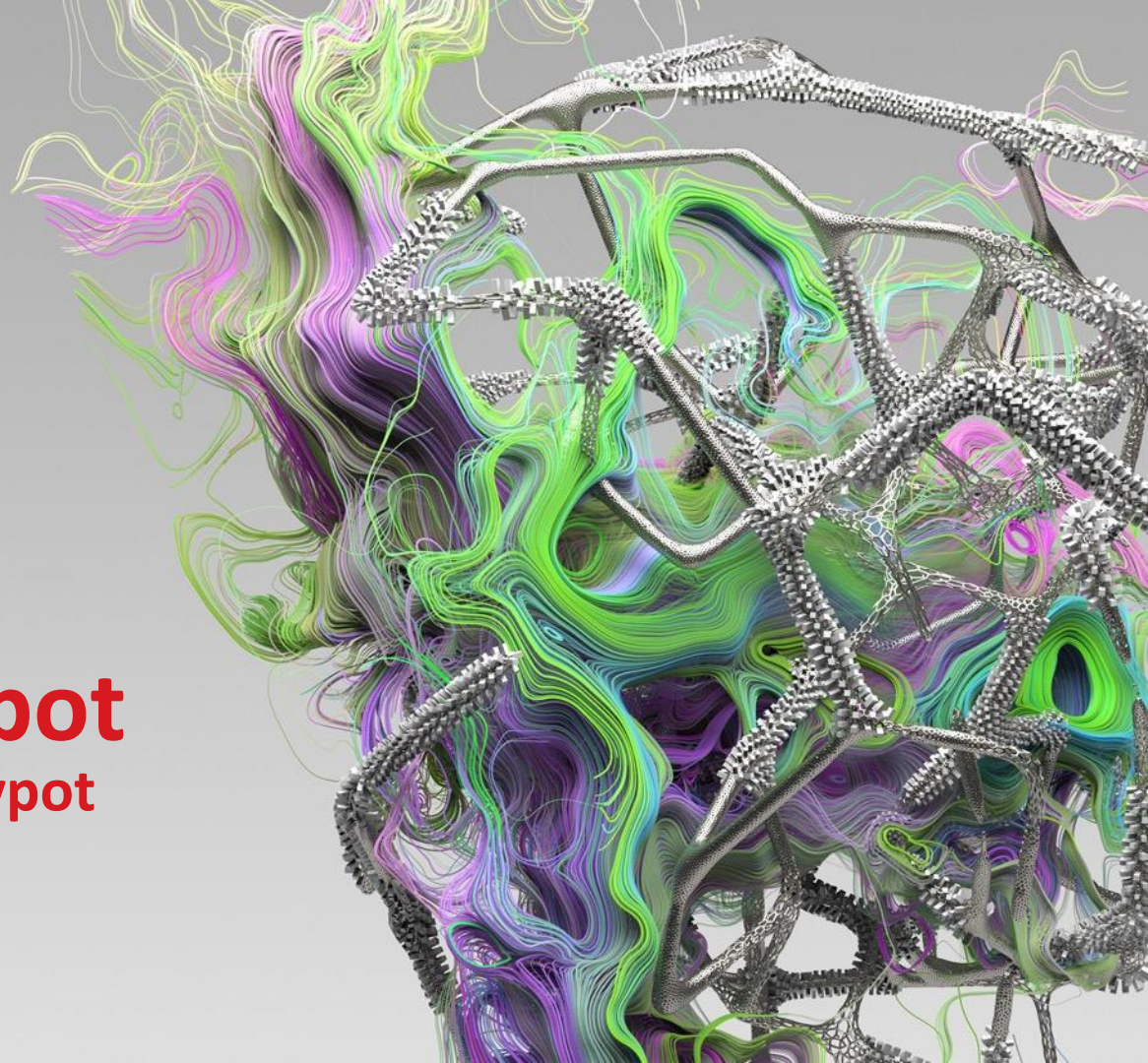


Factory Honeypot

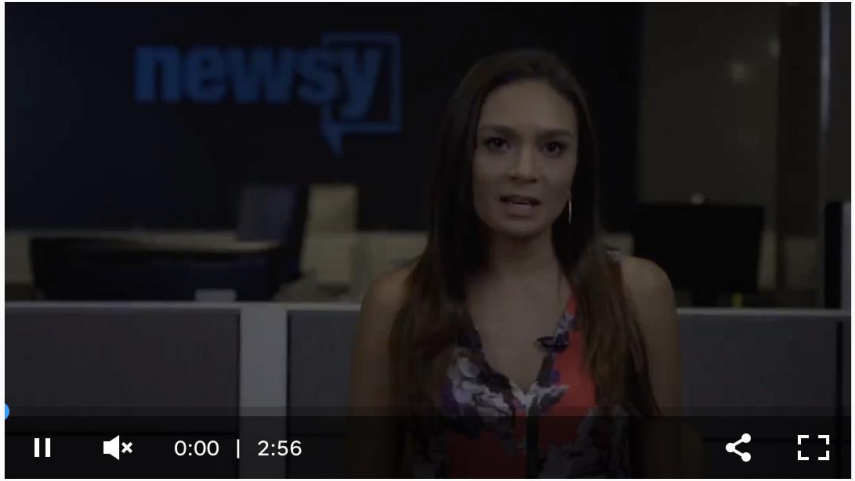
A High Interaction Honeypot

Stephen J. Hilt

1/21/2020

Hackers looking to shut down NC factories for pay

AP Business Writer Published 10:53 a.m. ET Aug. 9, 2017



A group of U.S. senators are urging the president to make moves protecting the nation's power grid. Video provided by Newsy Newslook

(Photo: AP)

CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

DURHAM - The malware entered the North Carolina transmission plant's computer network via email last August, just as the criminals wanted, spreading like a virus and threatening to lock up the production line until the company paid a ransom.

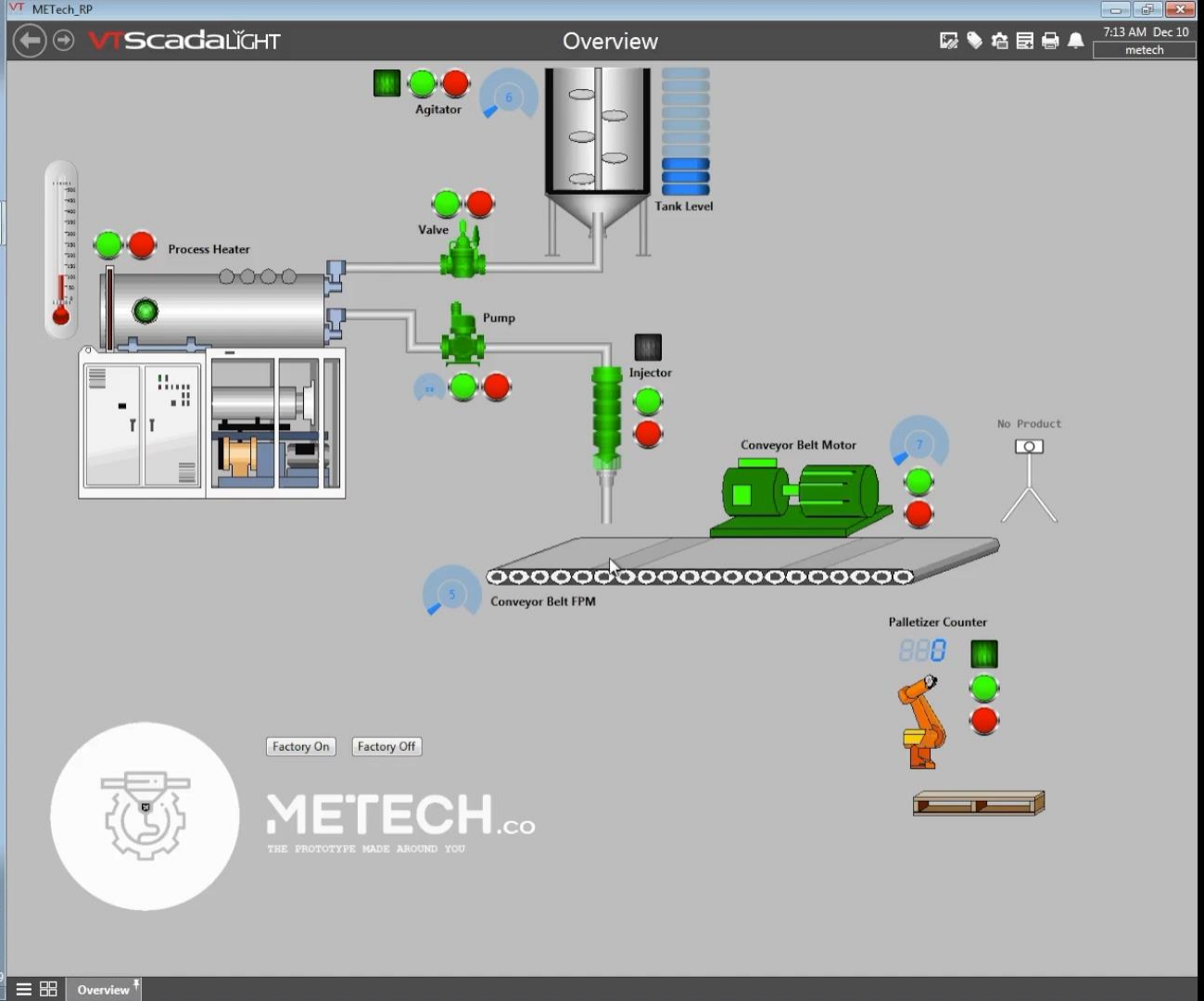
MORE STORIES

Buncombe property transfers for Nov. 18-27
Dec. 15, 2019, 6 a.m.

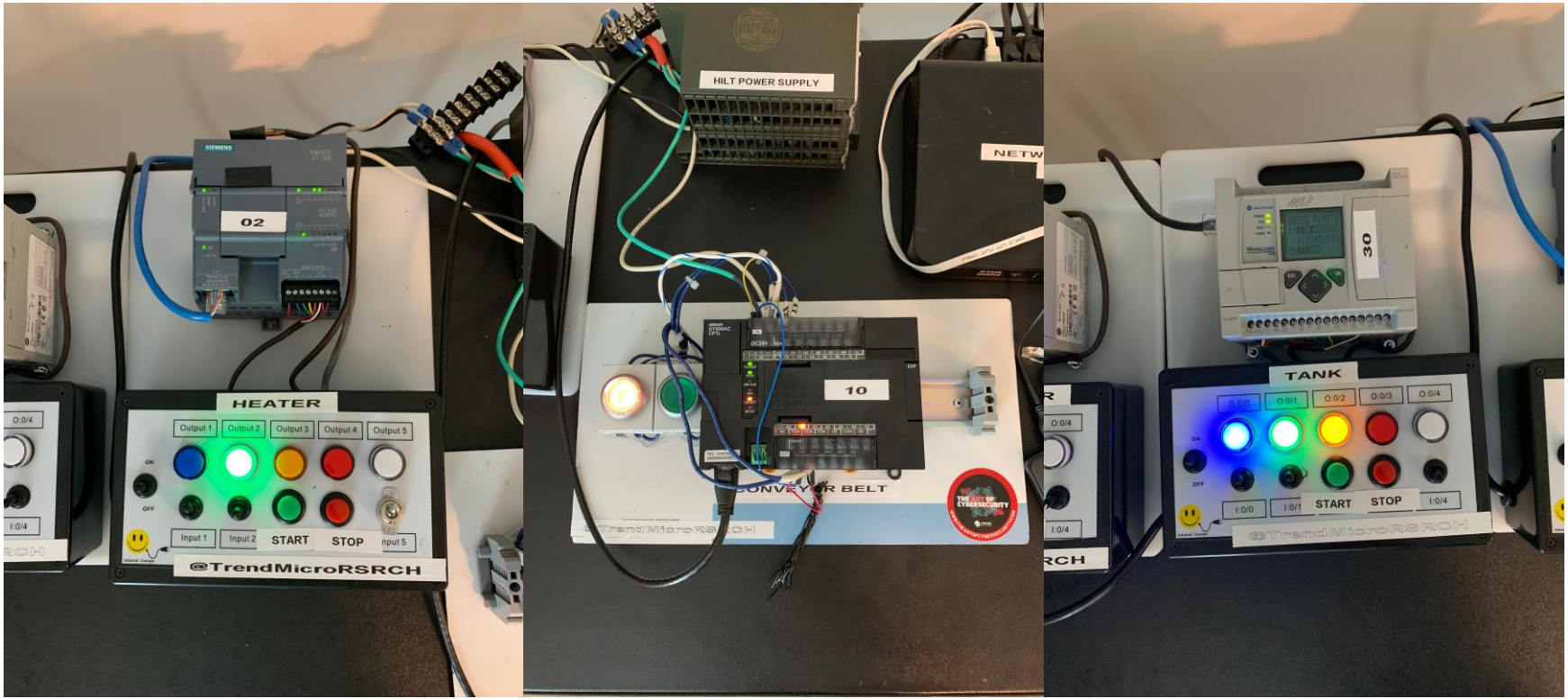
Buncombe property transfers for Nov. 12-15
Dec. 9, 2019, 7:05 a.m.

Buncombe, Asheville property transfers for Nov. 5-8
Dec. 1, 2019, 3:05 p.m.

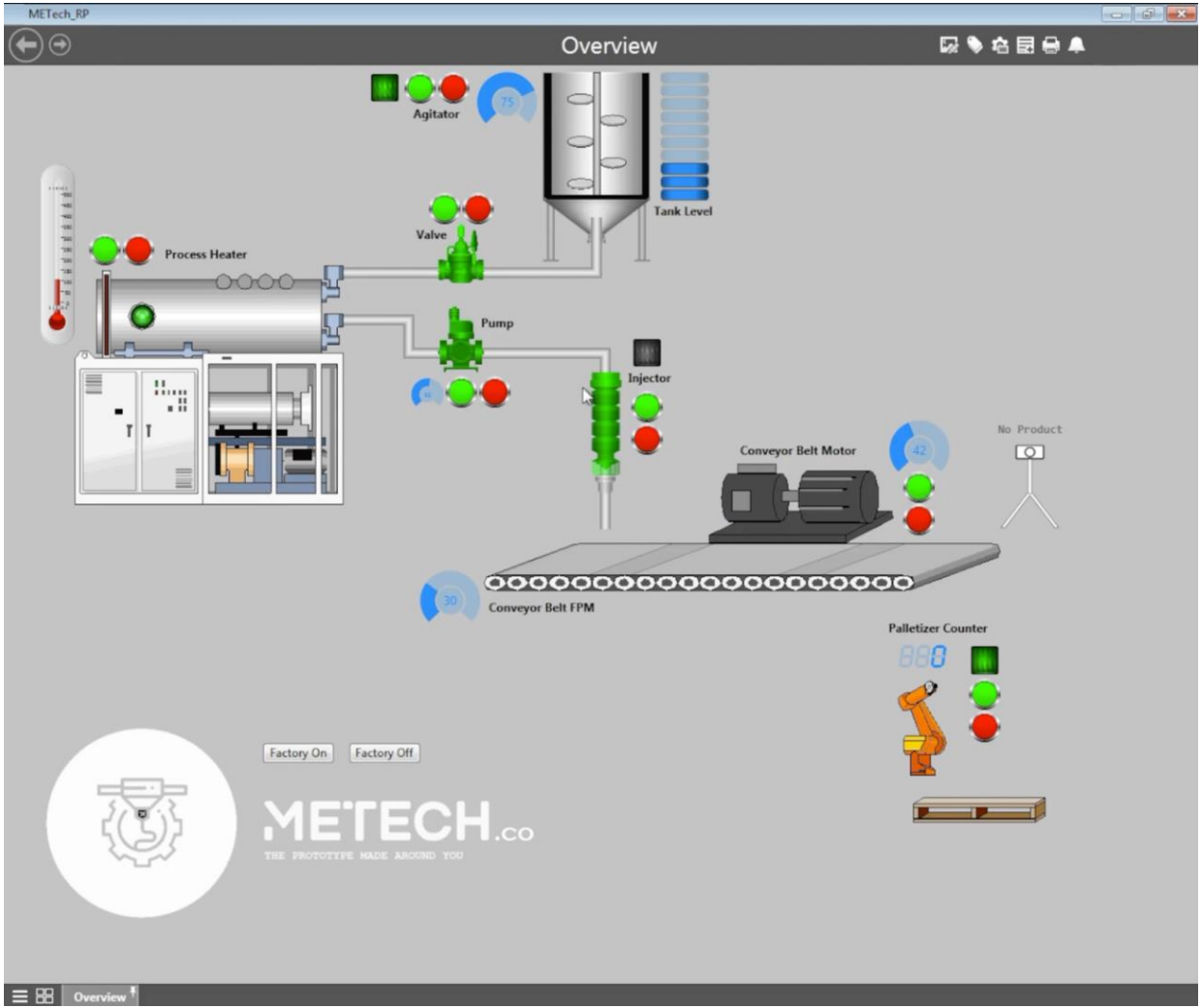
Buncombe property transfers for Nov. 1-4, 2019


METech_RP
VTScadaLIGHT
Overview
7:13 AM Dec 10
metech
Agitator
Tank Level
Valve
Process Heater
Pump
Injector
Conveyor Belt Motor
No Product
Conveyor Belt FPM
Palletizer Counter
Factory On
Factory Off
METECH.co
THE PROTOTYPE MADE AROUND YOU
Overview
7:13 AM
12/10/2019

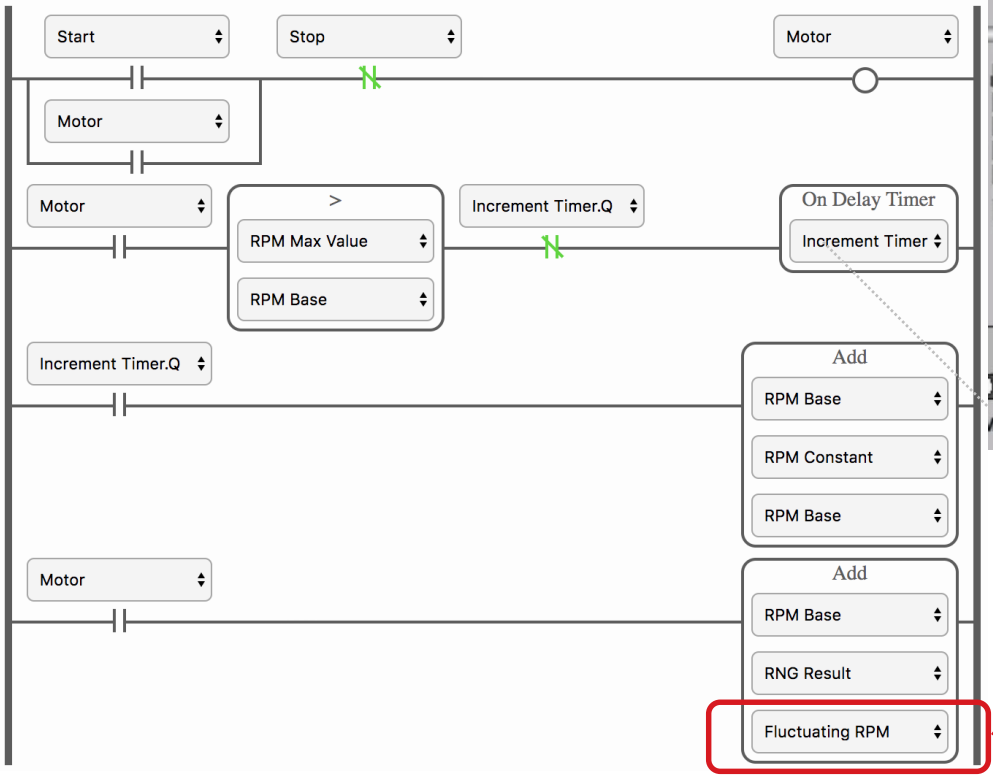
Equipment

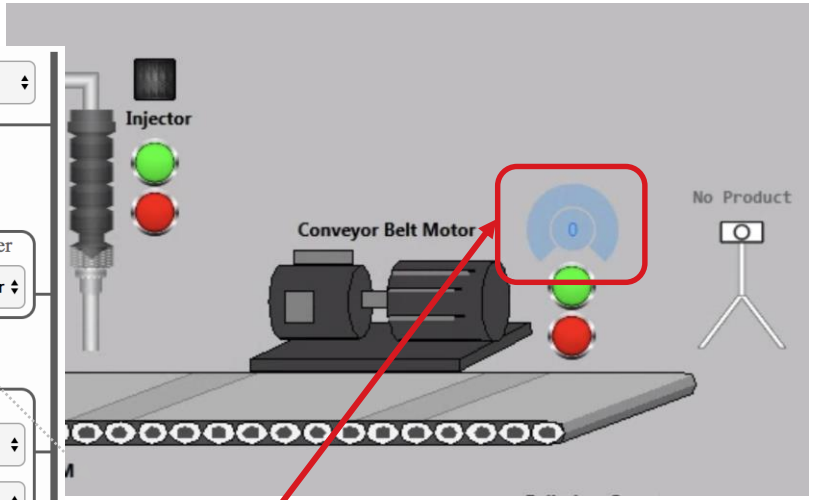

HILT POWER SUPPLY
02
10
30
HEATER
TANK
Output 1
Output 2
Output 3
Output 4
Output 5
Input 1
START
STOP
@TrendMicroRSRCH
CONVEYOR BELT

HMI


METech_RP
Overview
Agitator
Tank Level
Valve
Process Heater
Pump
Injector
No Product
Conveyor Belt Motor
Conveyor Belt FPM
Palletizer Counter
Factory On
Factory Off
METECH.co
THE PROTOTYPE MADE AROUND YOU
Overview

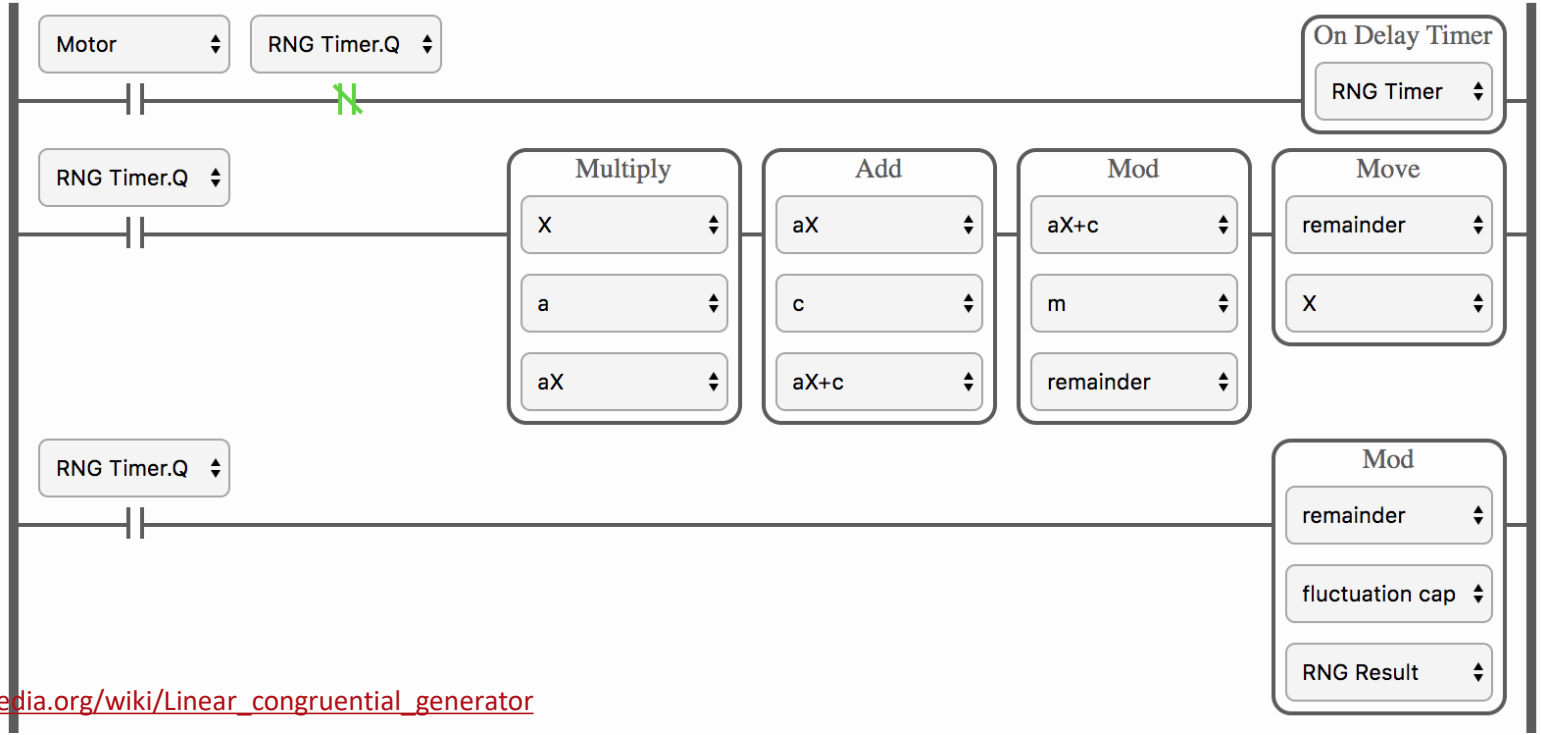
Logic – Motor RPM Fluctuations



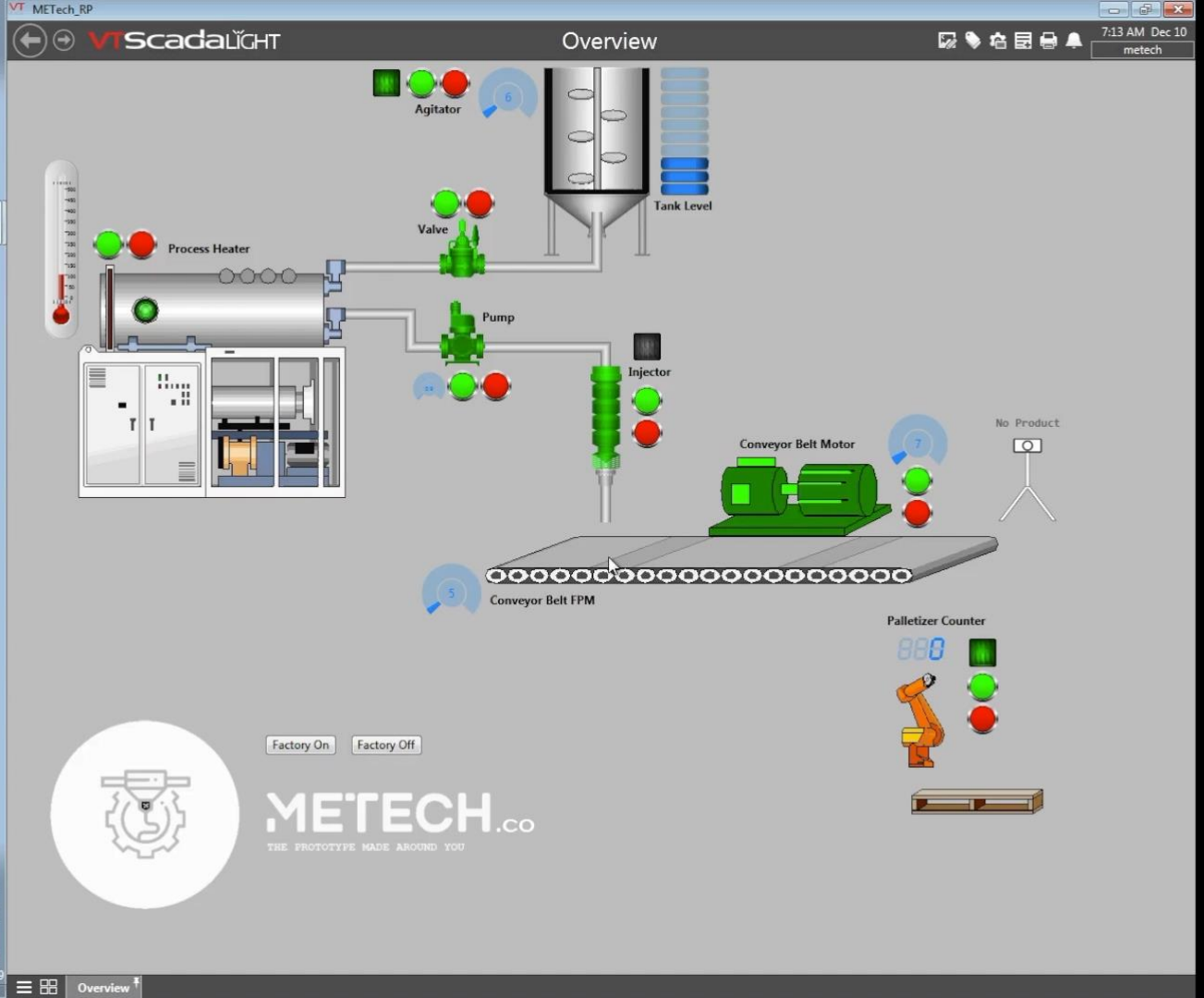


Logic – RNG Block

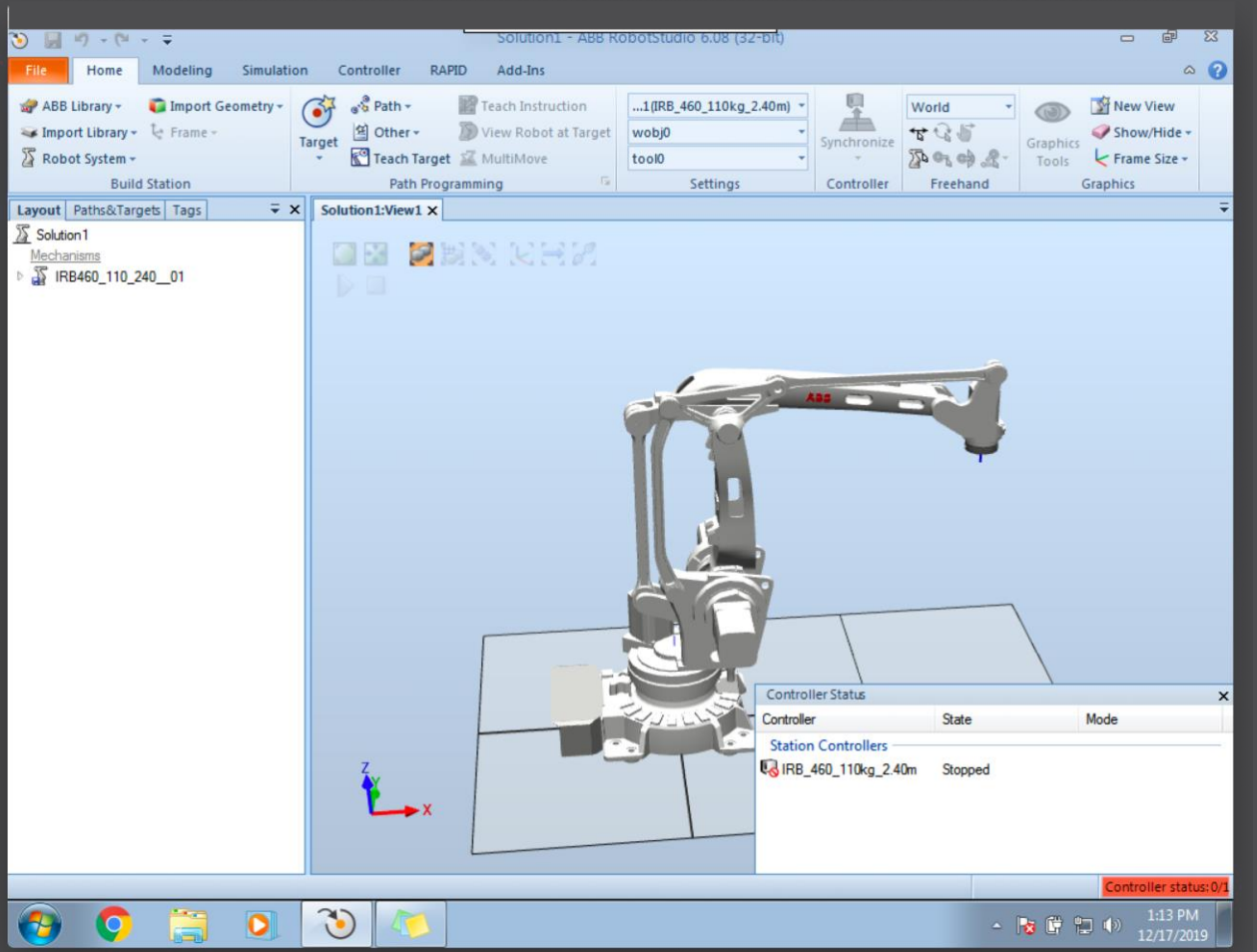
- Linear congruential generator $X_{n+1} = (aX_n + c) \mod m$



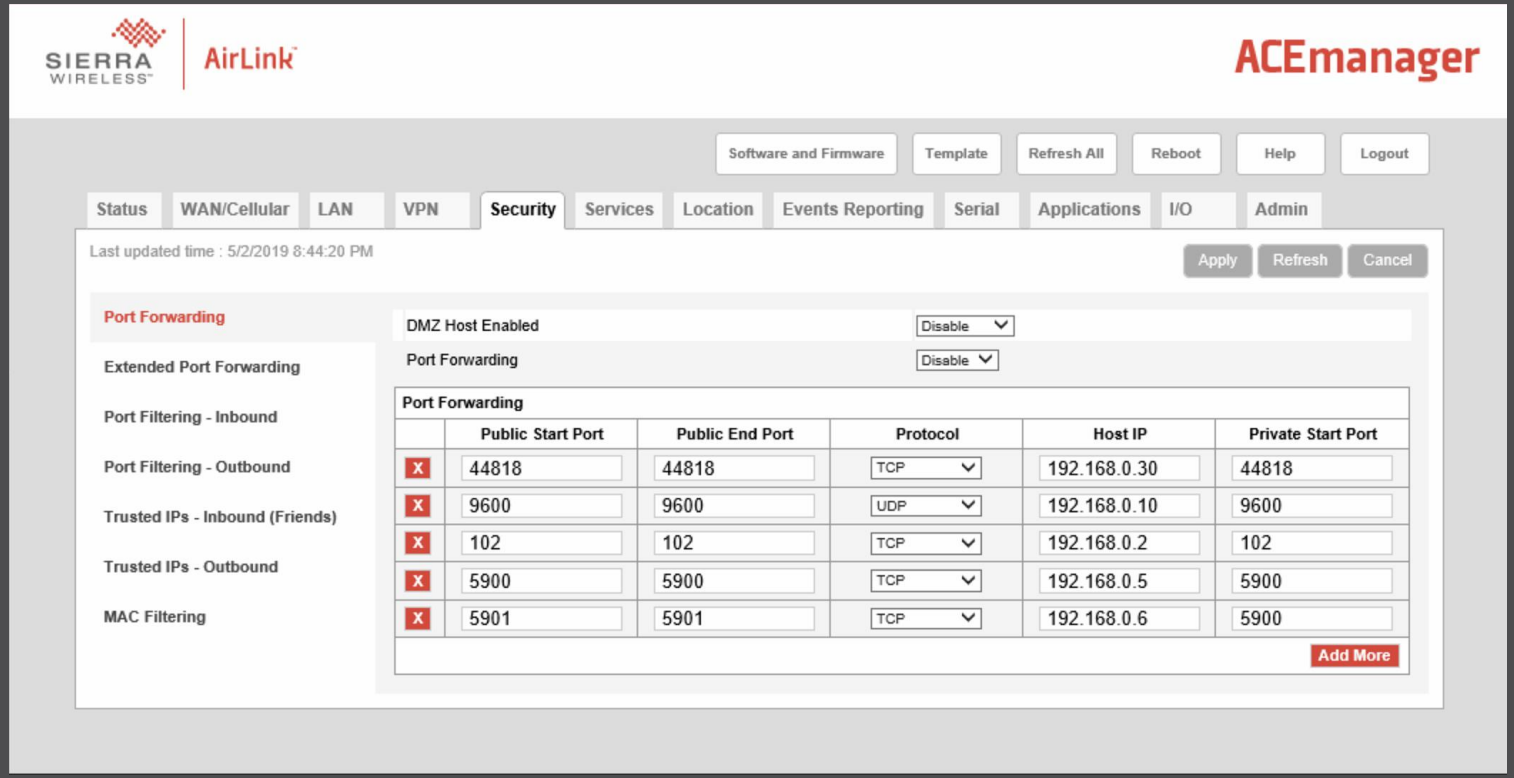
Source: https://en.wikipedia.org/wiki/Linear_congruential_generator


METech_RP
VTScadaLIGHT
Overview
7:13 AM Dec 10
metech
Agitator
Tank Level
Valve
Process Heater
Pump
Injector
Conveyor Belt Motor
No Product
Conveyor Belt FPM
Palletizer Counter
Factory On
Factory Off
METECH.co
THE PROTOTYPE MADE AROUND YOU
Overview
7:13 AM
12/10/2019

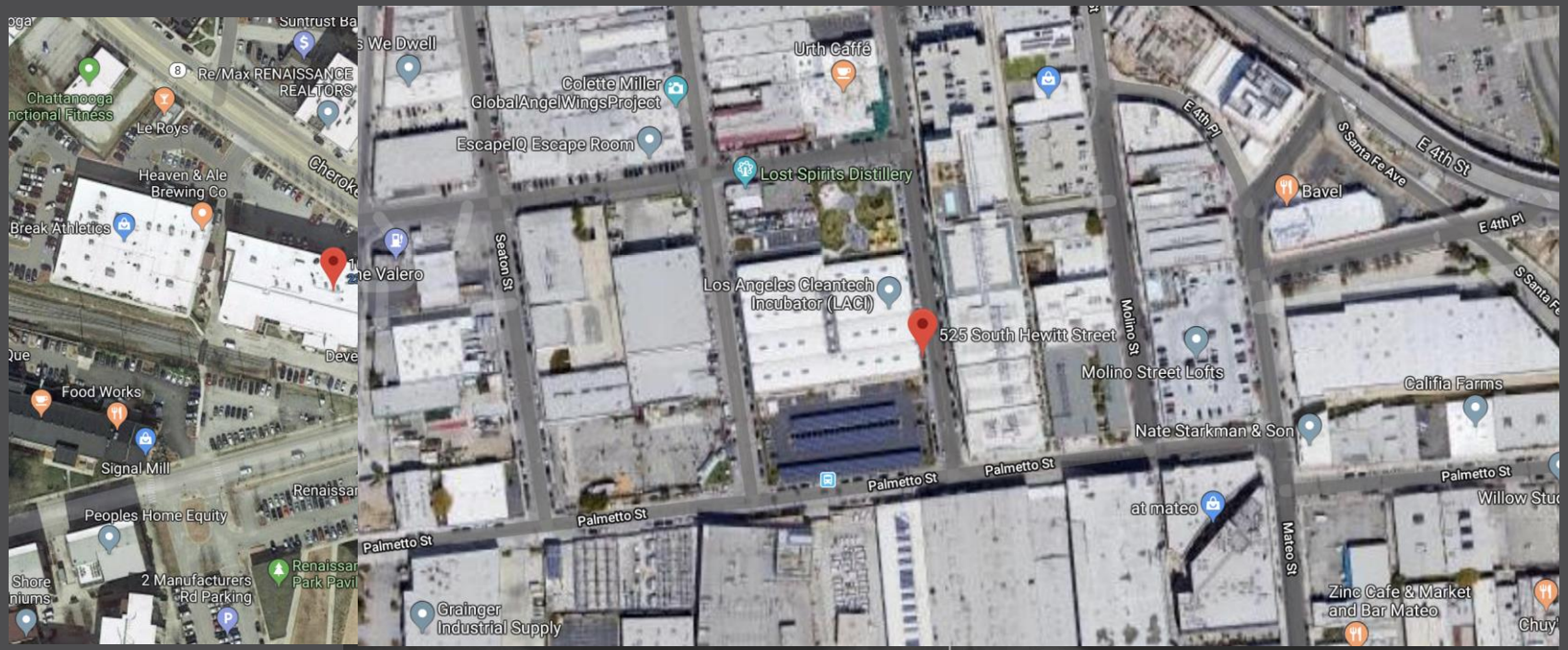
Robotics


Solution1 - ABB RobotStudio 6.08 (32-bit)
File
Home
Modeling
Simulation
Controller
RAPID
Add-Ins
ABB Library
Import Library
Robot System
Import Geometry
Frame
Build Station
Target
Path
Other
Teach Target
Teach Instruction
View Robot at Target
MultiMove
Path Programming
...1(IRB_460_110kg_2.40m)
wobj0
tool0
Settings
Synchronize
Controller
World
Freehand
Graphics Tools
New View
Show/Hide
Frame Size
Graphics
Layout
Paths&Targets
Tags
Solution1
Mechanisms
IRB460_110_240__01
Solution1:View1
Controller Status
Controller
State
Mode
Station Controllers
IRB_460_110kg_2.40m
Stopped
Controller status: 0/1
1:13 PM
12/17/2019

The Hole Story



The Company

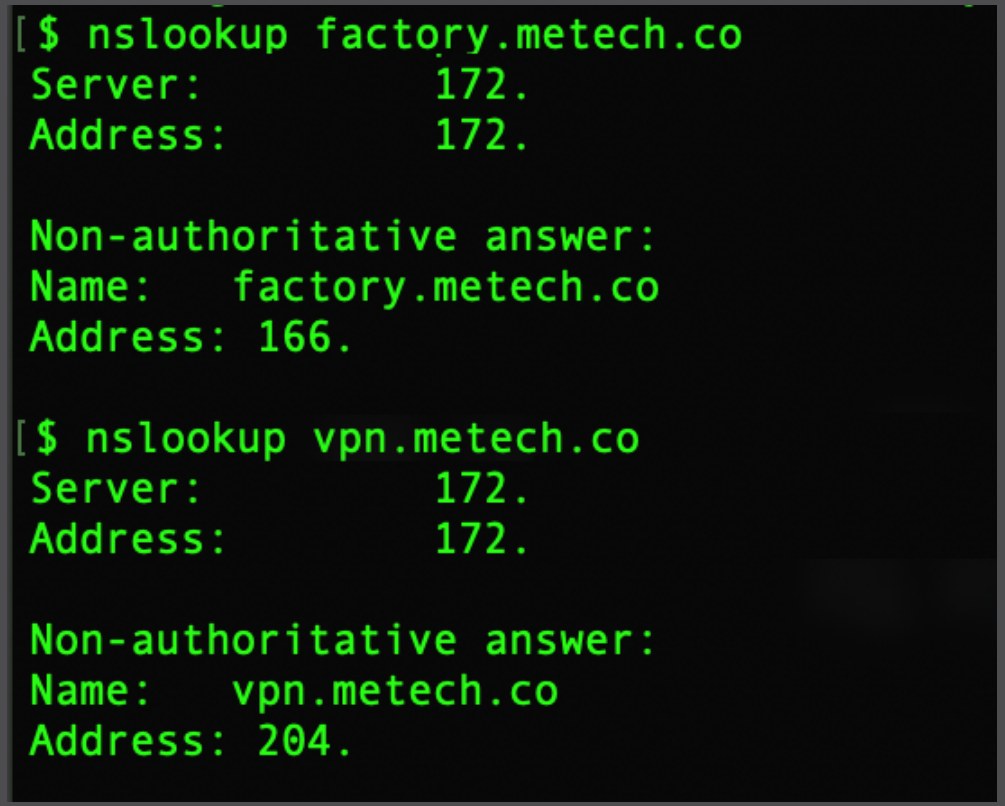


Engineering: +1 (423) 235-8388, 100 Cherokee Blvd, Chattanooga, TN 37405, USA.

Offices: +1 (213) 338-1513, 525 S Hewitt St, Los Angeles, CA 90013, USA

The Company

The Company


$ nslookup factory.metech.co
Server: 172.
Address: 172.
Non-authoritative answer:
Name: factory.metech.co
Address: 166.
$ nslookup vpn.metech.co
Server: 172.
Address: 172.
Non-authoritative answer:
Name: vpn.metech.co
Address: 204.

The Company

MIKE WILSON, PHD

Mike is an exceptional maker. His doctorate in Applied Mathematics gives him knowledge needed to design and create anything he can think of.

In his previous job, Mike learned how to make prototypes—which he is known to tinker in his garage long into the night —while still being able to meet enterprise-level quality requirements. This is why Mike is the natural fit to be our chief in house maker.

JANS FISHER, MSC

Jans knows how to automate anything, from a simple trigger switch to a complex building or industrial plant. Jans brings a long history of automation to the table, being able to automate our factory on the fly to meet the customers demands.

Jans has a master in Electronic Engineering, and worked for several firms in the oil, mining, and manufacturing sectors.

The Company

EMILY CLARK, MSC

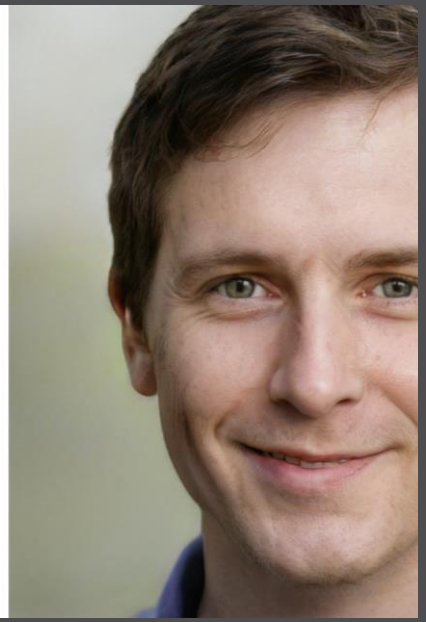
Emily is a very clever programmer and passionate 3D-printing geek. She created the custom firmware that runs on all our robots and 3D printers, which allows us unprecedented precision and speed compared to ready-made solutions.

Having learned CAD at college, she takes care of putting all our sketches into digital twins.

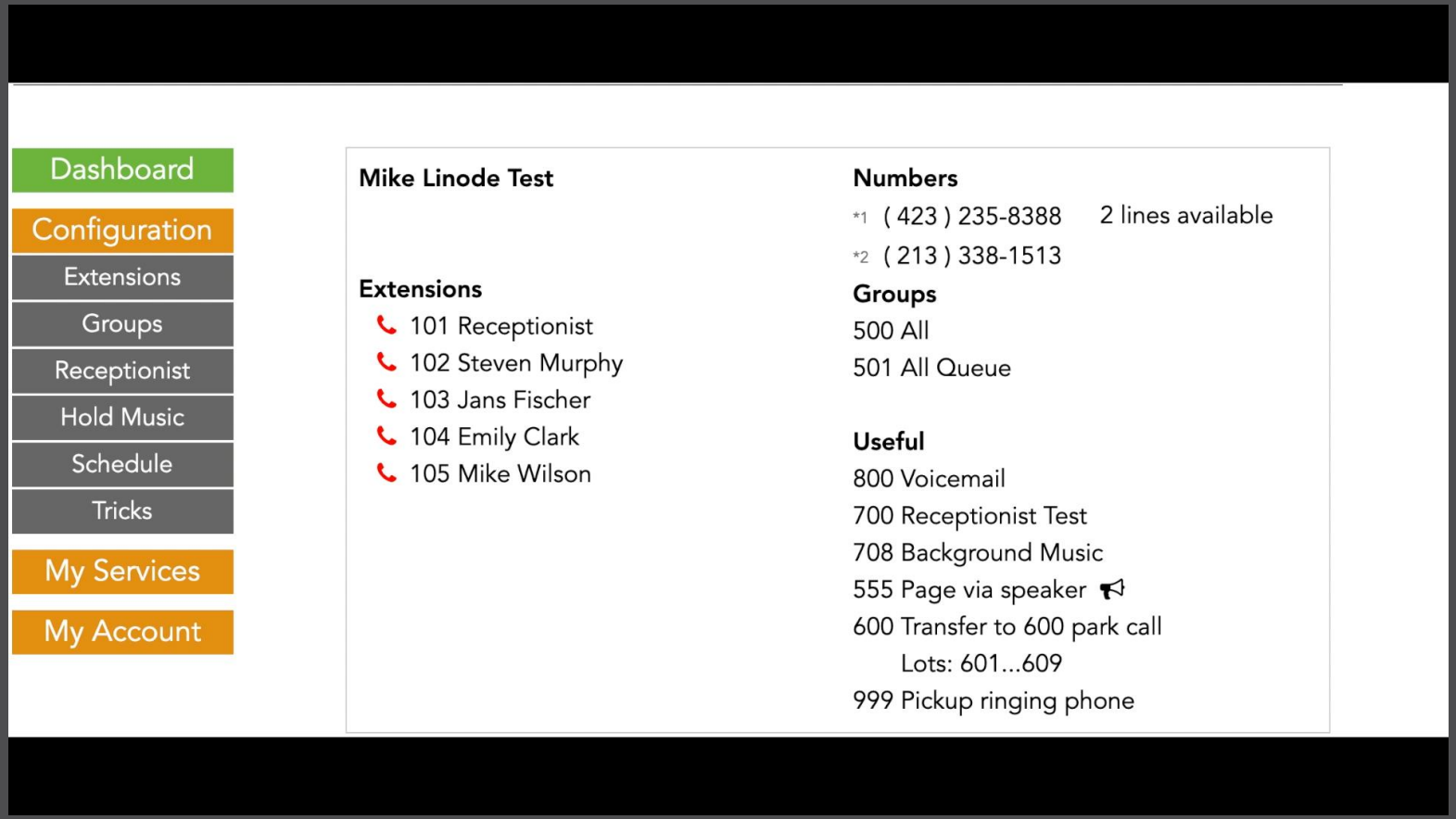
STEVEN MURPHY, PHD

Steven has a doctorate degree in Aviation Safety and started his career at one of the largest aircraft manufacturers in Europe, where he was responsible for implementing safety requirements for automated emergency landing procedures.

Steven knows all about international safety standards, and helps everyone ensure that the moving parts of our larger prototypes are compliant.

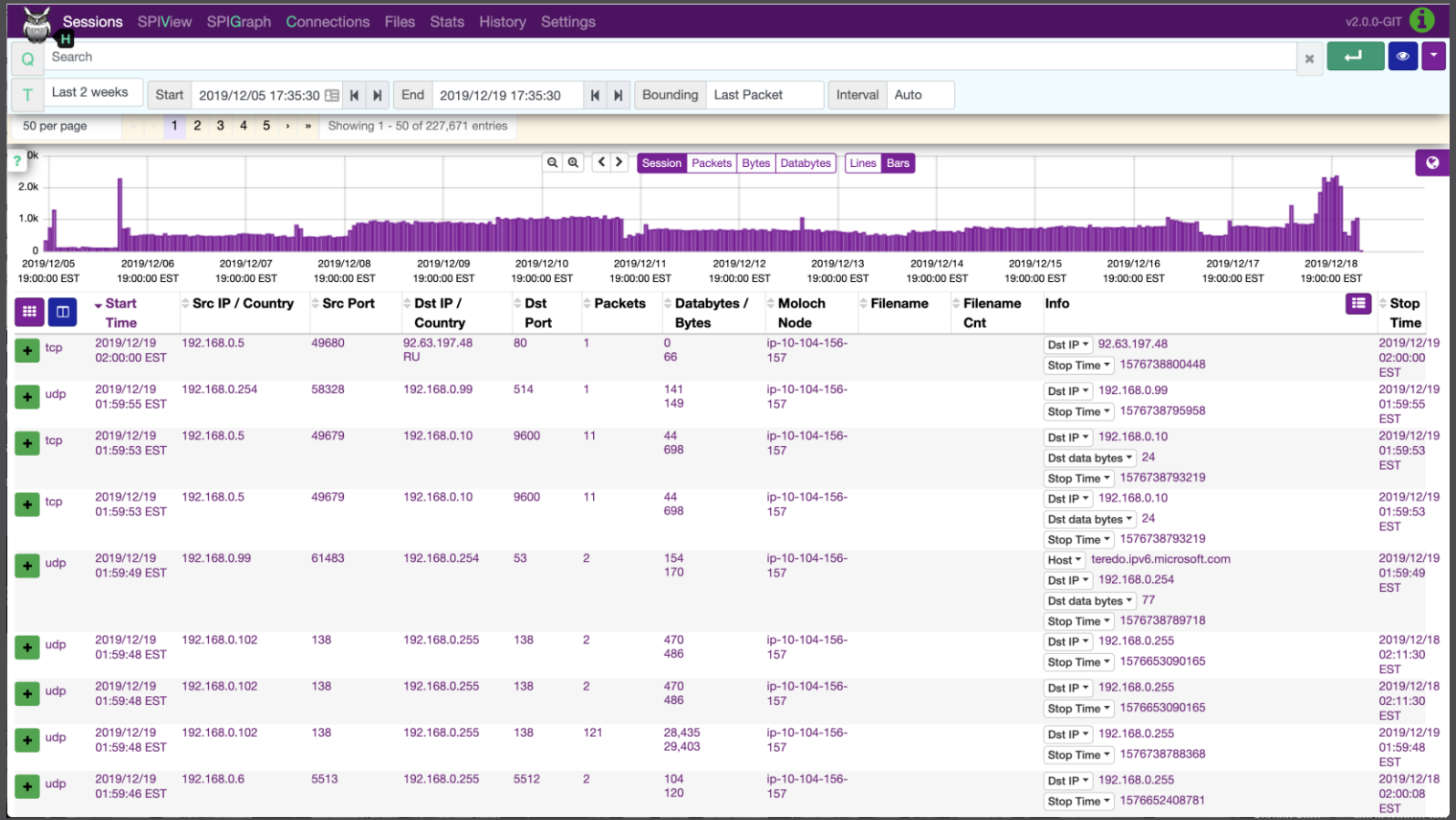


The Company


Dashboard
Configuration
Extensions
Groups
Receptionist
Hold Music
Schedule
Tricks
My Services
My Account
Mike Linode Test
Extensions
101 Receptionist
102 Steven Murphy
103 Jans Fischer
104 Emily Clark
105 Mike Wilson
Numbers
*1 (423) 235-8388 2 lines available
*2 (213) 338-1513
Groups
500 All
501 All Queue
Useful
800 Voicemail
700 Receptionist Test
708 Background Music
555 Page via speaker
600 Transfer to 600 park call
Lots: 601...609
999 Pickup ringing phone

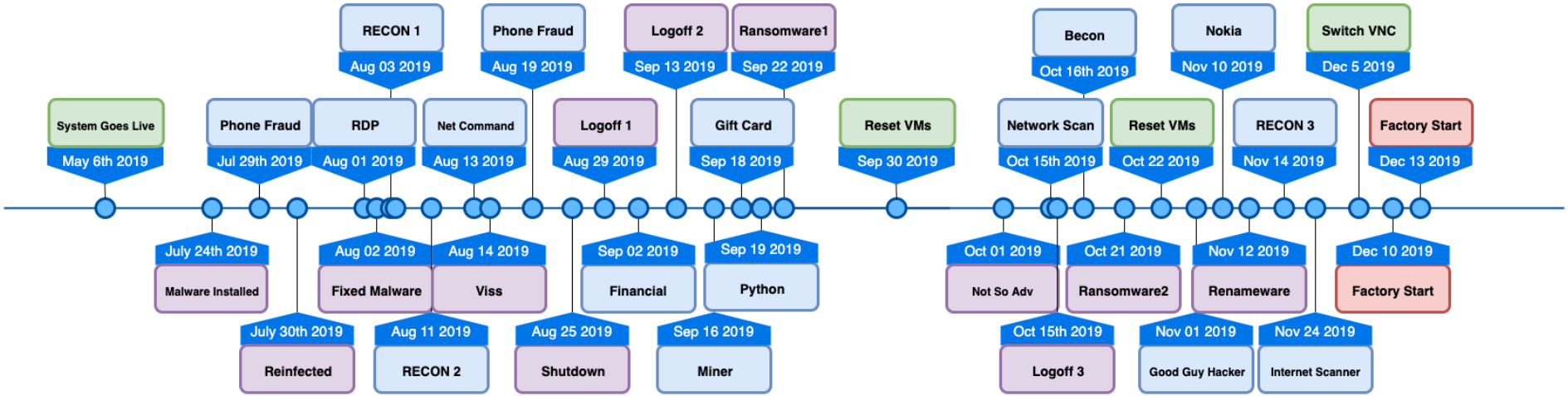
Monitoring the system

Moloch



Start Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Filename	Filename Cnt	Info	Stop Time
tcp 2019/12/19 02:00:00 EST	192.168.0.5	49680	92.63.197.48 RU	80	1	0 66	ip-10-104-156-157			Dst IP 92.63.197.48 Stop Time 1576738800448	2019/12/19 02:00:00 EST
udp 2019/12/19 01:59:55 EST	192.168.0.254	58328	192.168.0.99	514	1	141 149	ip-10-104-156-157			Dst IP 192.168.0.99 Stop Time 1576738795958	2019/12/19 01:59:55 EST
tcp 2019/12/19 01:59:53 EST	192.168.0.5	49679	192.168.0.10	9600	11	44 698	ip-10-104-156-157			Dst IP 192.168.0.10 Dst data bytes 24 Stop Time 1576738793219	2019/12/19 01:59:53 EST
tcp 2019/12/19 01:59:53 EST	192.168.0.5	49679	192.168.0.10	9600	11	44 698	ip-10-104-156-157			Dst IP 192.168.0.10 Dst data bytes 24 Stop Time 1576738793219	2019/12/19 01:59:53 EST
udp 2019/12/19 01:59:49 EST	192.168.0.99	61483	192.168.0.254	53	2	154 170	ip-10-104-156-157			Host teredo.ipv6.microsoft.com Dst IP 192.168.0.254 Dst data bytes 77 Stop Time 1576738789718	2019/12/19 01:59:49 EST
udp 2019/12/19 01:59:48 EST	192.168.0.102	138	192.168.0.255	138	2	470 486	ip-10-104-156-157			Dst IP 192.168.0.255 Stop Time 1576653090165	2019/12/18 02:11:30 EST
udp 2019/12/19 01:59:48 EST	192.168.0.102	138	192.168.0.255	138	2	470 486	ip-10-104-156-157			Dst IP 192.168.0.255 Stop Time 1576653090165	2019/12/18 02:11:30 EST
udp 2019/12/19 01:59:48 EST	192.168.0.102	138	192.168.0.255	138	121	28,435 29,403	ip-10-104-156-157			Dst IP 192.168.0.255 Stop Time 1576738788368	2019/12/19 01:59:48 EST
udp 2019/12/19 01:59:46 EST	192.168.0.6	5513	192.168.0.255	5512	2	104 120	ip-10-104-156-157			Dst IP 192.168.0.255 Stop Time 1576652408781	2019/12/18 02:00:08 EST

What Happened



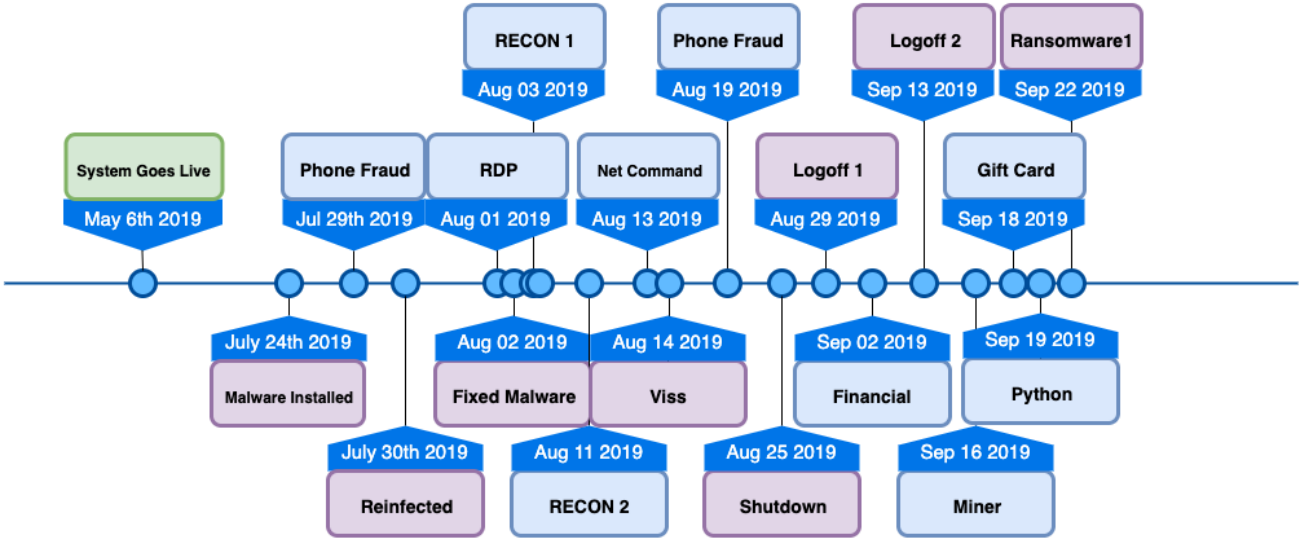
Admin Event

IT Event

OT Event

Hybrid Event

What Happened



Admin Event

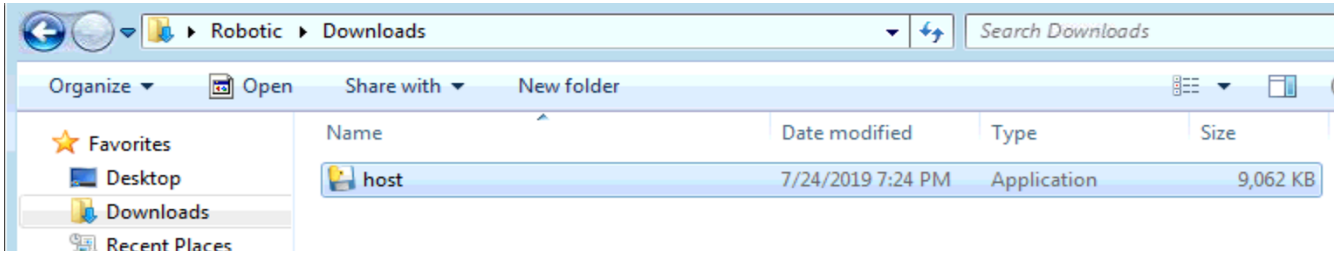
IT Event

OT Event

Hybrid Event

TREND MICRO

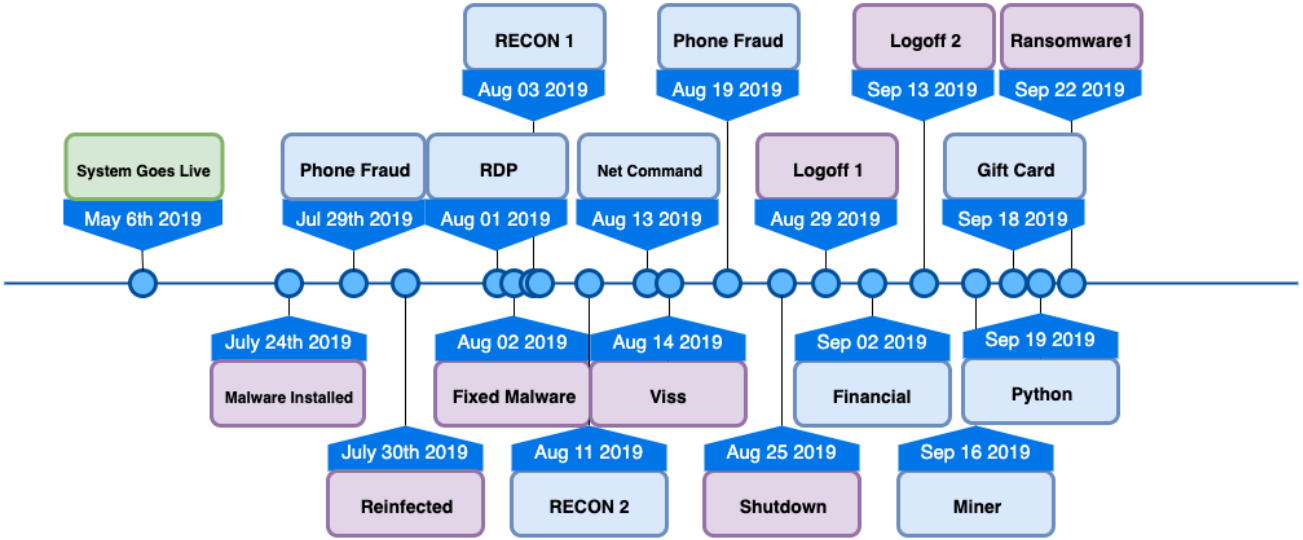
Host.exe




```
root@kali:~/Desktop/python-exe-unpacker# python pyinstxtractor.py ../host.exe1
[*] Processing ../host.exe1
[*] Pyinstaller version: 2.1+
[*] Python version: 27
[*] Length of package: 9036159 bytes
[*] Found 930 files in CArchive
[*] Beginning extraction...please standby
[*] Found 549 files in PYZ archive
[*] Successfully extracted pyinstaller archive: ../host.exe1

You can now use a python decompiler on the pyc files within the extracted direct
ory
```

What Happened

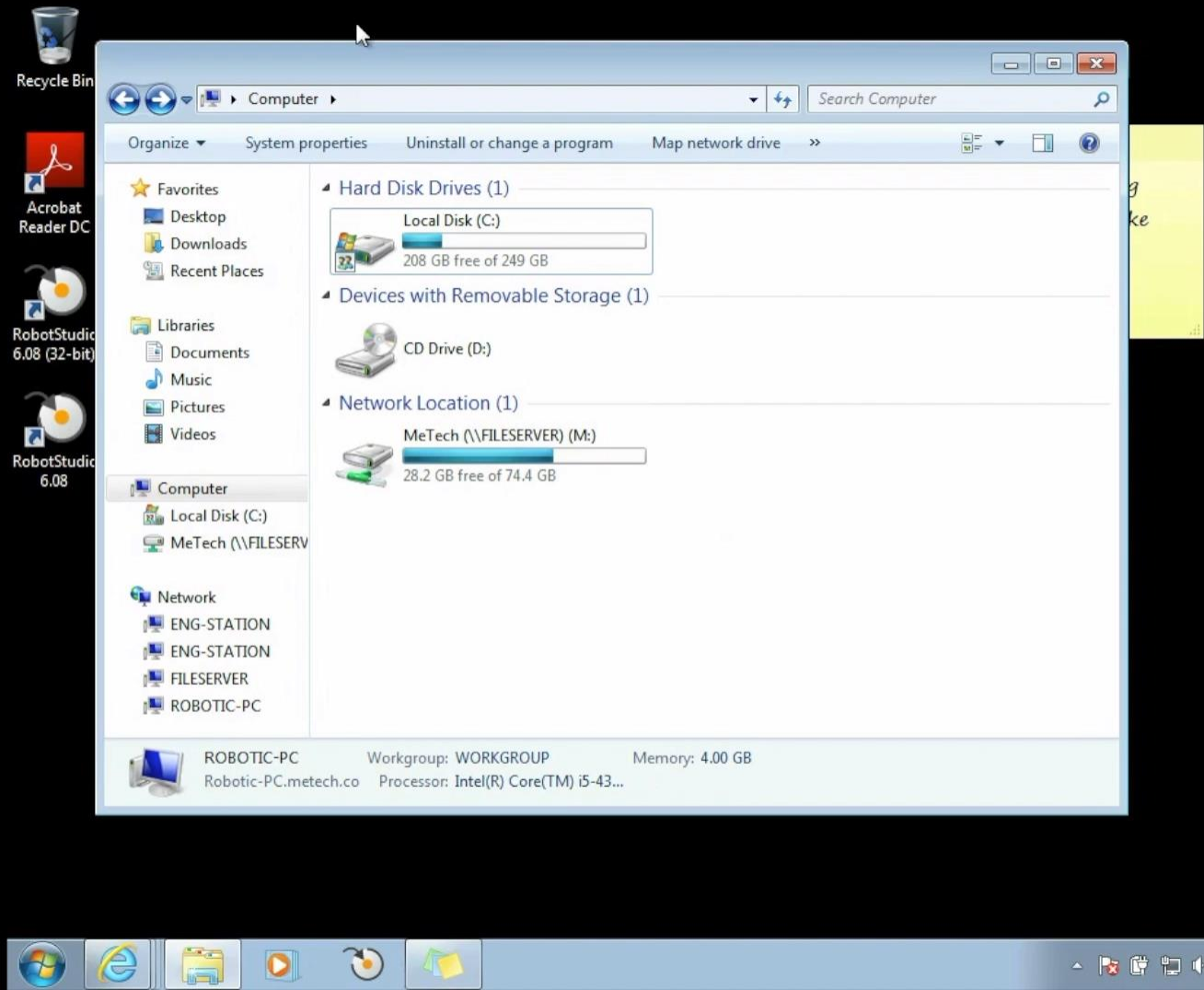


Admin Event

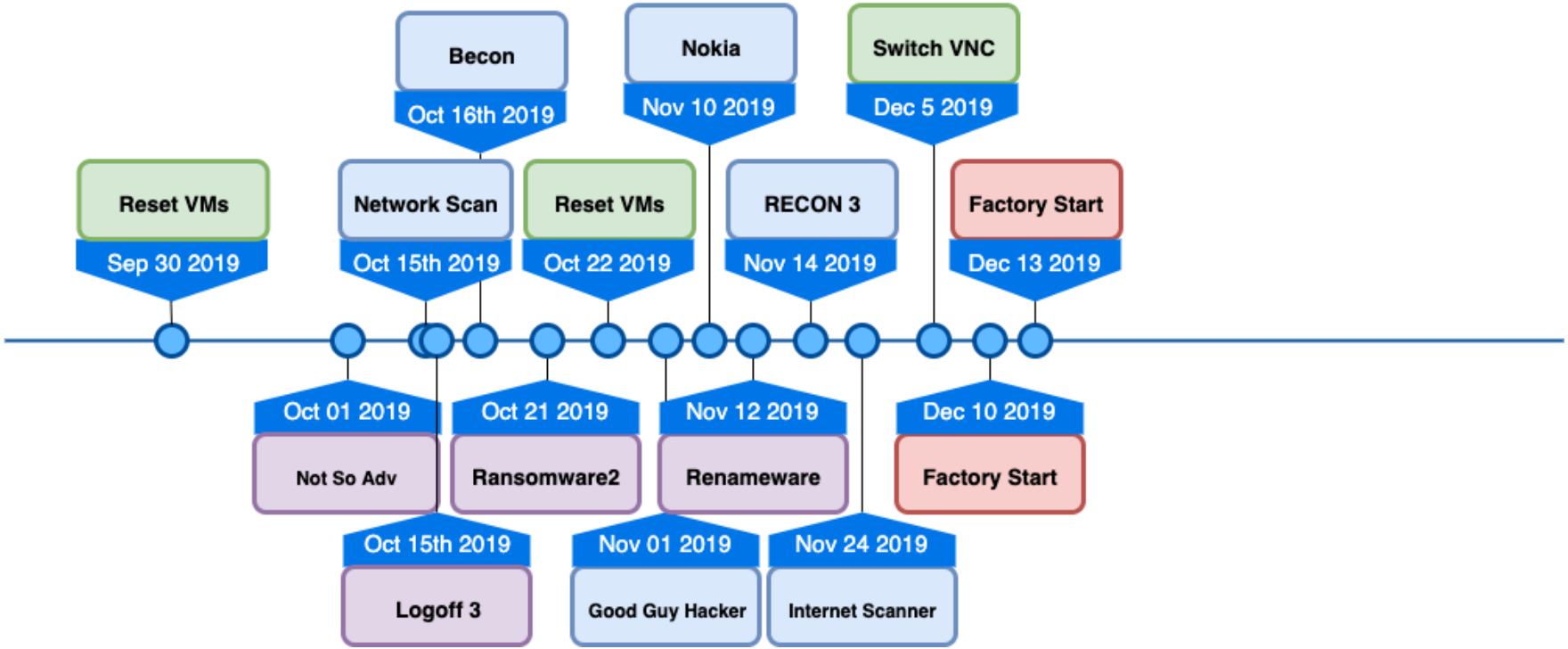
IT Event

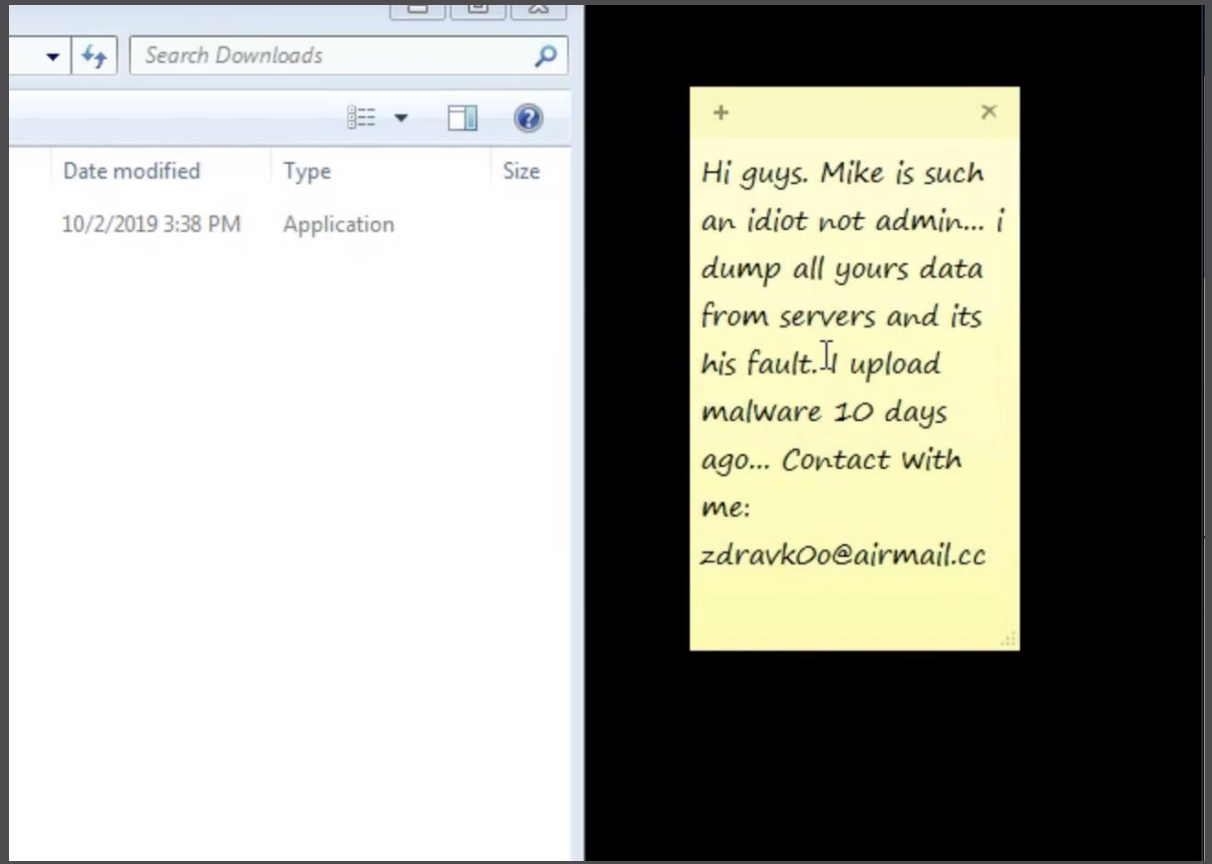
OT Event

Hybrid Event

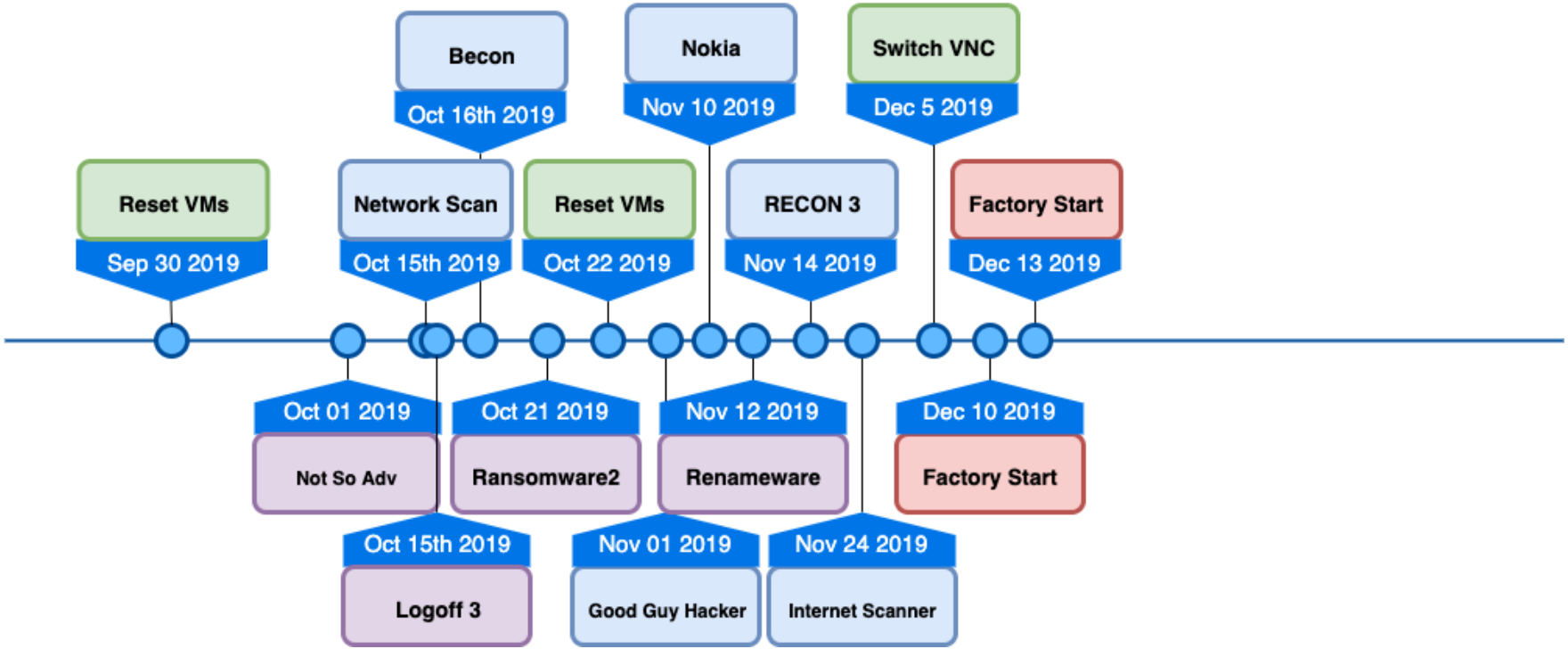

Recycle Bin
Acrobat Reader DC
RobotStudio 6.08 (32-bit)
RobotStudio 6.08
Computer
Search Computer
Organize
System properties
Uninstall or change a program
Map network drive
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
MeTech (\\FILESERV
Network
ENG-STATION
ENG-STATION
FILESERVER
ROBOTIC-PC
Hard Disk Drives (1)
Local Disk (C:)
208 GB free of 249 GB
Devices with Removable Storage (1)
CD Drive (D:)
Network Location (1)
MeTech (\\FILESERVER) (M:)
28.2 GB free of 74.4 GB
ROBOTIC-PC
Robotic-PC.metech.co
Workgroup: WORKGROUP
Processor: Intel(R) Core(TM) i5-43...
Memory: 4.00 GB
2:27 PM
9/22/2019

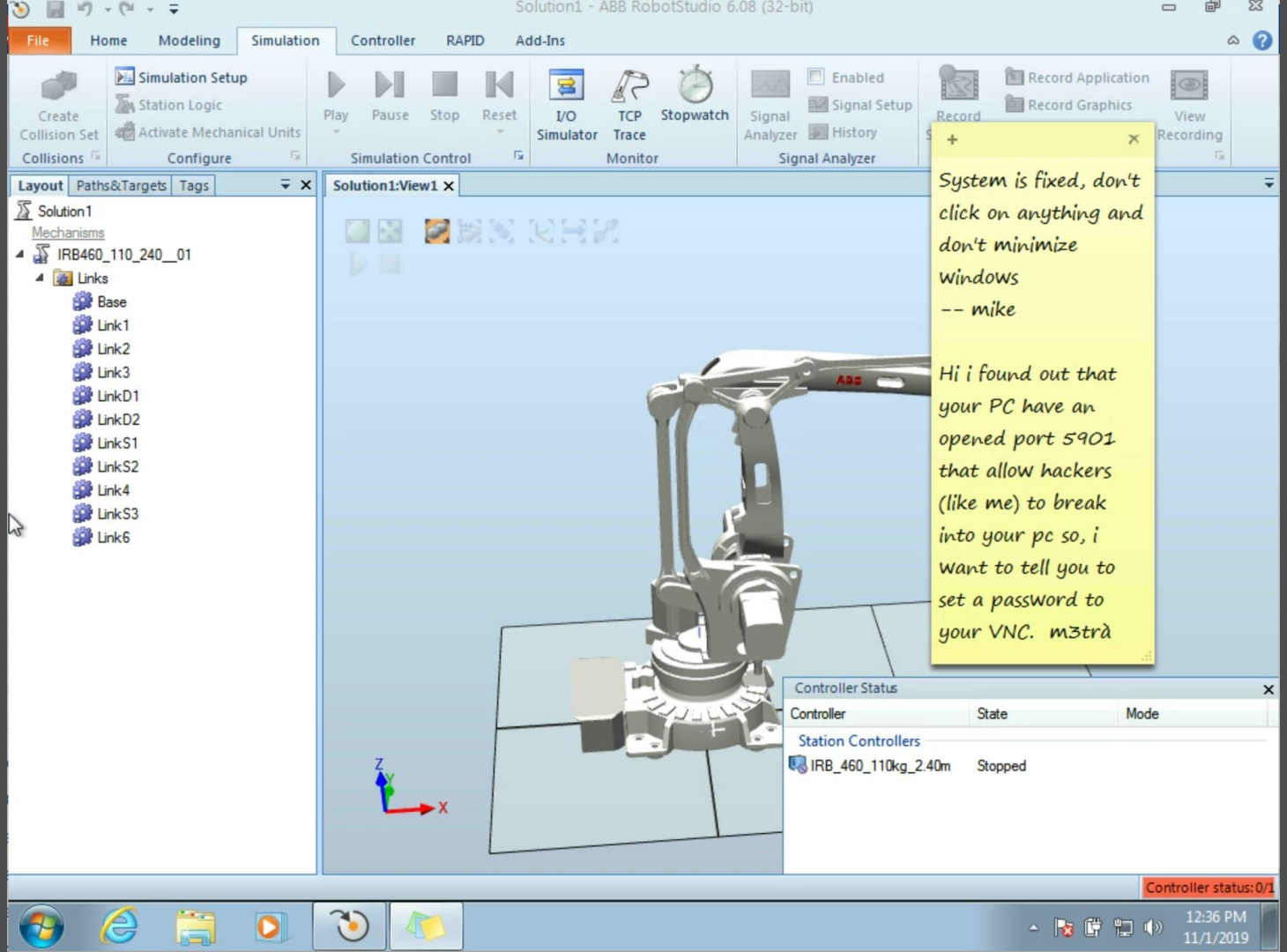
What Happened



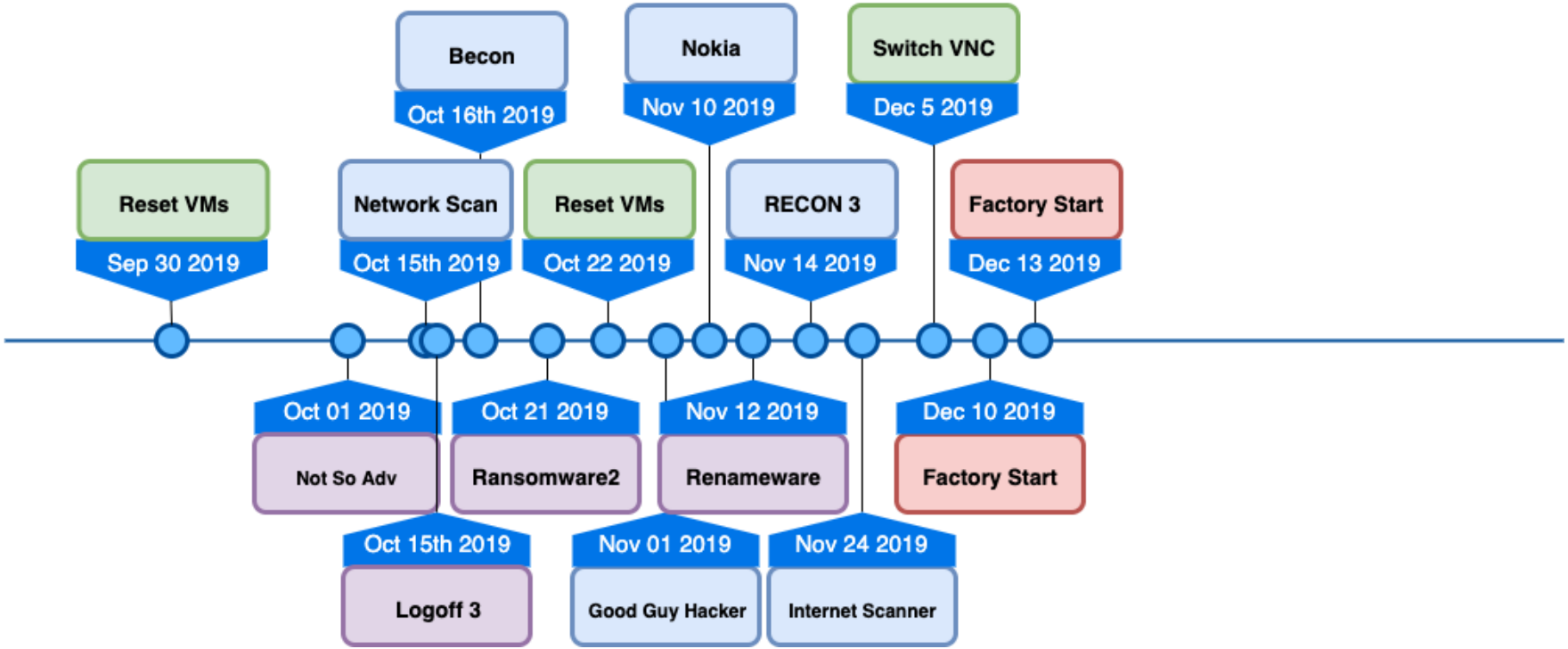

Search Downloads
Date modified
Type
Size
10/2/2019 3:38 PM
Application
Hi guys. Mike is such an idiot not admin... i dump all yours data from servers and its his fault. I upload malware 10 days ago... Contact with me:
zdravk00@airmail.cc

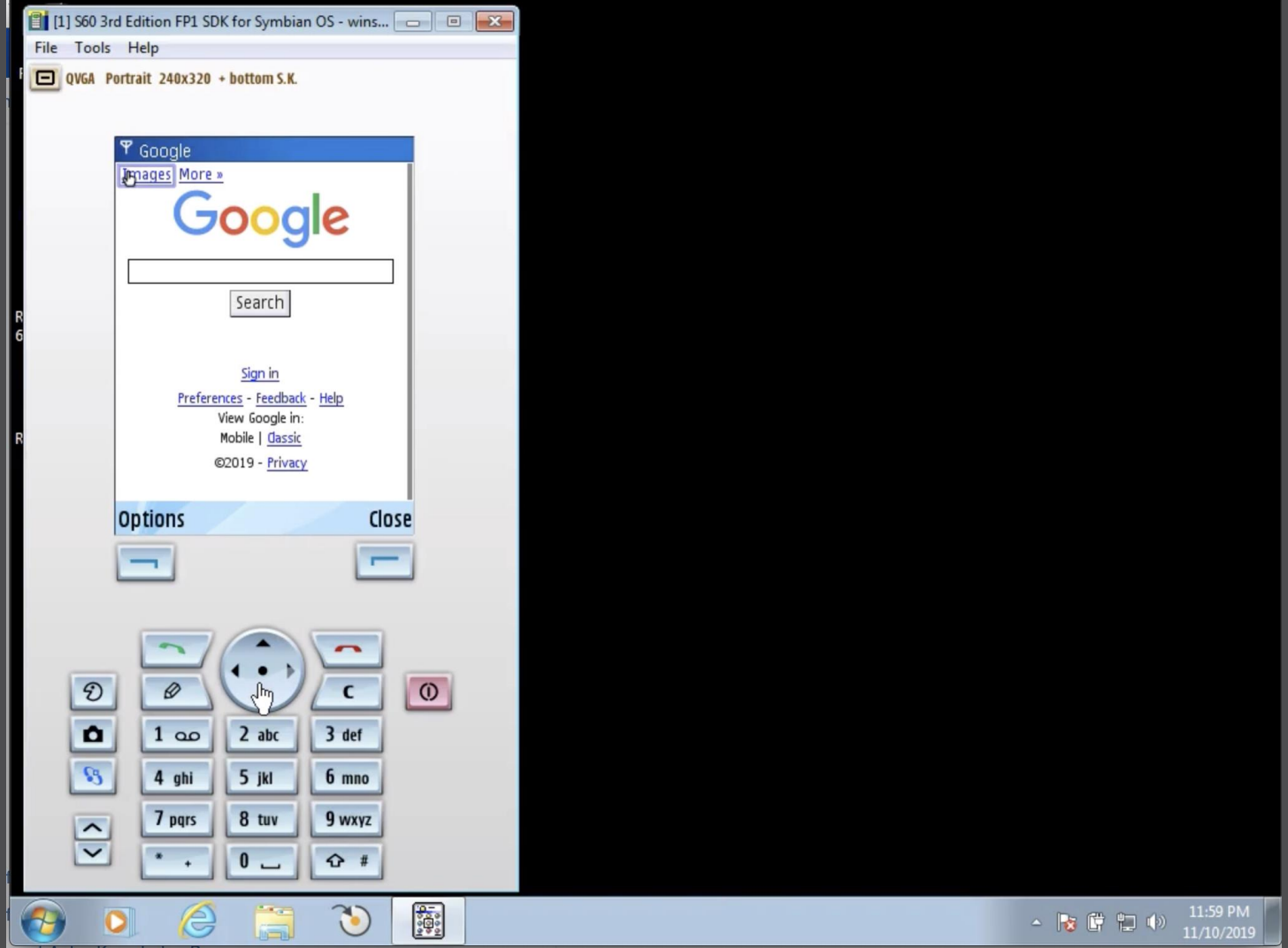
What Happened



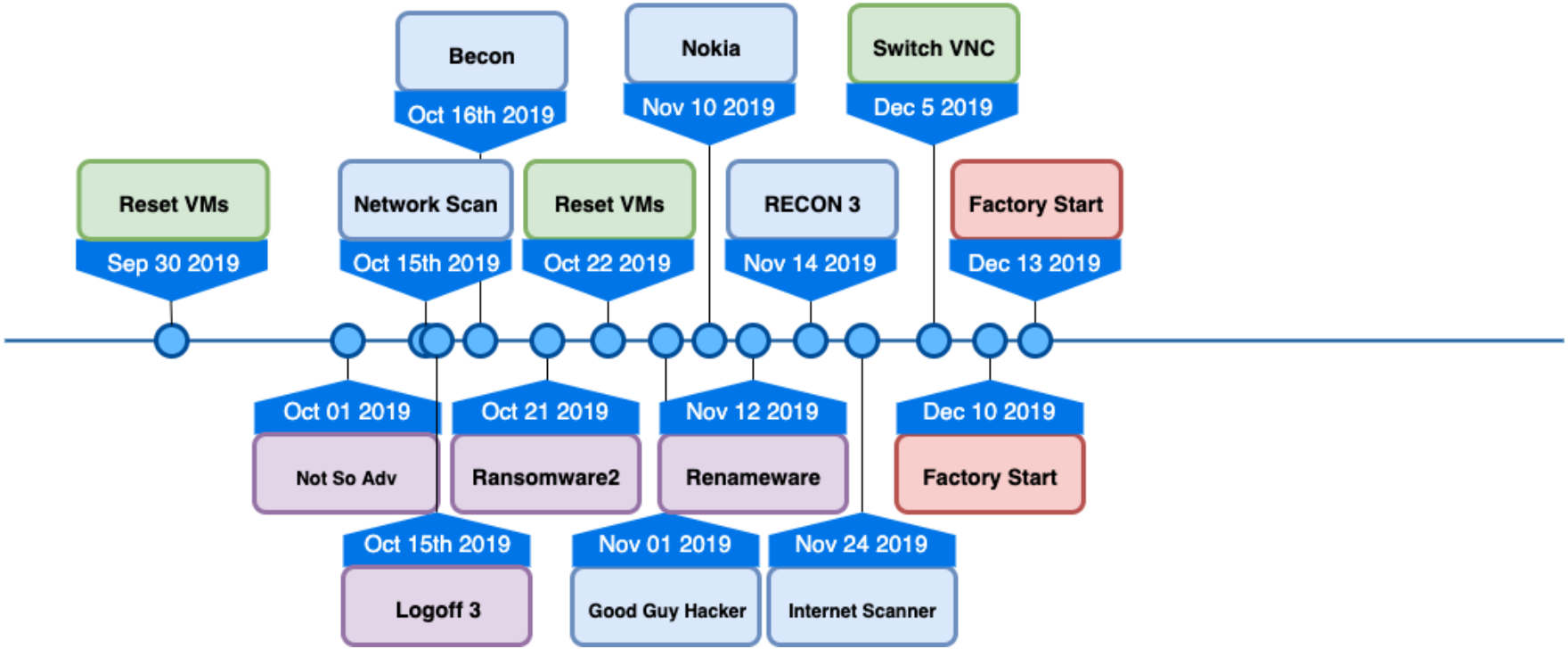

Solution1 - ABB RobotStudio 6.08 (32-bit)
File
Home
Modeling
Simulation
Controller
RAPID
Add-Ins
Create Collision Set
Collisions
Simulation Setup
Station Logic
Activate Mechanical Units
Configure
Play
Pause
Stop
Reset
Simulation Control
I/O Simulator
TCP Trace
Stopwatch
Monitor
Signal Analyzer
Enabled
Signal Setup
History
Signal Analyzer
Record
Record Application
Record Graphics
View Recording
Layout
Paths&Targets
Tags
Solution1
Mechanisms
IRB460_110_240__01
Links
Base
Link1
Link2
Link3
LinkD1
LinkD2
LinkS1
LinkS2
Link4
LinkS3
Link6
Solution1:View1
System is fixed, don't click on anything and don't minimize windows
-- mike
Hi i found out that your PC have an opened port 5901 that allow hackers (like me) to break into your pc so, i want to tell you to set a password to your VNC. m3trà
Controller Status
Controller
State
Mode
Station Controllers
IRB_460_110kg_2.40m
Stopped
Controller status: 0/1
12:36 PM
11/1/2019

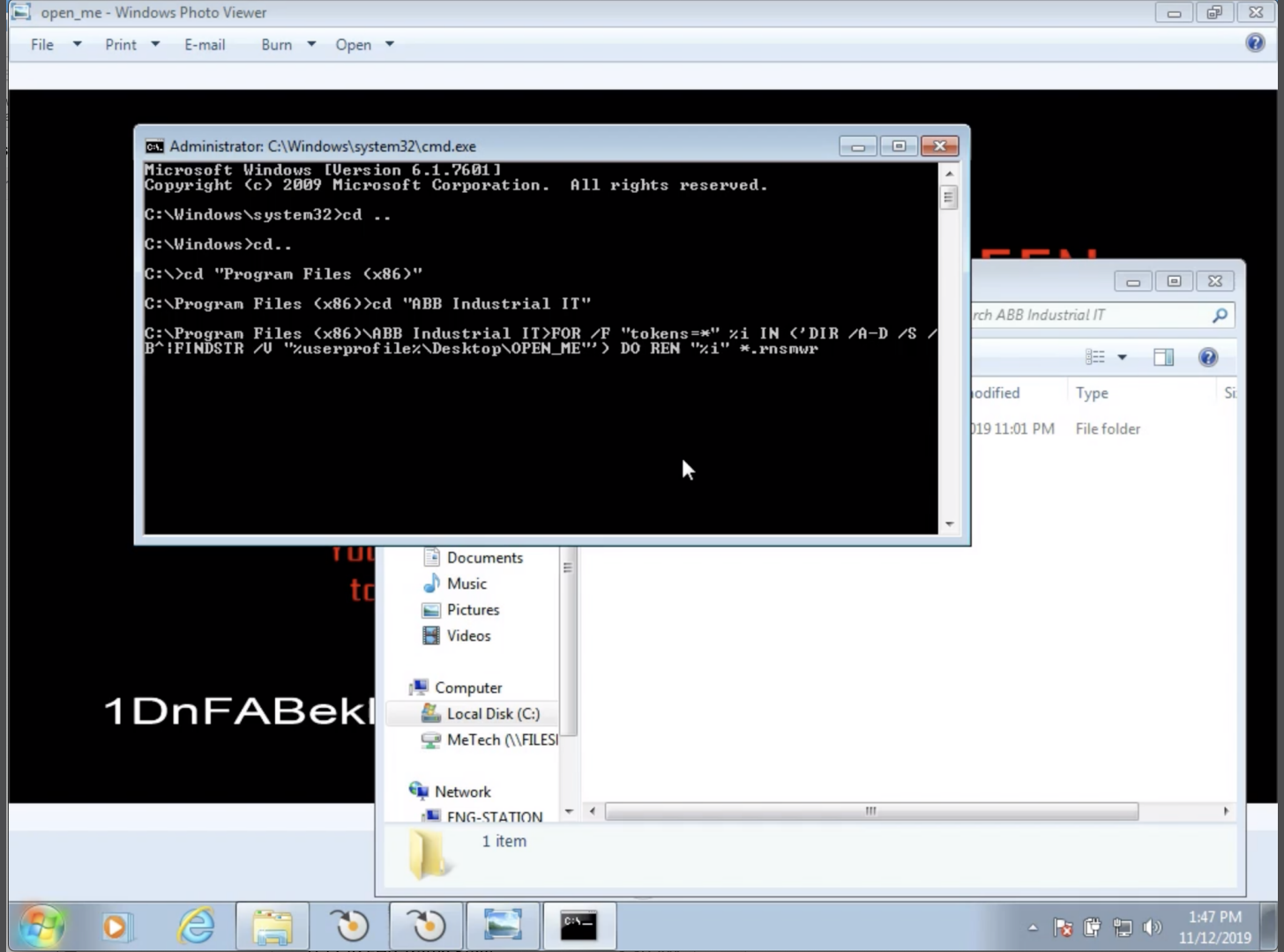
What Happened



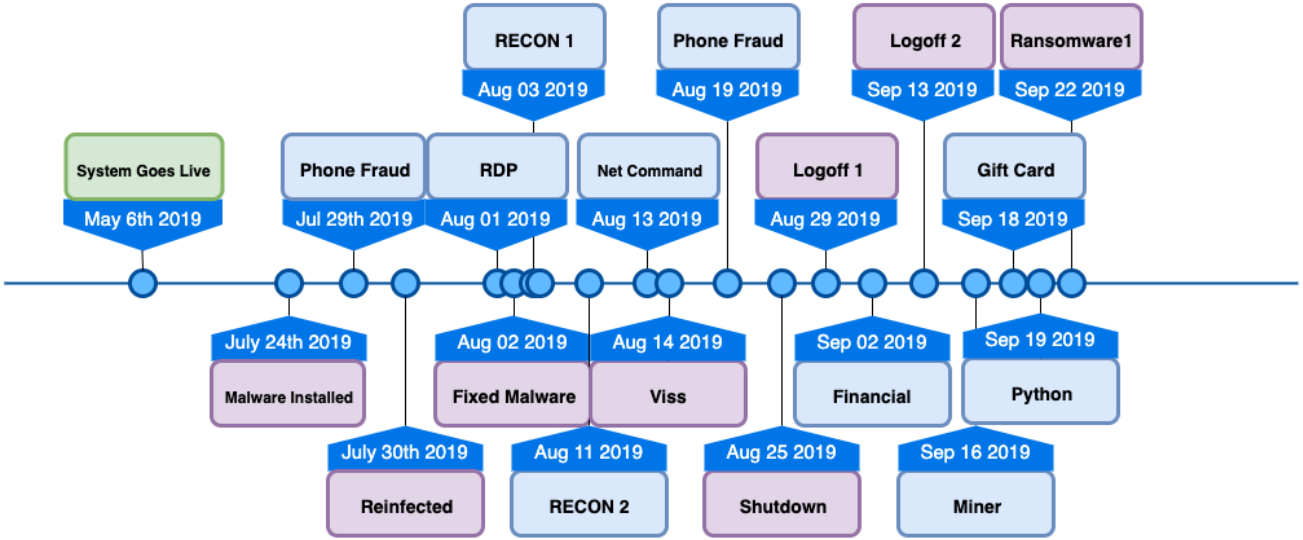

[1] S60 3rd Edition FP1 SDK for Symbian OS - wins...
File Tools Help
QVGA Portrait 240x320 + bottom S.K.
Google
Images More »
Google
Search
Sign in
Preferences - Feedback - Help
View Google in:
Mobile | Classic
©2019 - Privacy
Options Close
C
1 2 abc 3 def
4 ghi 5 jkl 6 mno
7 pqrs 8 tuv 9 wxyz
* 0 #
11:59 PM
11/10/2019

What Happened




open_me - Windows Photo Viewer
File
Print
E-mail
Burn
Open
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd ..
C:\Windows>cd..
C:\>cd "Program Files (x86)"
C:\Program Files (x86)>cd "ABB Industrial IT"
C:\Program Files (x86)\ABB Industrial IT>FOR /F "tokens=*" %i IN ('DIR /A-D /S /
B^|FINDSTR /V "%userprofile%\Desktop\OPEN_ME"') DO REN "%i" *.rnsmwr
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
MeTech (\\FILES
Network
FNG-STATION
1 item
Type
File folder
1DnFABekl
1:47 PM
11/12/2019

What Happened



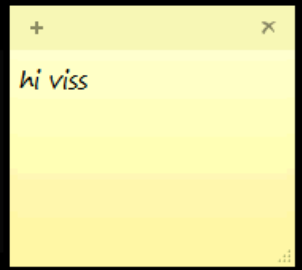
Admin Event

IT Event

OT Event

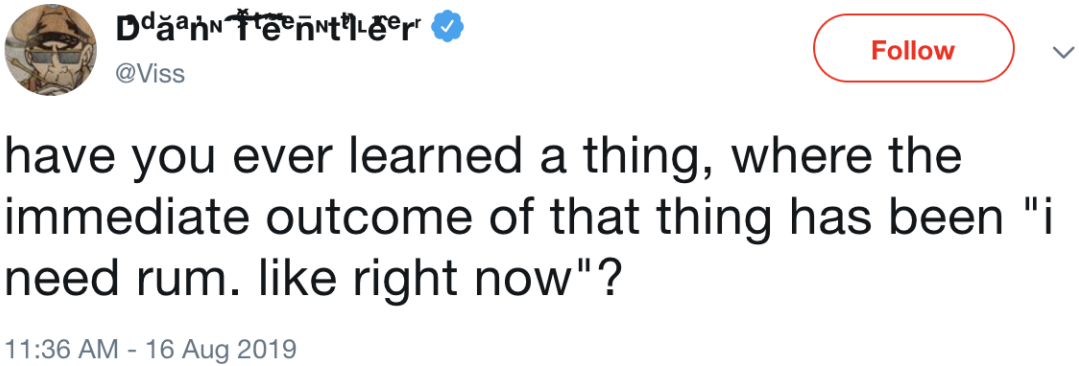
Hybrid Event


ScadaLIGHT 11.3
Source Debugger
Trace Viewer
Internet Client Monitor
Test Framework
MEtech_RP


hi viss

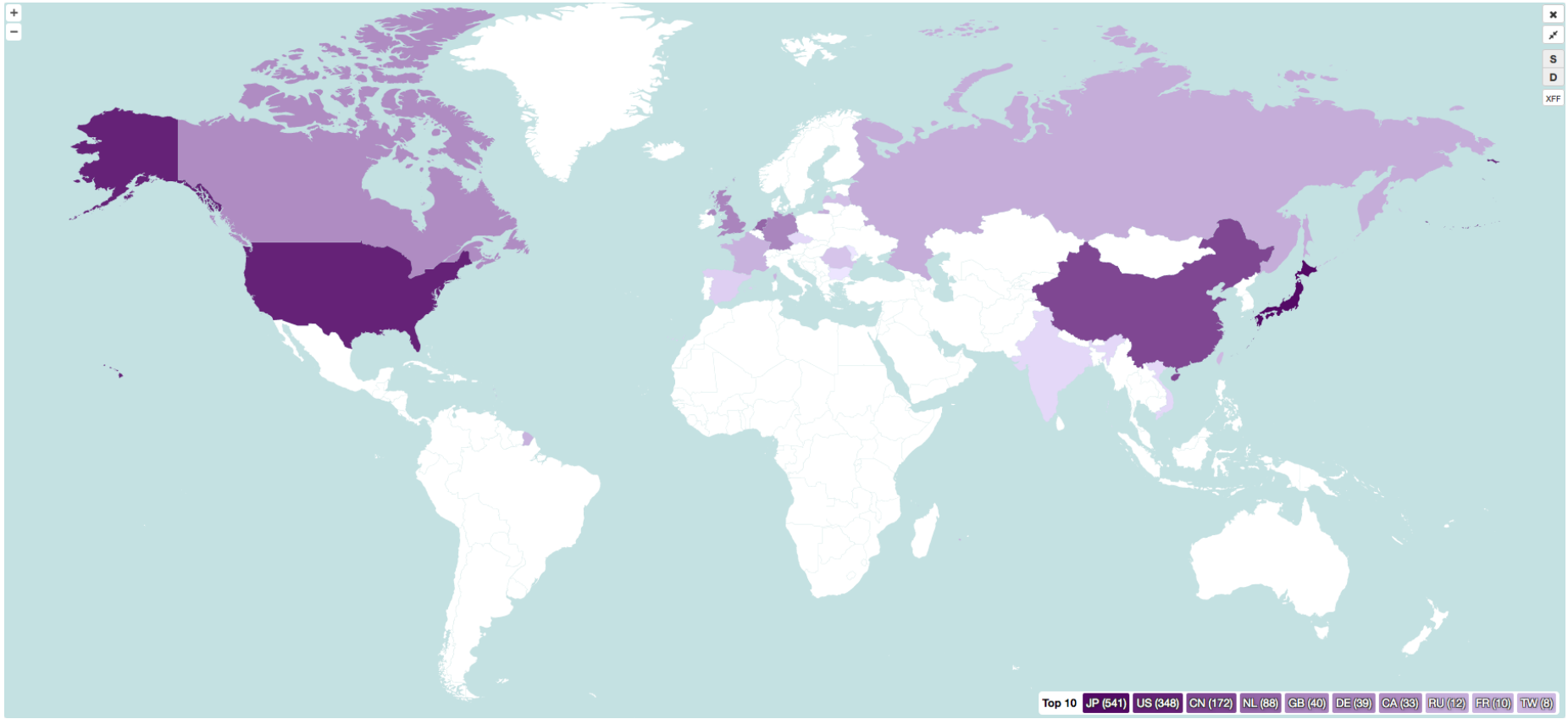
Validation

Subject: The most elaborate honeypot.
Date: Friday, August 16, 2019 at 3:21:06 PM Eastern Daylight Time
From: Dan Tentler
To: Stephen Hilt
CC:



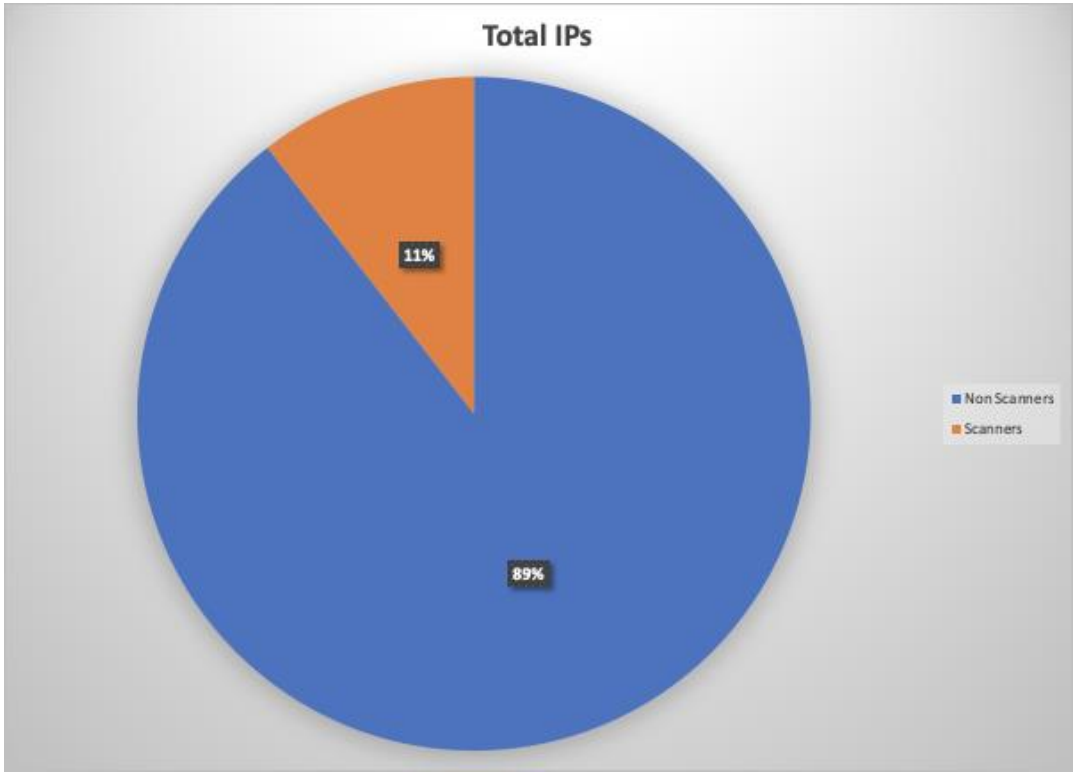
TREND MICRO

But WHO!?



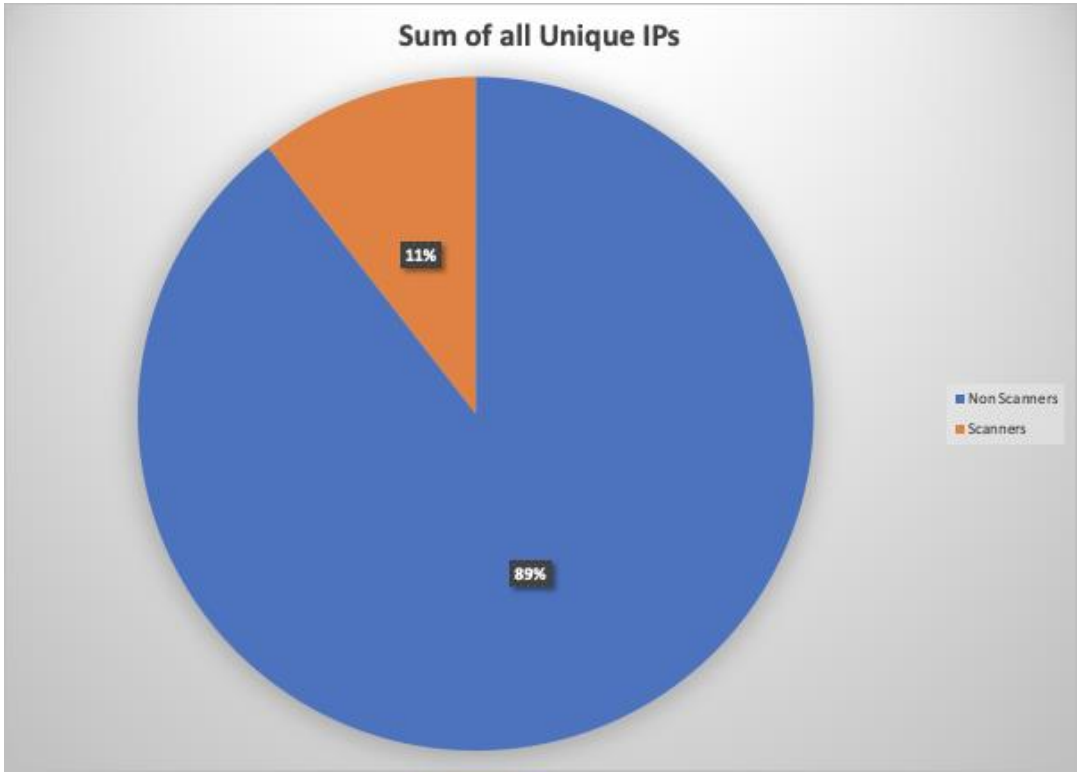
Stats: Total IPs Over Project

- 8905 Total IPs
- 592 Scanner IPs



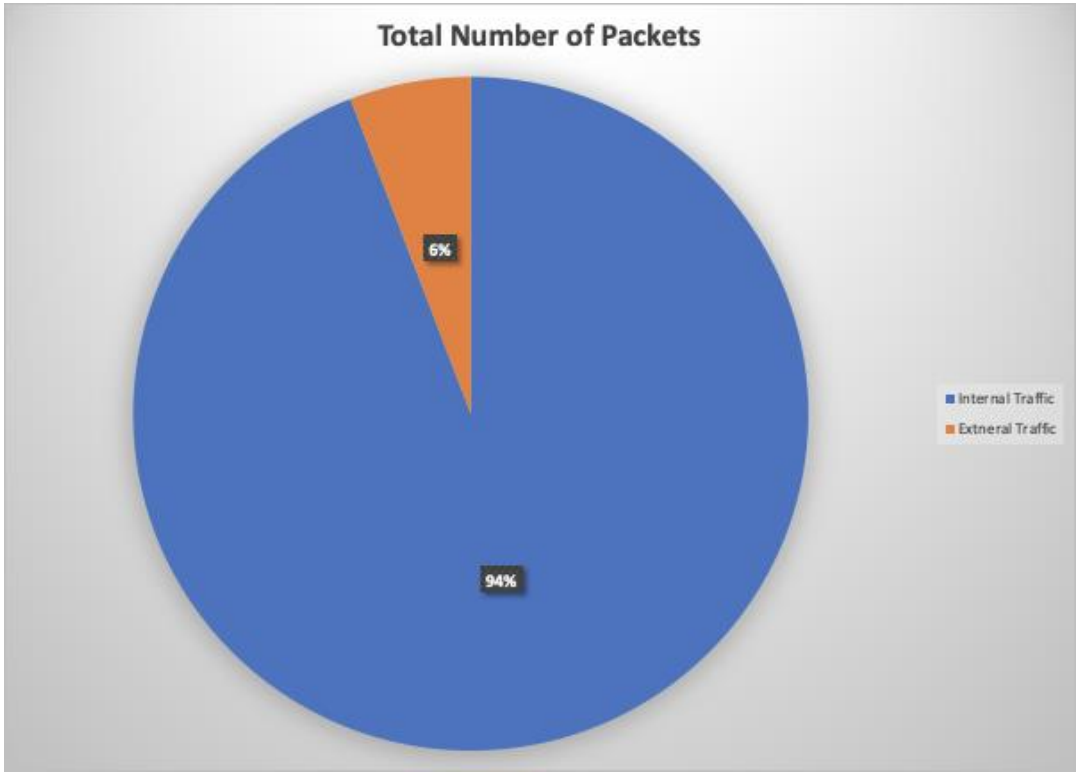
Stats: Sum of all unique IPs per day

- 19315 Total
  - 85.5 IPs / Day
- 2268 Total Scanner
  - 10 IPs / Day



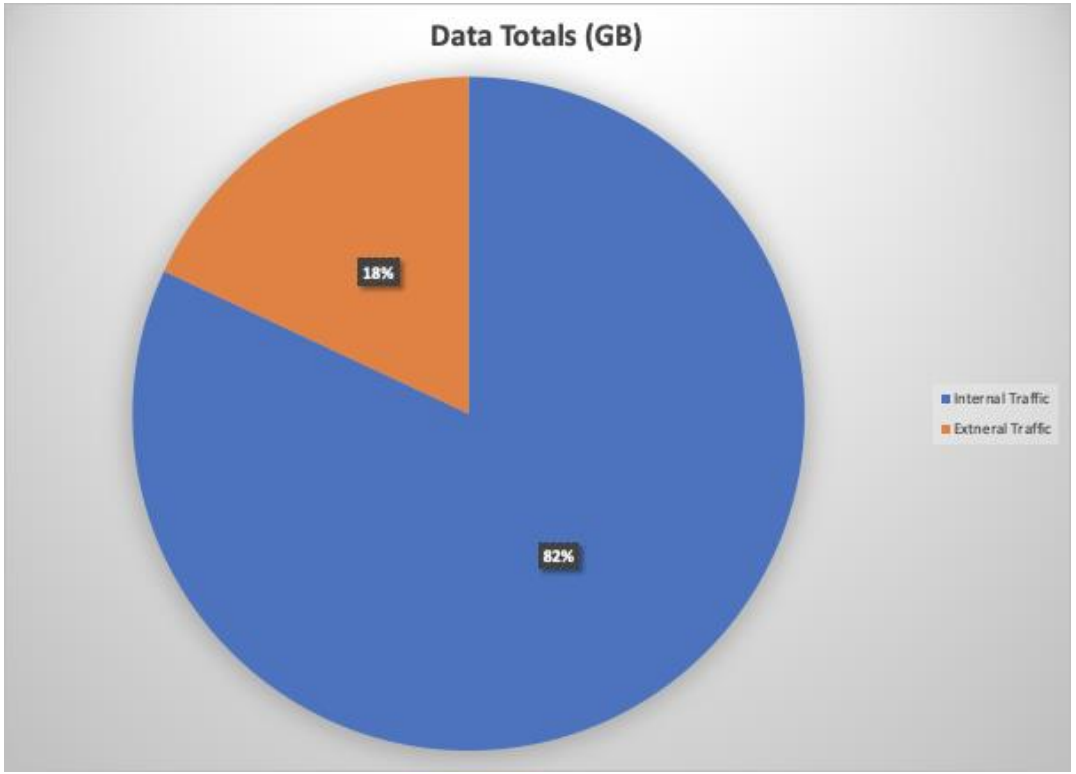
Stats: Total Packets/Bytes

- 549,147,728
  - ~550 Million
- 126,692,593,887B
  - 126.7GB



Stats: Total Packets/Bytes

- 549,147,728
  - ~550 Million
- 126,692,593,887B
  - 126.7GB



Conclusion

Don't put your control system on the internet, ever!

Attackers seem more interested in using the Clean IP than causing issues to production.

Maybe we were too realistic to attract lurkers who just wanted to play with a honeypot (APT Chattanooga)

TREND MICRO

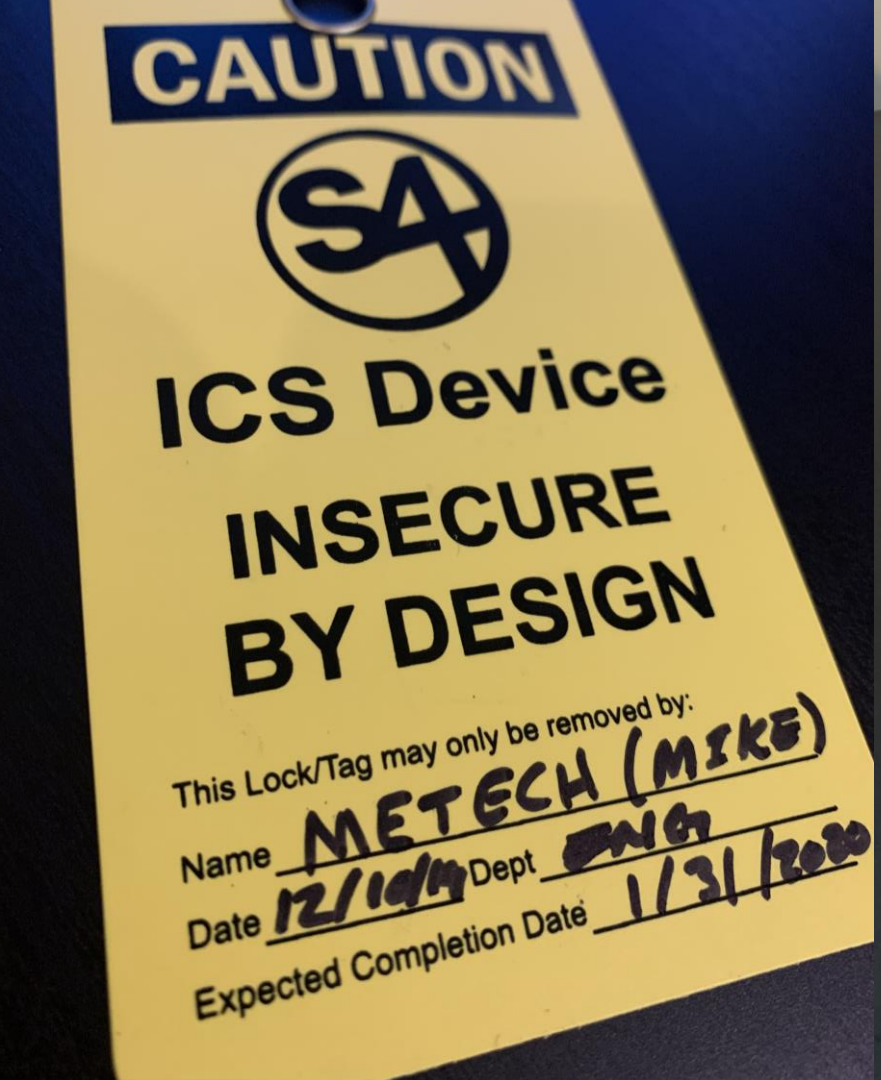
Conclusion

If you want to run a high-interaction honeypot, daily interactions are needed.

Deal with Incidents as they happen, do not wait otherwise you will see your honeypot collapse.

Attackers will be mean to Mike and hurt your feelings.

TREND MICRO


CAUTION
ICS Device
INSECURE
BY DESIGN
This Lock/Tag may only be removed by:
Name METECH (MIKE)
Dept ENG
Date 12/10/19
Expected Completion Date 1/31/2020


CAUTION
ICS Device
INSECURE
BY DESIGN
CONVEYOR BELT

https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot