

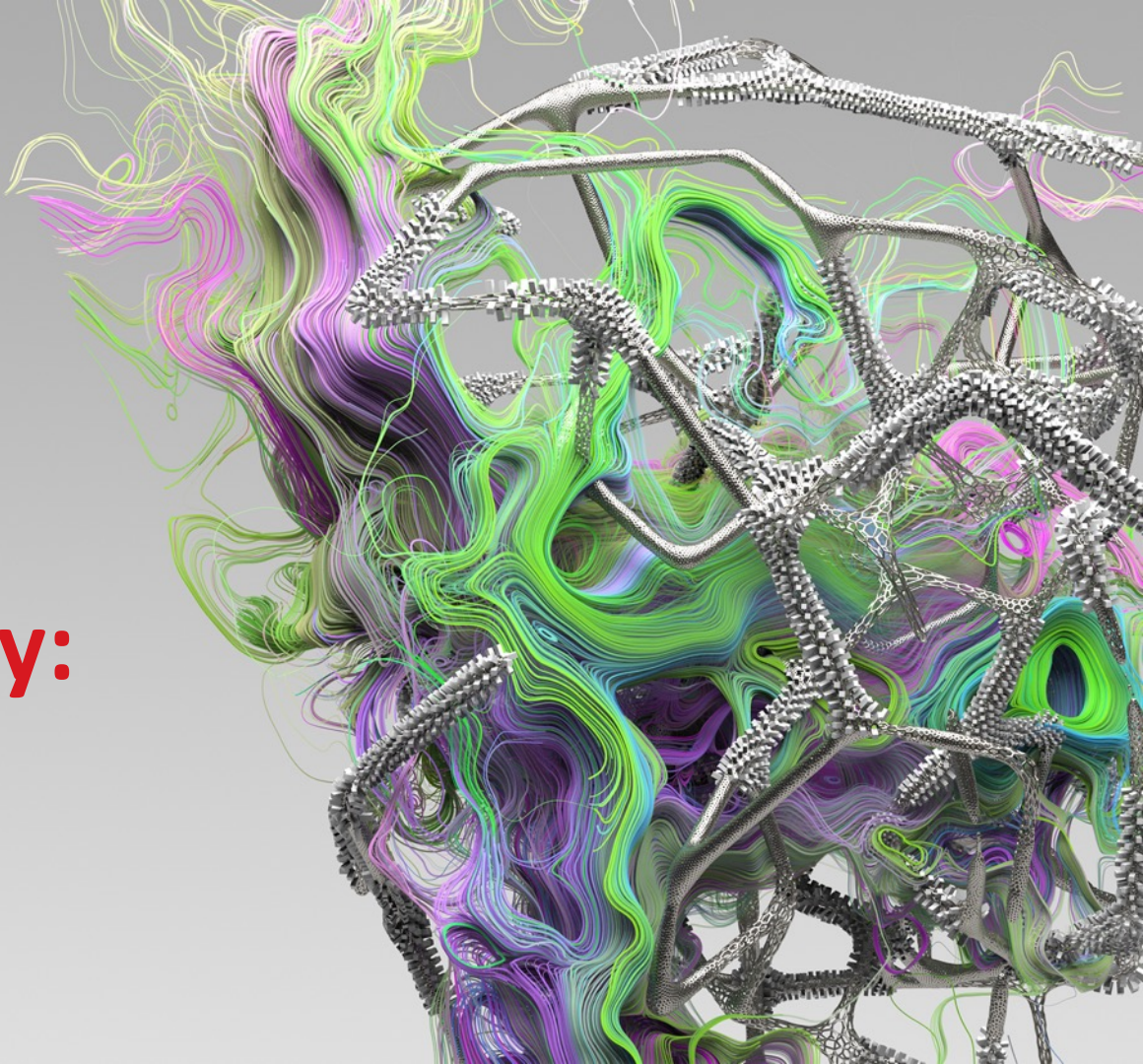


Faking a Factory:

Creating and Operating a Realistic Honeybot

Charles Perine

Oct 1, 2020





Hackers Are Targeting The Auto Industry, Stealing Data And Demanding Money

BY MICHAEL GAUTHIER | NOVEMBER 21, 2019 3

Ransomware attacks have targeted everything from city governments to hospitals. Now, attackers have their sights on the automotive industry.

Trending



German Automakers Might Face China's Wrath If Berlin Bans Huawei From 5G Networks



Nissan Patrol Fleeing Cops On One Tire In One Fire After



Hackers Are Targeting The Auto Industry, Stealing Data And Demanding Money

BY MICHAEL GAUTHIER | NOVEMBER 21, 2019

Ransomware attacks have targeted everything from city governments to hospitals. Now, attackers have their sights on the automotive industry.

Trending



German Automakers Face China's Wrath | Bans Huawei From 5 Networks



Nissan Patrol Flees | One Time In On Fire

9,652 views | Jun 22, 2017, 05:00am

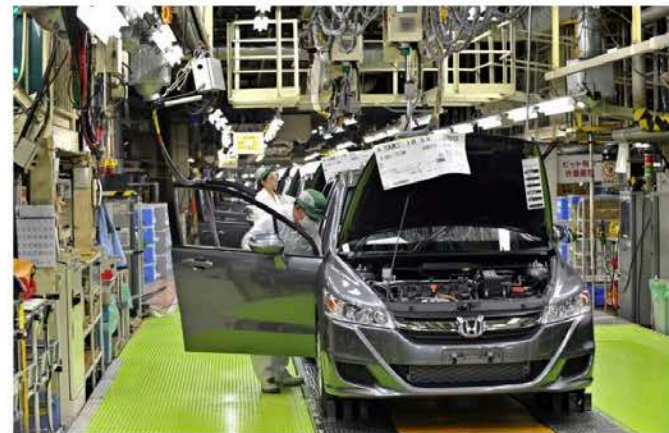
Cyber Attack At Honda Stops Production After WannaCry Worm Strikes



Peter Lyon Contributor

Cars & Bikes

I focus on all things to do with cars.



Honda was forced to halt production at its Sayama plant after WannaCry virus struck. Photo by... [+]



Hackers Are Targeting The Auto Industry, Stealing Data And Demanding Money

BY MICHAEL GALTHIER | NOVEMBER 21, 2016

US & WORLD | TECH | CYBERSECURITY

Boeing production plant hit with WannaCry ransomware attack

The widespread and devastating cyberattack reportedly from North Korea has hit a Boeing plant in Charleston

By Nick Statt | @nickstatt | Mar 28, 2018, 7:23pm EDT

f t SHARE



Trending

Some trending items

AD

9,652 views | Jun 22, 2017, 05:00am

Cyber Attack At Honda Stops Production After WannaCry Worm Strikes

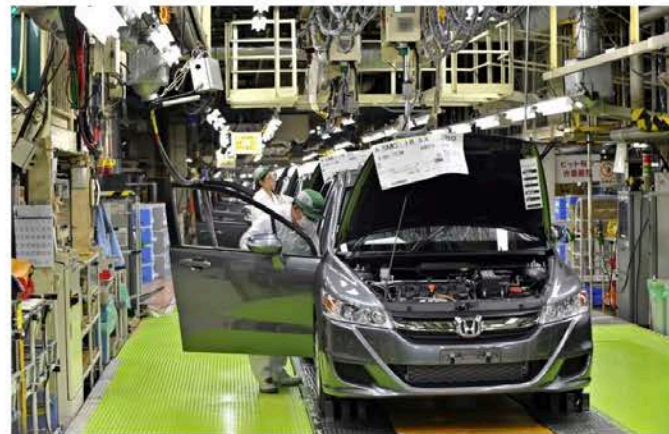


Peter Lyon Contributor

Cars & Bikes

I focus on all things to do with cars.

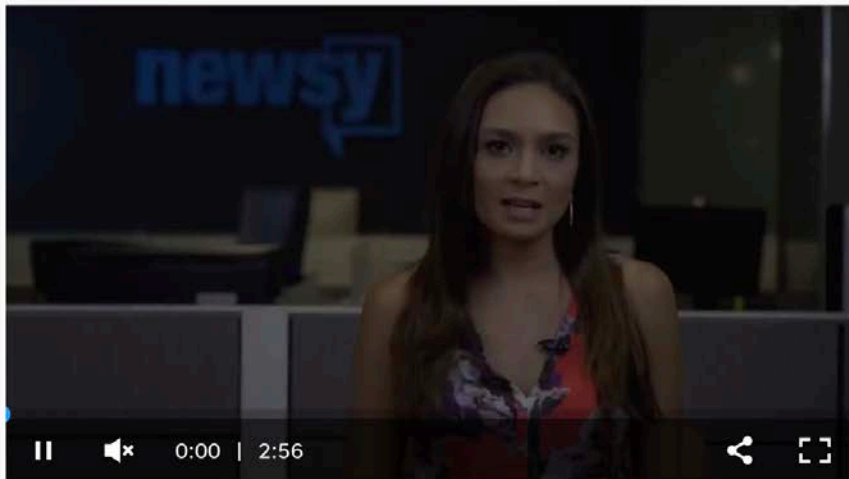
f



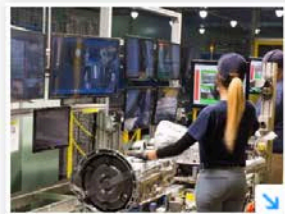
Honda was forced to halt production at its Sayama plant after WannaCry virus struck. Photo by... [+]

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.

Share your feedback to help improve our site experience!

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

da
ter
ikes



r WannaCry virus

Hackers Are T
Demanding M

BY MICHAEL GAULTHER

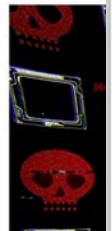
US & WORLD TECH

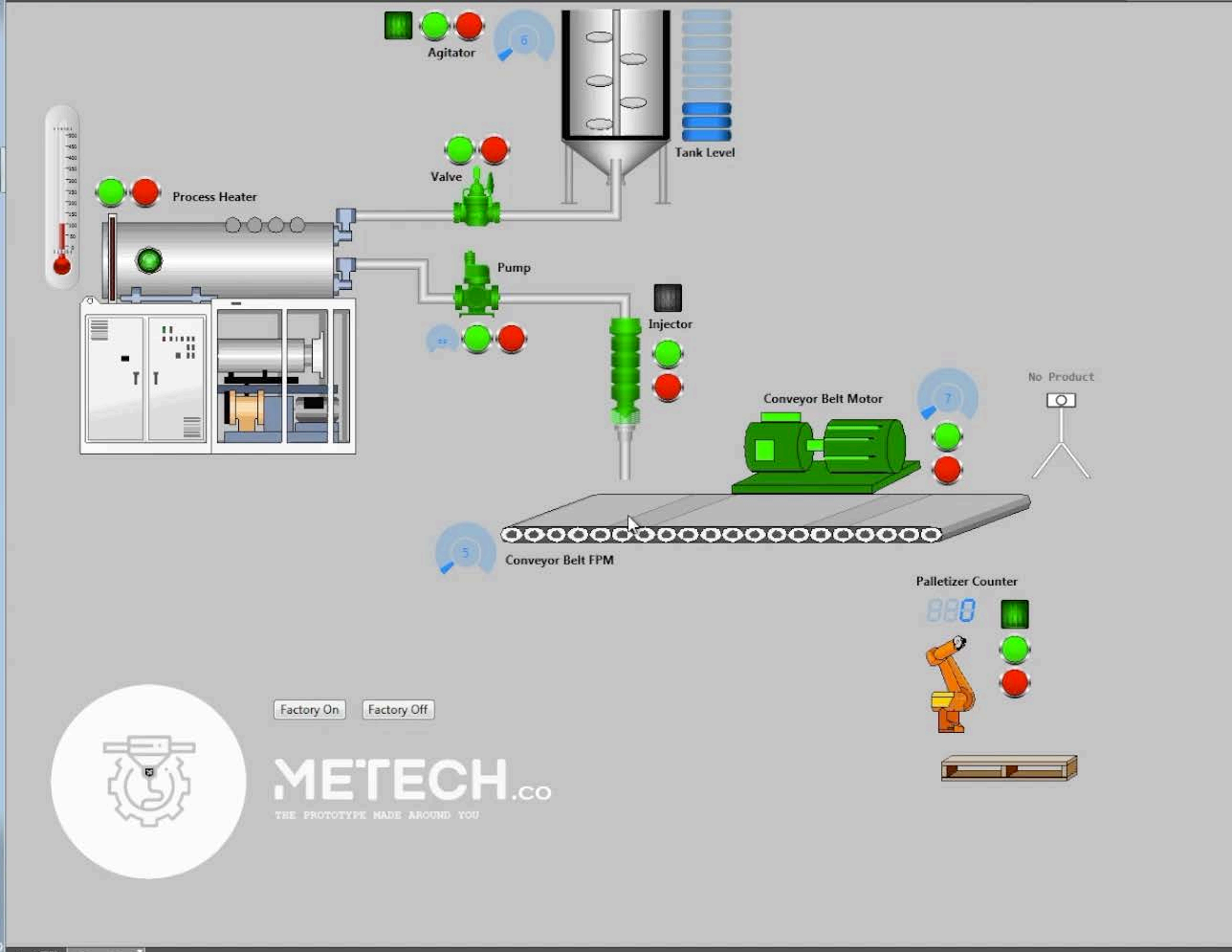
Boein
Wann

The widespr
Korea has h

By Nick Staff | @n

f t e

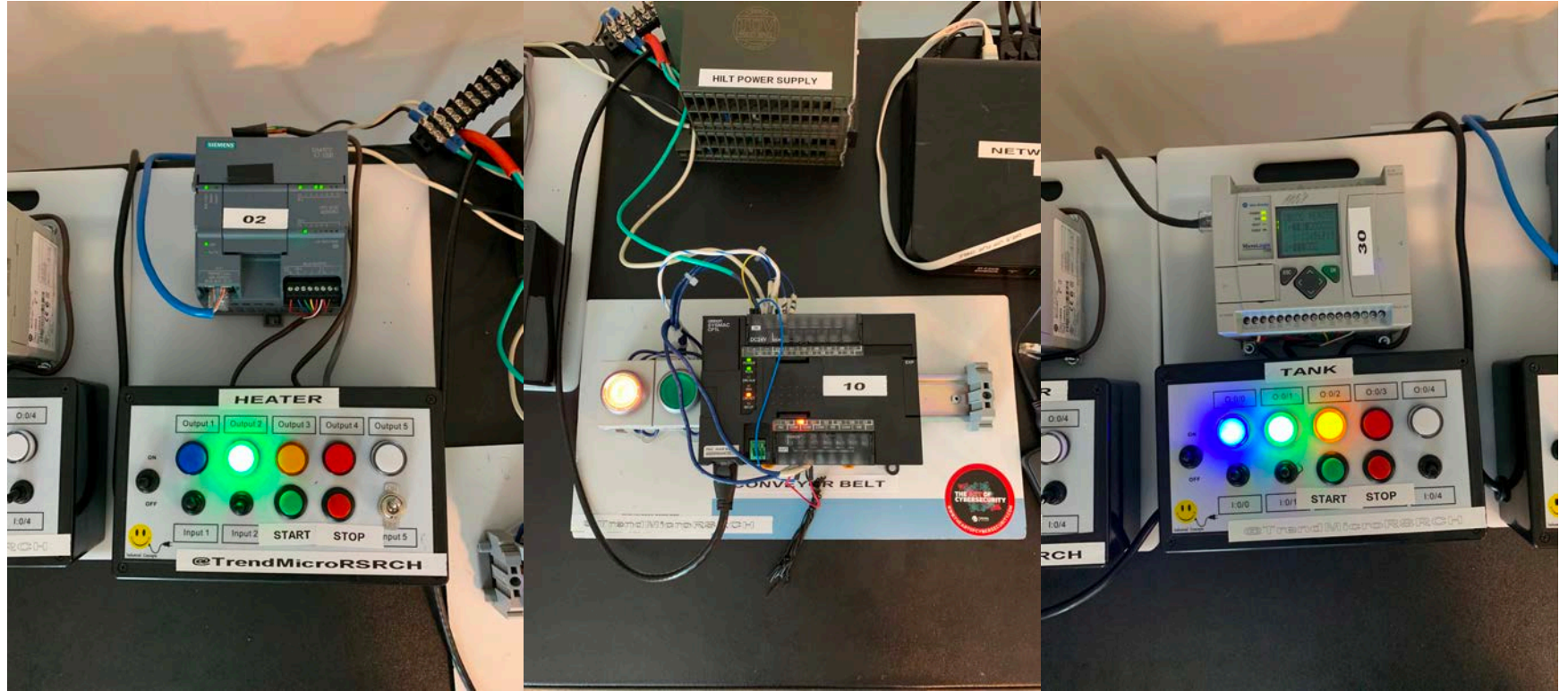




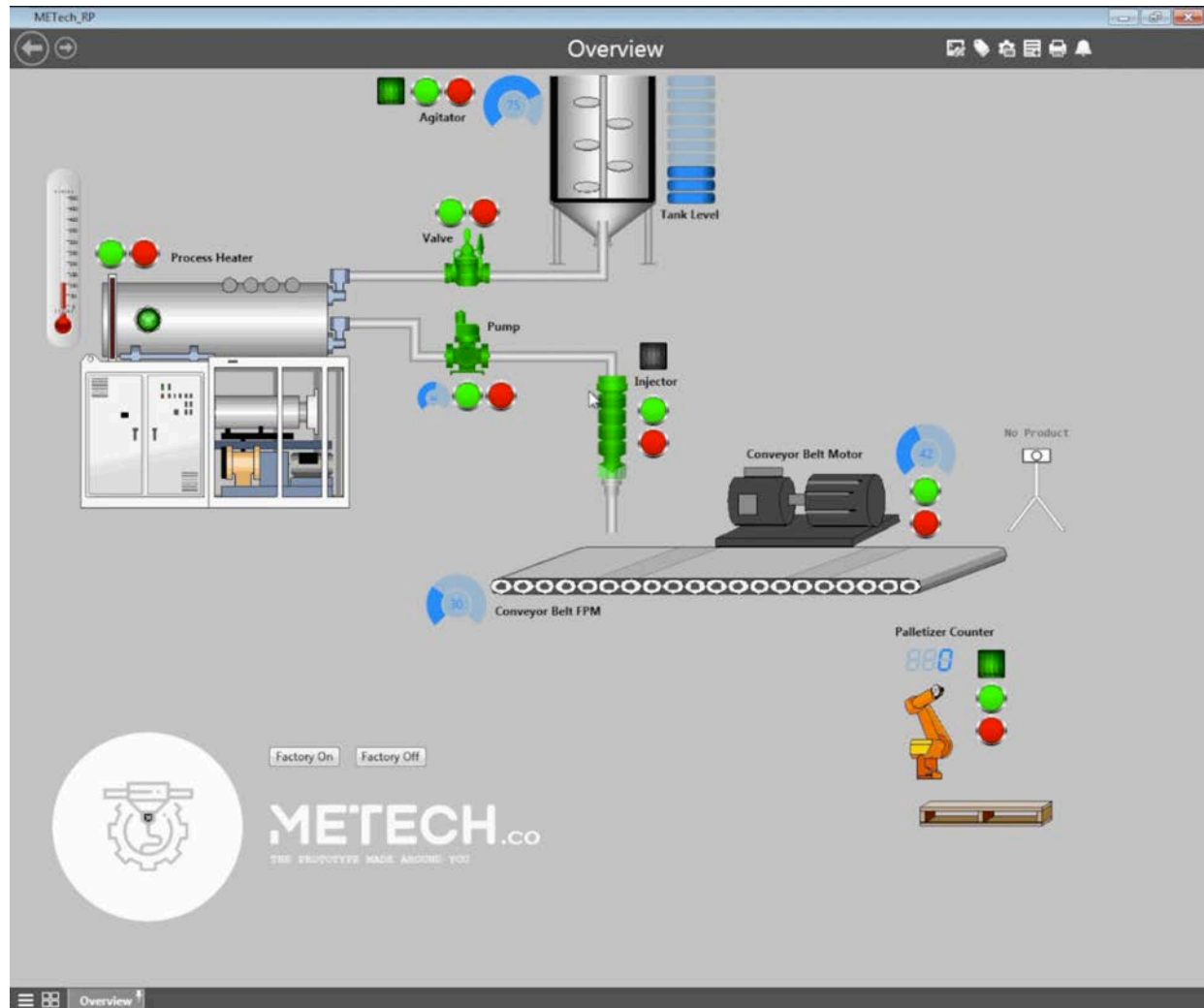
Factory On Factory Off

METECH.co
THE PROTOTYPE MADE AROUND YOU

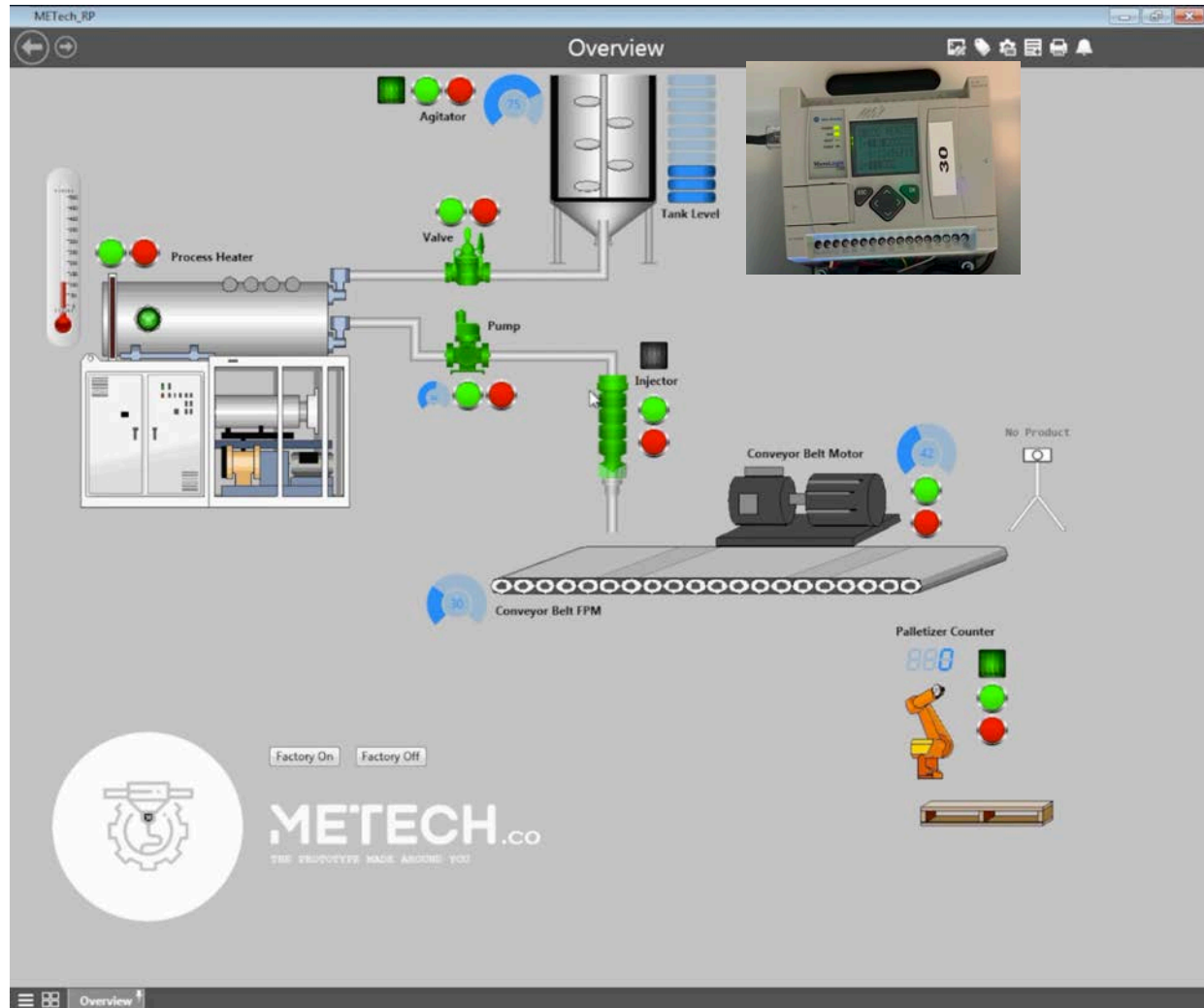
Equipment



HMI



HMI



HMI

The screenshot shows an HMI interface for a factory simulation. The main window is titled "ME'ech_RP" and "Overview". The interface displays a 3D schematic of a production line with various components and their status indicators:

- Agitator:** A green indicator light and a blue gauge showing 75.
- Tank Level:** A vertical bar chart showing the liquid level in a tank.
- Process Heater:** A red indicator light and a thermometer showing temperature.
- Valve:** A green indicator light.
- Pump:** A green indicator light and a blue gauge showing 30.
- Injector:** A green indicator light.
- Conveyor Belt FPM:** A blue gauge showing 30.
- Conveyor Belt Motor:** A green indicator light and a blue gauge showing 40.
- Palletizer Counter:** A blue digital display showing 888, a green indicator light, and a red indicator light.
- No Product:** A camera icon on a tripod.

At the bottom left, there is a circular logo with a gear and a stylized 'M' and 'S'. Below it, the text "ME'TECH.co" is displayed, with the tagline "THE FUTURE IS MADE AROUND YOU". To the right of the logo, there are two buttons: "Factory On" and "Factory Off".

At the bottom of the interface, there is a navigation bar with a menu icon and the text "Overview".

HMI

The screenshot shows an HMI interface for a factory simulation. The main window is titled "MEch_RP Overview" and features a 3D schematic of a production line. The components and their status are as follows:

- Agitator:** Status indicator is green, with a speed gauge set to 75.
- Tank Level:** A vertical bar chart shows the liquid level in a tank.
- Process Heater:** A cylindrical tank with a temperature gauge on the left.
- Valve:** Status indicator is green.
- Pump:** Status indicator is green.
- Injector:** Status indicator is green.
- Conveyor Belt Motor:** Status indicator is green, with a speed gauge set to 40.
- Conveyor Belt FPM:** Status indicator is green, with a speed gauge set to 30.
- Palletizer Counter:** A digital display shows "888", with status indicators for green and red.
- No Product:** A camera icon on a tripod indicates no product is currently on the conveyor.

At the bottom of the interface, there are two buttons: "Factory On" and "Factory Off". A circular logo with a gear and a stylized 'M' is visible in the bottom left. The text "METEC" and "CONVEYOR BELT" is partially visible at the bottom center. The bottom status bar shows "Overview" and a menu icon.

Three inset images show physical hardware components:

- A Siemens PLC rack with a module labeled "02".
- A PLC rack with a module labeled "10".
- A digital display unit with a screen showing "30" and a keypad.

HMI

The screenshot displays the 'MEch_RP' HMI software interface, titled 'Overview'. The main area features a 3D schematic of a production line with the following components and controls:

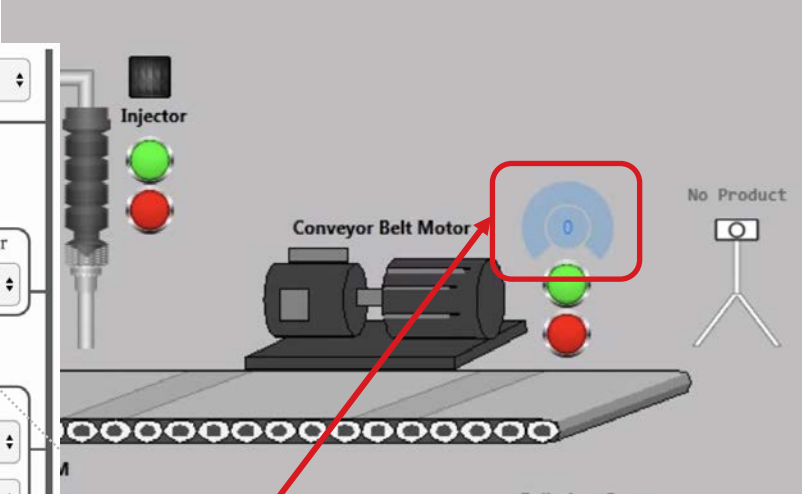
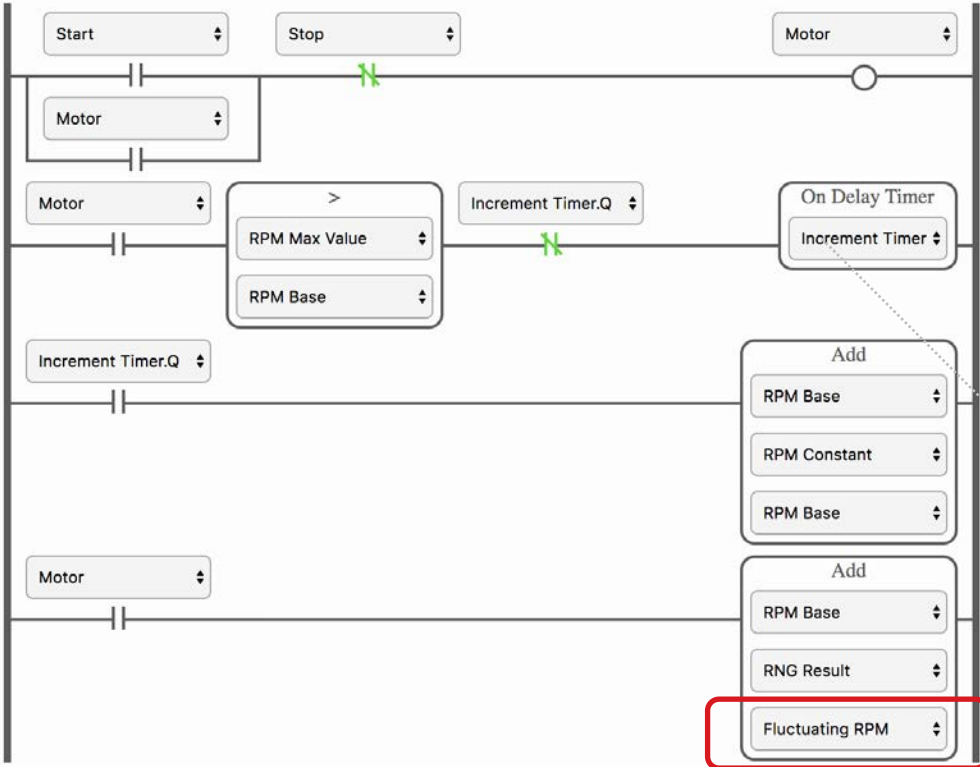
- Agitator:** A green indicator light and a blue gauge showing a value of 75.
- Tank Level:** A vertical bar chart showing the liquid level in a tank.
- Process Heater:** A cylindrical unit with a red indicator light and a temperature gauge.
- Valve:** A green indicator light and a red stop button.
- Pump:** A green indicator light and a blue gauge.
- Injector:** A vertical assembly with a green indicator light and a red stop button.
- Conveyor Belt Motor:** A motor unit with a blue gauge showing 40, a green indicator light, and a red stop button.
- Conveyor Belt FPM:** A gauge showing 30.
- Palletizer Counter:** A digital display showing '888', a green indicator light, and a red stop button.
- No Product:** A camera icon on a tripod.

Four inset images show physical hardware components:

- 02:** A Siemens PLC (Programmable Logic Controller) unit.
- 10:** A control panel with a digital display and various indicator lights.
- 30:** A control panel with a digital display showing '30'.
- 31:** A control panel with a digital display showing '31'.

At the bottom, there are 'Factory On' and 'Factory Off' buttons, a circular logo with a gear and a 'G' inside, and the text 'METEC CONVEYOR BELT THE FRODOFFS MAKE ABOVE YOU'. The bottom status bar shows 'Overview'.

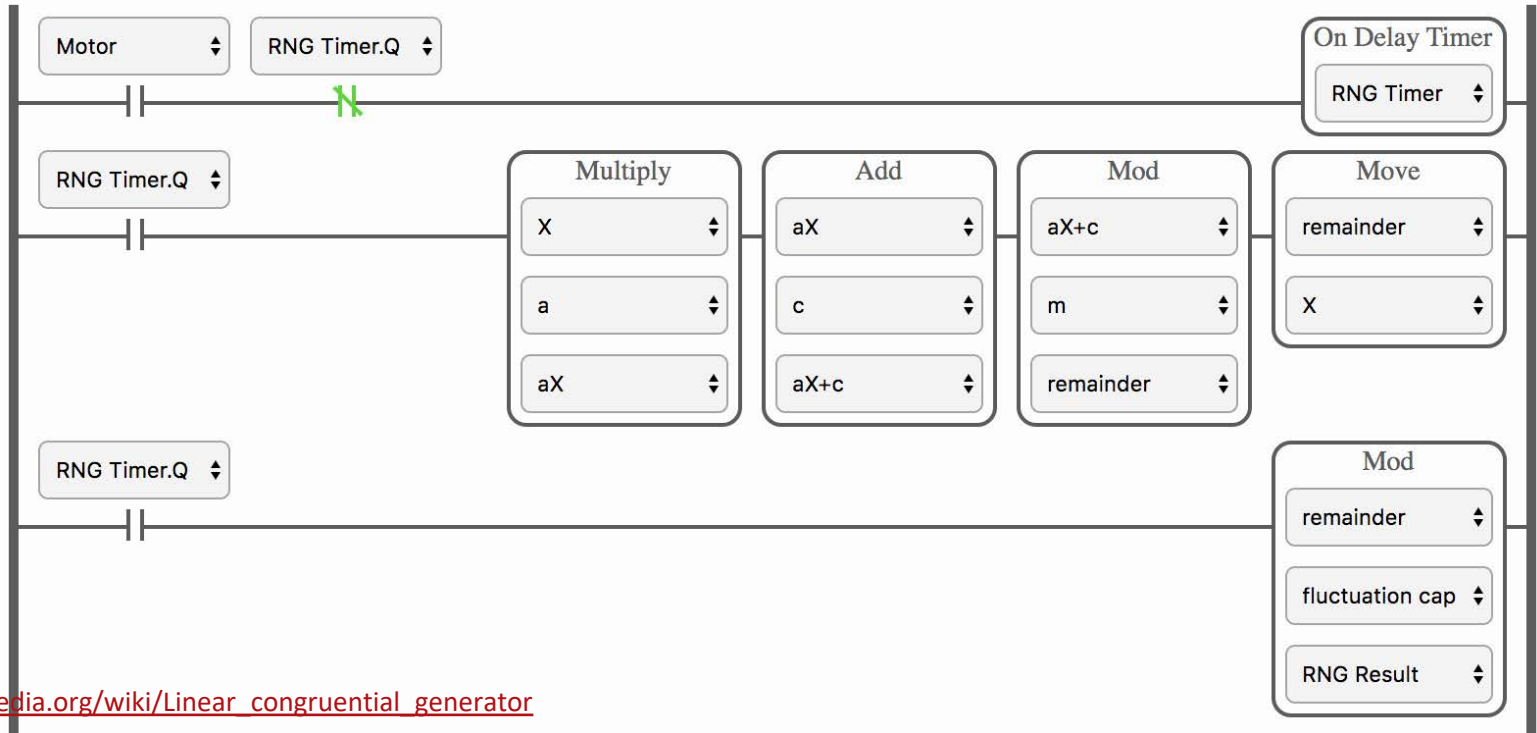
Logic – Motor RPM Fluctuations



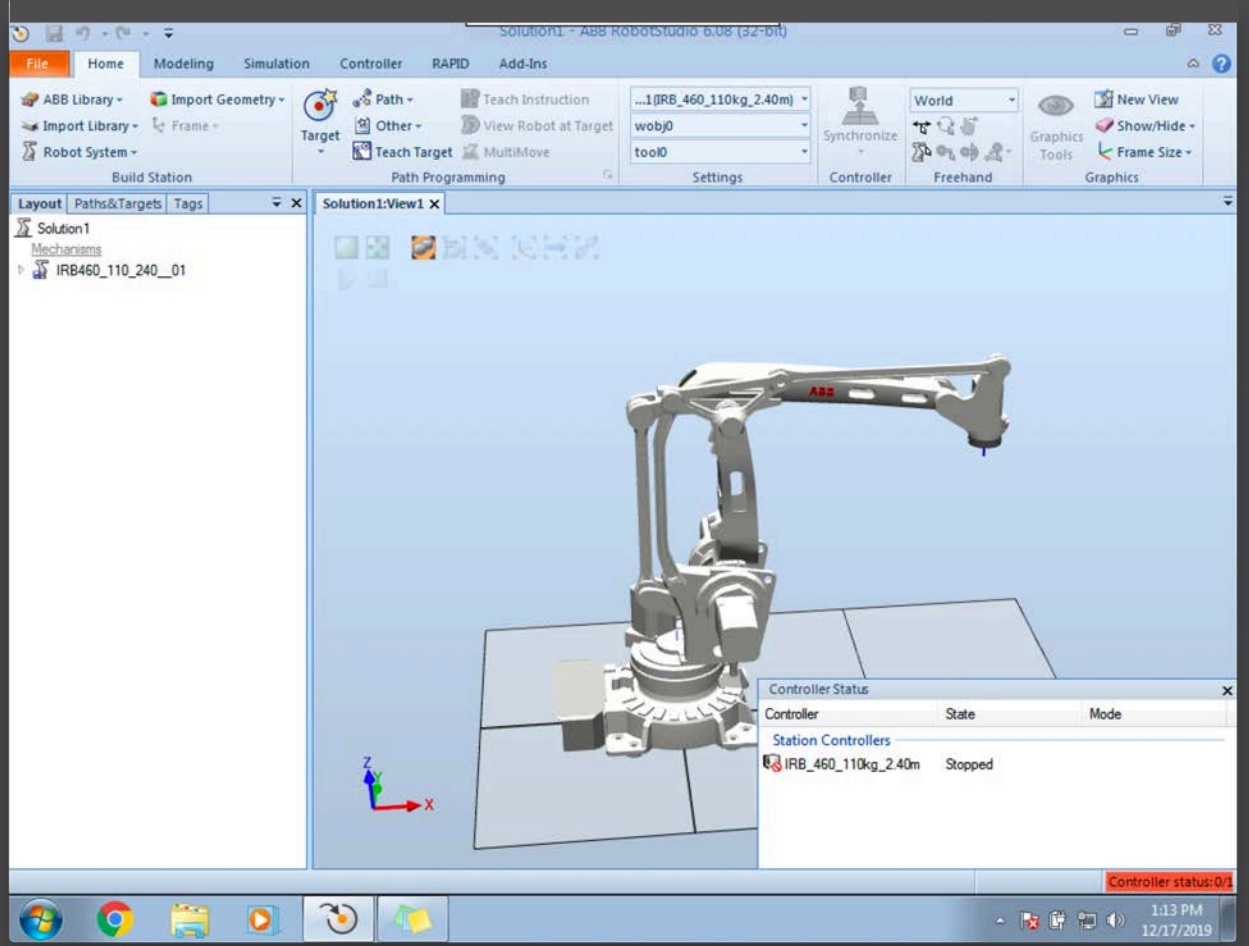
Logic – RNG Block

- Linear congruential generator

$$X_{n+1} = (aX_n + c) \bmod m$$



Robotics



Port Forwarding



AirLink

ACEmanager

Software and Firmware

Template

Refresh All

Reboot

Help

Logout

Status

WAN/Cellular

LAN

VPN

Security

Services

Location

Events Reporting

Serial

Applications

I/O

Admin

Last updated time : 5/2/2019 8:44:20 PM

Apply

Refresh

Cancel

Port Forwarding

DMZ Host Enabled

Disable

Extended Port Forwarding

Port Forwarding

Disable

Port Filtering - Inbound

Port Filtering - Outbound

Trusted IPs - Inbound (Friends)

Trusted IPs - Outbound

MAC Filtering

Port Forwarding

	Public Start Port	Public End Port	Protocol	Host IP	Private Start Port
X	44818	44818	TCP	192.168.0.30	44818
X	9600	9600	UDP	192.168.0.10	9600
X	102	102	TCP	192.168.0.2	102
X	5900	5900	TCP	192.168.0.5	5900
X	5901	5901	TCP	192.168.0.6	5900

Add More

Port Forwarding

SIERRA WIRELESS | AirLink | ACEmanager

Software and Firmware | Template | Refresh All | Reboot | Help | Logout

Status | WAN/Cellular | LAN | VPN | **Security** | Services | Location | Events Reporting | Serial | Applications | I/O | Admin

Last updated time : 5/2/2019 8:44:20 PM Apply Refresh Cancel

Port Forwarding

DMZ Host Enabled Disable

Port Forwarding Disable

Port Forwarding

	Public Start Port	Public End Port	Protocol	Host IP	Private Start Port
<input checked="" type="checkbox"/>	44818		TCP	192.168.0.30	44818
<input checked="" type="checkbox"/>	9600		UDP	192.168.0.10	9600
<input checked="" type="checkbox"/>	102		TCP	192.168.0.2	102
<input checked="" type="checkbox"/>	5900		TCP	192.168.0.5	5900
<input checked="" type="checkbox"/>	5901		TCP	192.168.0.6	5900

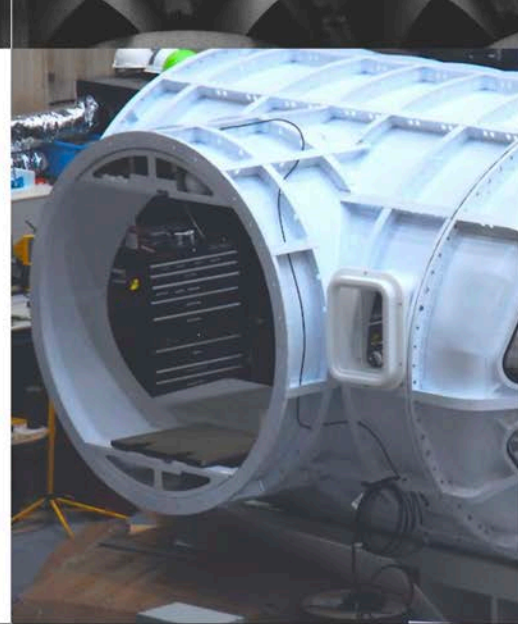
Micrologix
Omron
Siemens
VNC
VNC

Add More

The Company

WHAT CAN WE CREATE?

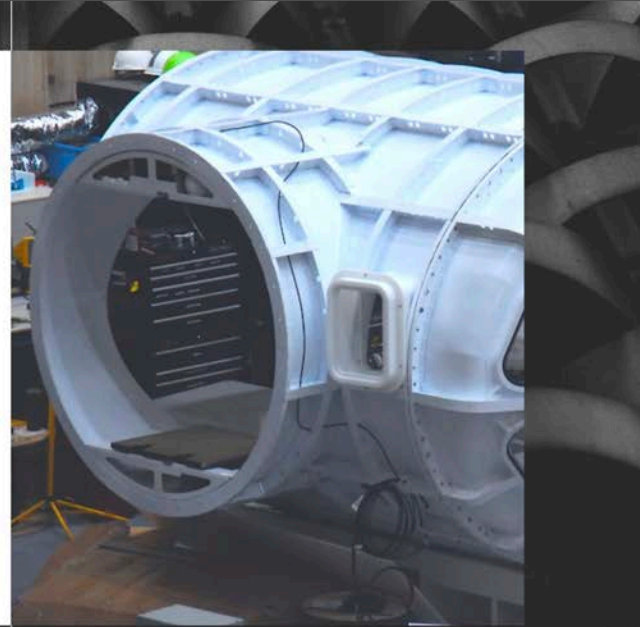
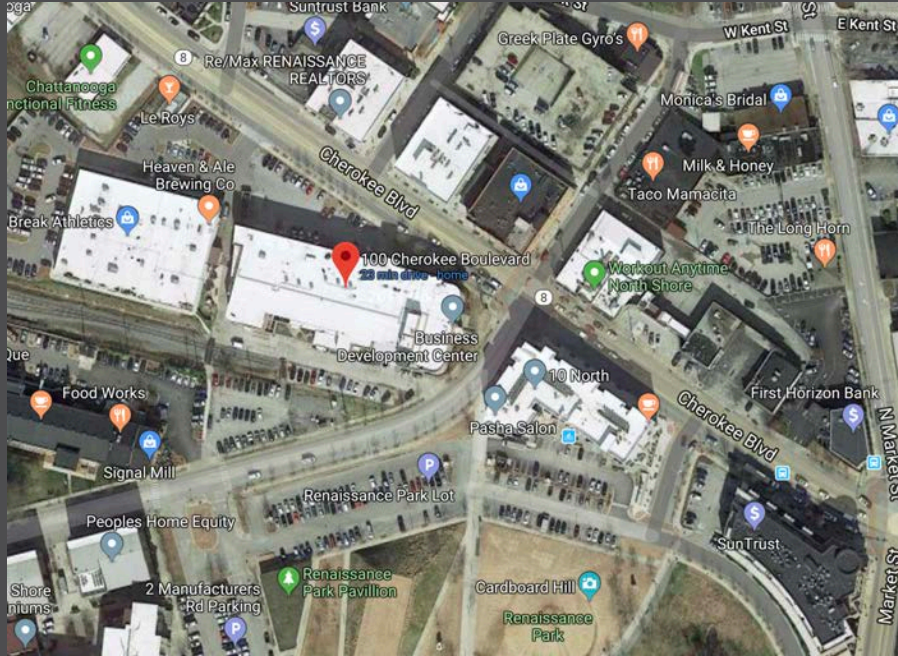
Our engineers are specialized in **virtual 3D modeling**, **digital twins**, as well as physical mockups. Our flexible **production floor** can quickly turn models into **plastic and metal** parts, which we can optionally assemble and brand for your business.



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

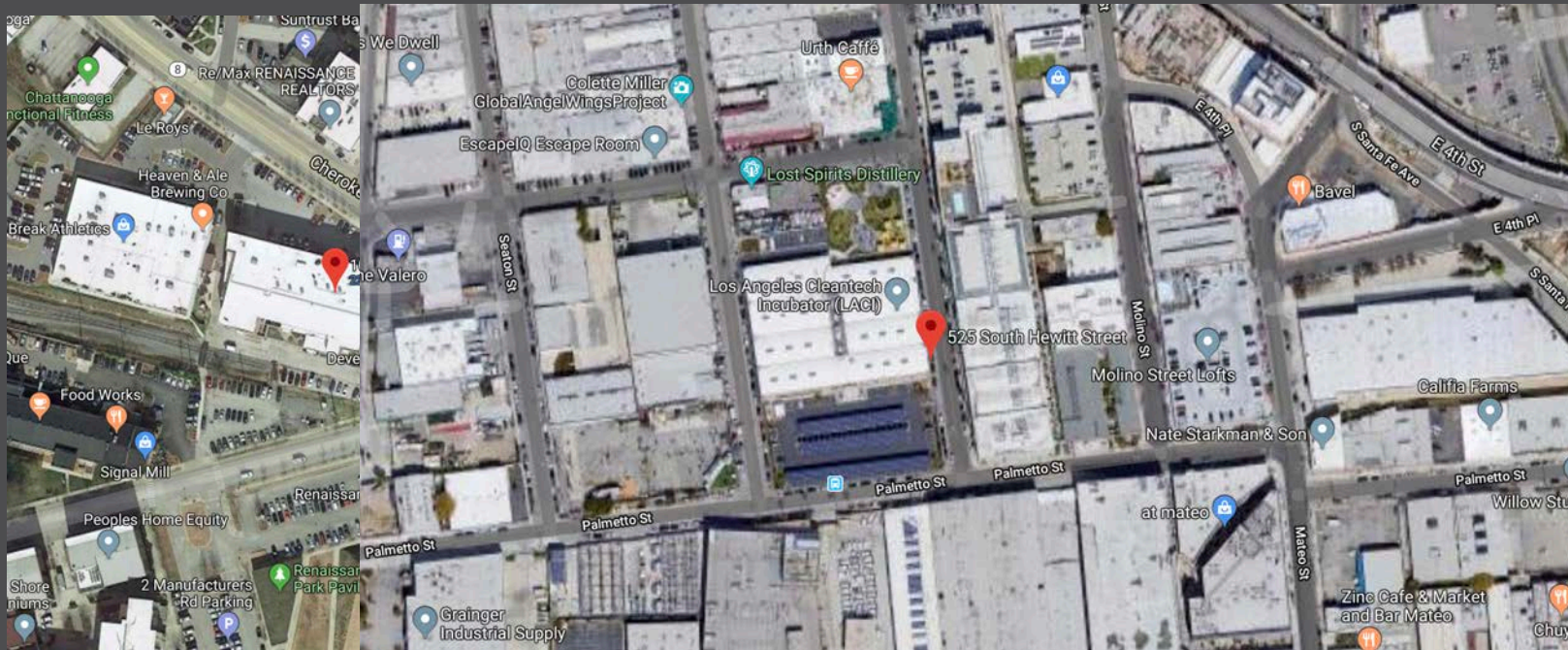
Offices: +1 (213) 338-1513, 525 S Hewitt St, Los Angeles, CA 90013, USA

The Company



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



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

WHAT CAN WE CREATE?

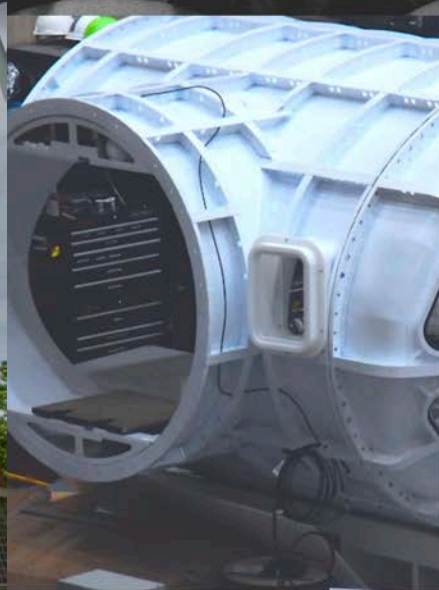
Our engineers are specialized in **virtual 3D modeling**, **digital twins**, as well as physical mockups. Our flexible **production floor** can quickly turn models into **plastic and metal** parts, which we can optionally assemble and brand for your business.



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



Bldg, Chattanooga, TN 37405, USA.

1st, 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.
```

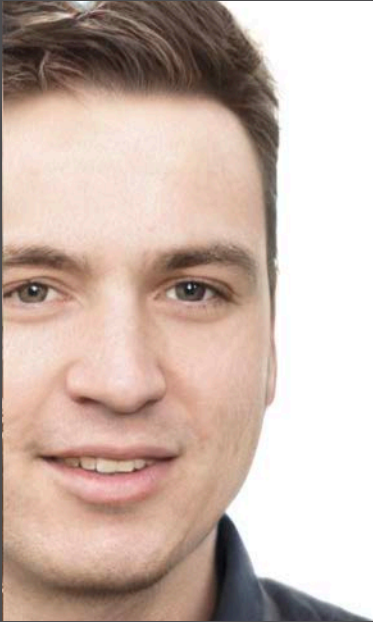
```
Address:         172.
```

```
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

The screenshot shows a web interface for a VoIP system. On the left is a vertical navigation menu with buttons for 'Dashboard', 'Configuration', 'Extensions', 'Groups', 'Receptionist', 'Hold Music', 'Schedule', 'Tricks', 'My Services', and 'My Account'. The main content area is titled 'Mike Linode Test' and is divided into three sections: 'Extensions', 'Numbers', and 'Useful'. The 'Extensions' section lists five entries with red telephone handset icons. The 'Numbers' section lists two entries with asterisks. The 'Useful' section lists several entries, including a speaker icon next to '555 Page via speaker'.

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

Screen Remote Display **Recording**

Enable Recording

Recording Mode: Video Only

File Path: 

Frame Size: 1024 x 768 (4:3) 1024 768

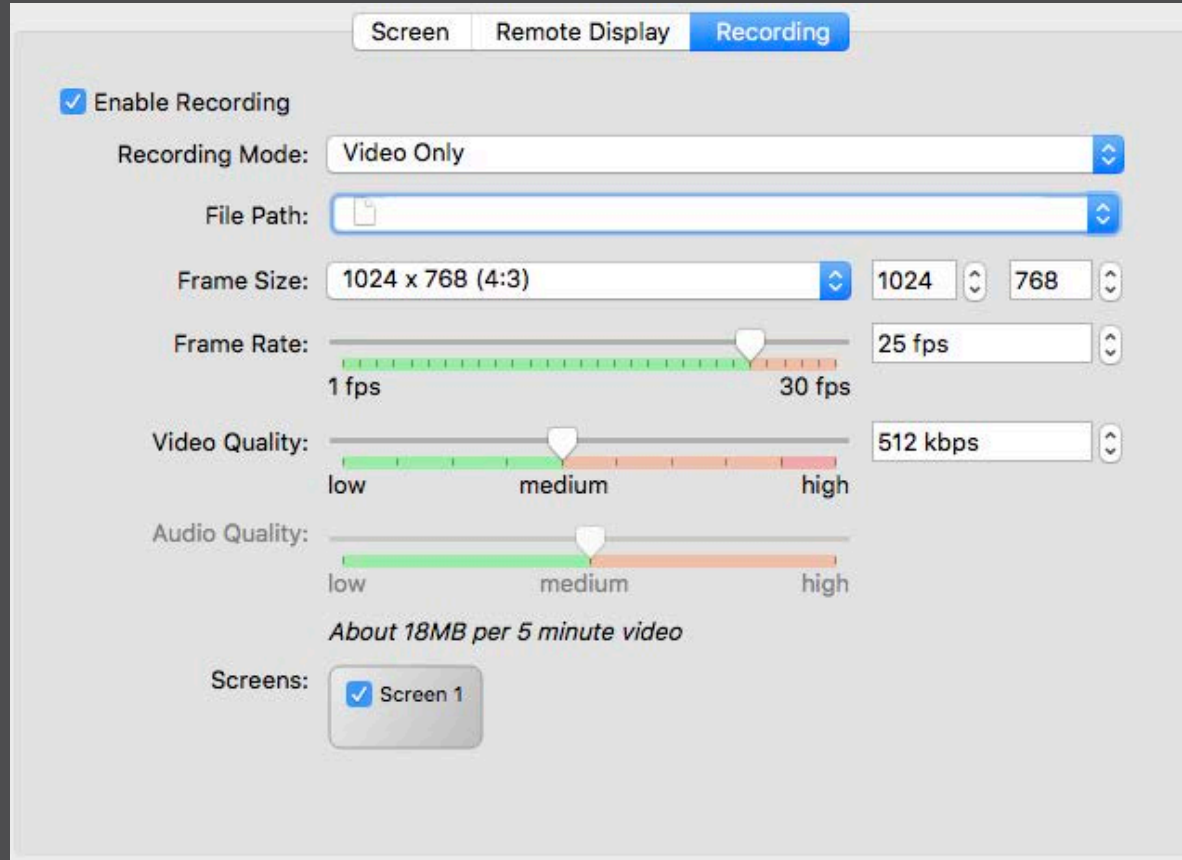
Frame Rate: 1 fps 25 fps 30 fps

Video Quality: low medium high 512 kbps

Audio Quality: low medium high

About 18MB per 5 minute video

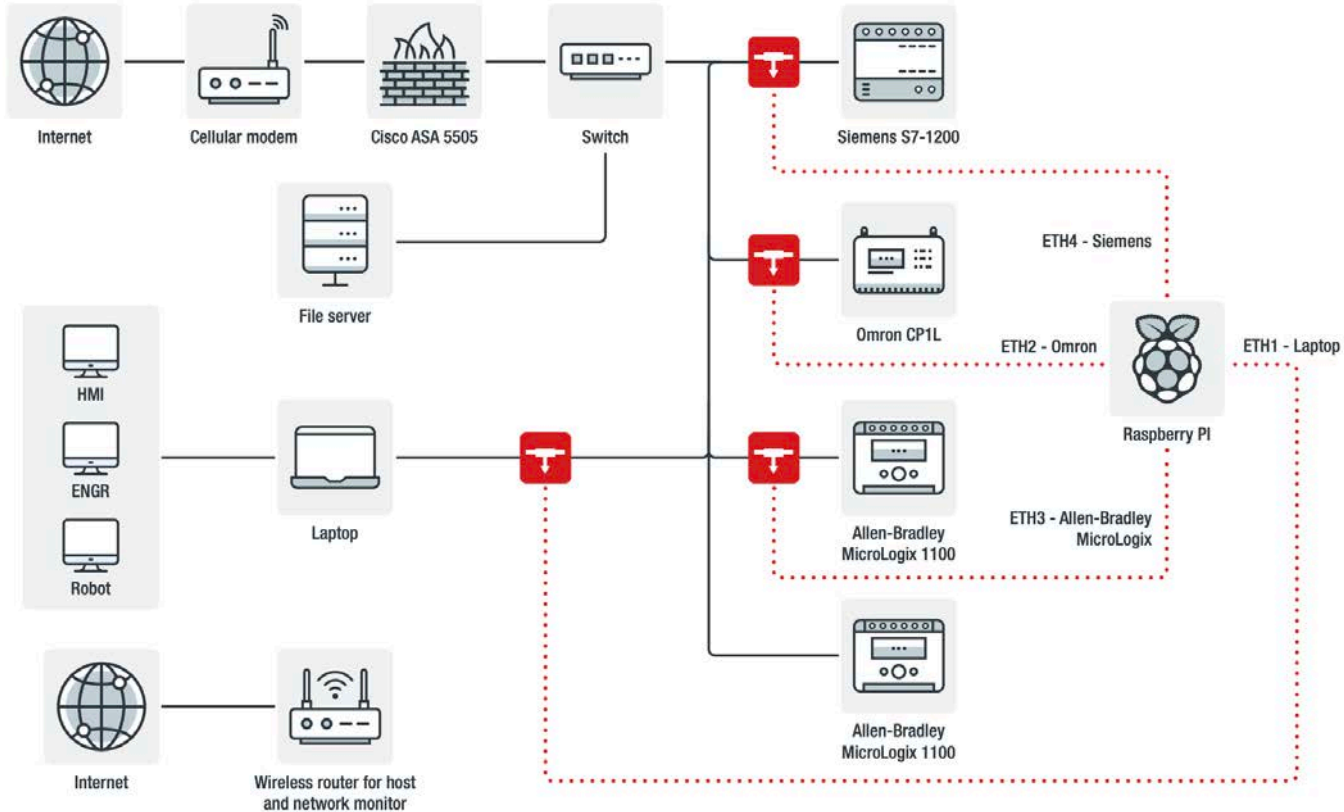
Screens: Screen 1



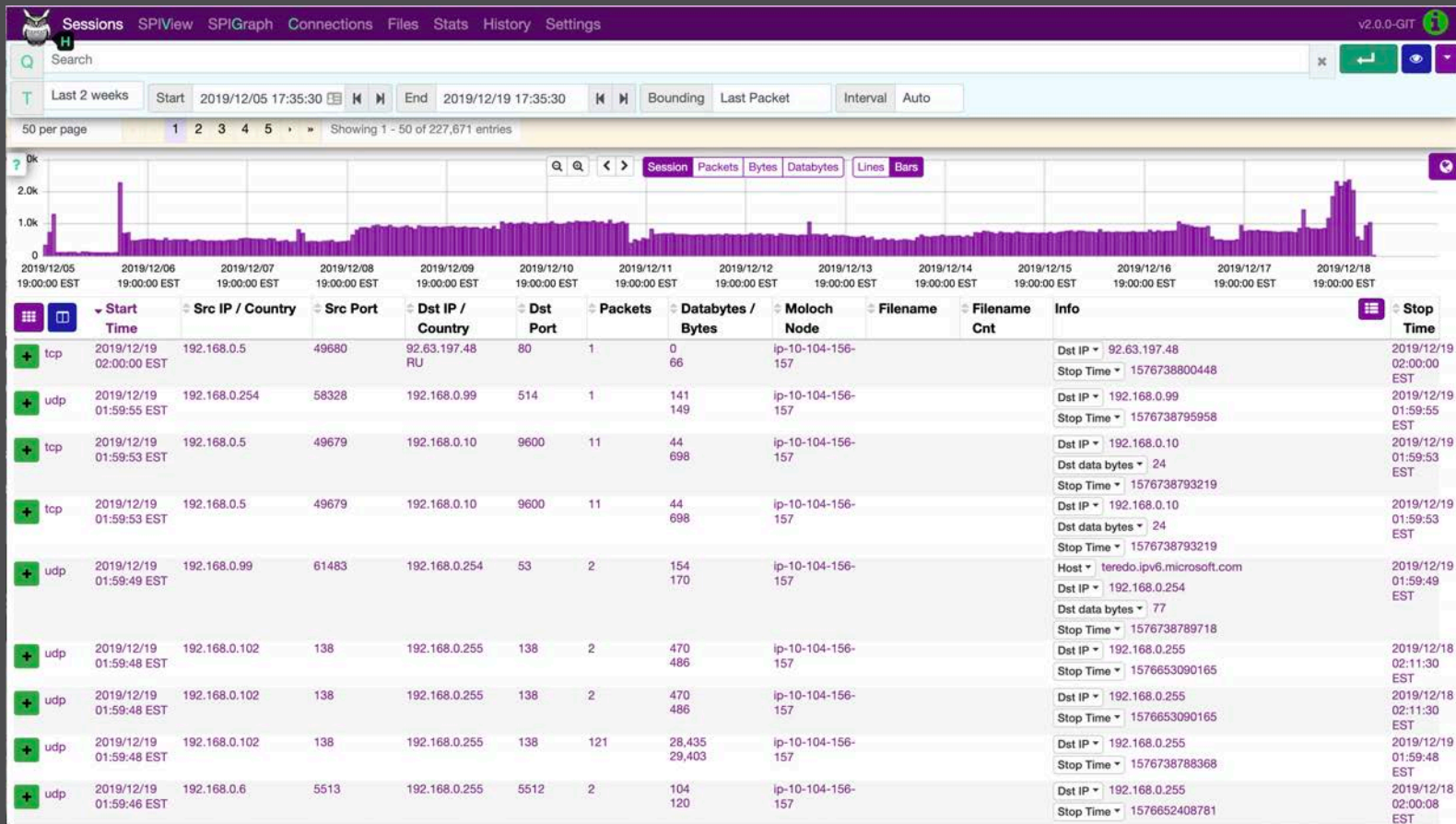
Monitoring the system



Monitoring the system



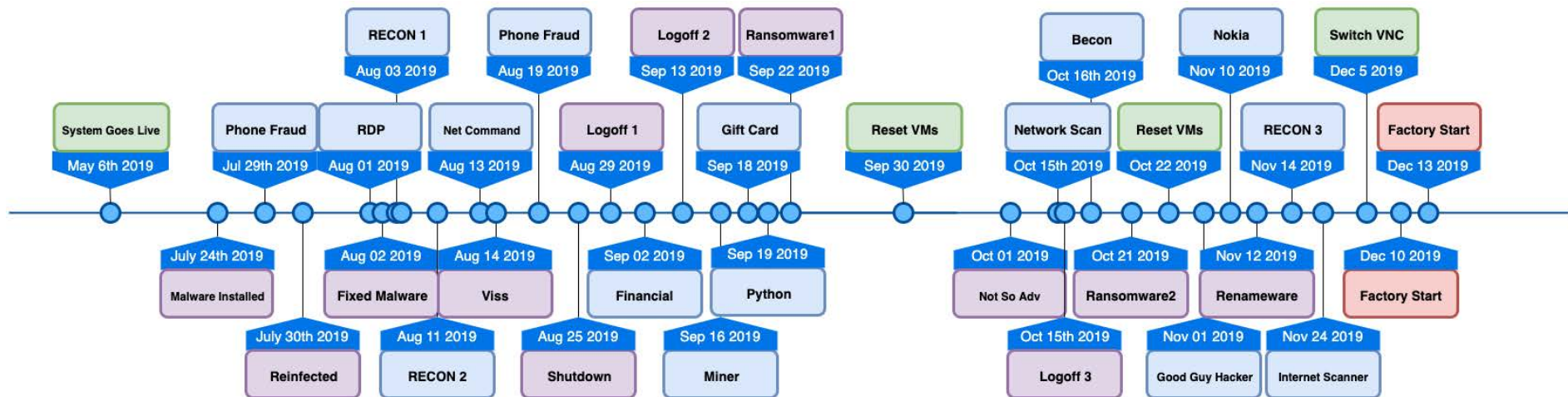
Moloch



Scripts

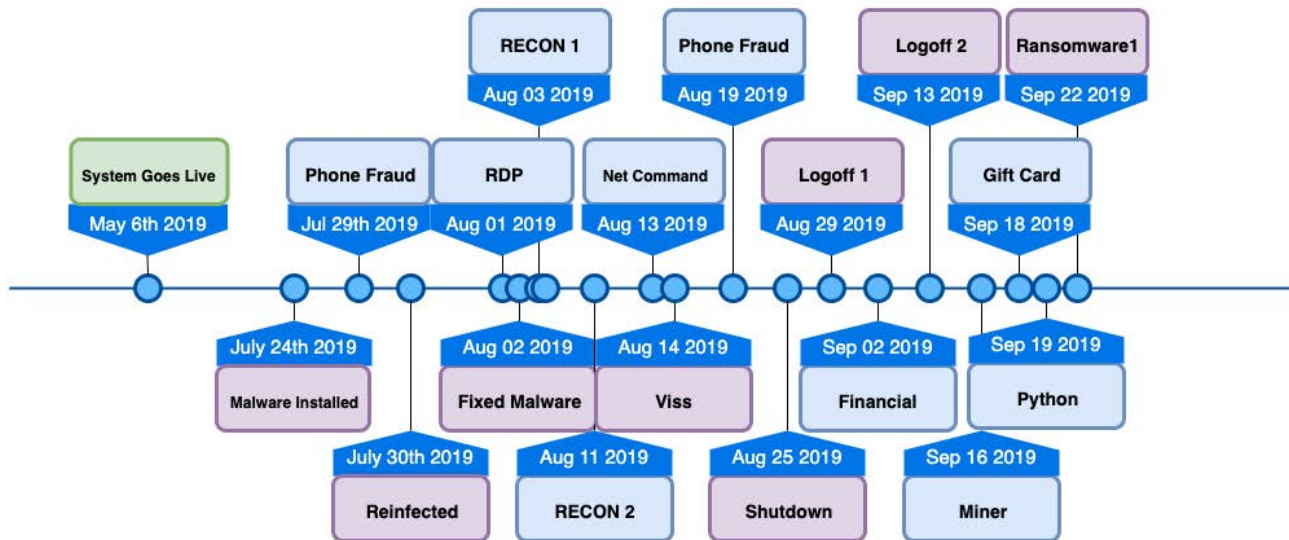
Laptop Sniffer IP Conversations								DNS <-> DNS				
IP	GEO	<->	IP	GEO	Bytes	<->	Bytes	TotalB	Duration	DNS	<->	DNS
192.168.1.1	AA	<->	196.200.1.1	SC	23452	<->	18658	210035	43908.29		<->	Resolve
13.33.1.1	US	<->	192.168.1.1	AA	56267	<->	26965	275283	45708.44		<->	ax3.r.cloudfront.net <-> localnet
192.168.1.1	AA	<->	192.168.1.1	ZZ	19839	<->	0	198391	0.000000		<->	Resolve
194.168.1.1	US	<->	192.168.1.1	AA	24204	<->	47162	495832	44488.71		<->	localnet
169.168.1.1	CH	<->	192.168.1.1	AA	20768	<->	18219	38974	45895.16		<->	iewer.com <-> localnet
188.168.1.1	AA	<->	192.168.1.1	AA	33363	<->	14586	179227	45941.10		<->	iewer.com <-> localnet
104.168.1.1	US	<->	192.168.1.1	AA	20572	<->	14623	166806	44487.27		<->	localnet
96.168.1.1	US	<->	192.168.1.1	AA	60057	<->	24350	249511	9419.517		<->	static.akamaitechnologies.com <-> localnet
72.216.1.1	US	<->	192.168.1.1	AA	44206	<->	24828	252703	12000.88		<->	localnet
23.68.1.1	US	<->	192.168.1.1	AA	51094	<->	24558	250693	645.9369		<->	tatic.akamaitechnologies.com <-> localnet
23.68.1.1	US	<->	192.168.1.1	AA	27678	<->	24722	249988	669.0907		<->	tatic.akamaitechnologies.com <-> localnet
23.68.1.1	US	<->	192.168.1.1	AA	81044	<->	13911	147214	44079.78		<->	.static.akamaitechnologies.com <-> localnet
108.7.1.1	US	<->	192.168.1.1	AA	10757	<->	42044	149616	42185.33		<->	rtmd.east.verizon.net <-> localnet
13.136.1.1	US	<->	192.168.1.1	AA	16622	<->	59307	759300	44079.38		<->	localnet
185.23.1.1	ZZ	<->	192.168.1.1	AA	61793	<->	37682	655620	2129.563		<->	localnet
142.171.1.1	CA	<->	192.168.1.1	AA	63078	<->	29579	358875	2073.864		<->	ral.com <-> localnet
31.136.1.1	IE	<->	192.168.1.1	AA	31608	<->	92317	960782	44494.83		<->	rbcdn.net <-> localnet
136.148.1.1	US	<->	192.168.1.1	AA	57680	<->	60612	118292	44518.73		<->	alesforceliveagent.com <-> localnet
64.233.1.1	US	<->	192.168.1.1	AA	34936	<->	74693	781867	44099.79		<->	localnet
192.168.1.1	AA	<->	205.188.1.1	US	30734	<->	49450	356790	44107.37		<->	dn.net
72.216.1.1	US	<->	192.168.1.1	AA	30060	<->	74510	775167	44126.96		<->	localnet
23.208.1.1	US	<->	192.168.1.1	AA	68646	<->	46850	537153	44083.21		<->	y.static.akamaitechnologies.com <-> localnet
68.67.1.1	US	<->	192.168.1.1	AA	11754	<->	12133	238876	44090.29		<->	ncer.mgmt.nym2.adnexus.net <-> localnet
192.168.1.1	AA	<->	204.15.1.1	US	49156	<->	42882	92038	44098.98		<->	22.doubleverify.com
38.112.1.1	US	<->	192.168.1.1	AA	22344	<->	15119	173538	2079.425		<->	m <-> localnet
64.233.1.1	US	<->	192.168.1.1	AA	72600	<->	11840	191008	44750.01		<->	localnet
108.7.1.1	US	<->	192.168.1.1	AA	33578	<->	10120	134782	44086.79		<->	kedin.com <-> localnet
68.67.1.1	US	<->	192.168.1.1	AA	18306	<->	56400	239462	44095.42		<->	ncer.mgmt.nym2.adnexus.net <-> localnet
31.136.1.1	IE	<->	192.168.1.1	AA	73716	<->	61655	135371	44508.08		<->	-at13.facebook.com <-> localnet
104.7.1.1	US	<->	192.168.1.1	AA	14666	<->	6353	133003	44098.85		<->	.com <-> localnet
65.55.1.1	US	<->	192.168.1.1	AA	14666	<->	53300	199966	5995.872		<->	localnet
104.7.1.1	US	<->	192.168.1.1	AA	23420	<->	67659	91079	44507.87		<->	localnet
64.233.1.1	US	<->	192.168.1.1	AA	21140	<->	16370	184844	44772.18		<->	-> localnet
192.168.1.1	AA	<->	204.15.1.1	US	13908	<->	48230	187315	44087.20		<->	ginx-loadbalancer.mgmt.nym2.adnexus.net
52.33.1.1	US	<->	192.168.1.1	AA	34164	<->	18247	216641	44755.68		<->	te-1.amazonaws.com <-> localnet
104.9.1.1	US	<->	192.168.1.1	AA	12544	<->	20229	214836	9666.629		<->	.static.akamaitechnologies.com <-> localnet
185.23.1.1	ZZ	<->	192.168.1.1	AA	16930	<->	8991	178291	7071.010		<->	localnet
13.33.1.1	US	<->	192.168.1.1	AA	21032	<->	11997	141004	44768.74		<->	ax3.r.cloudfront.net <-> localnet
72.216.1.1	US	<->	192.168.1.1	AA	16088	<->	61350	77438	44069.24		<->	localnet
50.112.1.1	US	<->	192.168.1.1	AA	25084	<->	39339	64423	44095.50		<->	n.com <-> localnet
74.125.1.1	US	<->	192.168.1.1	AA	35244	<->	11310	148353	44215.94		<->	localnet
40.112.1.1	US	<->	192.168.1.1	AA	20986	<->	72532	93518	7623.911		<->	localnet
104.24.1.1	US	<->	192.168.1.1	AA	22004	<->	54417	76421	44507.87		<->	localnet
64.233.1.1	US	<->	192.168.1.1	AA	14198	<->	12714	141343	44089.41		<->	localnet
192.168.1.1	AA	<->	199.168.1.1	US	24396	<->	15830	259792	44097.10		<->	fw.adsafeprotected.com
13.33.1.1	US	<->	192.168.1.1	AA	23040	<->	98714	121754	44496.40		<->	localnet
74.125.1.1	US	<->	192.168.1.1	AA	36788	<->	60742	97530	44103.82		<->	localnet
172.216.1.1	US	<->	192.168.1.1	AA	11178	<->	13261	143788	44083.08		<->	net <-> localnet
52.7.1.1	US	<->	192.168.1.1	AA	22916	<->	34439	57355	44106.07		<->	ute-1.amazonaws.com <-> localnet
192.168.1.1	AA	<->	204.79.1.1	US	14934	<->	13570	162911	14079.19		<->	-msedge.net
192.168.1.1	AA	<->	199.168.1.1	US	15132	<->	14046	165370	44111.79		<->	pixel.adsafeprotected.com
40.112.1.1	US	<->	192.168.1.1	AA	17290	<->	59656	76946	2381.940		<->	localnet
184.24.1.1	NL	<->	192.168.1.1	AA	32870	<->	12455	157422	44262.72		<->	.static.akamaitechnologies.com <-> localnet
13.33.1.1	US	<->	192.168.1.1	AA	21276	<->	72239	93515	44451.16		<->	localnet
104.24.1.1	US	<->	192.168.1.1	AA	11970	<->	41194	53164	44495.03		<->	localnet
104.24.1.1	US	<->	192.168.1.1	AA	8396	<->	12418	132576	44271.18		<->	localnet
104.24.1.1	US	<->	192.168.1.1	AA	7714	<->	10021	107926	44762.34		<->	localnet

What Happened

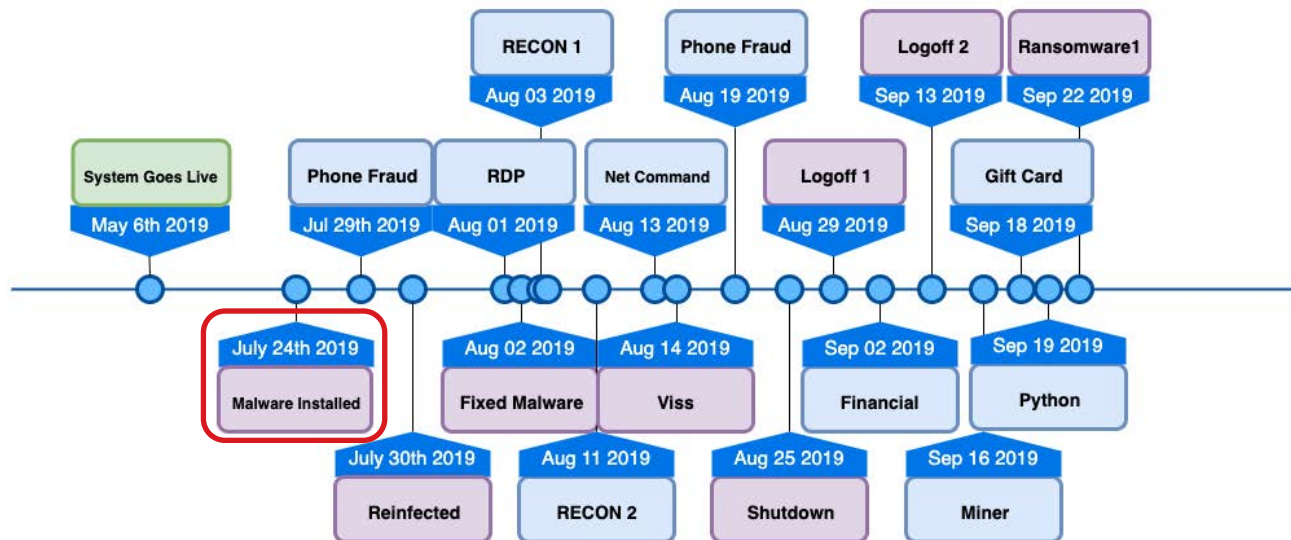


- Admin Event
- IT Event
- OT Event
- Hybrid Event

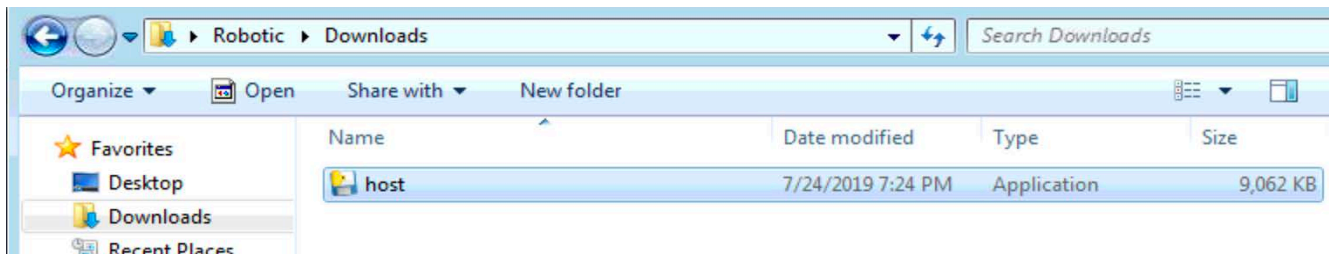
What Happened



What Happened



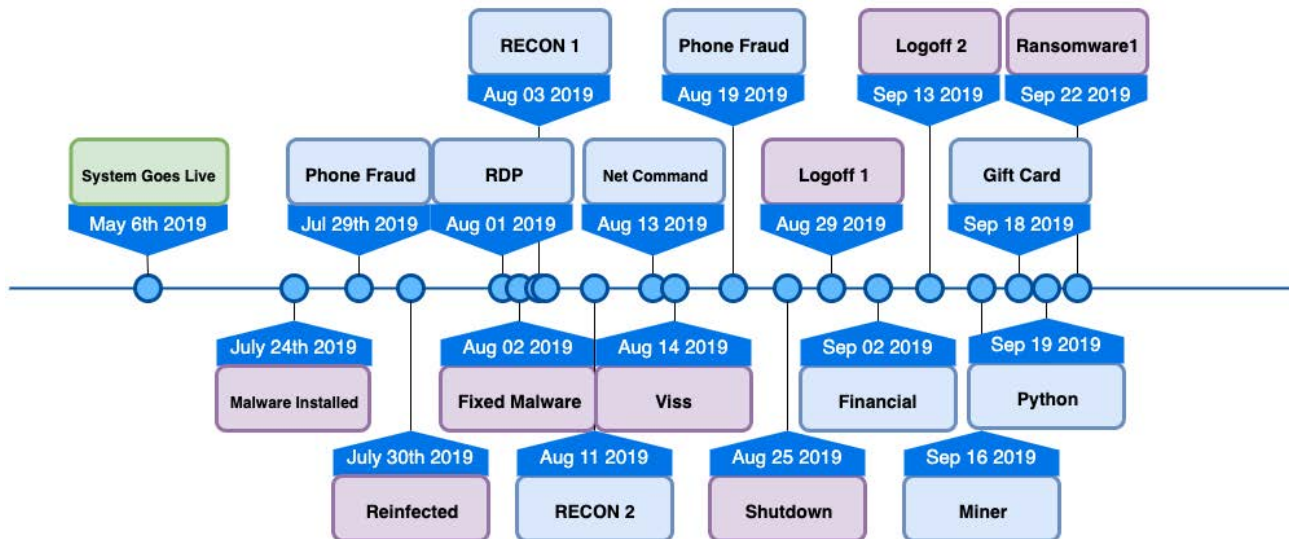
Host.exe



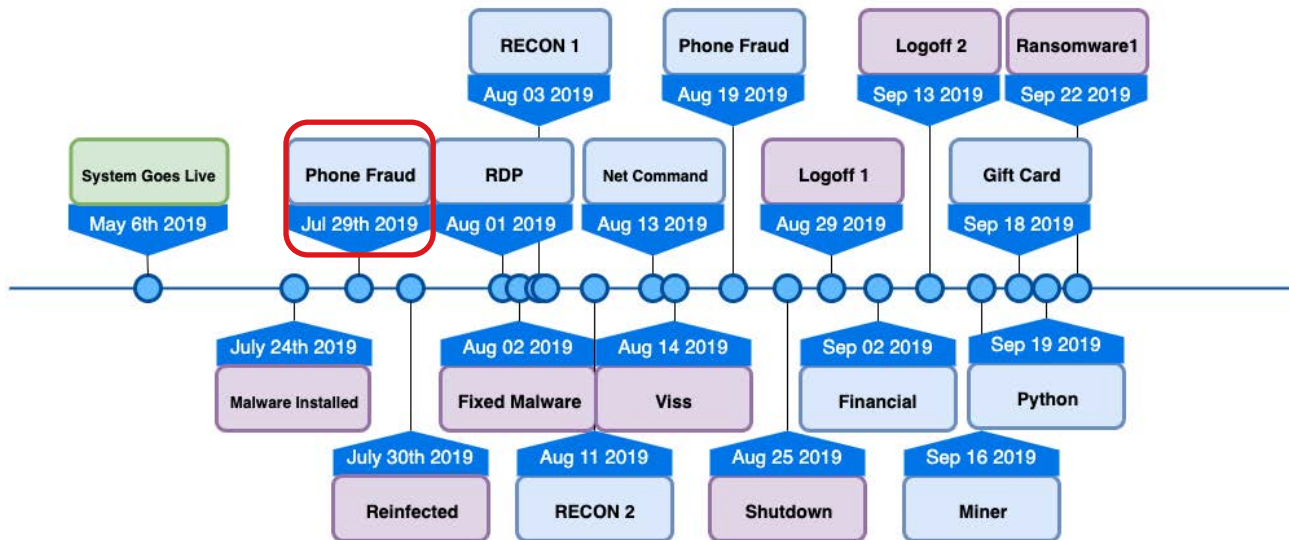
```
root@kali:~/Desktop/python-exe-unpacker# python pyinstxtractor.py ../host.exe1
[*] Processing ../host.exe1
[*] Pyinstaller version: 2.1+
[*] Python version: 27
[*] Length of package: 9036159 bytes
[*] Found 930 files in CArchive
[*] Beginning extraction...please standby
[*] Found 549 files in PYZ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

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

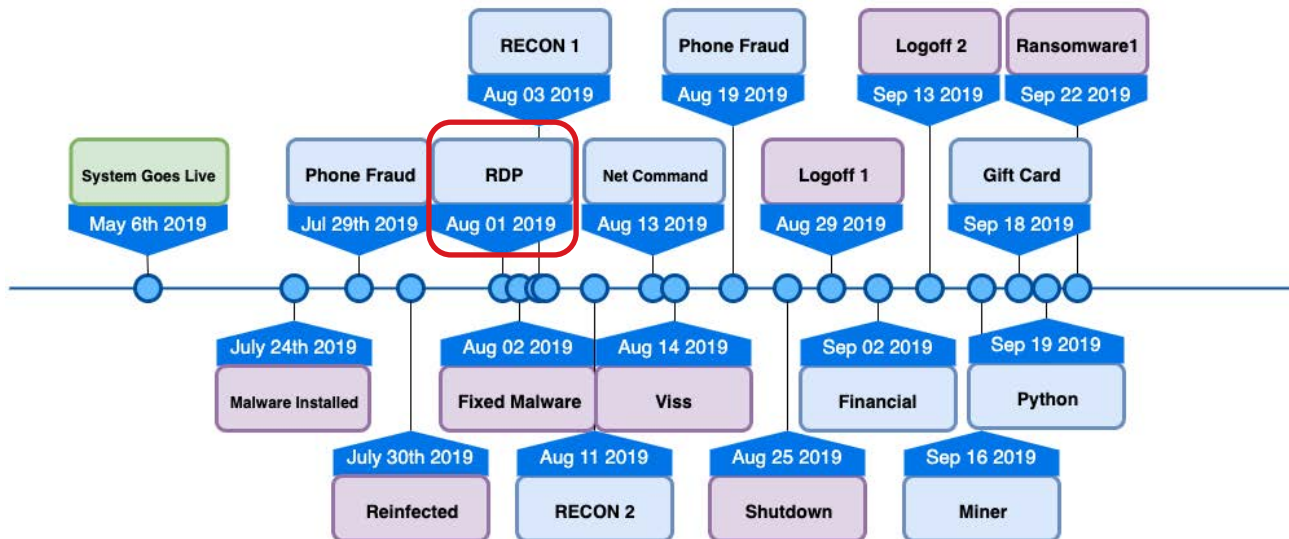
What Happened



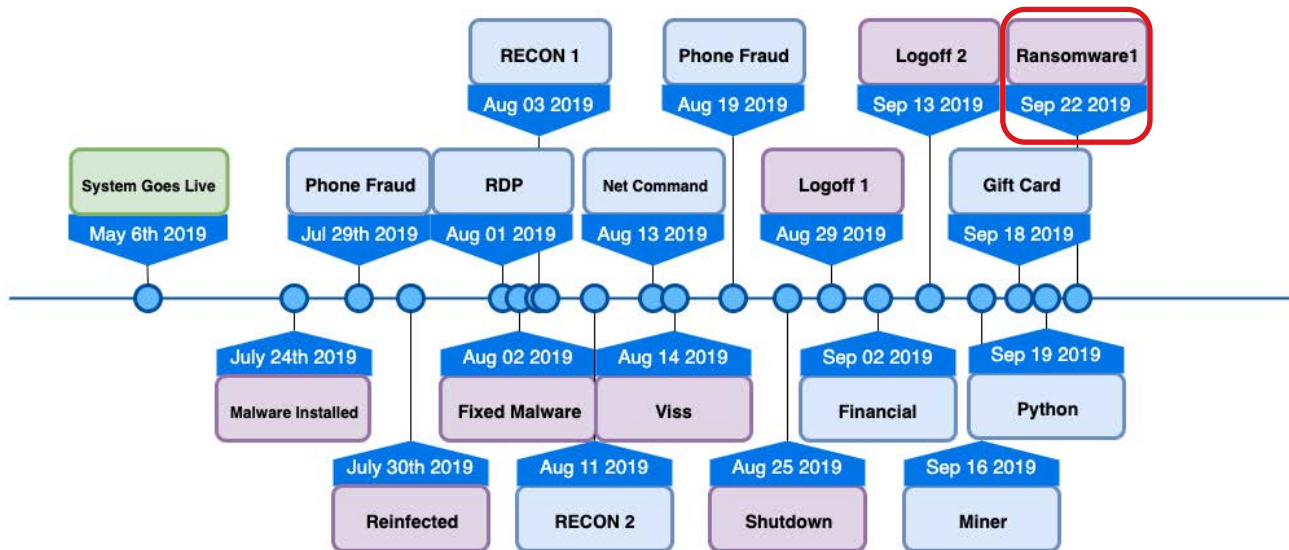
What Happened



What Happened



What Happened





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 >>

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

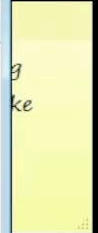
Devices with Removable Storage (1)

- CD Drive (D:)

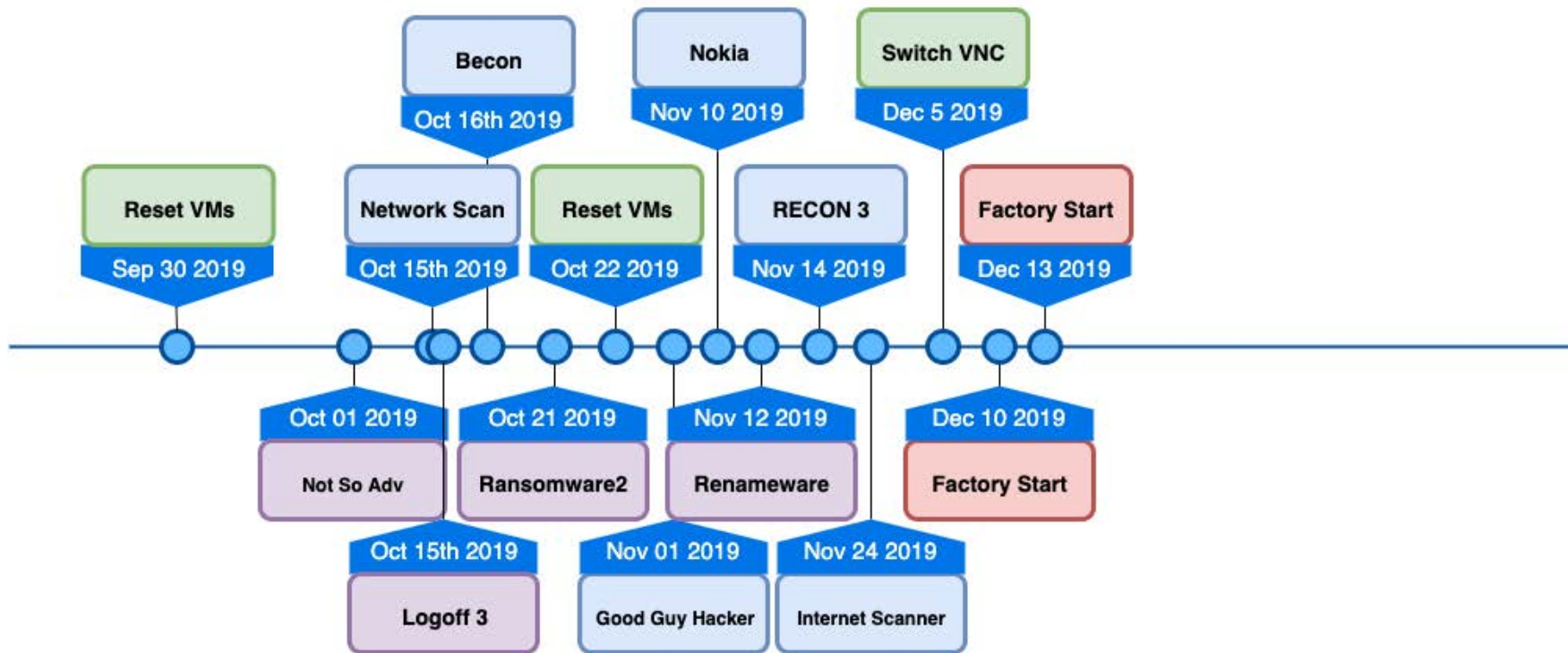
Network Location (1)

- MeTech (\\FILESERVER) (M:)
28.2 GB free of 74.4 GB

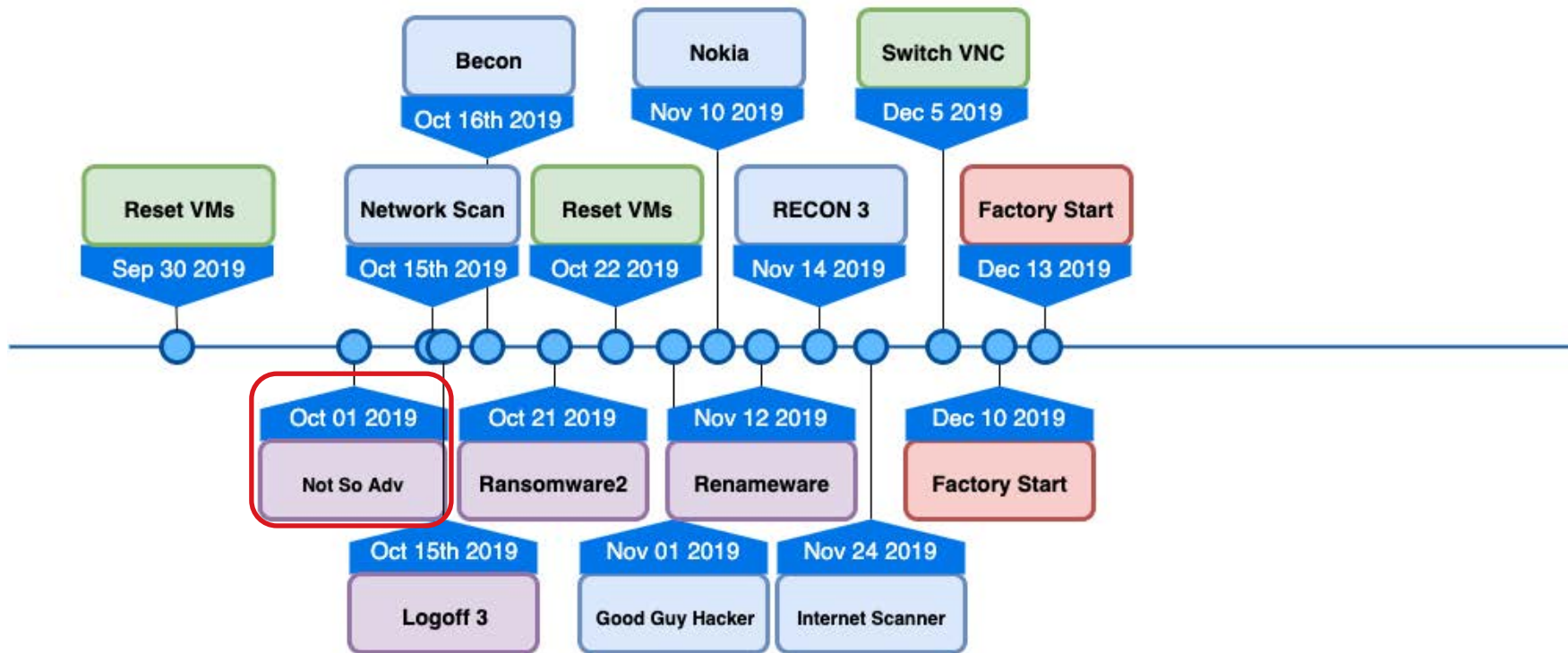
ROBOTIC-PC Workgroup: WORKGROUP Memory: 4.00 GB
 Robot-PC.metech.co Processor: Intel(R) Core(TM) i5-43...

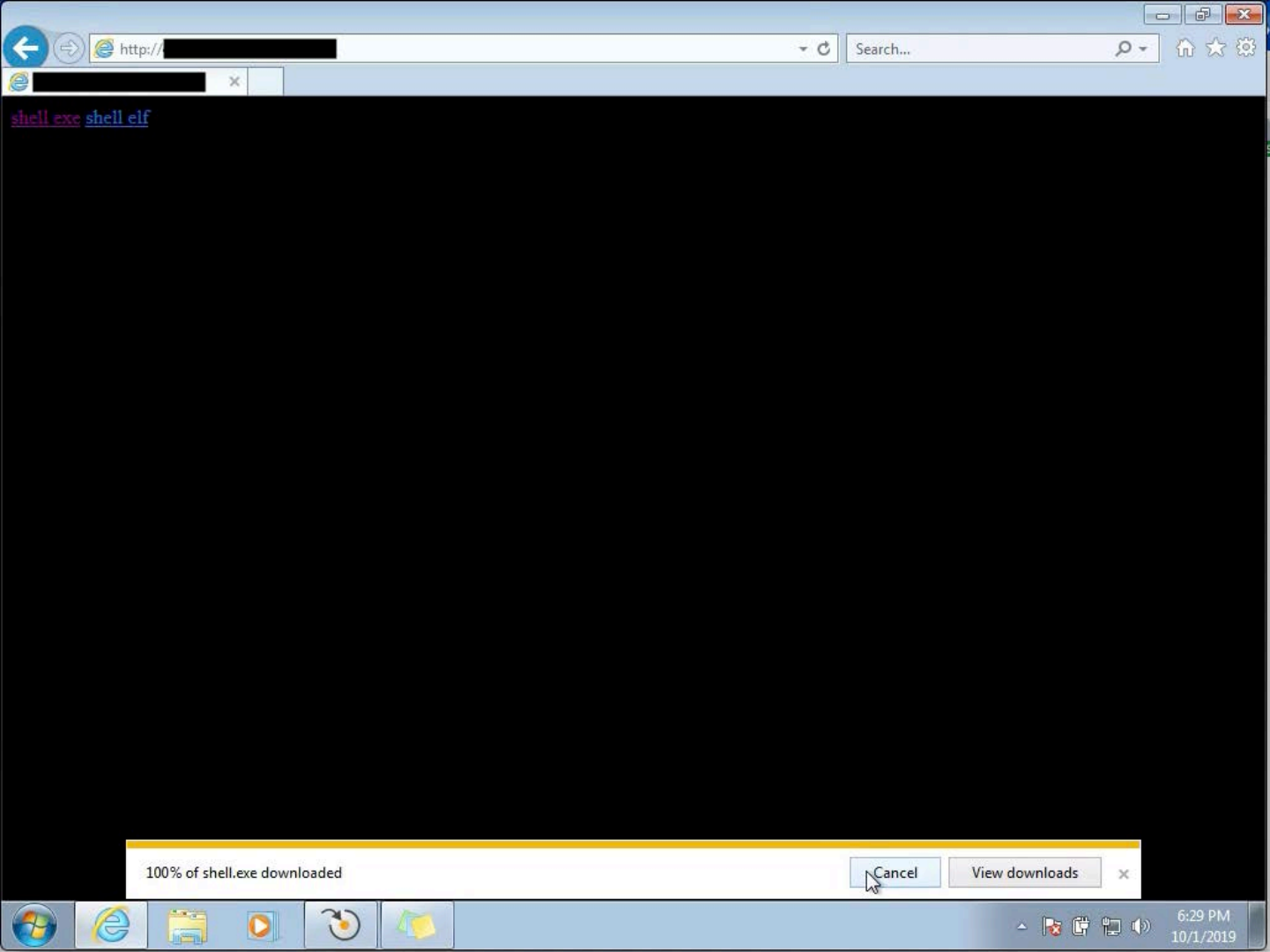


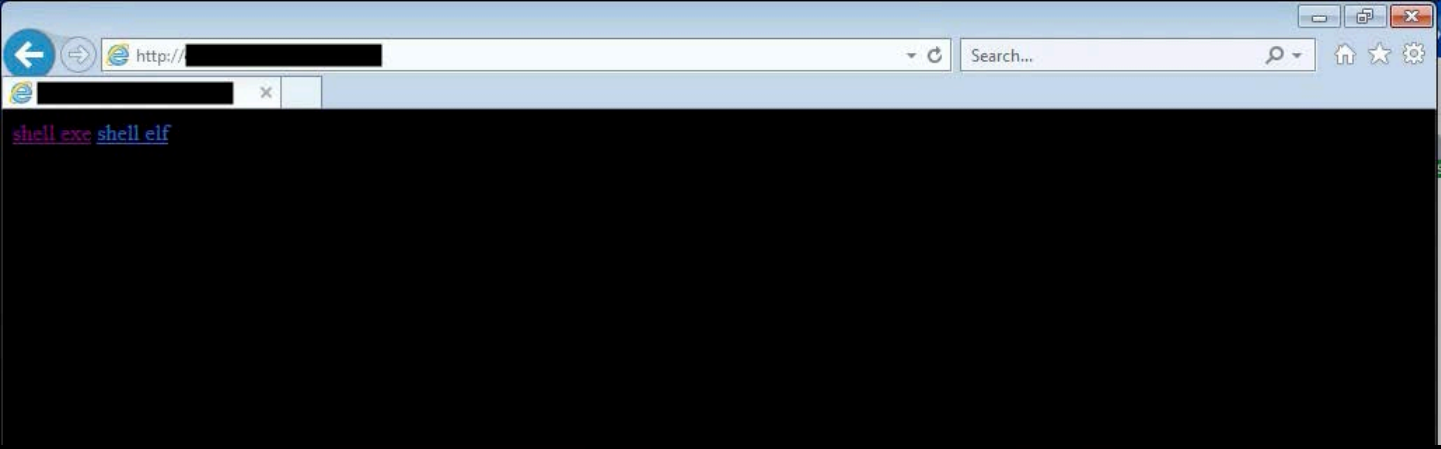
What Happened



What Happened

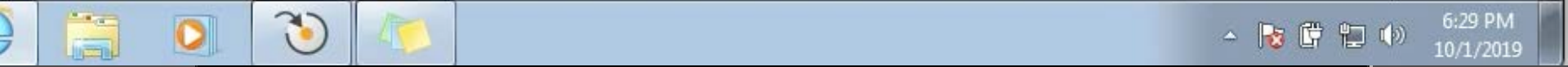






shell.exe is not commonly downloaded and could harm your computer.

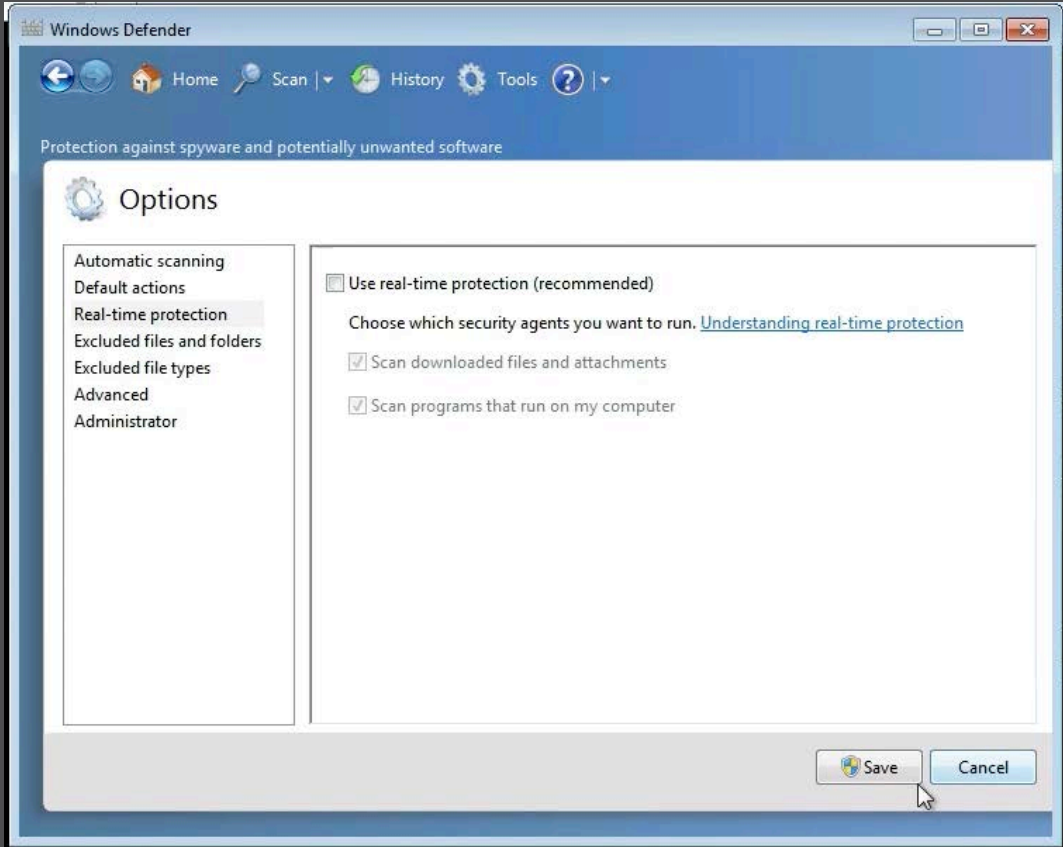
Buttons: Delete, Actions, View downloads, Close (X)

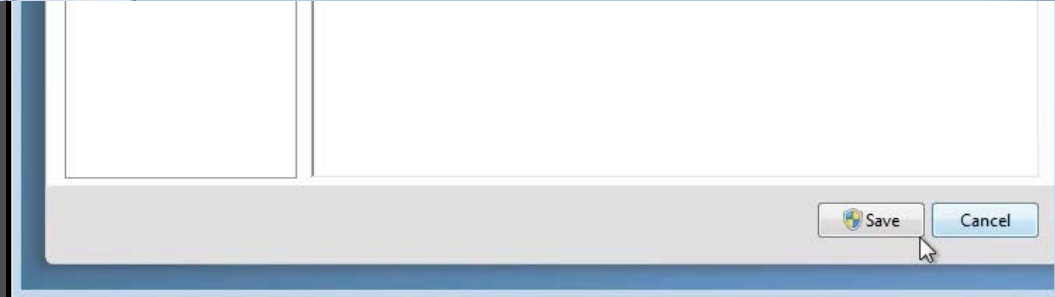
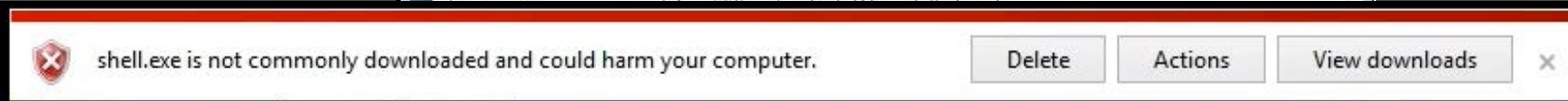


100% of shell.exe downloaded

Buttons: Cancel, View downloads, Close (X)







Solution1 - ABB RobotStudio 6.08 (32-bit)

File Home Modeling Simulation Controller RAPID Add-Ins

ABB Library Import Library Robot System Build Status

Layout Paths&Targets

Solution1
Mechanisms
IRB460_110_240

Windows Defender

Home Scan History Tools

Protection against spyware and potentially unwanted software

Options

- Automatic scanning
- Default actions
- Real-time protection
- Excluded files and folders
- Excluded file types
- Advanced
- Administrator

Windows Defender

This program is turned off

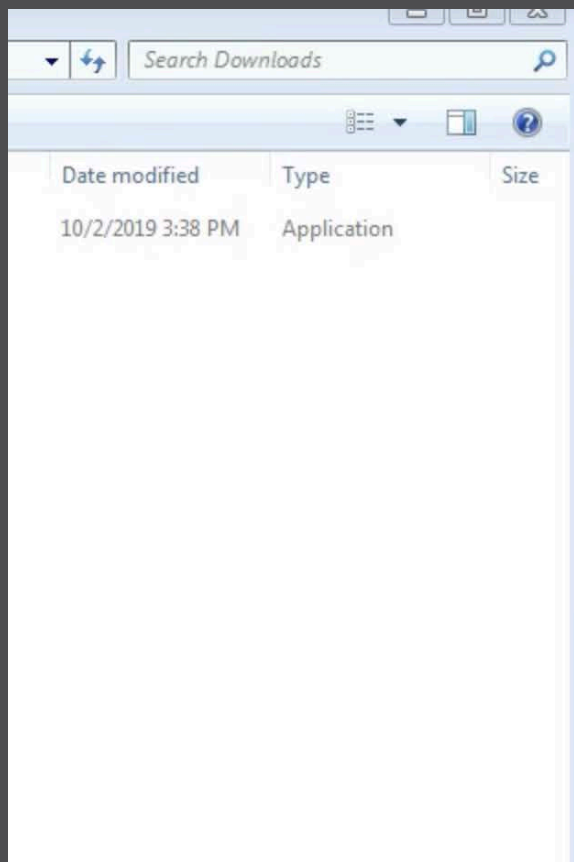
If you are using another program that checks for harmful or unwanted software, use the Action Center to check that program's status.

If you would like to use this program, [click here to turn it on.](#)

Close

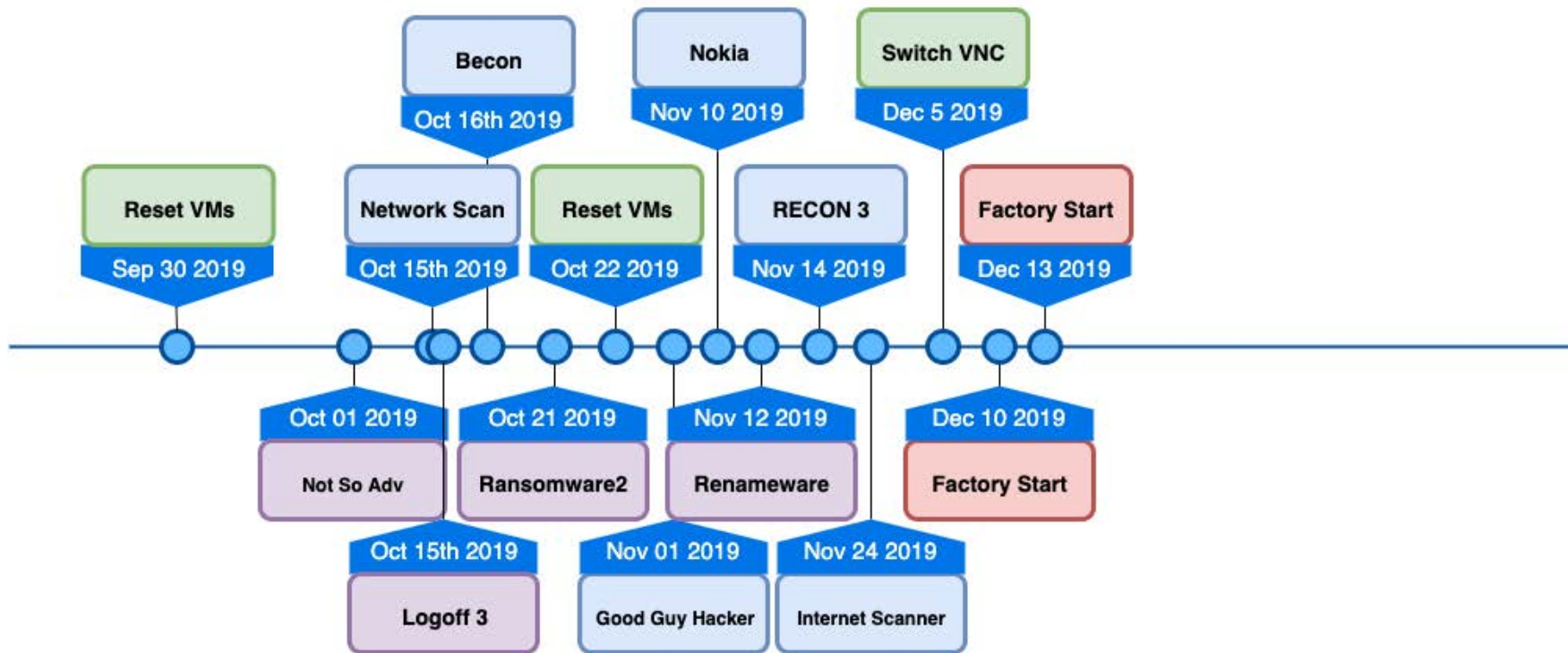
Save Cancel

other potentially
y, Allowed items, and
protect user privacy.

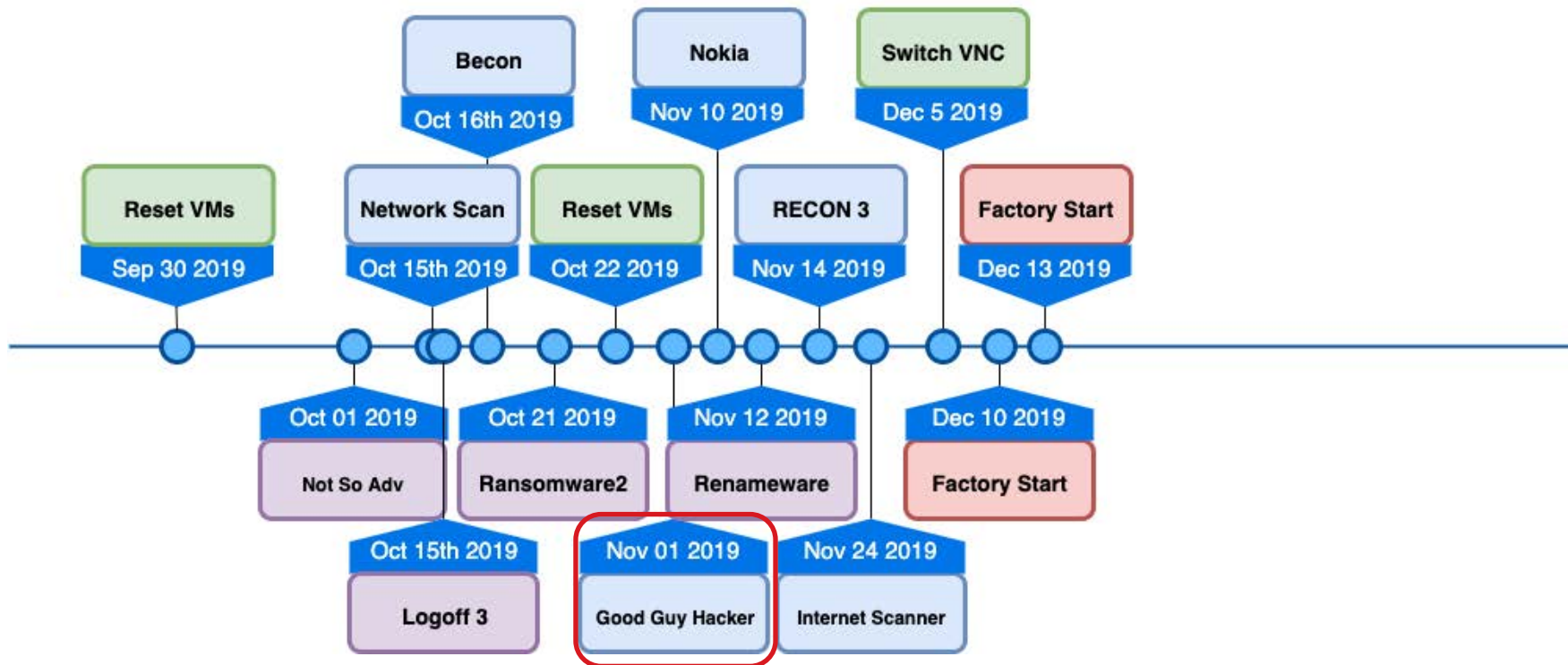


Hi guys. Mike is such an idiot not admin... i dump all yours data from servers and its his fault. I upload malware 10 days ago... Contact with me:
zdravk00@airmail.cc

What Happened



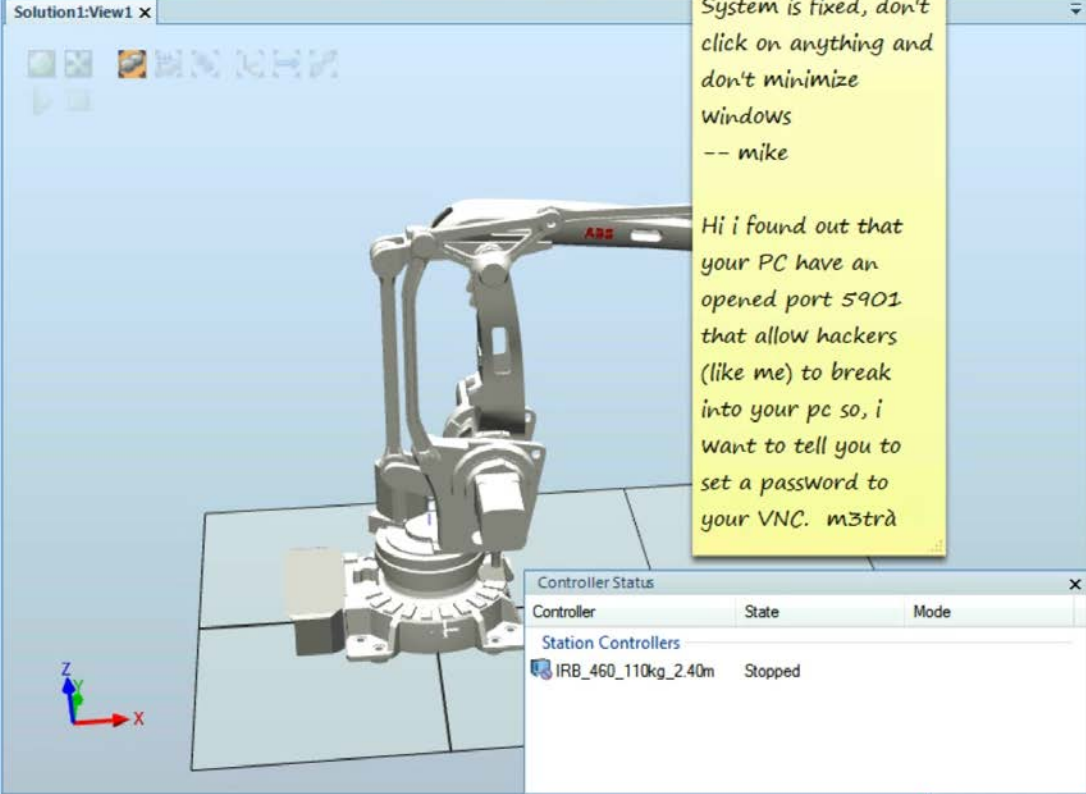
What Happened



Simulation Setup
 Station Logic
 Activate Mechanical Units
 Collisions Configure

Simulation Control
 Play Pause Stop Reset
 I/O Simulator
 TCP Trace
 Stopwatch
 Signal Analyzer
 Enabled
 Signal Setup
 History
 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



System is fixed, don't click on anything and don't minimize windows -- mike

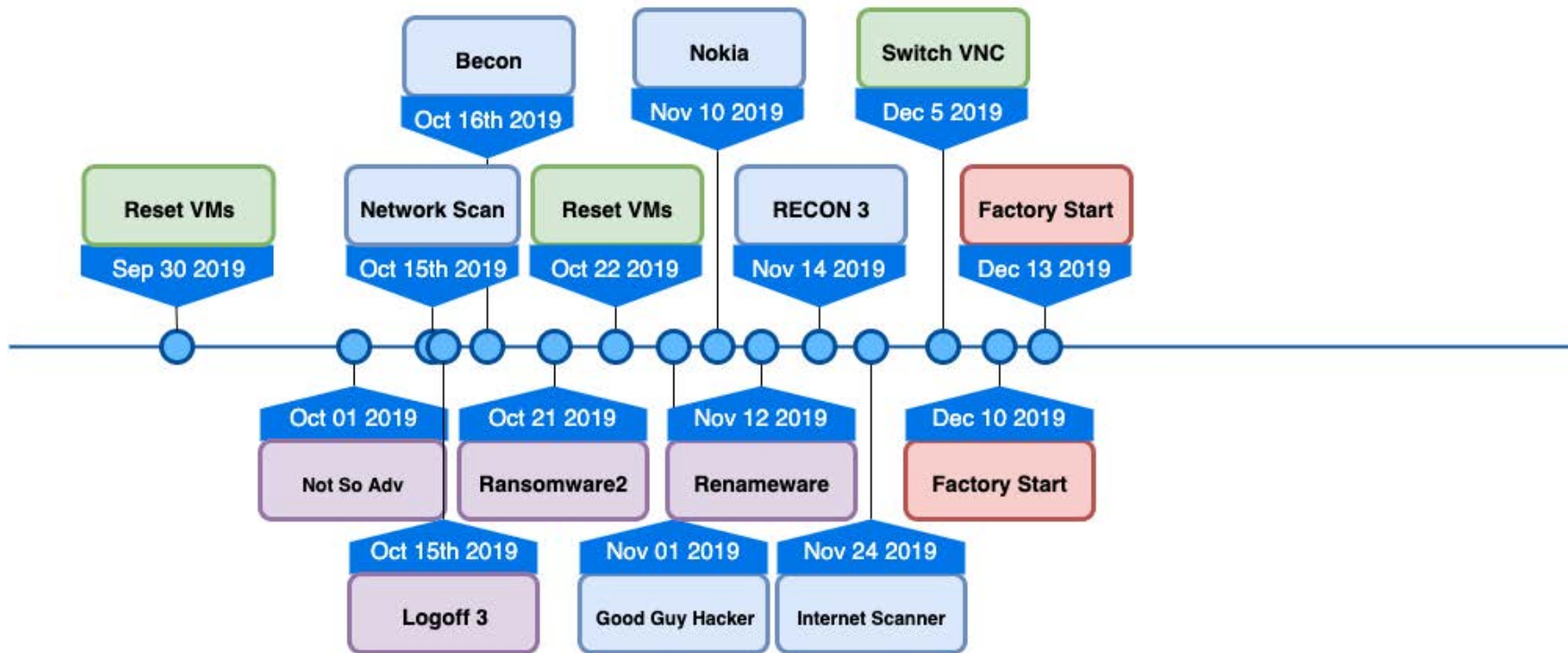
Hi i found out that your PC have an opened port 5901 that allow hackers (like me) to break into your pc so, i want to tell you to set a password to your VNC. m3trà

Controller Status

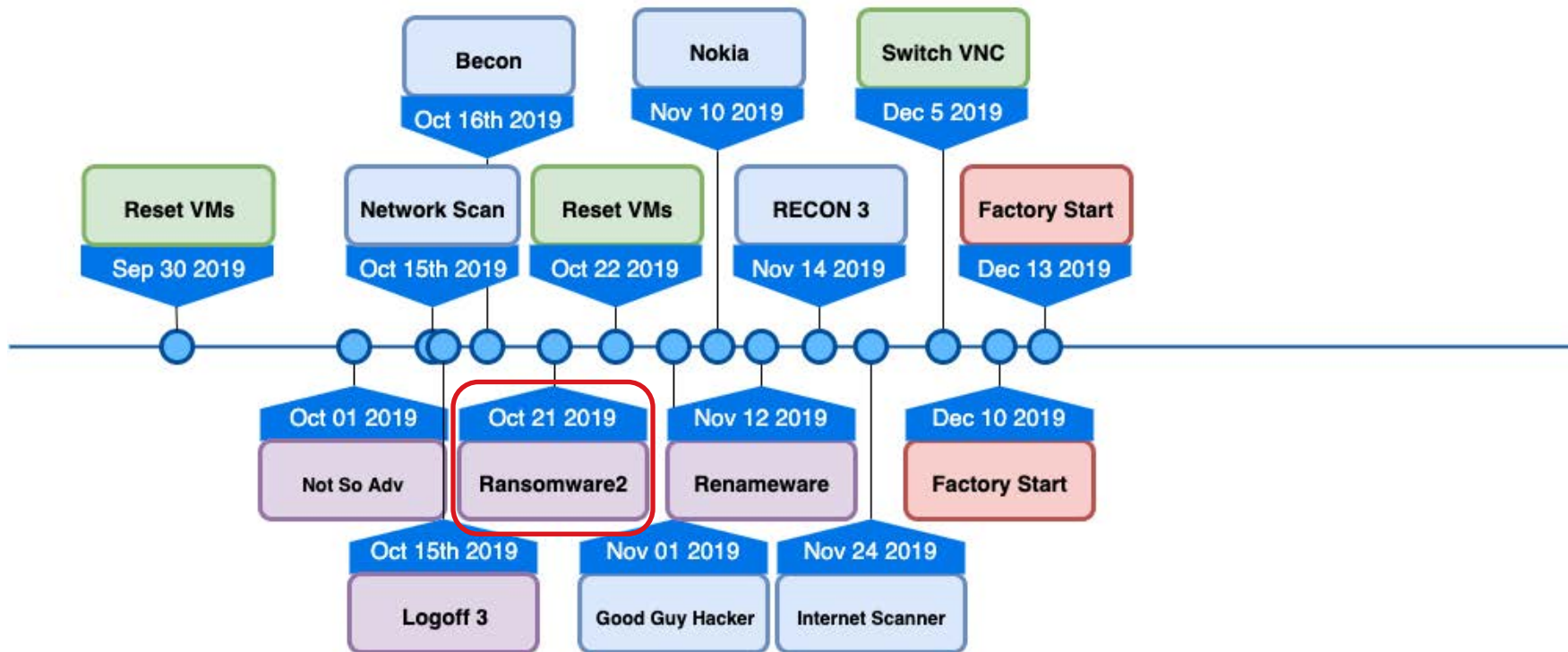
Controller	State	Mode
Station Controllers		
IRB_460_110kg_240m	Stopped	

Controller status: 0/1

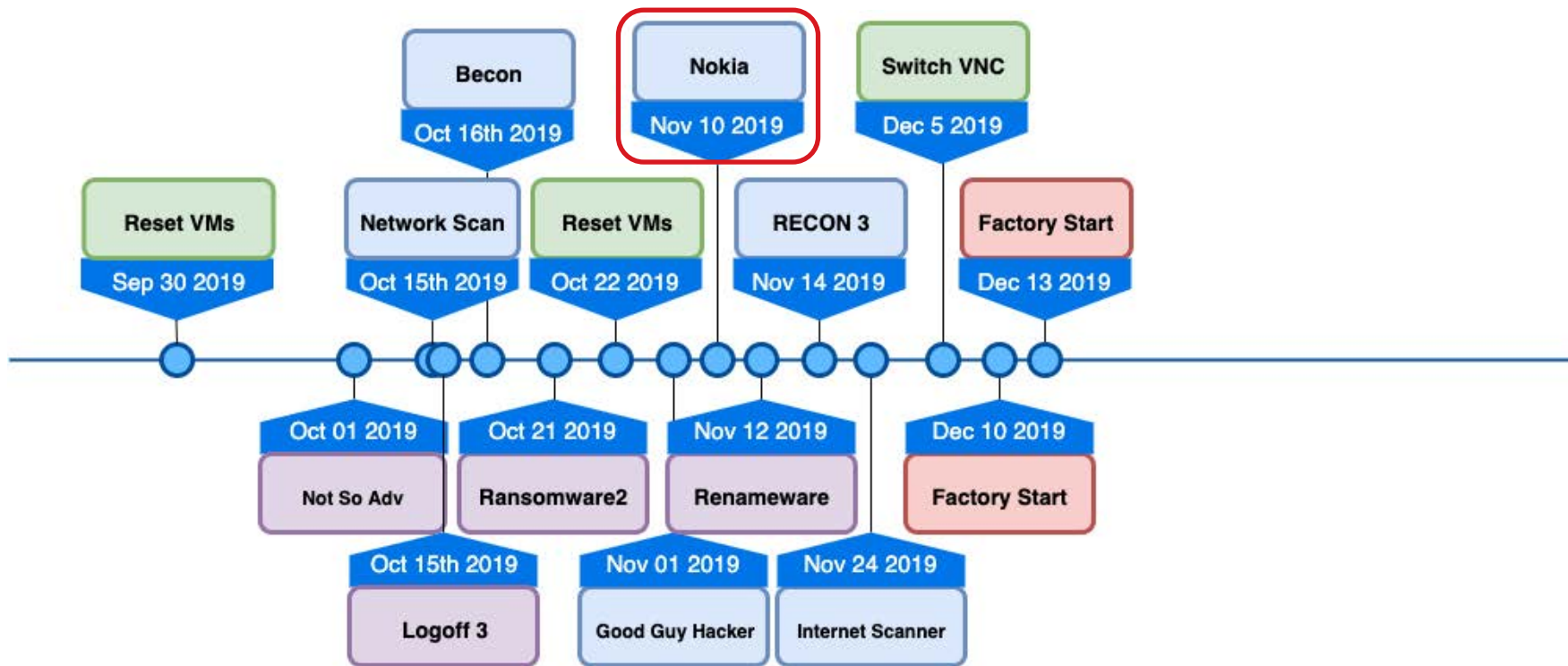
What Happened



What Happened



What Happened





Acrobat
Reader DC

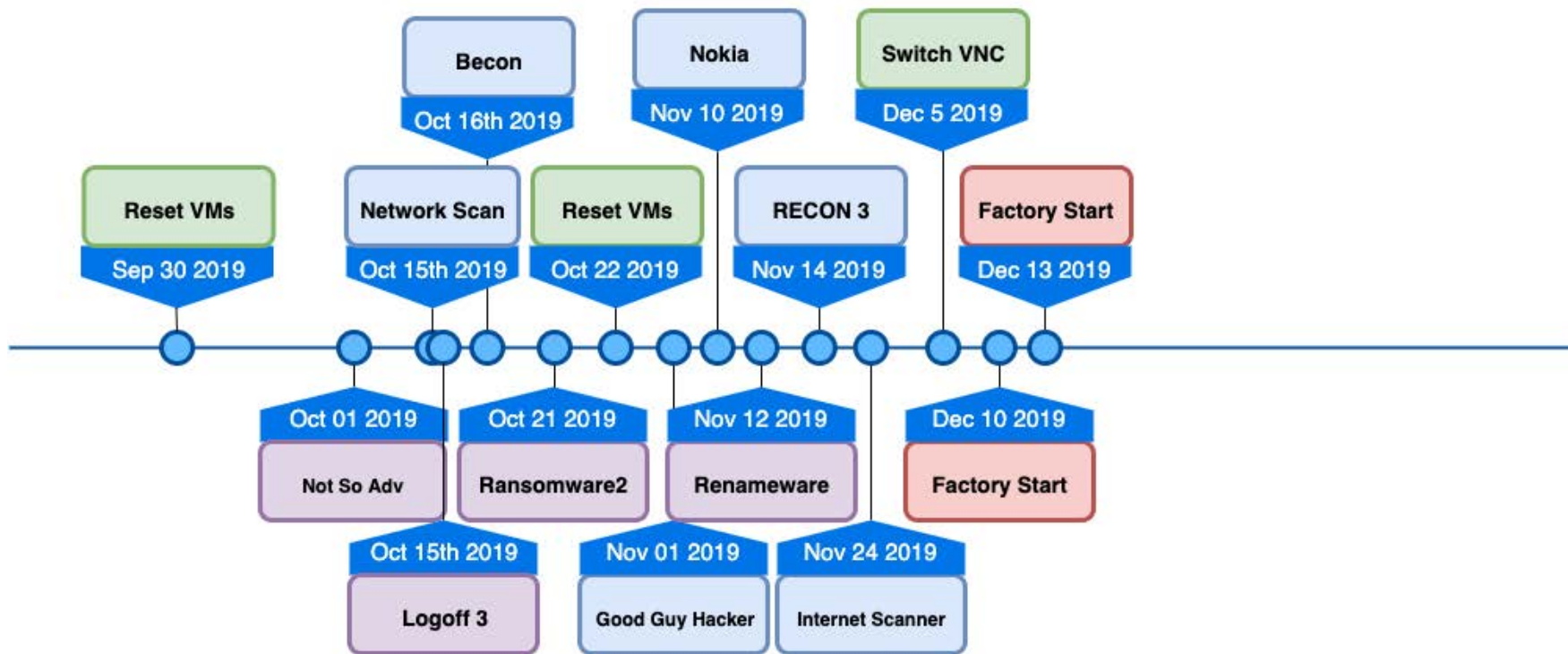


RobotStudio
6.08 (32-bit)

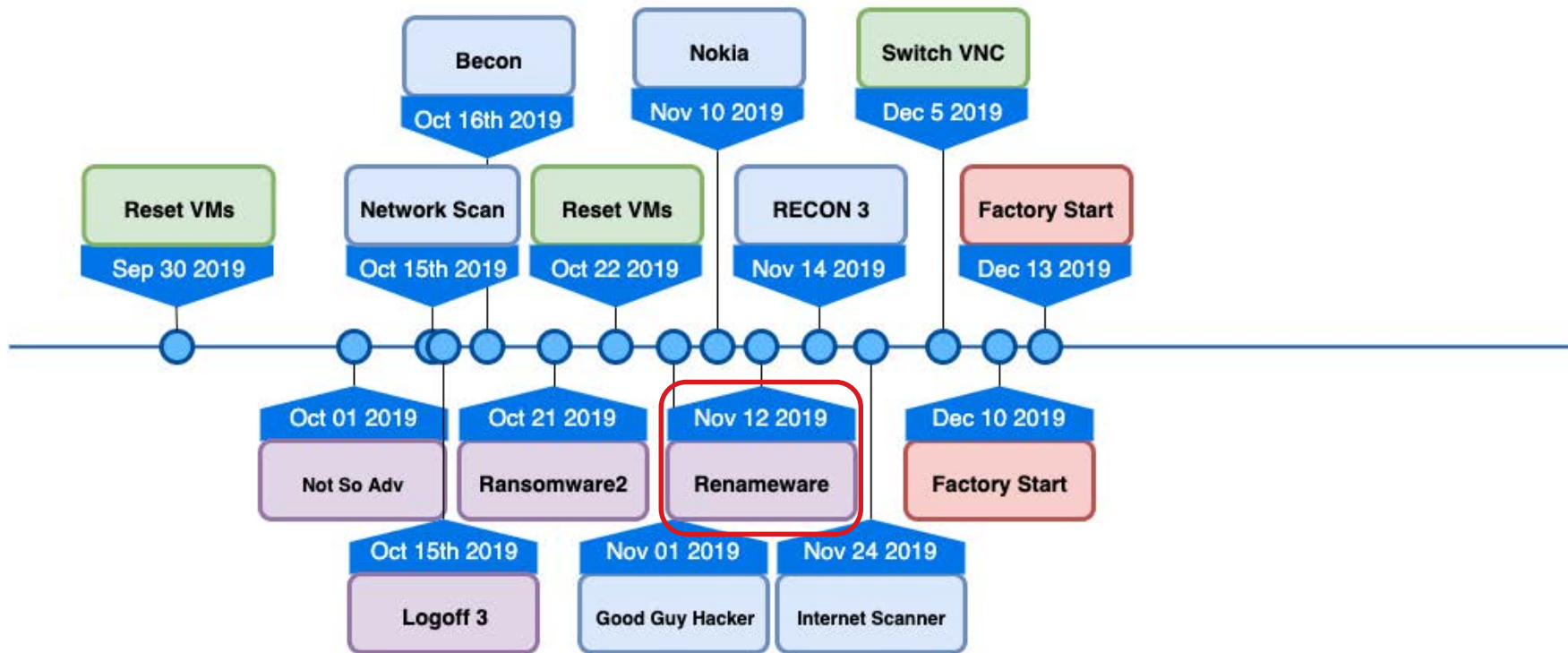


RobotStudio
6.08

What Happened



What Happened



```
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 /O "%userprofile%\Desktop\OPEN_ME"') DO REM "%i" *.rnsmvr
```

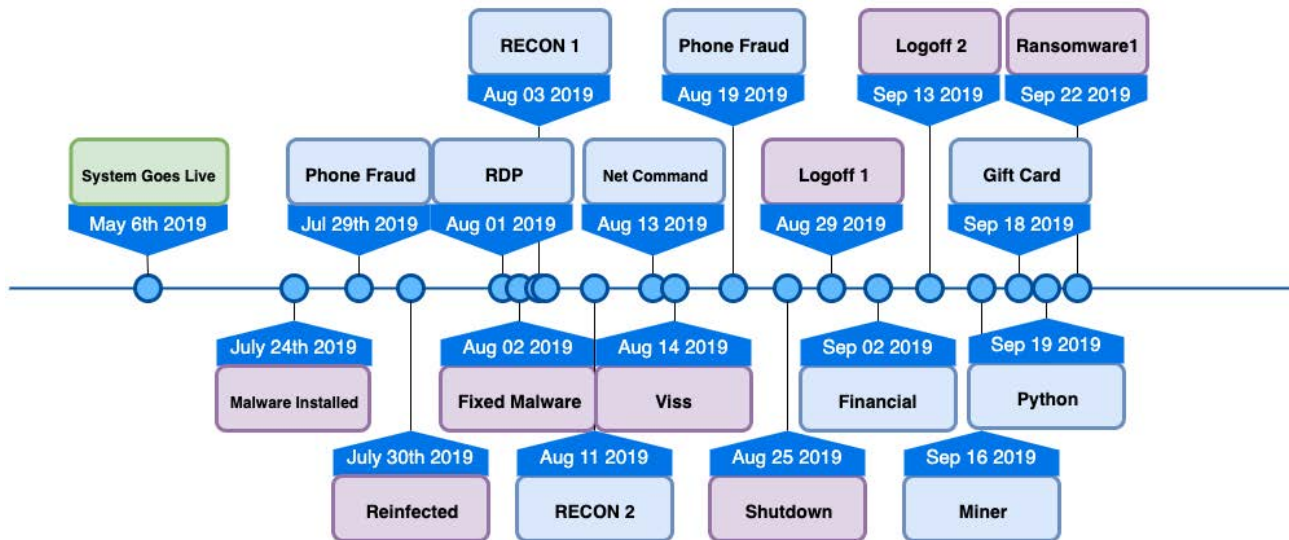
Search ABB Industrial IT

Modified	Type	Size
11/19 11:01 PM	File folder	

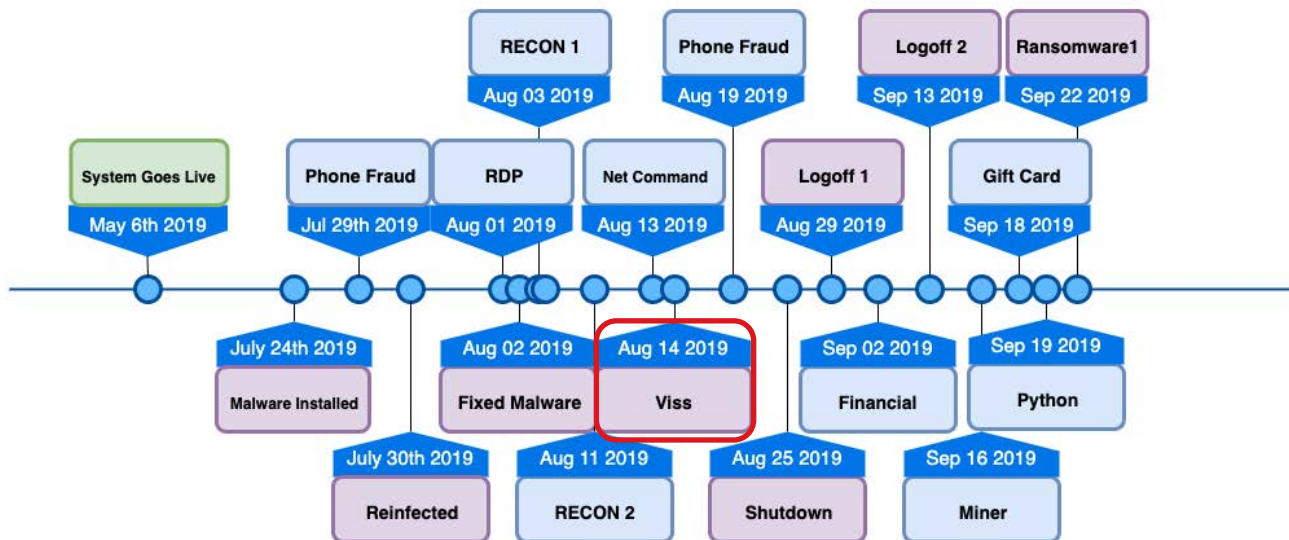
1DnFABek

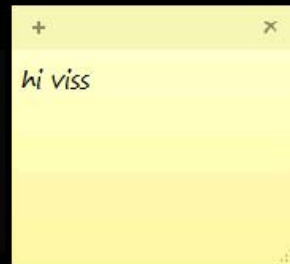
- Documents
- Music
- Pictures
- Videos
- Computer
 - Local Disk (C:)
 - MeTech (\\FILES)
- Network
 - FNG-STATION
 - 1 item

What Happened



What Happened





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:



Dan Tentler 

@Viss

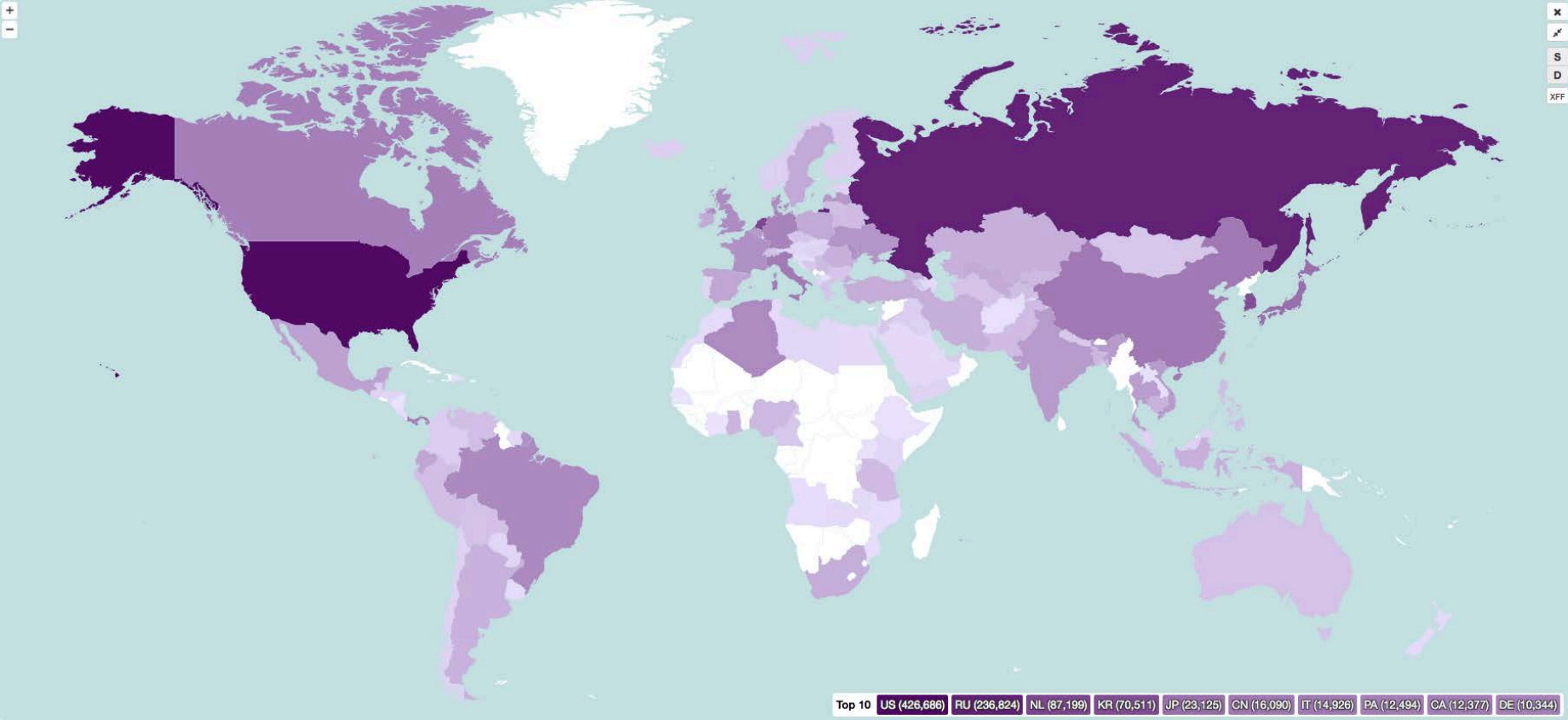
Follow



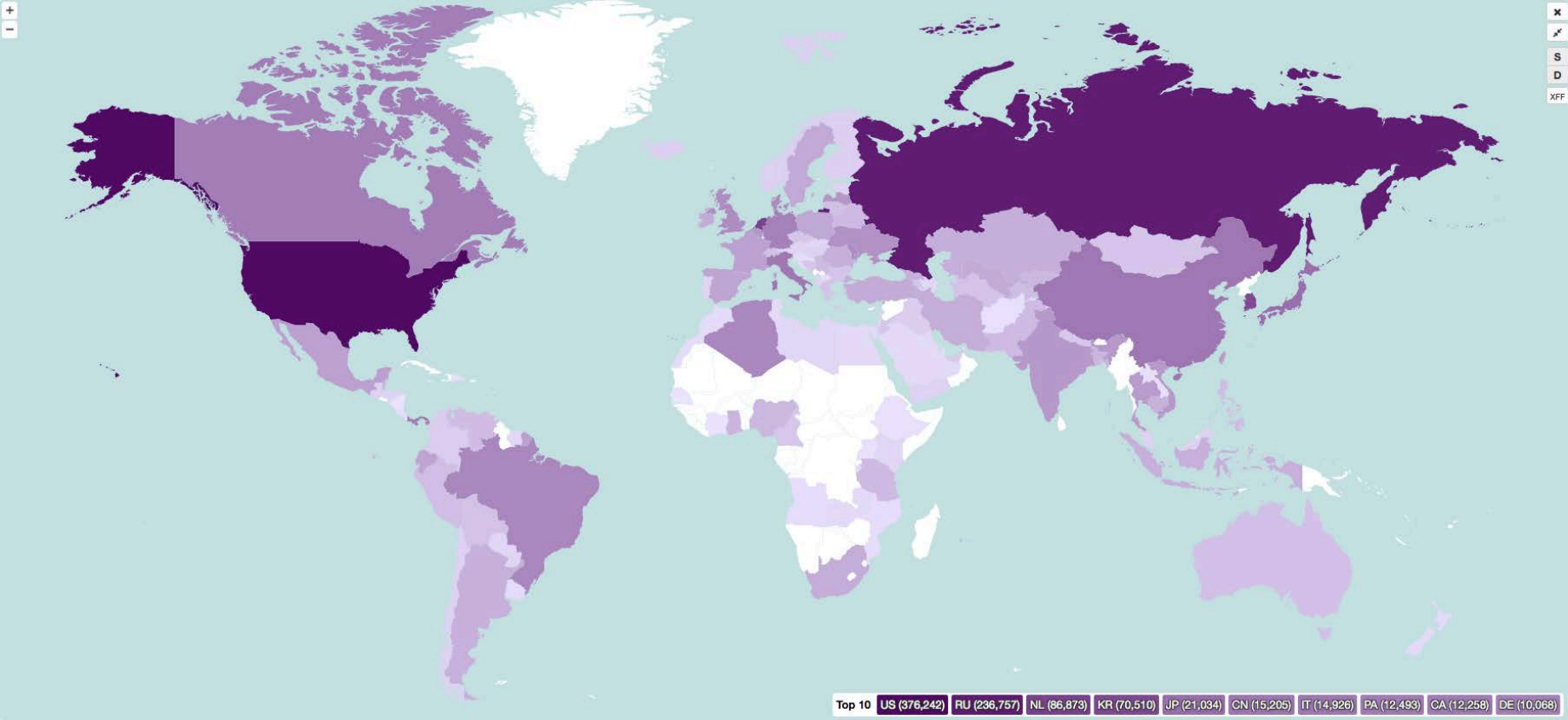
have you ever learned a thing, where the immediate outcome of that thing has been "i need rum. like right now"?

11:36 AM - 16 Aug 2019

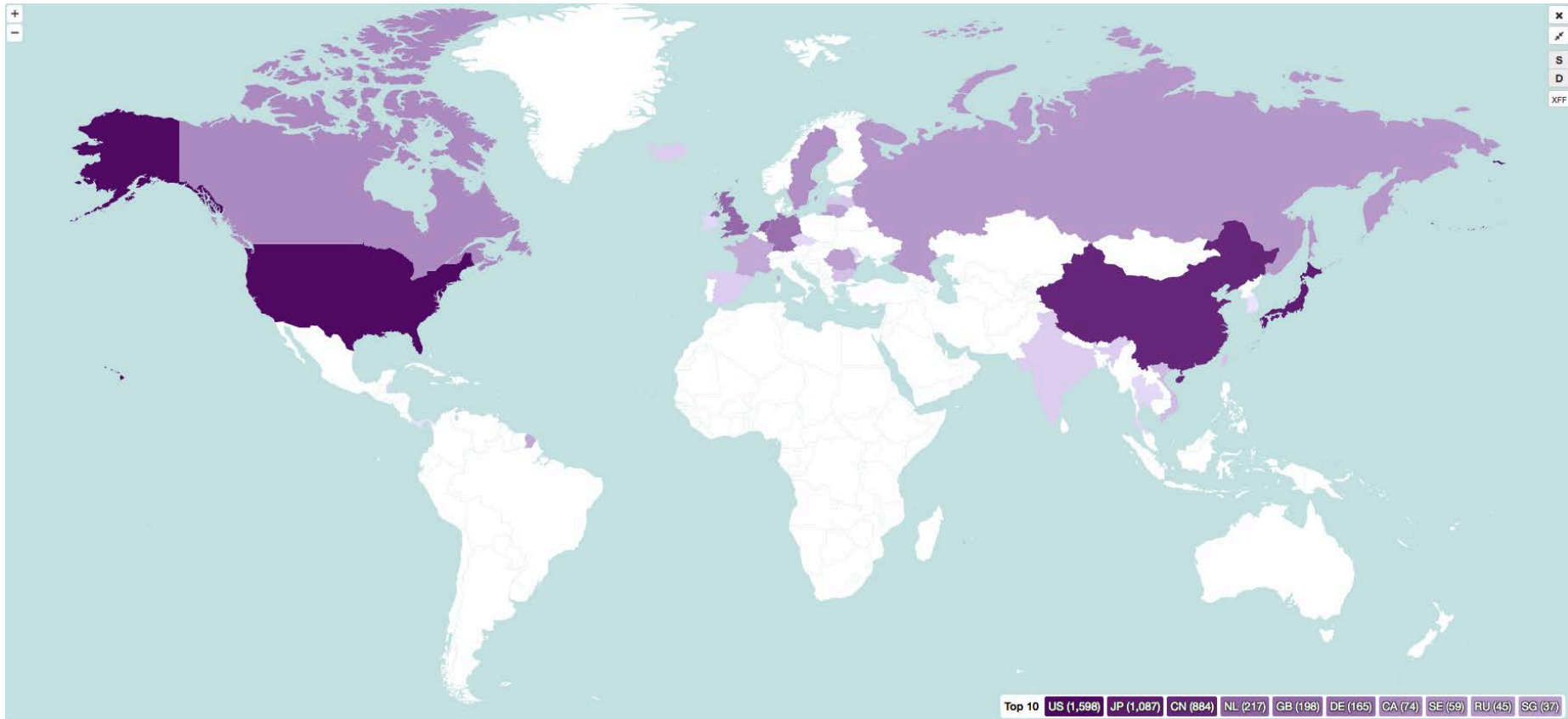
But WHO!?



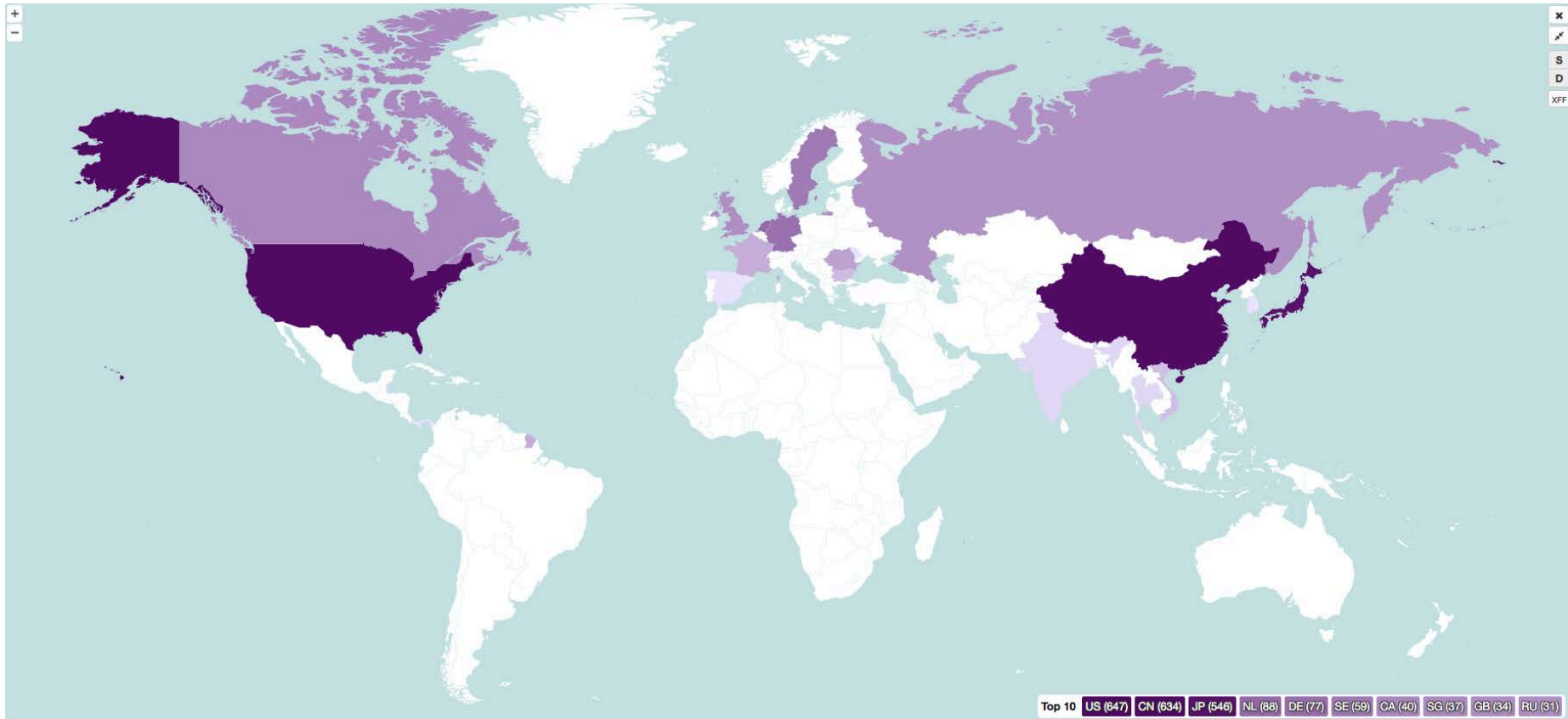
But WHO!?



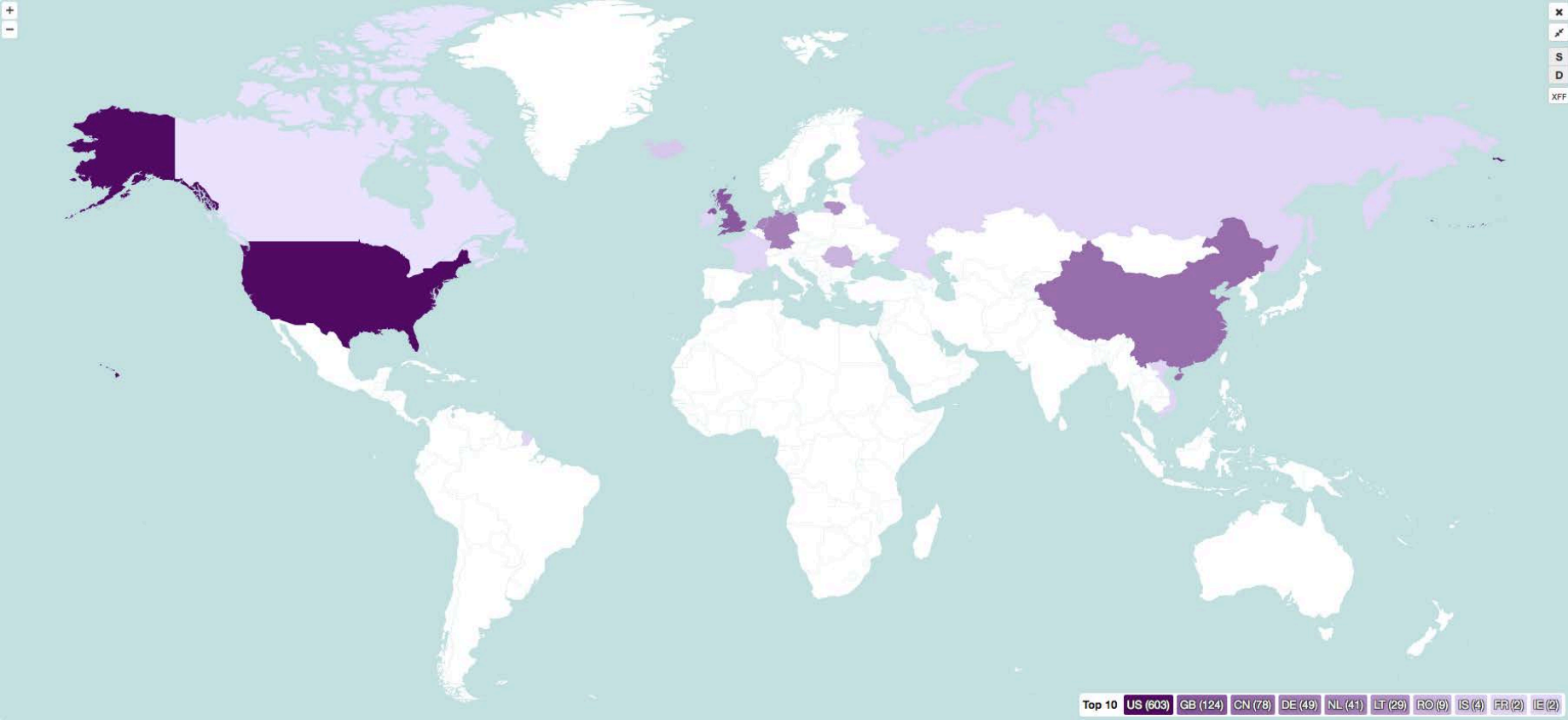
But WHO!?



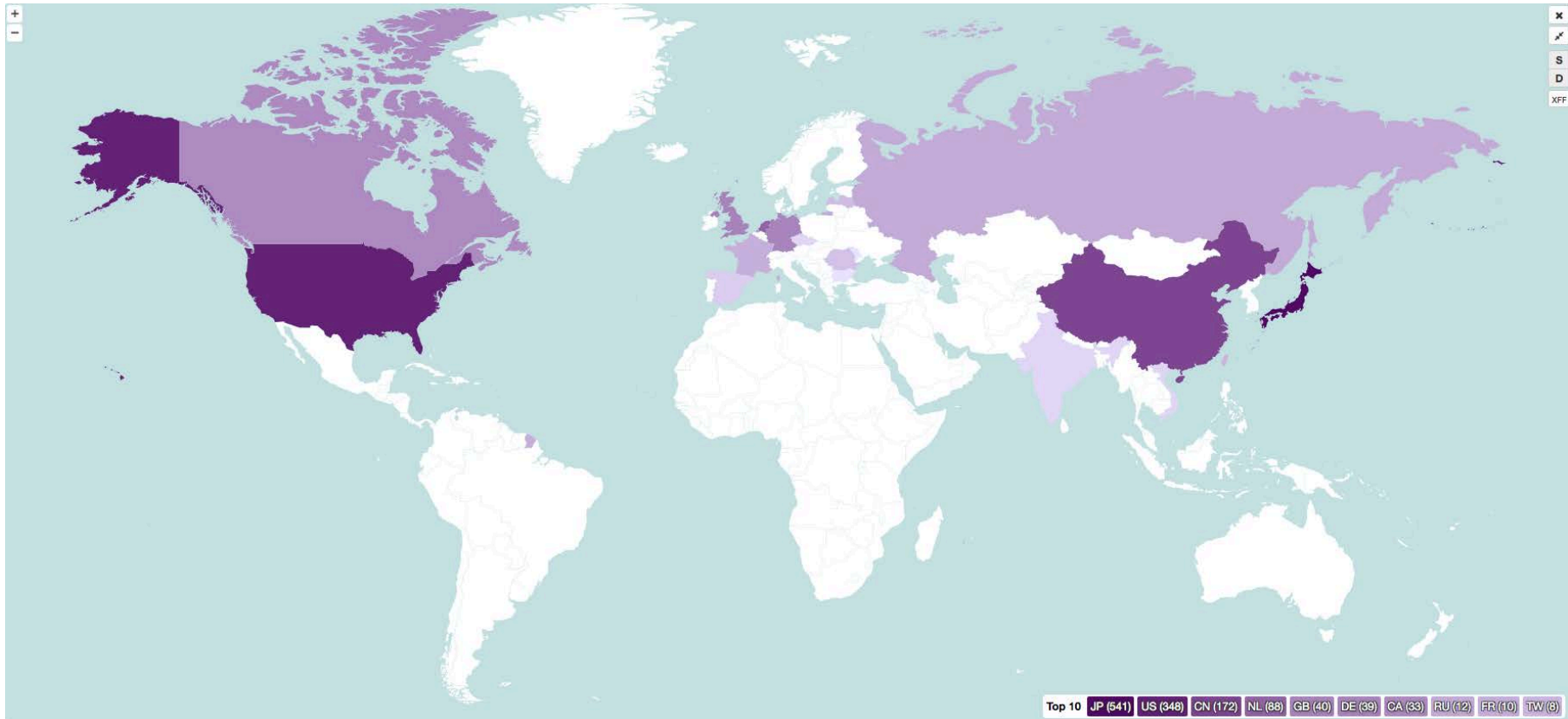
But WHO!?



But WHO!?

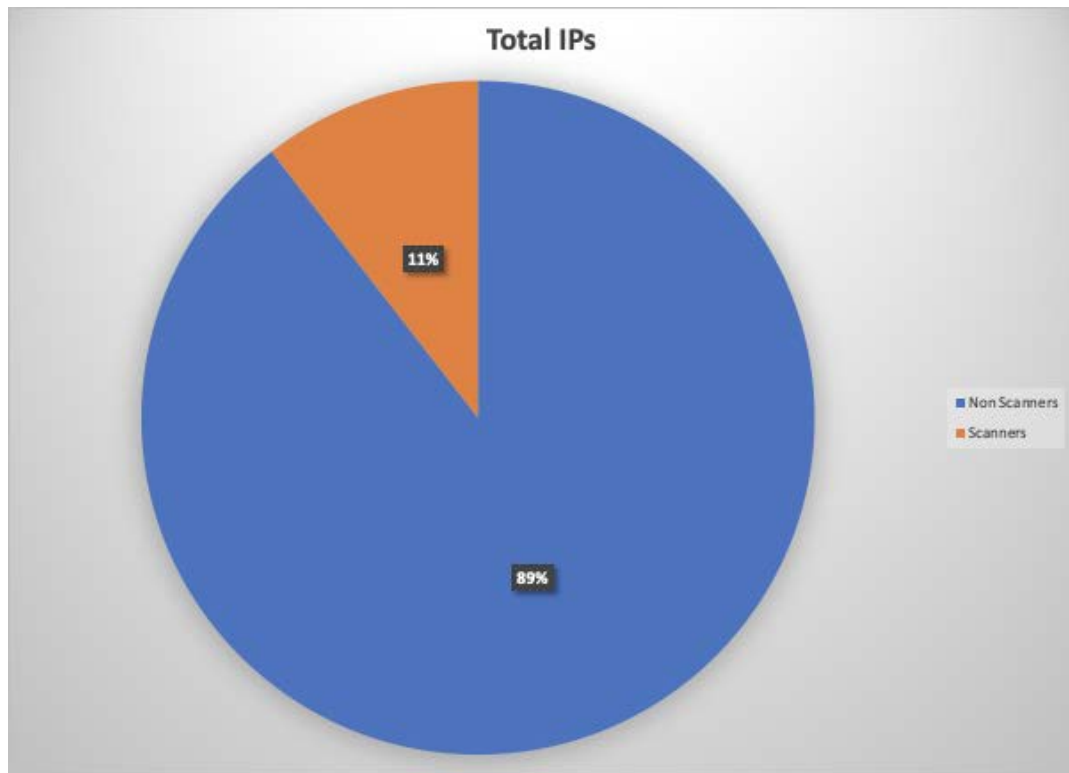


But WHO!?



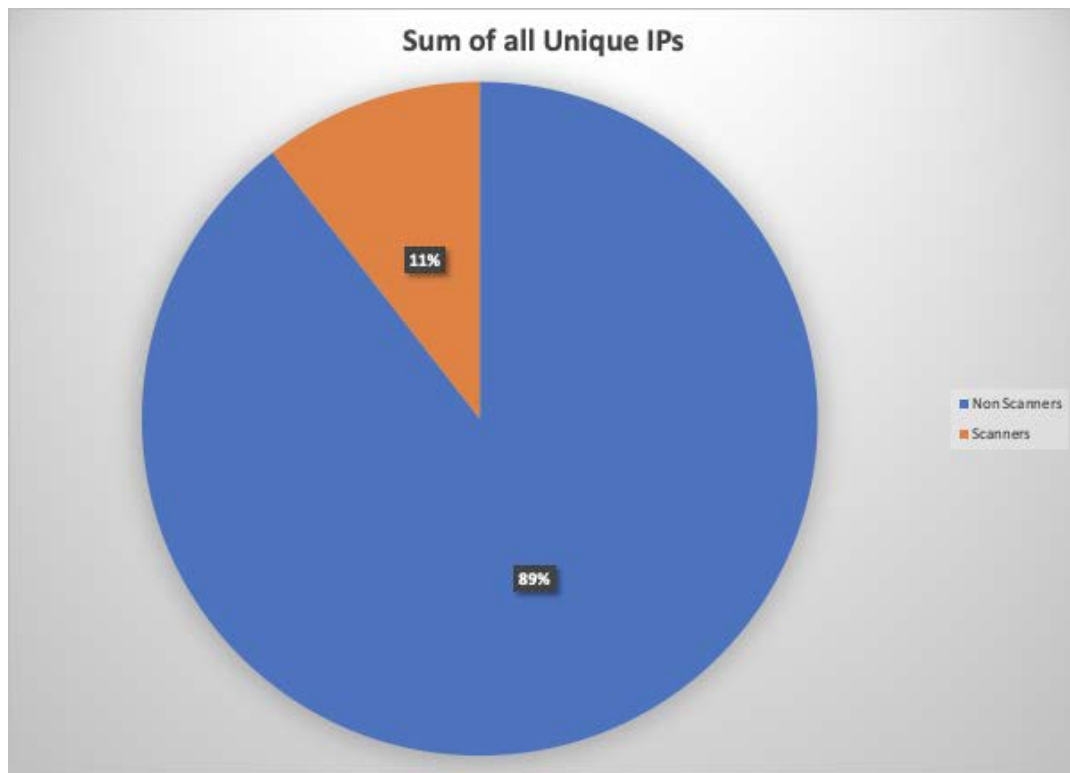
Stats: Total IPs Over Project

- 8905 Total IPs
- 592 Scanner IPs



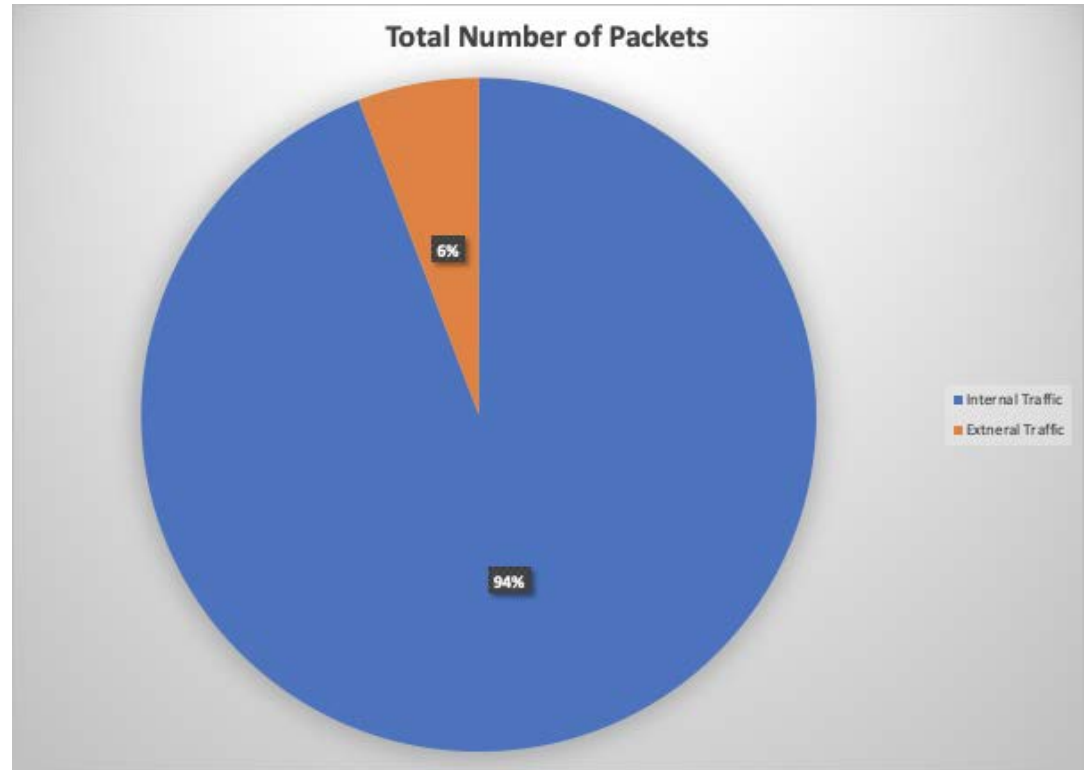
Stats: Sum of all unique IPs per day

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



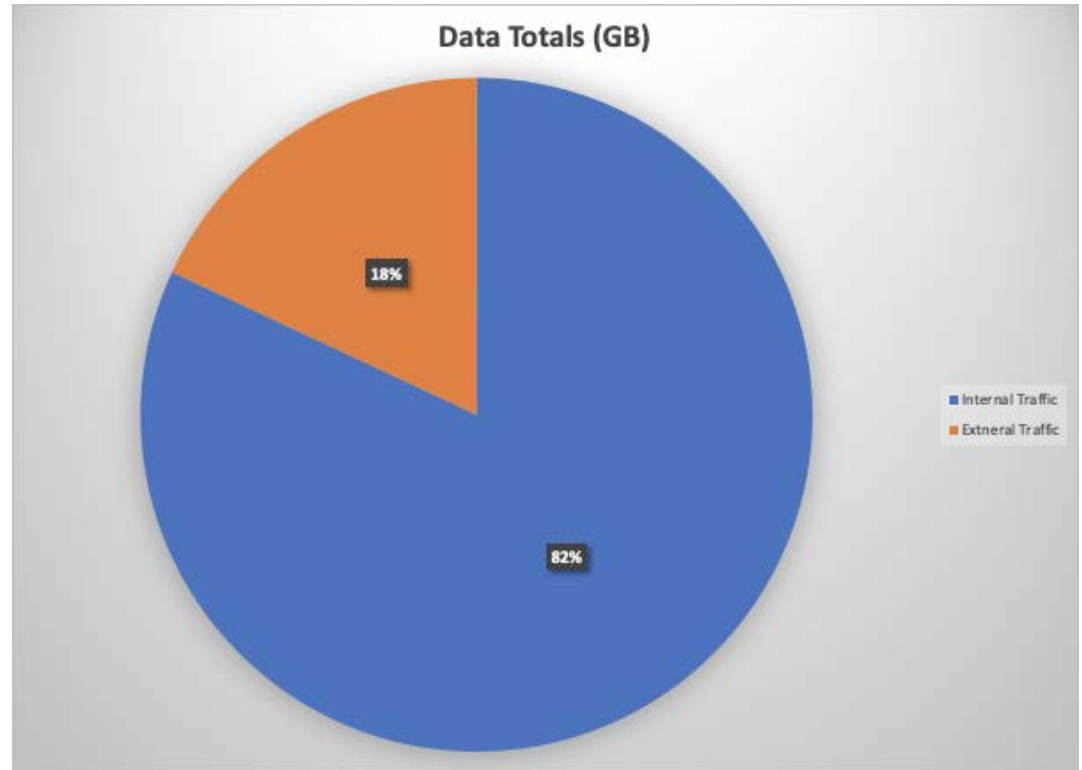
Stats: Total Packets/Bytes

- 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



Honeypot Tips

- Remove VM identifiers
- Virtual Box screen recording
- File and network forensics
- Make it interesting

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

Conclusion

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

Attackers will be mean to Mike and hurt your feelings.



Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats

Stephen Hill, Federico Maggi, Charles Perine, Lord Remoris, Martin Röger, and Rainer Vosseler



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