer
PLC PASSWORD UNLOCK
Email:- hasanplc2050@gmail.com
WhatsApp:- +8801318614920
Follow

**PLC & HMI Password Unlock**
@UnlockPlc

I sell All types PLC & HMI password unlock software and programming software.
My
Email: hasanplc2050@gmail.com
WhatsApp: +8801318614920



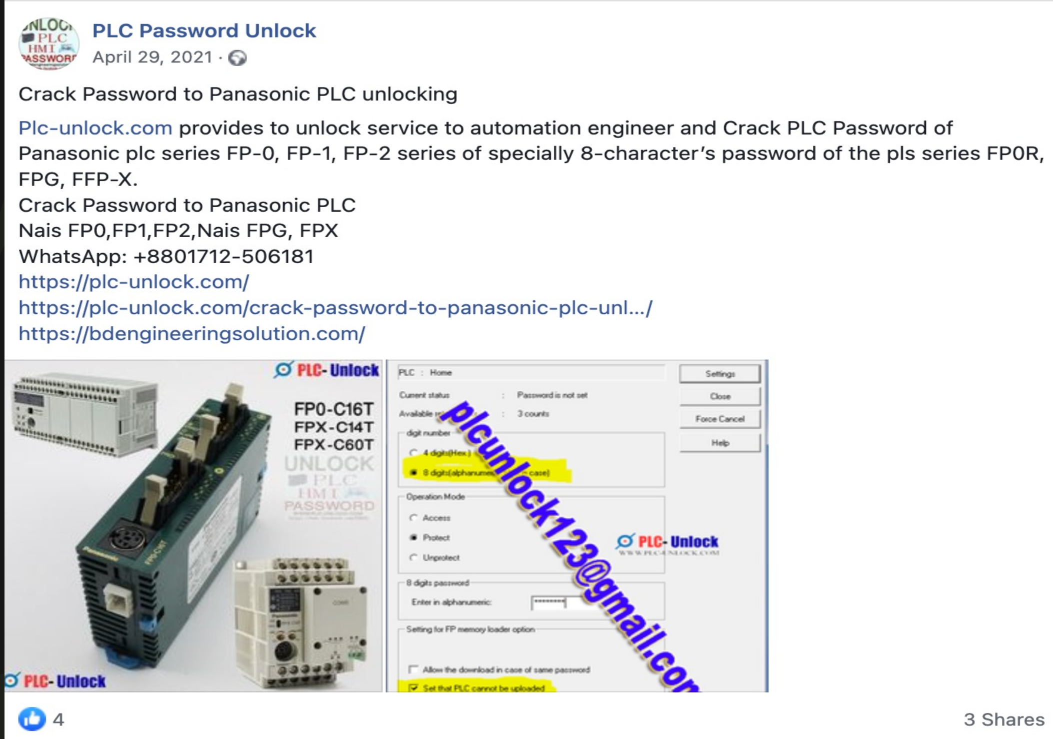
**Crack password PLC HMI**
@plc_hmi

Joined February 2020

**1** Following **2** Followers

# Ecosystem of Password Cracking Software

Simple Google searches lead to multiple Facebook accounts:



**PLC Password Unlock**
April 29, 2021 ·

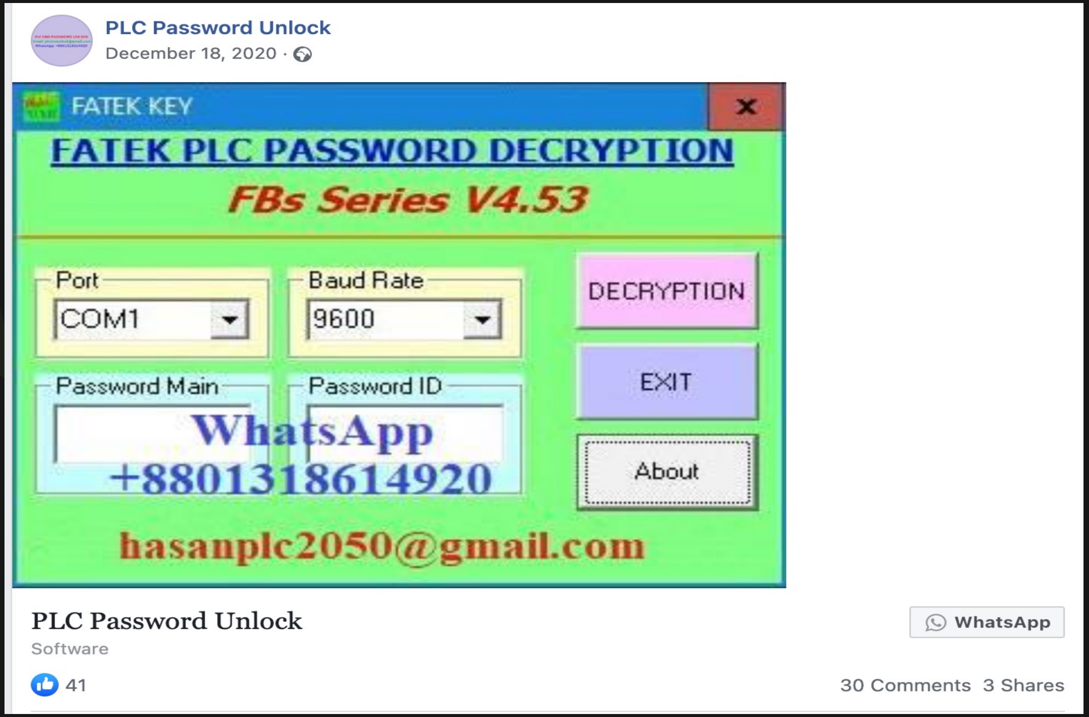
Crack Password to Panasonic PLC unlocking

Plc-unlock.com provides to unlock service to automation engineer and Crack PLC Password of Panasonic plc series FP-0, FP-1, FP-2 series of specially 8-character's password of the pls series FP0R, FPG, FFP-X.
Crack Password to Panasonic PLC
Nais FP0,FP1,FP2,Nais FPG, FPX
WhatsApp: +8801712-506181
https://plc-unlock.com/
https://plc-unlock.com/crack-password-to-panasonic-plc-unl.../
https://bdengineeringsolution.com/

PLC : Home
Current status : Password is not set
Available ... : 3 counts
digit number
○ 4 digits(Hex)
● 8 digits(alphanume... case)
Operation Mode
○ Access
● Protect
○ Unprotect
8 digits password
Enter in alphanumeric: ********
Setting for FP memory loader option
□ Allow the download in case of same password
☑ Set that PLC cannot be uploaded

4

3 Shares



**PLC Password Unlock**
December 18, 2020 ·

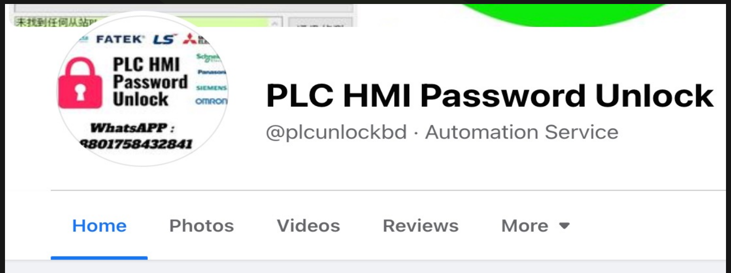
FATEK KEY
FATEK PLC PASSWORD DECRYPTION
FBs Series V4.53
Port: COM1
Baud Rate: 9600
Password Main
Password ID
WhatsApp +8801318614920
hasanplc2050@gmail.com

PLC Password Unlock
Software

WhatsApp

41

30 Comments 3 Shares



**PLC HMI Password Unlock**
@plcunlockbd · Automation Service

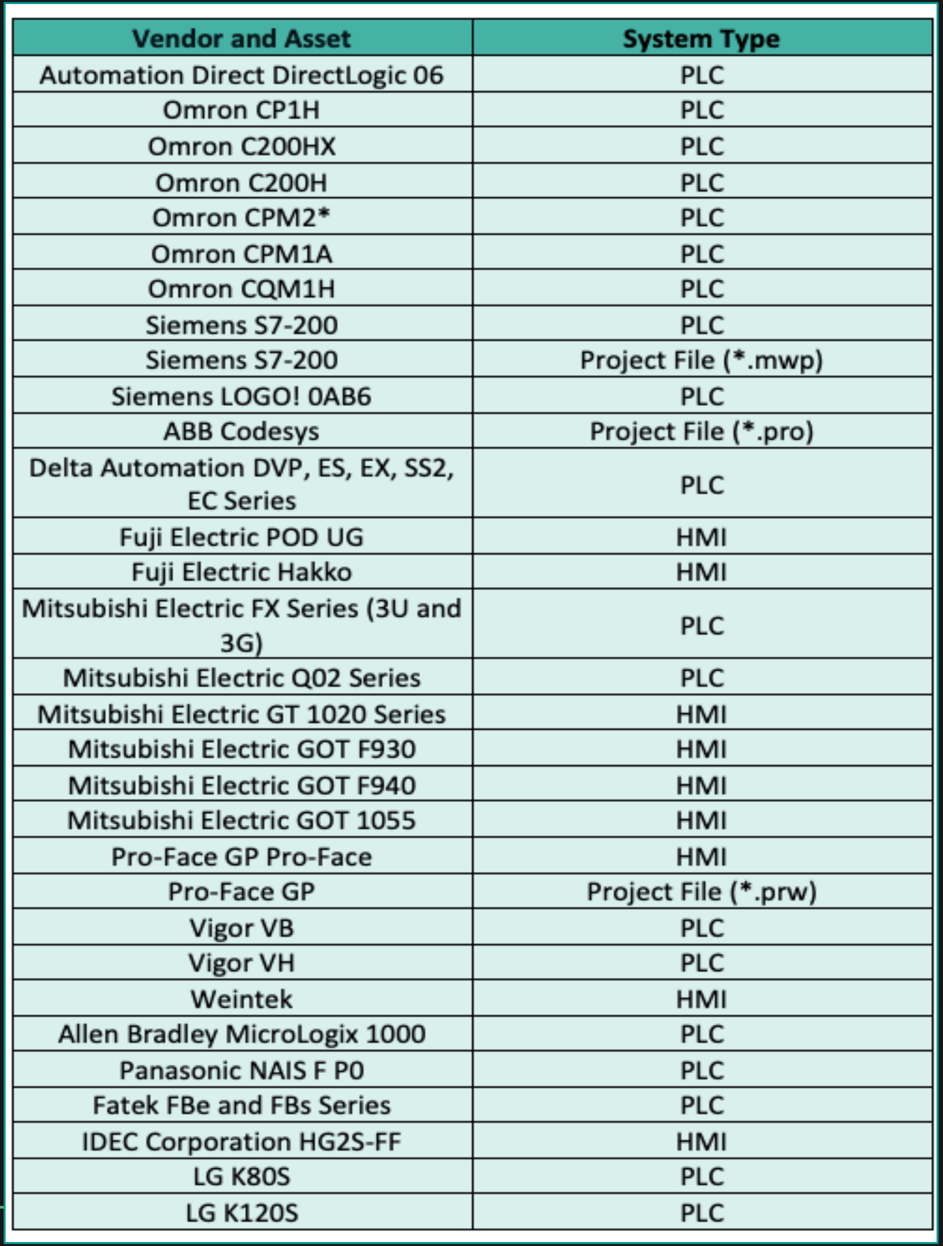
Home Photos Videos Reviews More ▾

# Complete List of Targeted Systems

Generated by combining samples found on VT and advertisements. Only a few of these have been tested!

S7-200 sample contains CoinMiner, which is exactly what it sounds like.

Variety of system types: PLC, HMI, and password-protected project files.



| Vendor and Asset | System Type |
|---|---|
| Automation Direct DirectLogic 06 | PLC |
| Omron CP1H | PLC |
| Omron C200HX | PLC |
| Omron C200H | PLC |
| Omron CPM2* | PLC |
| Omron CPM1A | PLC |
| Omron CQM1H | PLC |
| Siemens S7-200 | PLC |
| Siemens S7-200 | Project File (*.mwp) |
| Siemens LOGO! 0AB6 | PLC |
| ABB Codesys | Project File (*.pro) |
| Delta Automation DVP, ES, EX, SS2, EC Series | PLC |
| Fuji Electric POD UG | HMI |
| Fuji Electric Hakko | HMI |
| Mitsubishi Electric FX Series (3U and 3G) | PLC |
| Mitsubishi Electric Q02 Series | PLC |
| Mitsubishi Electric GT 1020 Series | HMI |
| Mitsubishi Electric GOT F930 | HMI |
| Mitsubishi Electric GOT F940 | HMI |
| Mitsubishi Electric GOT 1055 | HMI |
| Pro-Face GP Pro-Face | HMI |
| Pro-Face GP | Project File (*.prw) |
| Vigor VB | PLC |
| Vigor VH | PLC |
| Weintek | HMI |
| Allen Bradley MicroLogix 1000 | PLC |
| Panasonic NAIS F P0 | PLC |
| Fatek FBe and FBs Series | PLC |
| IDEC Corporation HG2S-FF | HMI |
| LG K80S | PLC |
| LG K120S | PLC |

# In Conclusion...

This research led to the discovery of a new attack methodology targeting industrial asset owners and operators.

As well as a variety of CVEs (happy to go more in depth on these vulnerabilities in the discussion room):

- CVE-2022-2003: Insufficiently Protected Credentials, CVSSv3 7.5
- CVE-2022-2004: Uncontrolled Resource Consumption, CVSSv3 7.5
- CVE-2022-2005: Cleartext Transmission of Sensitive Information, CVSSv3 7.5
- CVE-2022-2006: Uncontrolled Search Path Element, CVSSv3 7.0

# Questions to Kickstart Discussion

1. 0-day exploits are valuable and can be hard to find - why would a threat actor "waste" one on this?

2. Utilizing the intelligence collected on the malware and threat actor, how can we pivot to discover more malware artifacts?

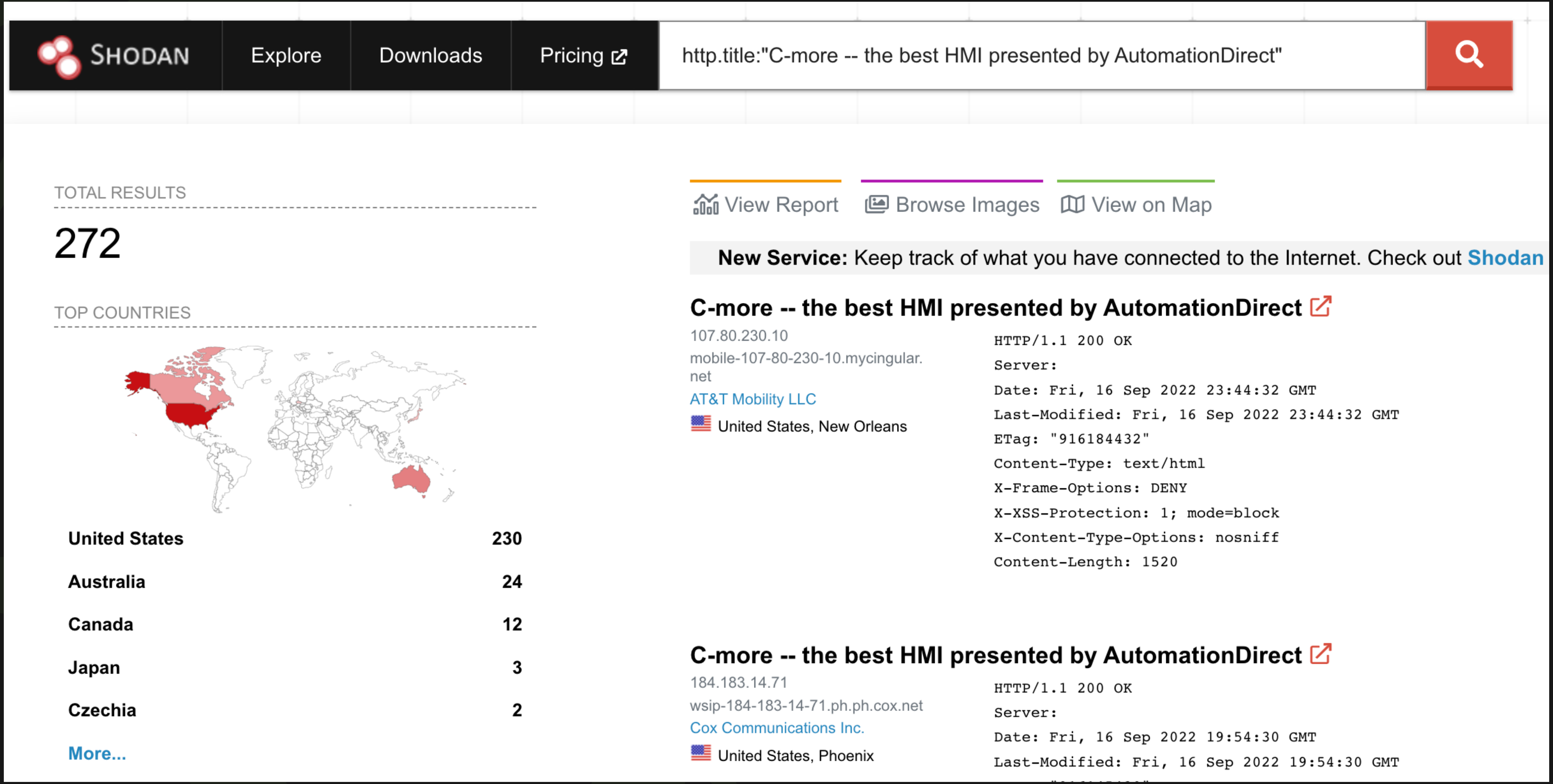
3. Assuming we lack basic antivirus, how could we know whether a machine was infected with Sality?

# Thank you!

Contact Information:

- Email: shanson@dragos.com
- Twitter: @secureloon

# Shodan



http.title:"C-more -- the best HMI presented by AutomationDirect"

TOTAL RESULTS

272

TOP COUNTRIES

| | |
|---|---|
| United States | 230 |
| Australia | 24 |
| Canada | 12 |
| Japan | 3 |
| Czechia | 2 |

More...

**New Service:** Keep track of what you have connected to the Internet. Check out Shodan

**C-more -- the best HMI presented by AutomationDirect**

107.80.230.10
mobile-107-80-230-10.mycingular.net
AT&T Mobility LLC
United States, New Orleans

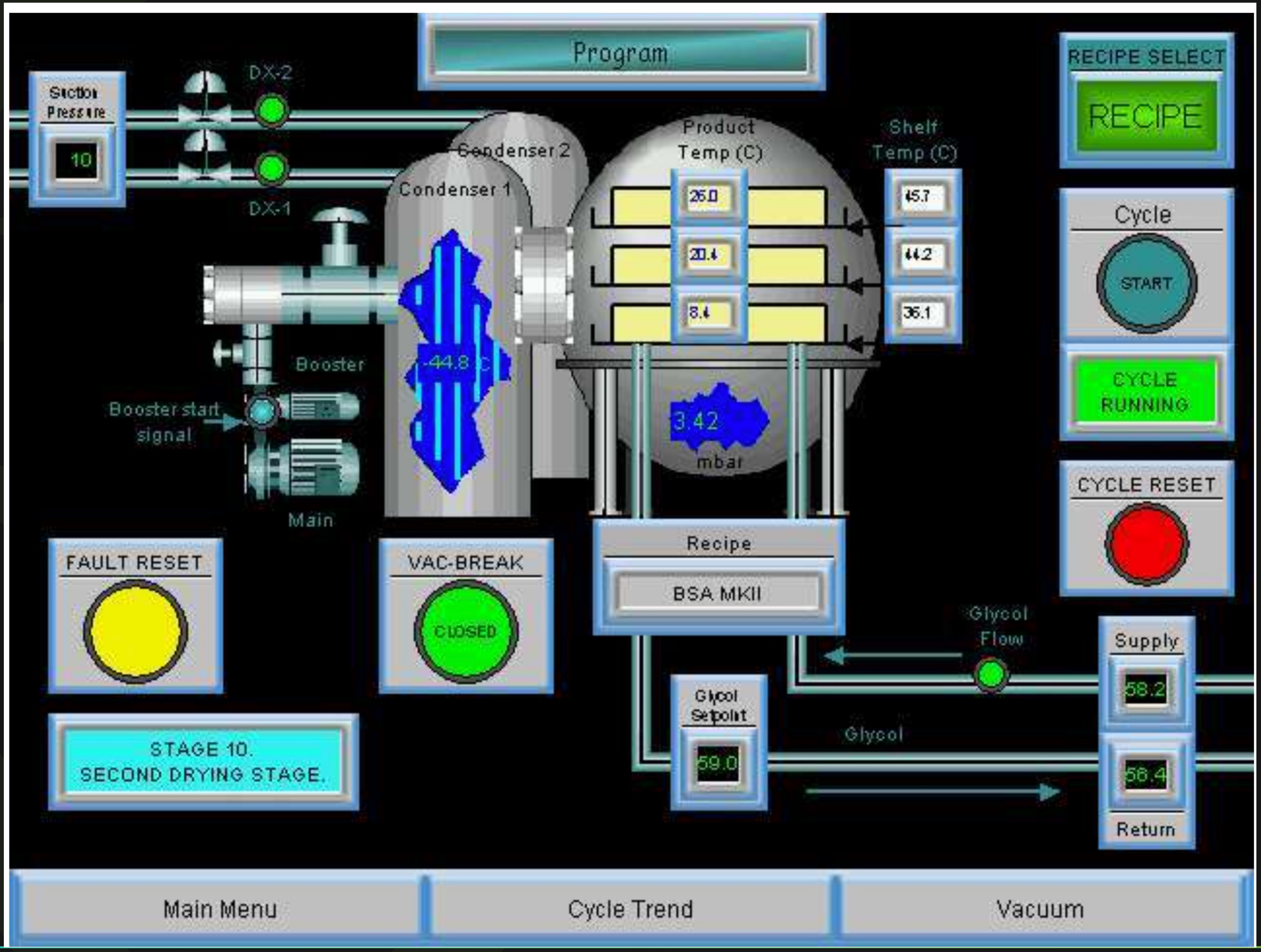
```
HTTP/1.1 200 OK
Server:
Date: Fri, 16 Sep 2022 23:44:32 GMT
Last-Modified: Fri, 16 Sep 2022 23:44:32 GMT
ETag: "916184432"
Content-Type: text/html
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 1520
```

**C-more -- the best HMI presented by AutomationDirect**

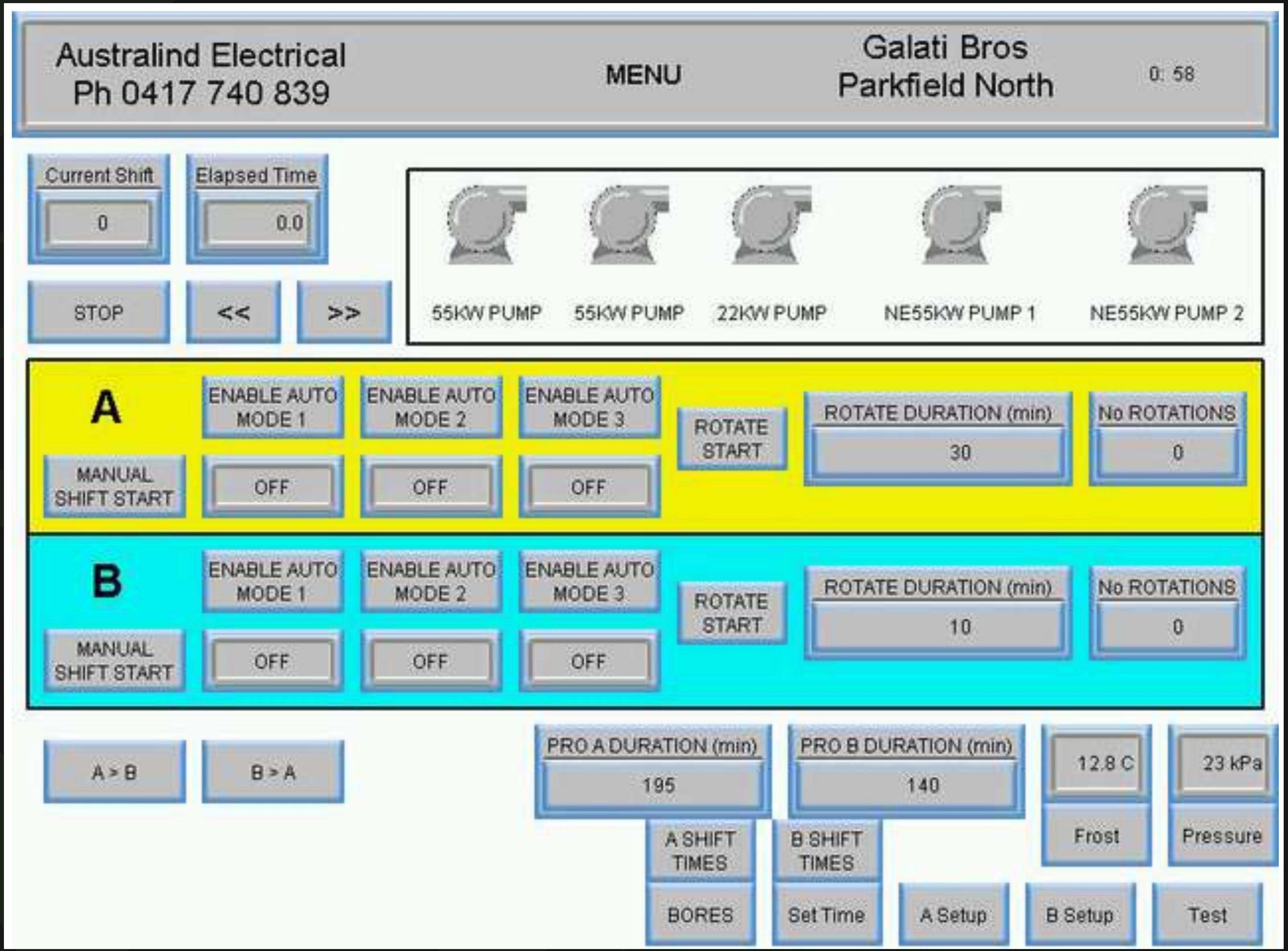
184.183.14.71
wsip-184-183-14-71.ph.ph.cox.net
Cox Communications Inc.
United States, Phoenix

```
HTTP/1.1 200 OK
Server:
Date: Fri, 16 Sep 2022 19:54:30 GMT
Last-Modified: Fri, 16 Sep 2022 19:54:30 GMT
```

# Shodan


Program
Suction Pressure
10
DX-2
DX-1
Condenser 2
Condenser 1
-44.8 C
Booster
Booster start signal
Main
Product Temp (C)
26.0
20.4
8.4
Shelf Temp (C)
45.7
44.2
36.1
3.42
mbar
RECIPE SELECT
RECIPE
Cycle
START
CYCLE RUNNING
CYCLE RESET
FAULT RESET
VAC-BREAK
CLOSED
Recipe
BSA MKII
Glycol Flow
Supply
58.2
Glycol Setpoint
59.0
Glycol
56.4
Return
STAGE 10.
SECOND DRYING STAGE.
Main Menu
Cycle Trend
Vacuum

# Shodan



Australind Electrical
Ph 0417 740 839

MENU

Galati Bros
Parkfield North

0: 58

Current Shift
0

Elapsed Time
0.0

A

ROTATE DURATION (min)
30

No ROTATIONS
0

B

ROTATE DURATION (min)
10

No ROTATIONS
0

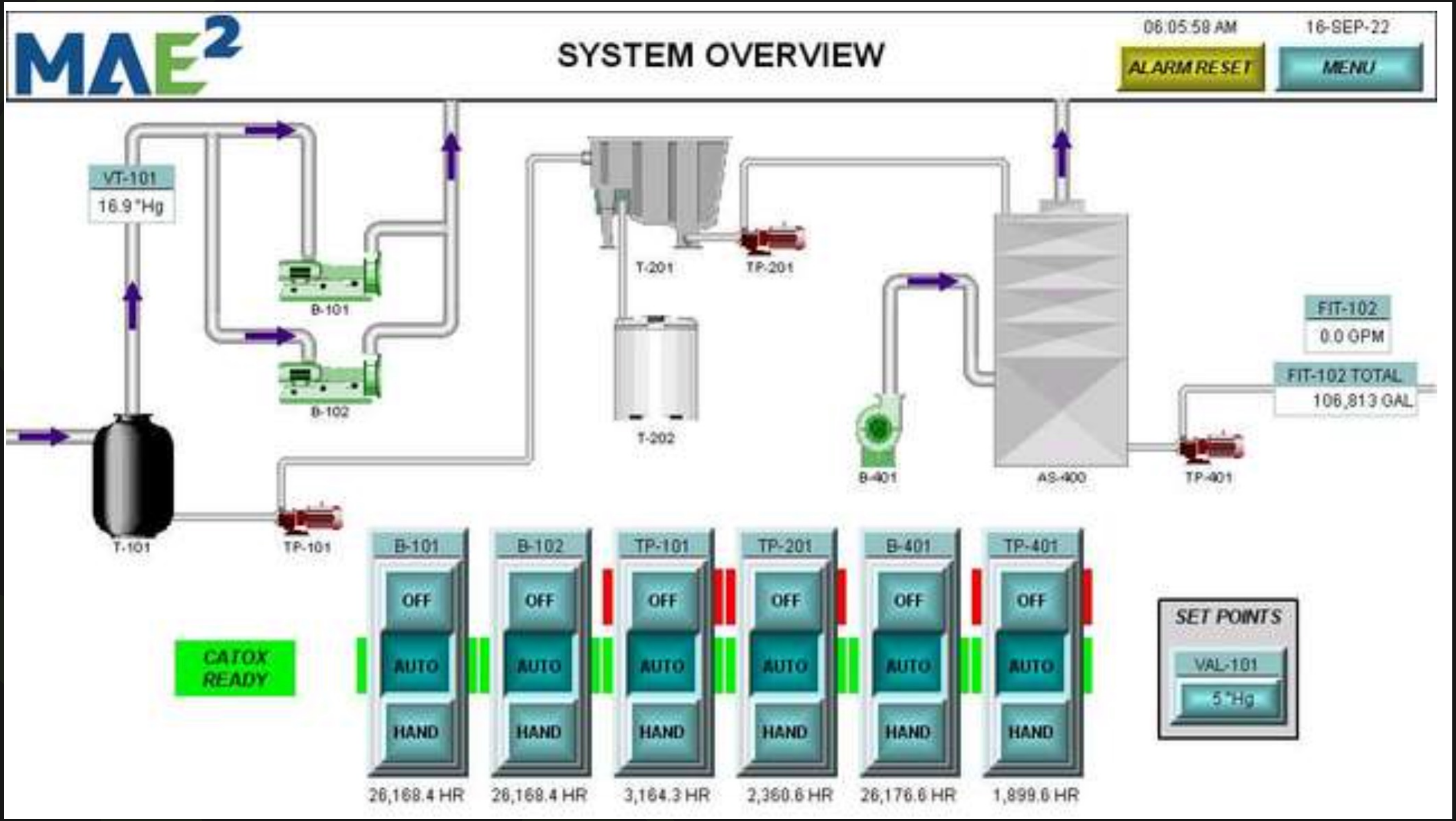
PRO A DURATION (min)
195

PRO B DURATION (min)
140

12.8 C
Frost

23 kPa
Pressure

# Shodan



SYSTEM OVERVIEW

06:05:58 AM 16-SEP-22

VT-101 16.9 "Hg

FIT-102 0.0 GPM

FIT-102 TOTAL 106,813 GAL

SET POINTS

VAL-101 5 "Hg

| B-101 | B-102 | TP-101 | TP-201 | B-401 | TP-401 |
|---|---|---|---|---|---|
| 26,168.4 HR | 26,168.4 HR | 3,164.3 HR | 2,360.6 HR | 26,176.6 HR | 1,899.6 HR |