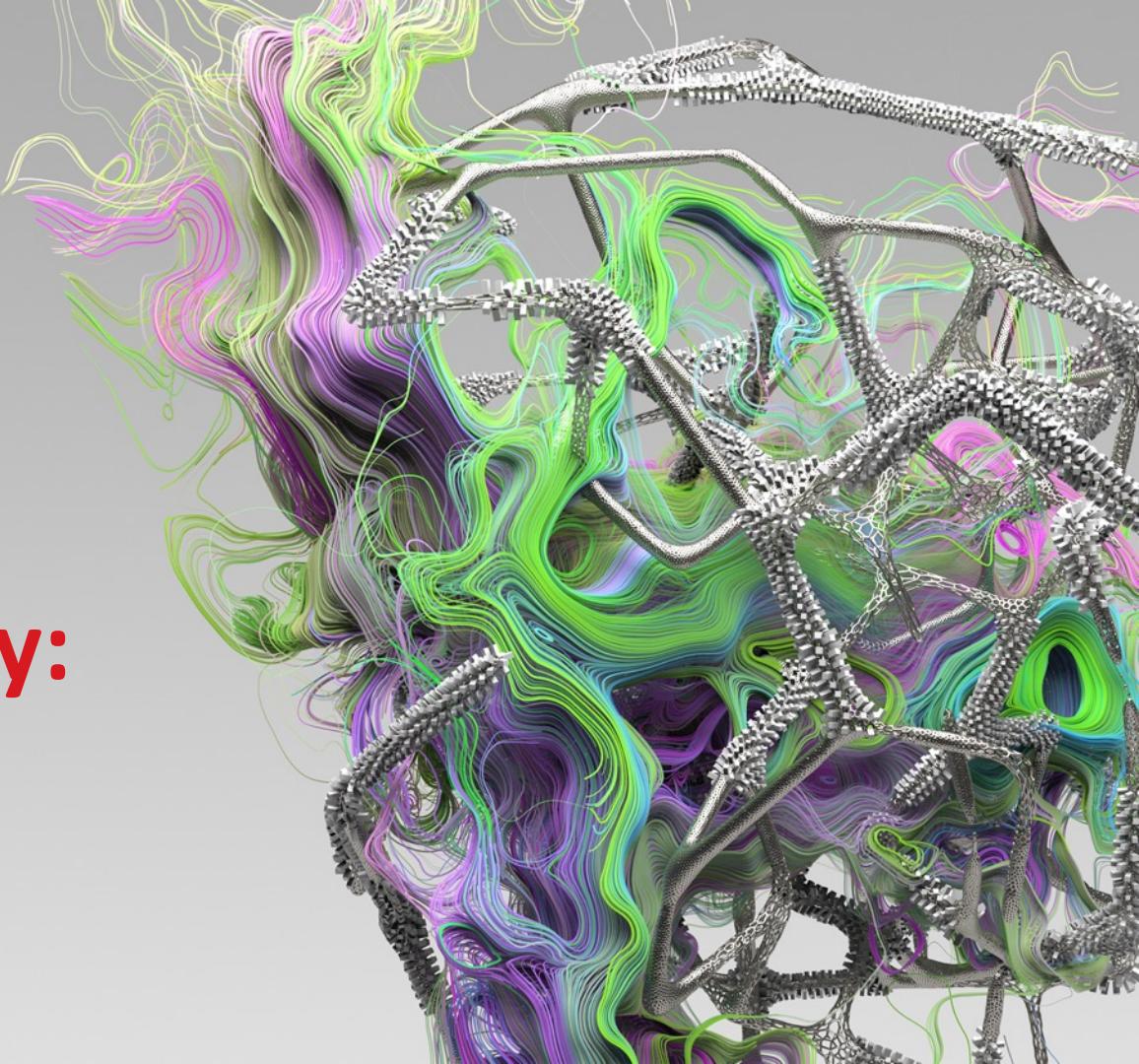




Faking a Factory: Creating and Operating a Realistic HoneyPot

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 Is On Fire After



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

BY MICHAEL GAUTHIER | NOVEMBER 21, 2018 3

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 I Bans Huawei From 5 Networks



Nissan Patrol Fleets One Tires In On Five A

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 GAUTHIER | NOVEMBER 21, 2016 3

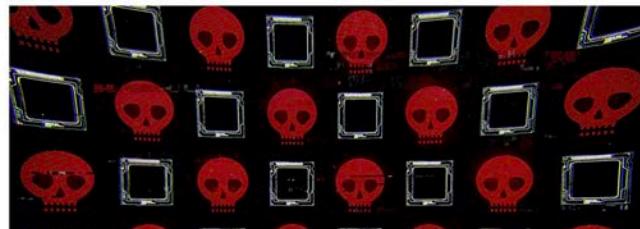
US & WORLD TECH CYBERSECURITY

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

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.



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



Hackers Are T Demanding M

By MICHAEL GAUTHIER | N

US & WORLD

TECH

Boein Wann

The widespread
Korea has h

By Nick Statt | @nick

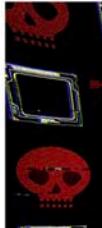
f

t

g



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.

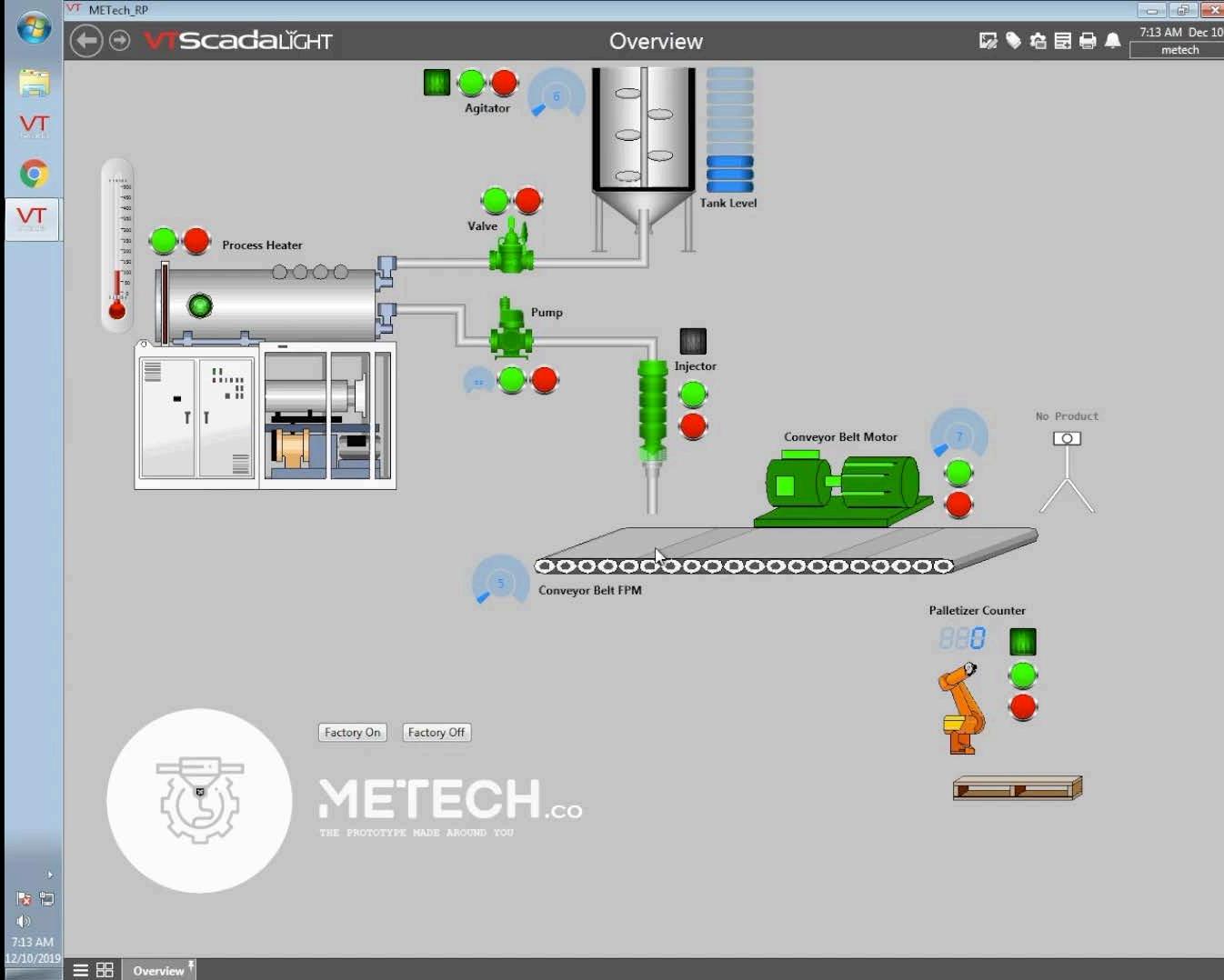


Buncombe property transfers for Nov. 1-4, 2019

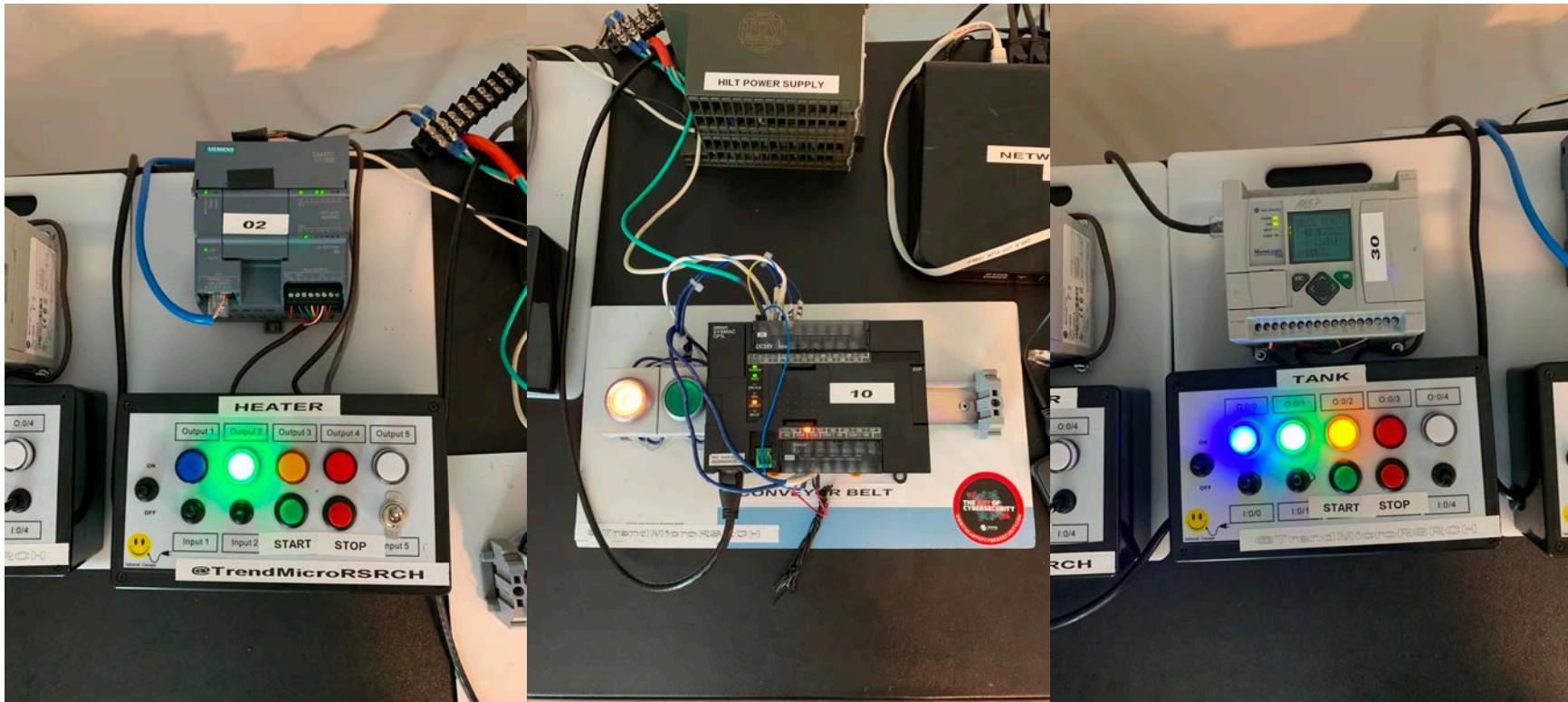


r WannaCry virus

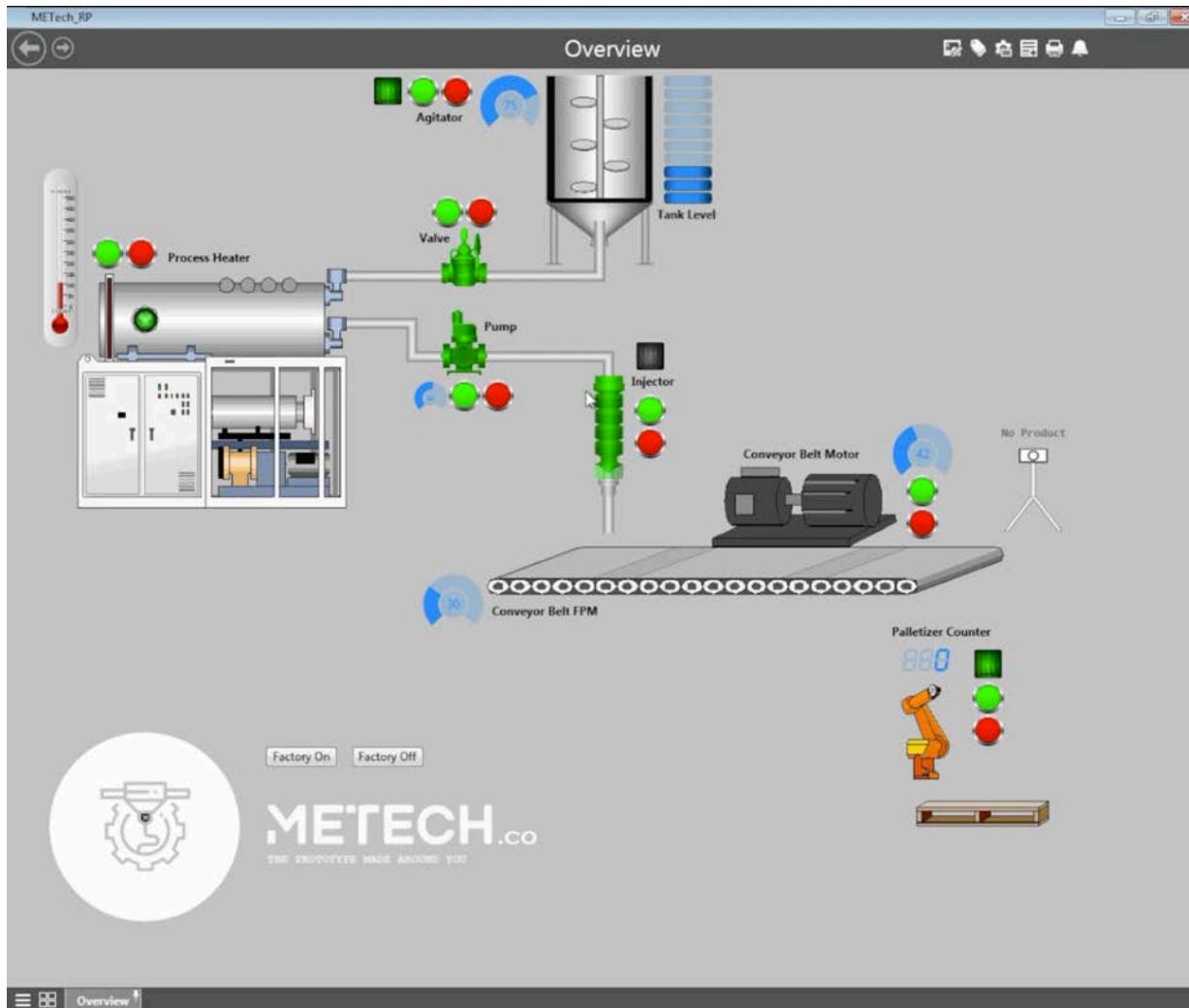
da
ter
ikes



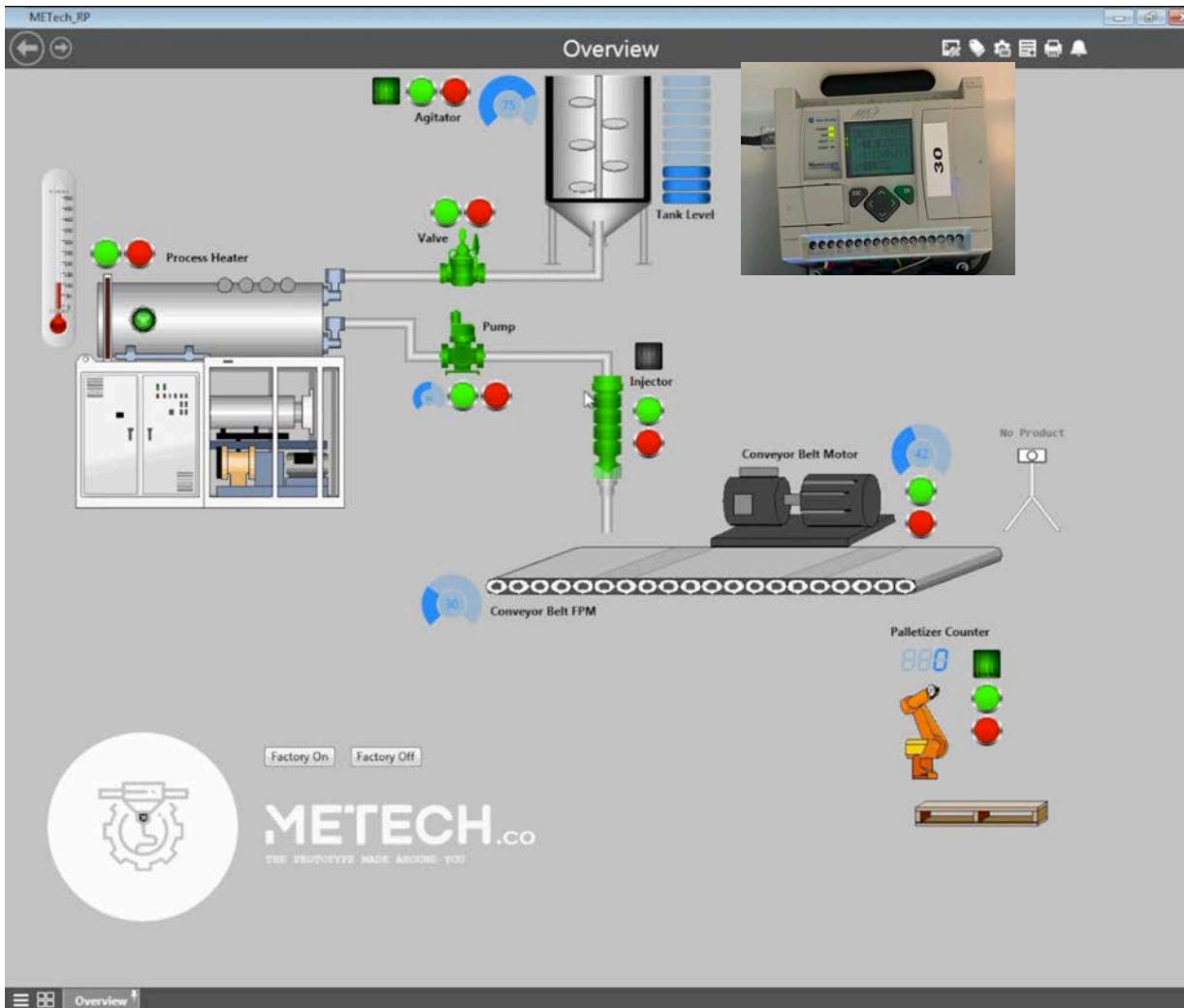
Equipment



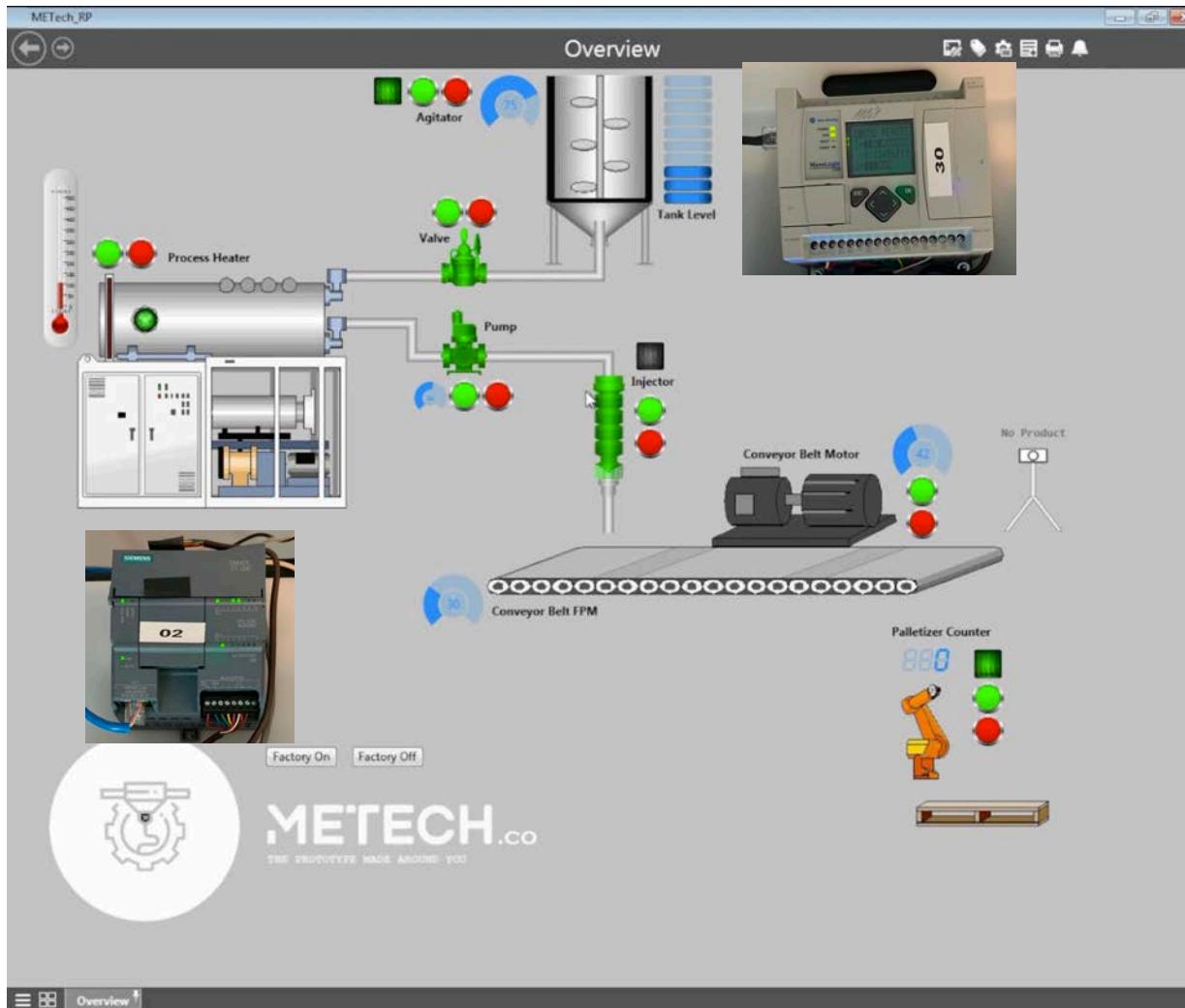
HMI



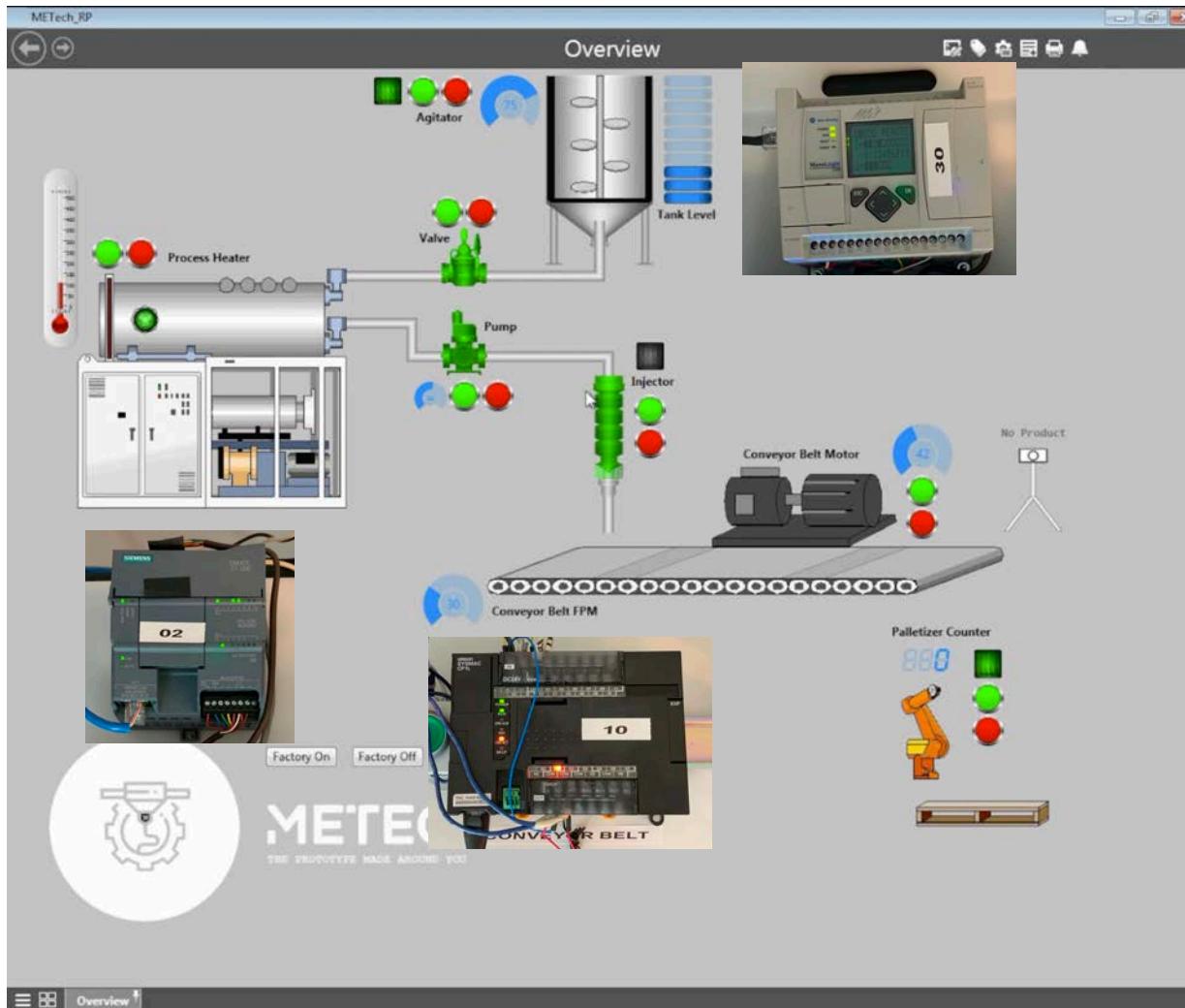
HMI



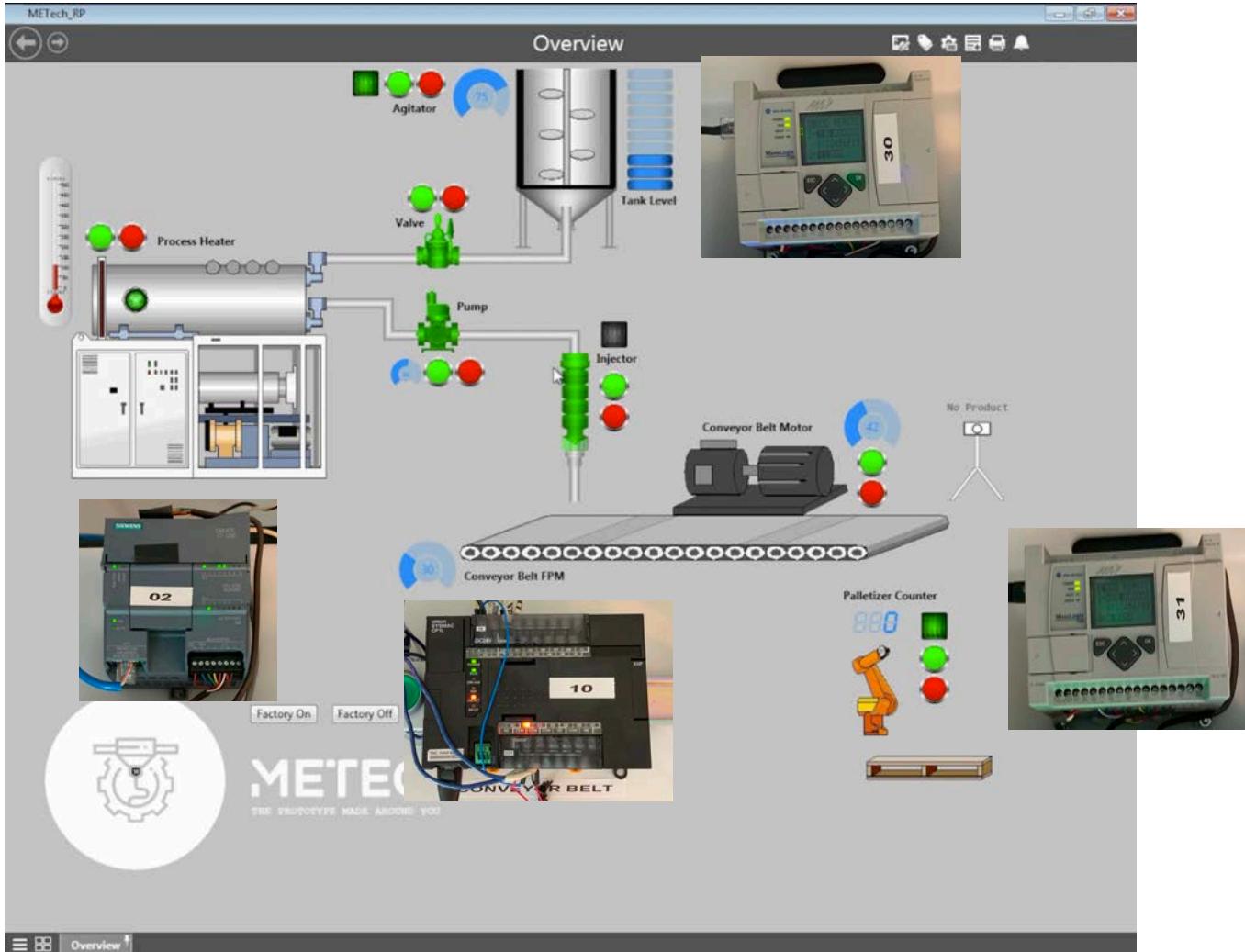
HMI



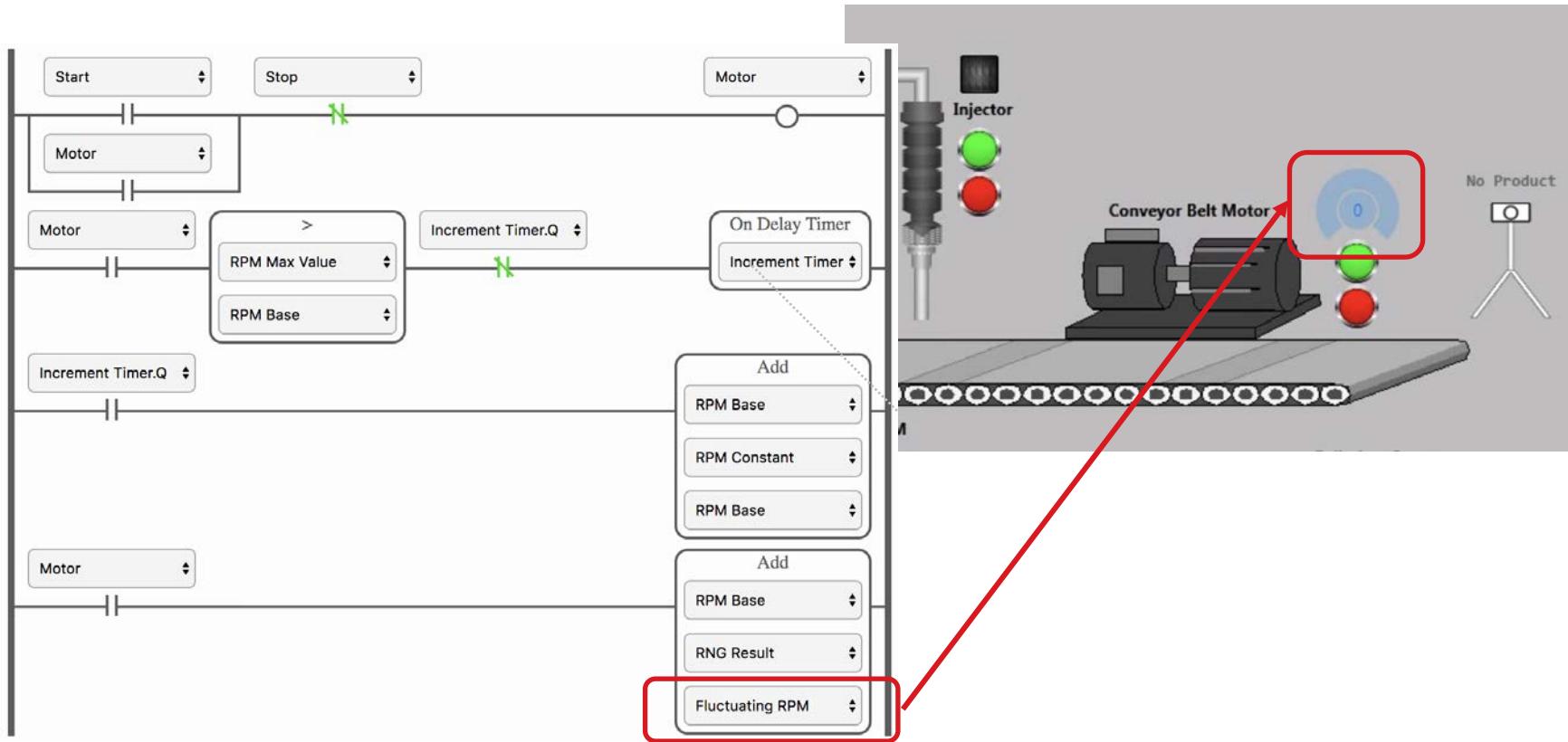
HMI



HMI



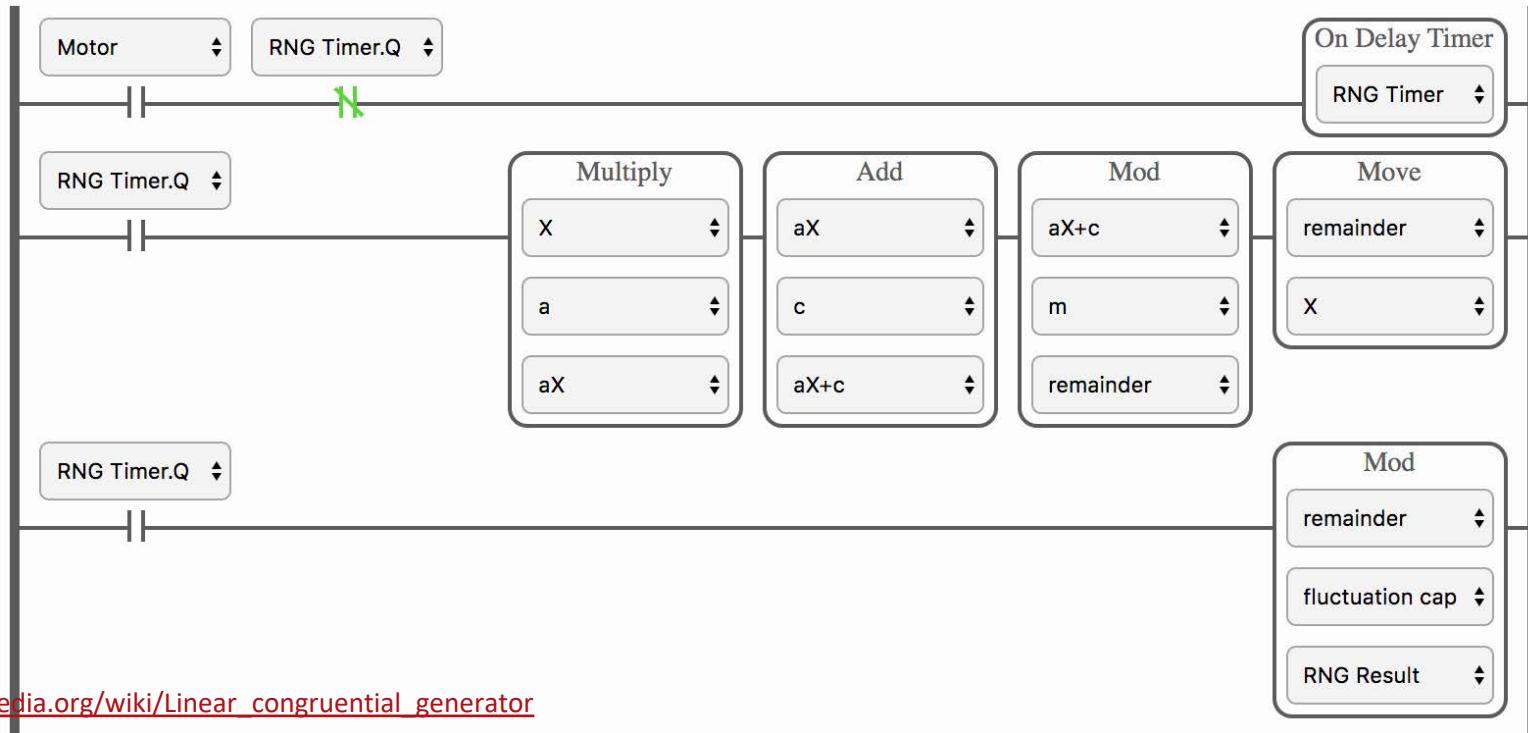
Logic – Motor RPM Fluctuations



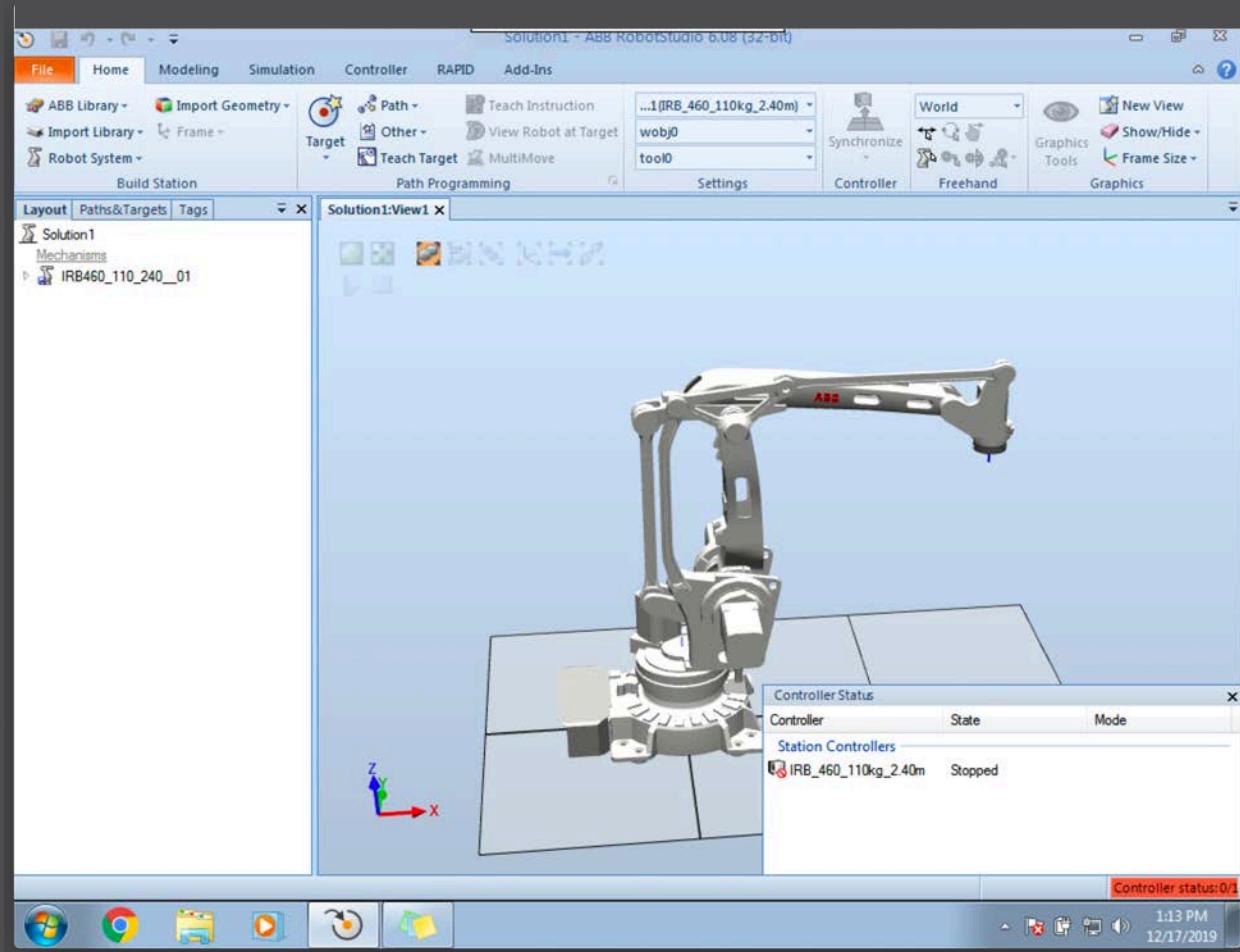
Logic – RNG Block

- Linear congruent generator

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



Robotics



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

Extended Port Forwarding

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

The screenshot shows the ACEmanager web interface for a SIERRA WIRELESS AirLink router. The top navigation bar includes links for Software and Firmware, Template, Refresh All, Reboot, Help, and Logout. Below the navigation is a menu bar with tabs: Status, WAN/Cellular, LAN, VPN, Security (selected), Services, Location, Events Reporting, Serial, Applications, I/O, and Admin.

The main content area displays the Port Forwarding configuration. A sidebar on the left lists other management options: Extended Port Forwarding, Port Filtering - Inbound, Port Filtering - Outbound, Trusted IPs - Inbound (Friends), Trusted IPs - Outbound, and MAC Filtering. The Port Forwarding section contains two dropdown menus: "DMZ Host Enabled" set to "Disable" and "Port Forwarding" set to "Disable".

The "Port Forwarding" table lists the following entries:

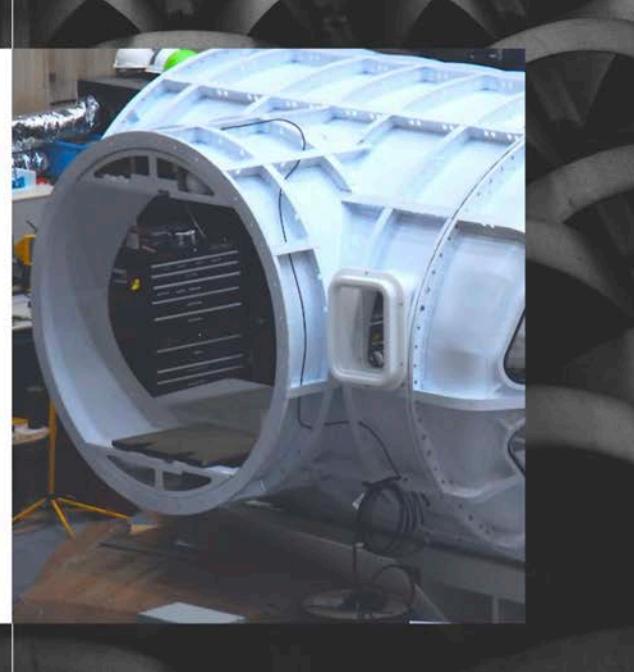
	Public Start Port	Public End Port	Protocol	Host IP	Private Start Port
X	44818		TCP	192.168.0.30	44818
X	9600		UDP	192.168.0.10	9600
X	102		TCP	192.168.0.2	102
X	5900		TCP	192.168.0.5	5900
X	5901		TCP	192.168.0.6	5900

A red box highlights the entries for Micrologix, Omron, Siemens, VNC, and VNC. At the bottom right of the table is a red "Add More" button.

The Company

WHAT CAN WE CREATE?

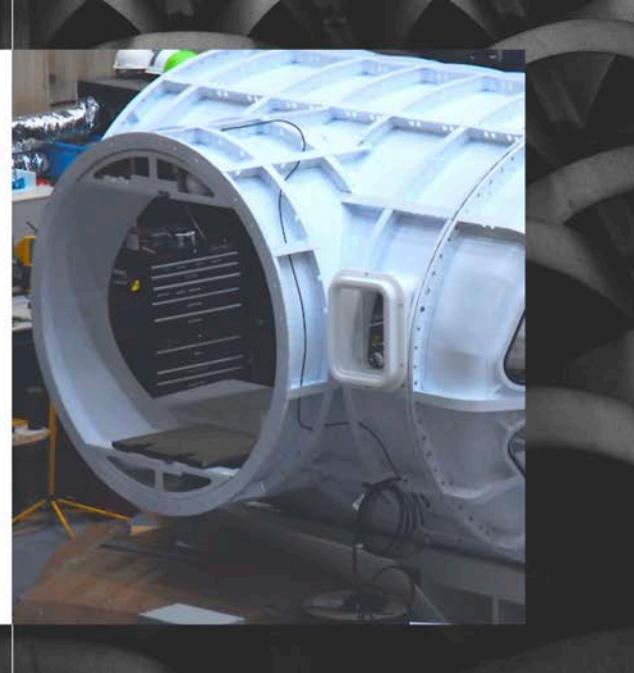
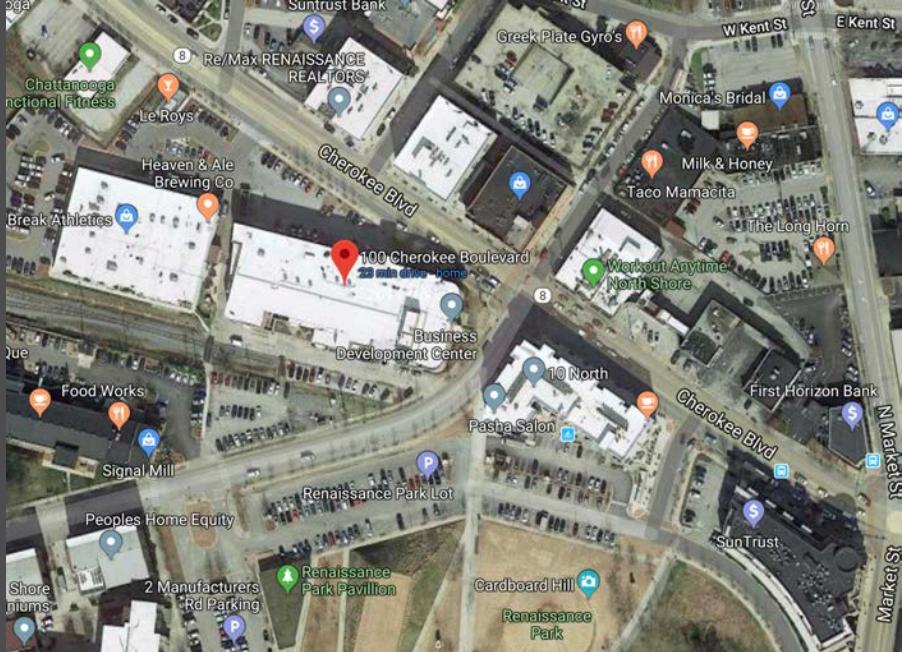
Our engineers are specialized in virtual 3D modeling, digital twins, as well as physical mockups. Our flexible **production floor** can quickly turn models into **plastic** and **metal** parts, which we can optionally assemble and brand for your business.



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



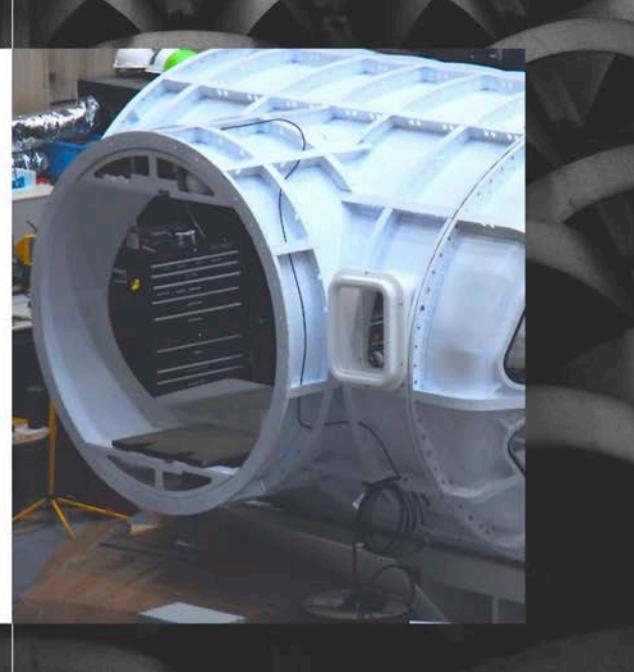
Engineering: +1 (423) 235-8388, 100 Cherokee Blvd, Chattanooga, TN 37405, USA.

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



Bld, Chattanooga, TN 37405, USA.

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

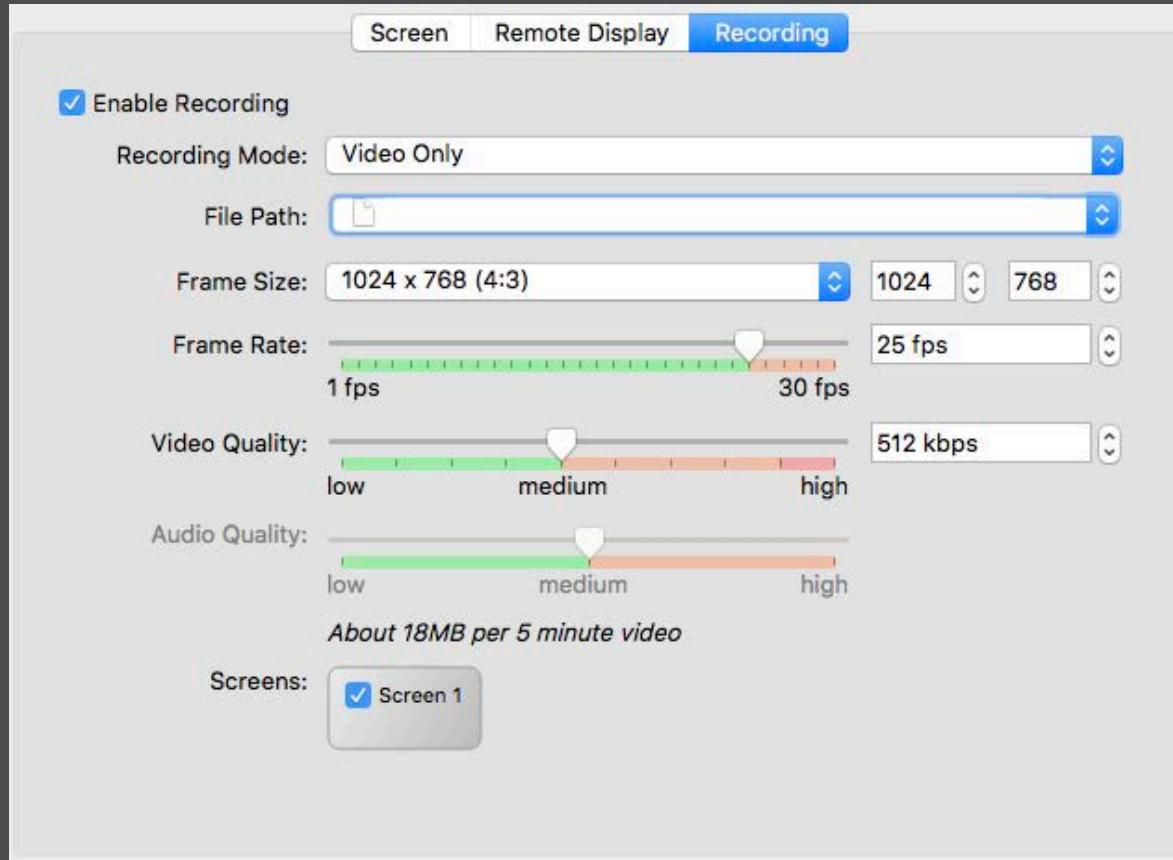
Groups

- 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

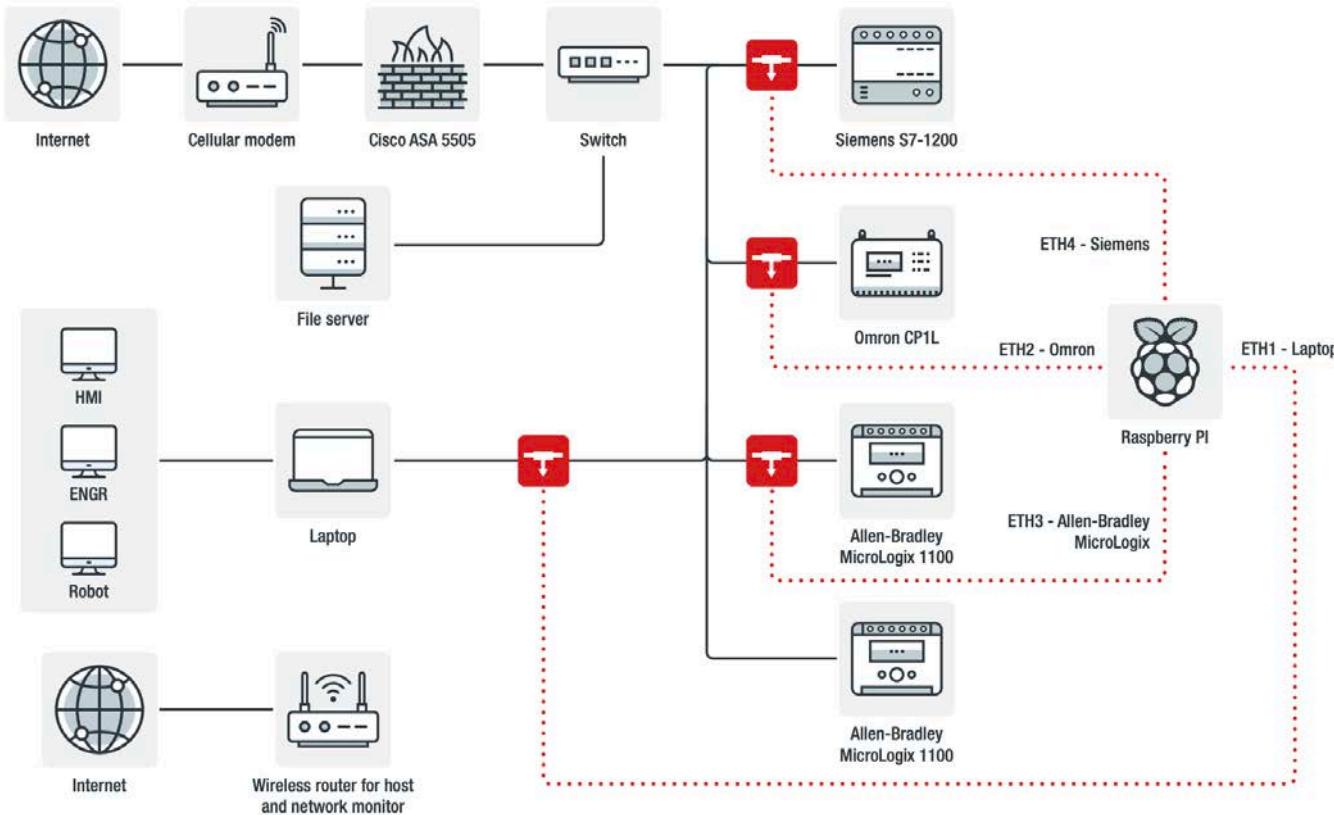
Monitoring the system



Monitoring the system



Monitoring the system



Moloch

Sessions SPIView SPIGraph Connections Files Stats History Settings v2.0.0-GIT ⓘ

Search

Last 2 weeks Start 2019/12/05 17:35:30 End 2019/12/19 17:35:30 Bounding Last Packet Interval Auto

50 per page 1 2 3 4 5 Showing 1 - 50 of 227,671 entries

Session Packets Bytes Databytes Lines Bars

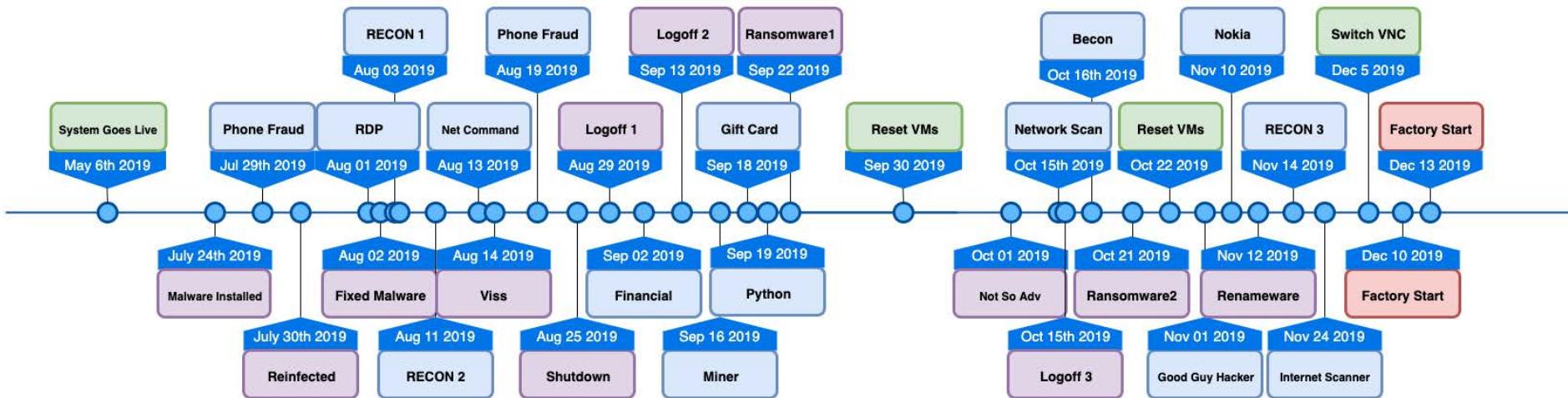
Start Time Src IP / Country Src Port Dst IP / Country Dst Port Packets Databytes / Bytes Moloch Node Filename Cnt Info Stop Time

Start Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Filename Cnt	Info	Stop Time
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
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
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
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
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
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
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
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
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

Scripts

Laptop Sniffer IP Conversations										
IP	GEO	<->	IP	GEO	Bytes	<->	Bytes	TotalB	Duration	DNS
192.1	AA	<->	196.2	SC	23452	<->	18658	210035	43908.29	Resolve
13.1	US	<->	192.	AA	56267	<->	26965	275283	45708.44	x3.r.cloudfront.net <-> localnet
192.1	AA	<->	192.1	ZZ	19839	<->	0	198391	0.000000	Resolve
104.1	US	<->	192.	AA	24204	<->	47162	495832	44488.71	localnet
169.6	CH	<->	192.	AA	20768	<->	18219	389874	45896.16	iewer.com <-> localnet
188.17	AT	<->	192.	AA	33363	<->	14586	179227	45941.10	iewer.com <-> localnet
104.1	US	<->	192.	AA	20572	<->	14623	166806	44487.27	localnet
96.11	US	<->	192.1	AA	60057	<->	24350	249511	9419.517	static.akamaitechnologies.com <-> localnet
72.21	US	<->	192.1	AA	44206	<->	24828	252703	12000.88	localnet
23.6	US	<->	192.	AA	51094	<->	24558	250693	645.9369	tatic.akamaitechnologies.com <-> localnet
23.6	US	<->	192.	AA	27678	<->	24722	249988	669.0907	tatic.akamaitechnologies.com <-> localnet
23.6	US	<->	192.	AA	81044	<->	13911	147214	44079.78	.static.akamaitechnologies.com <-> localnet
108.1	US	<->	192.	AA	10757	<->	42044	149616	42185.33	rtmd.east.verizon.net <-> localnet
13.14	US	<->	192.	AA	16622	<->	59307	759300	44079.38	localnet
185.23	ZZ	<->	192.	AA	61793	<->	37683	655620	2129.563	localnet
142.17	CA	<->	192.	AA	63078	<->	29570	358875	2073.864	ral.com <-> localnet
31.1	IE	<->	192.	AA	31608	<->	92917	960782	44494.83	fcdn.net <-> localnet
136.14	US	<->	192.	AA	57680	<->	60612	118292	4518.73	alesforceagent.com <-> localnet
64.233	US	<->	192.	AA	34936	<->	74693	781867	44090.79	<-> localnet
192.	AA	<->	205.18	US	30734	<->	49456	356790	44107.37	dn.net
72.21	US	<->	192.	AA	30060	<->	74510	775167	44126.96	localnet
23.208	US	<->	192.	AA	68646	<->	46850	537153	44083.21	y.static.akamaitechnologies.com <-> localnet
68.67	US	<->	192.	AA	11754	<->	12133	238876	44090.29	ncer.mgmt.nym2.adnexus.net <-> localnet
192.	AA	<->	204.15	US	49156	<->	42882	92038	44098.98	22.doubleverify.com
38.12	US	<->	192.	AA	22344	<->	15119	173538	2079.425	m <-> localnet
64.233	US	<->	192.	AA	72600	<->	11840	191008	44750.01	<-> localnet
108.1	US	<->	192.	AA	33578	<->	10120	134782	44086.79	kedin.com <-> localnet
68.67	US	<->	192.	AA	18306	<->	56400	239462	44095.42	ncer.mgmt.nym2.adnexus.net <-> localnet
31.1	IE	<->	192.	AA	73716	<->	61655	135371	44508.08	-atl3.facebook.com <-> localnet
104.1	US	<->	192.	AA	69770	<->	63533	133303	44108.85	.com <-> localnet
65.53	US	<->	192.	AA	14666	<->	53300	199966	5995.872	localnet
104.1	US	<->	192.	AA	23420	<->	67659	91079	44507.87	localnet
64.23	US	<->	192.	AA	21140	<->	16370	184844	44772.18	> localnet
192.	AA	<->	204.13	US	13908	<->	48230	187315	44087.20	ginx-loadbalancer.mgmt.nym2.adnexus.net
52.3	US	<->	192.	AA	34164	<->	18247	216641	44755.68	te-1.amazonaws.com <-> localnet
104.9	US	<->	192.1	AA	12544	<->	29229	214836	9666.629	.static.akamaitechnologies.com <-> localnet
185.23	ZZ	<->	192.	AA	16930	<->	8991	178291	7071.010	localnet
13.33	US	<->	192.	AA	21032	<->	11997	141004	44768.74	ax3.r.cloudfront.net <-> localnet
72.2	US	<->	192.	AA	16088	<->	61350	77438	44069.24	localnet
50.11	US	<->	192.	AA	25084	<->	39339	64423	44095.50	n.com <-> localnet
74.12	US	<->	192.	AA	35244	<->	11310	148353	44215.94	<-> localnet
40.11	US	<->	192.	AA	20986	<->	72532	93518	7623.911	localnet
104.24	US	<->	192.	AA	22004	<->	54417	76421	44507.87	<-> localnet
64.233	US	<->	192.	AA	14198	<->	12714	141343	44089.41	fw.adsafeprotected.com
192.	AA	<->	199.1	US	24396	<->	15830	259792	44097.10	localnet
13.6	US	<->	192.	AA	23040	<->	98714	121754	44496.40	<-> localnet
74.12	US	<->	192.	AA	36788	<->	60742	97530	44103.82	net-1.localnet
172.21	US	<->	192.	AA	11178	<->	13261	143788	44083.08	ute-1.amazonaws.com <-> localnet
52.71	US	<->	192.	AA	22916	<->	34439	57355	44106.07	-msedge.net
192.	AA	<->	204.79	US	14934	<->	13570	162911	44079.19	pixel.adsafeprotected.com
192.	AA	<->	199.1	US	15132	<->	14046	165370	44111.79	localnet
40.11	US	<->	192.1	AA	17290	<->	59656	76946	2381.940	.static.akamaitechnologies.com <-> localnet
184.2	NL	<->	192.	AA	32870	<->	12455	157422	44262.72	localnet
13.1	US	<->	192.	AA	21276	<->	72239	93515	44451.16	localnet
104.1	US	<->	192.	AA	11970	<->	41194	53164	44495.03	localnet
104.19	US	<->	192.	AA	8396	<->	12418	132576	44271.18	localnet
104.1	US	<->	192.	AA	7714	<->	10021	107926	44762.34	localnet

What Happened



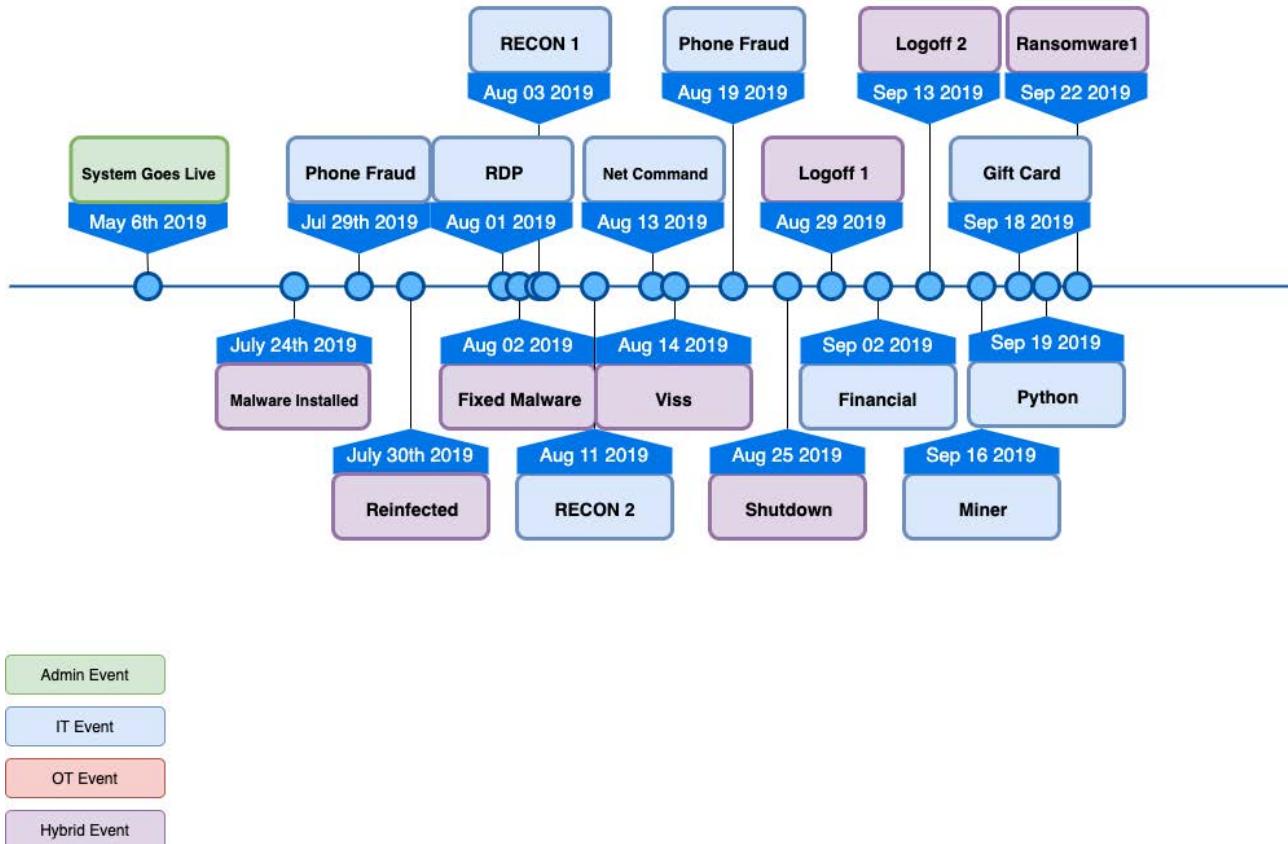
Admin Event

IT Event

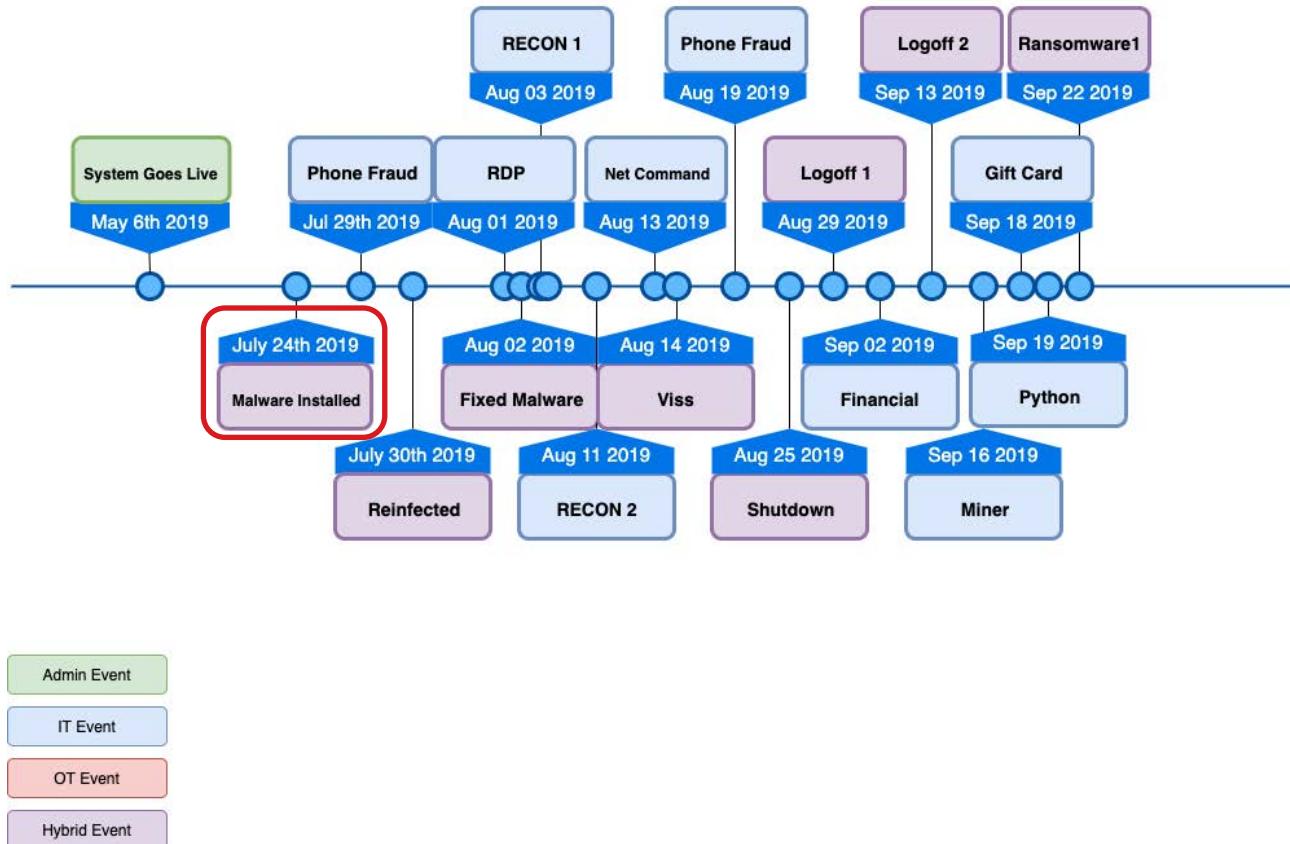
OT Event

Hybrid Event

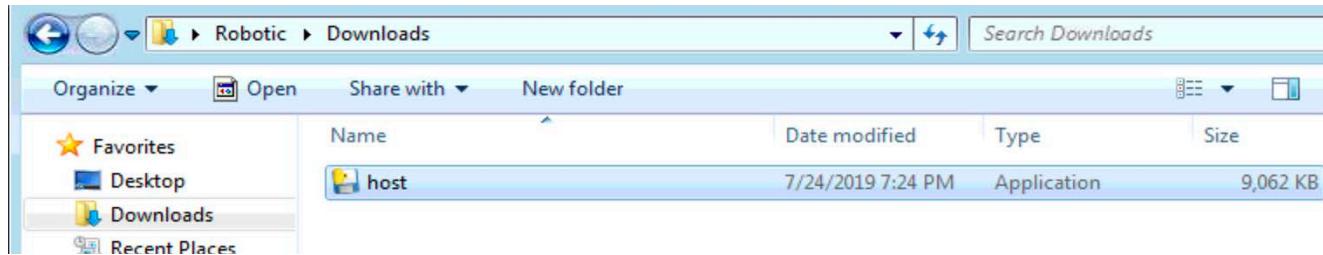
What Happened



What Happened



Host.exe

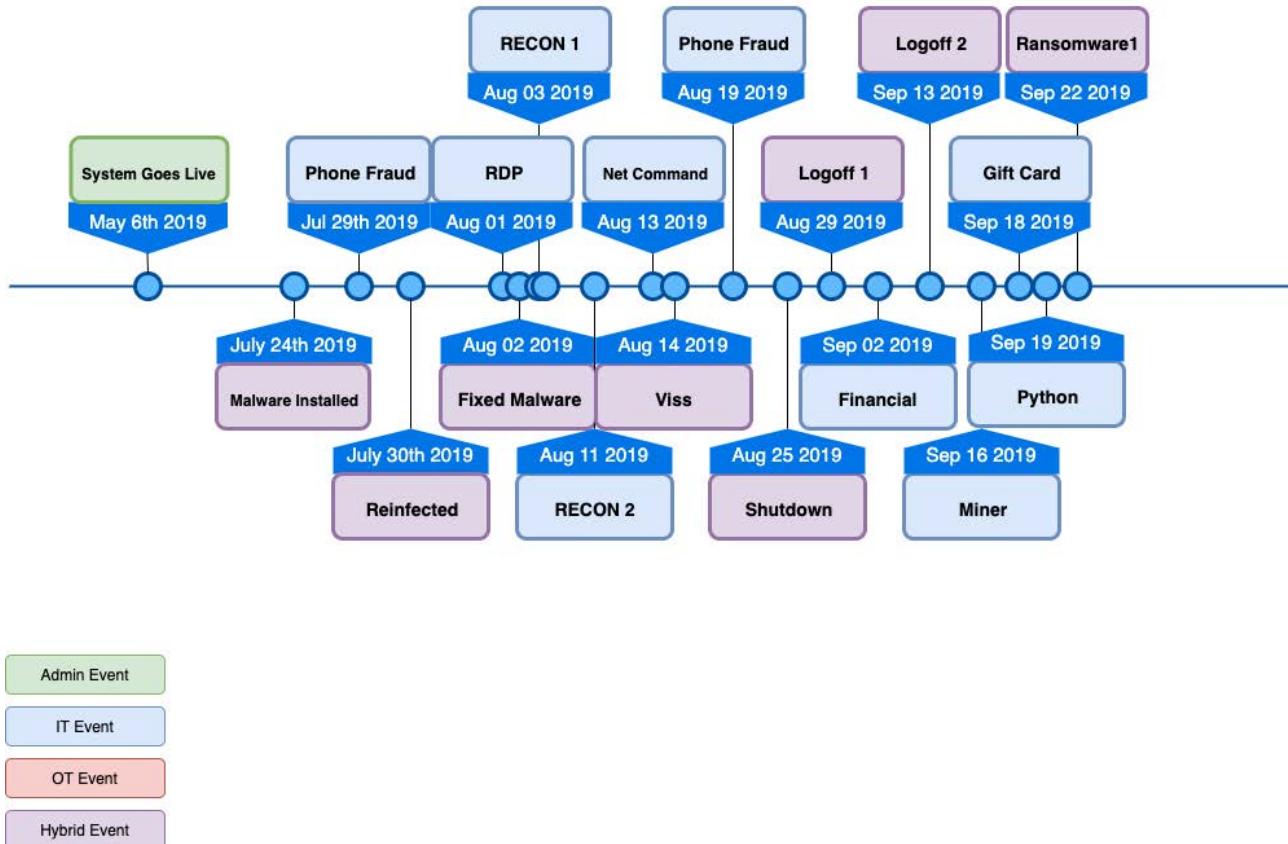


A screenshot of a Windows File Explorer window. The title bar says "Robotic > Downloads". The toolbar includes "Organize", "Open", "Share with", "New folder", and search fields. The left sidebar shows "Favorites" with "Desktop" and "Downloads" selected, and "Recent Places". The main area lists a file named "host" with the details: Name: host, Date modified: 7/24/2019 7:24 PM, Type: Application, Size: 9,062 KB.

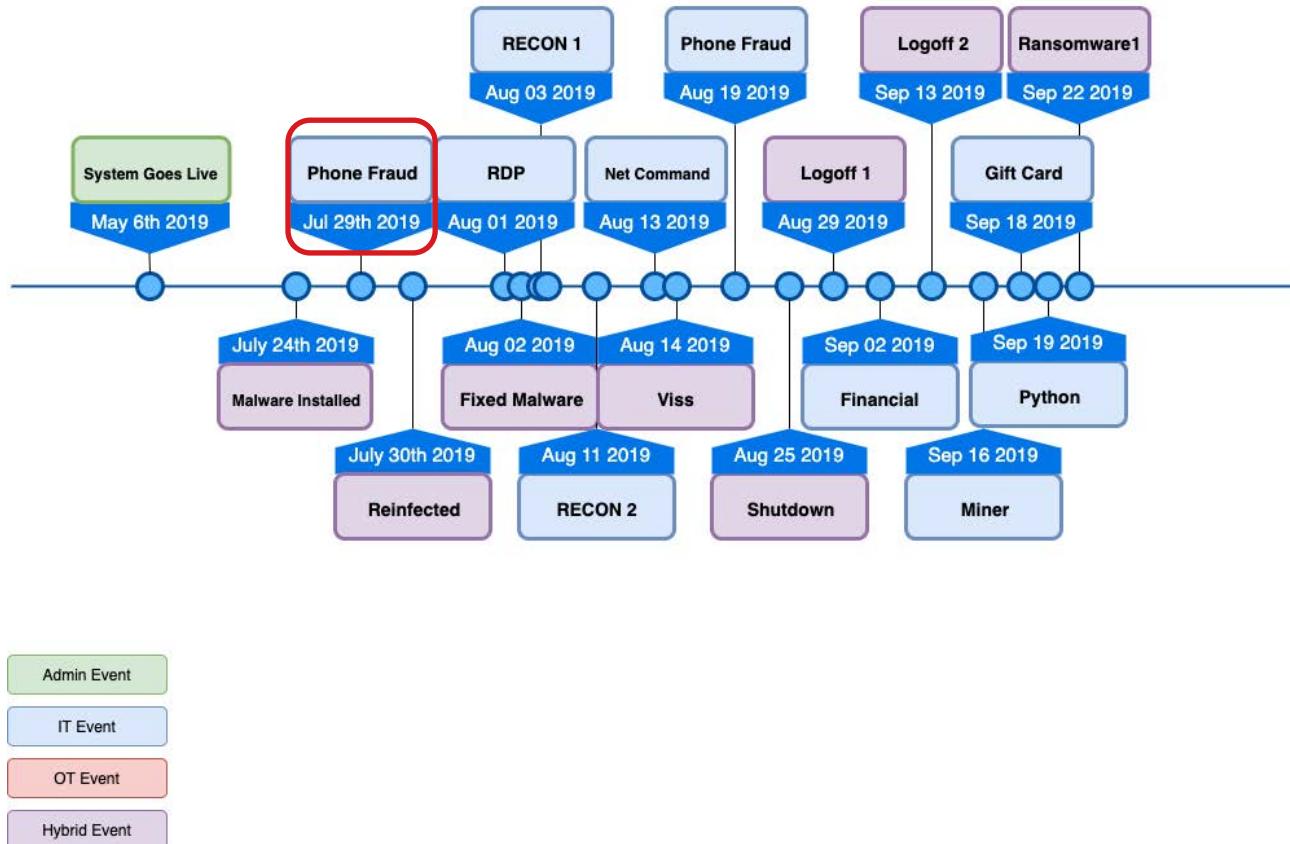
```
root@kali:~/Desktop/python-exe-unpacker# python pyinstxtractor.py ../host.exe1
[*] Processing ../host.exe1
[*] Pyinstaller version: 2.1+
[*] Python version: 27
[*] Length of package: 9036159 bytes
[*] Found 930 files in CArchive
[*] Beginning extraction...please standby
[*] Found 549 files in PYZ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

You can now use a python decompiler on the pyc files within the extracted directory
root@kali:~/Desktop/python-exe-unpacker#
```

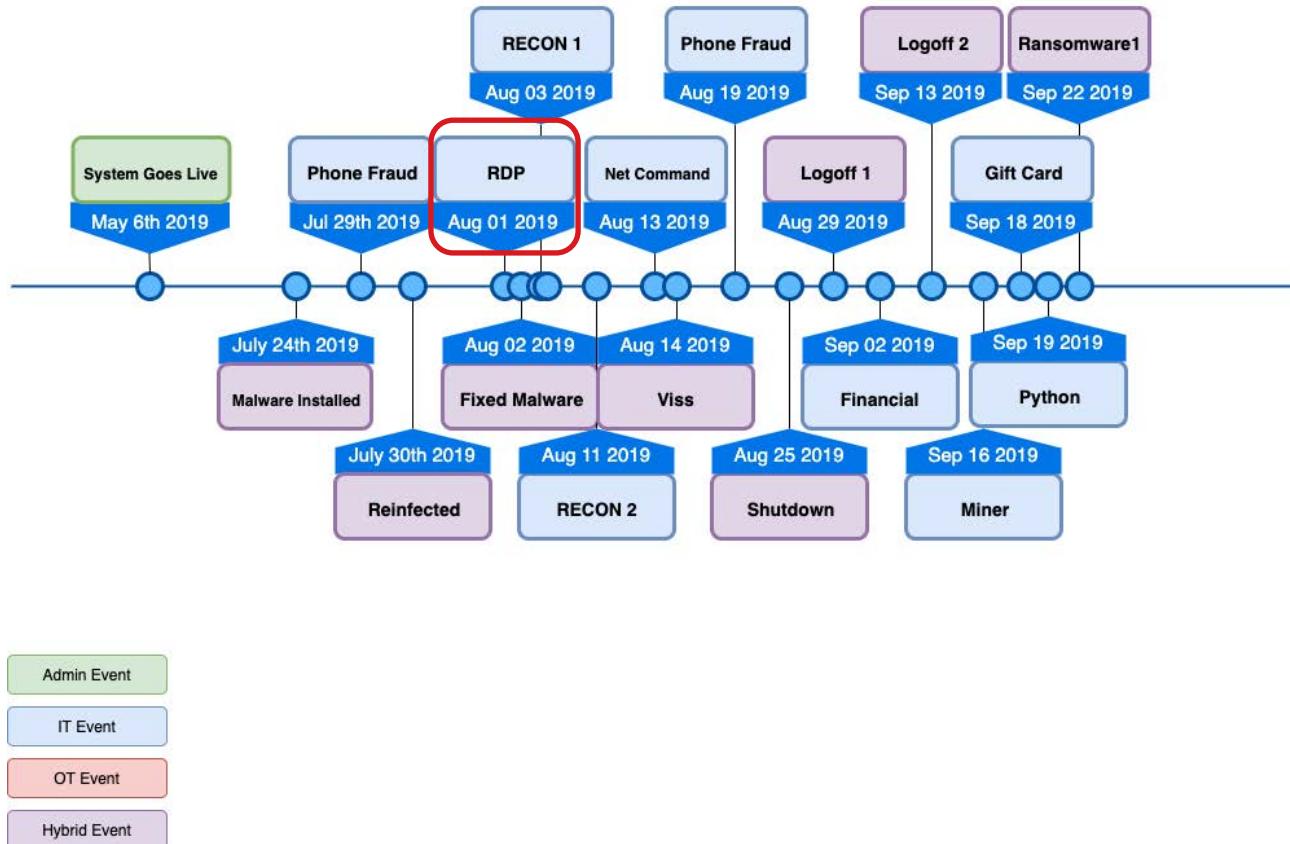
What Happened



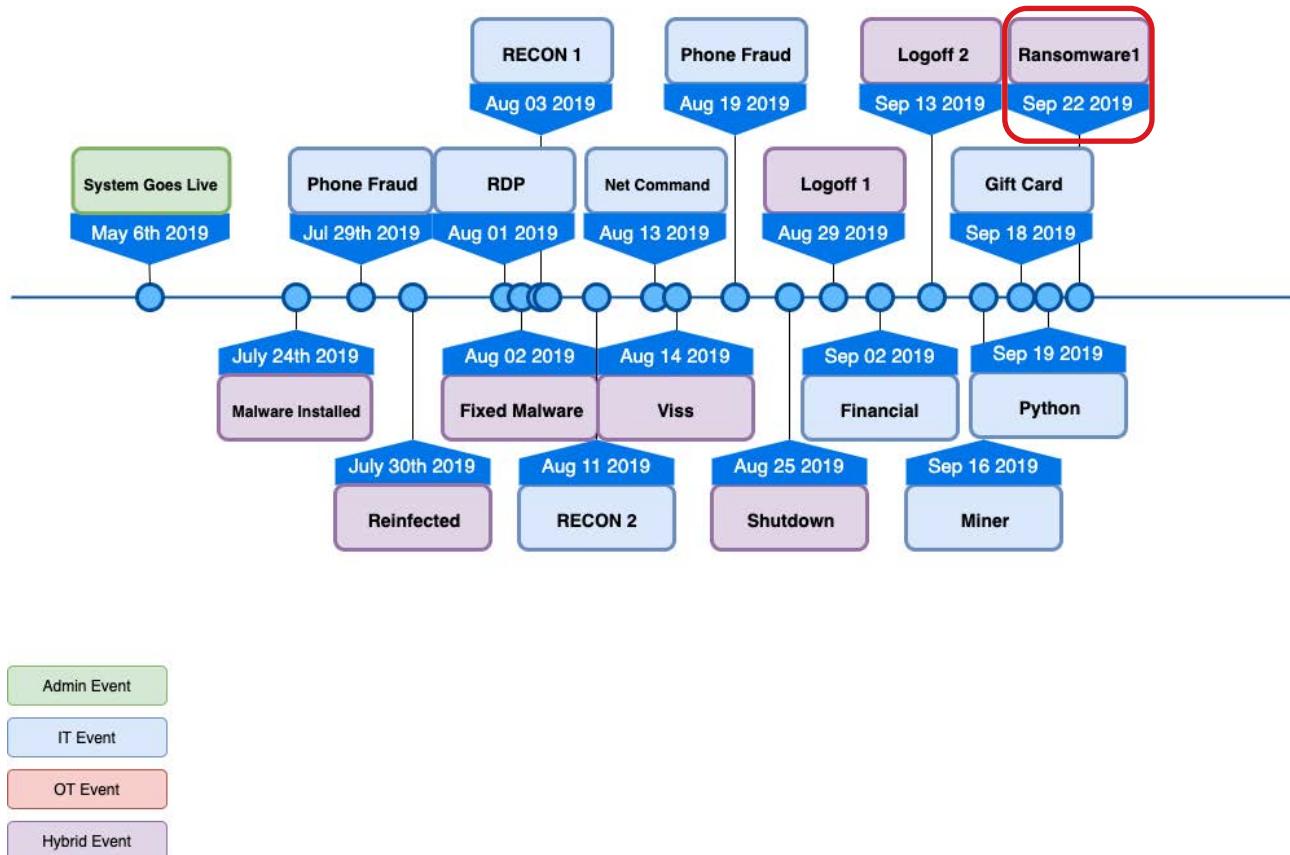
What Happened



What Happened



What Happened





Recycle Bin

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 (\FILESERVER) (M:)

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

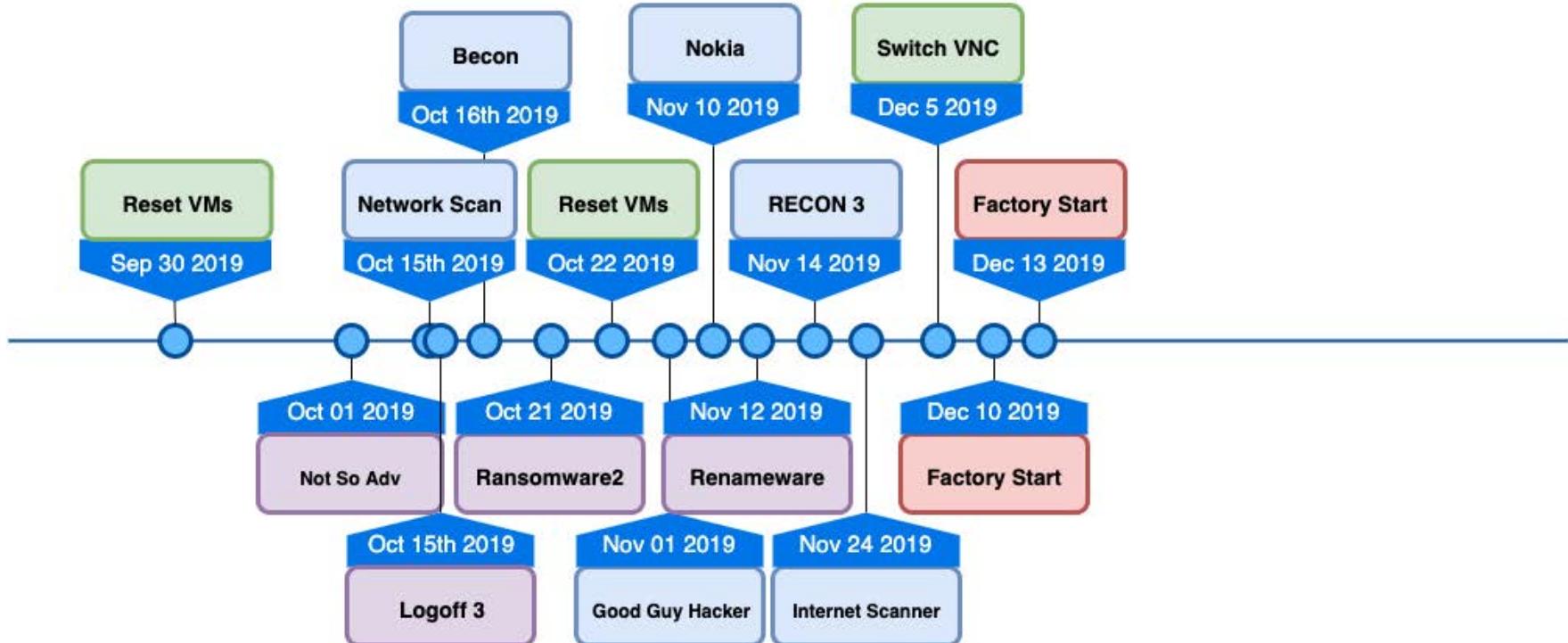
ROBOTIC-PC Workgroup: WORKGROUP Memory: 4.00 GB
Robotic-PC.metech.co Processor: Intel(R) Core(TM) i5-43...

g
ke
...

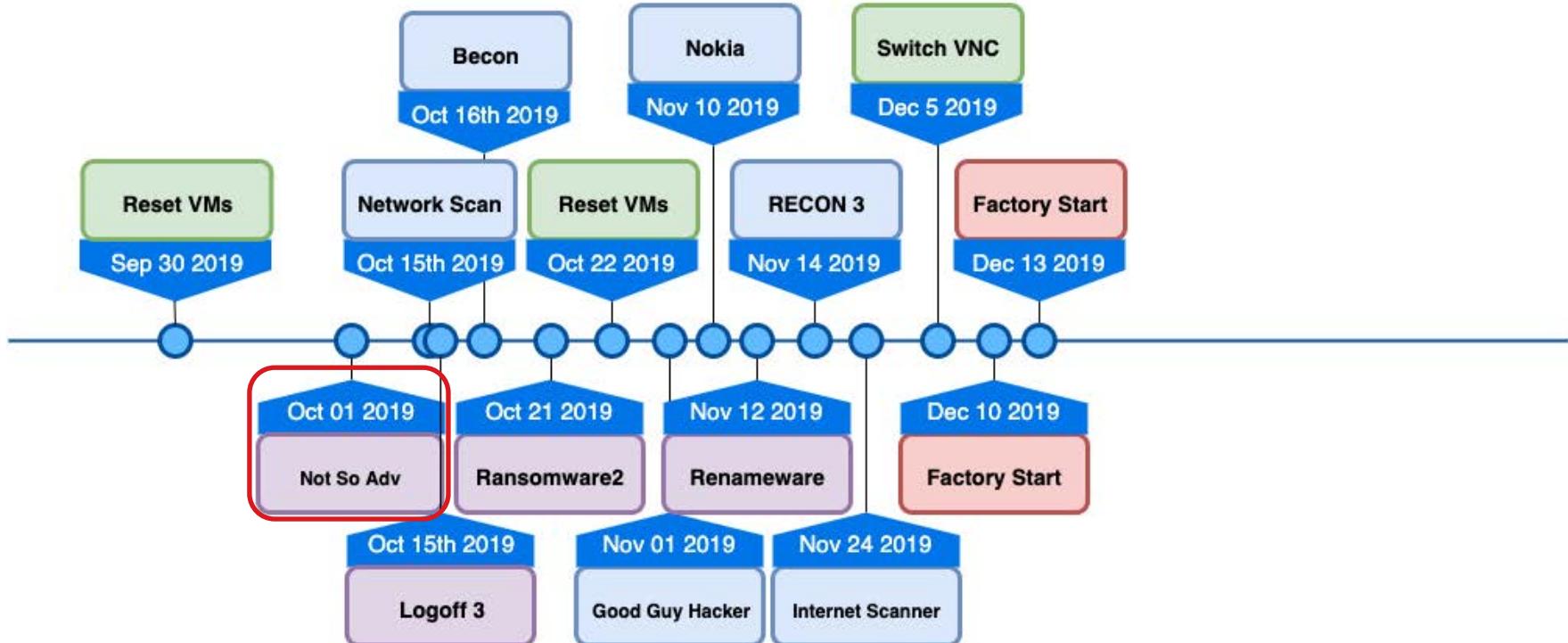


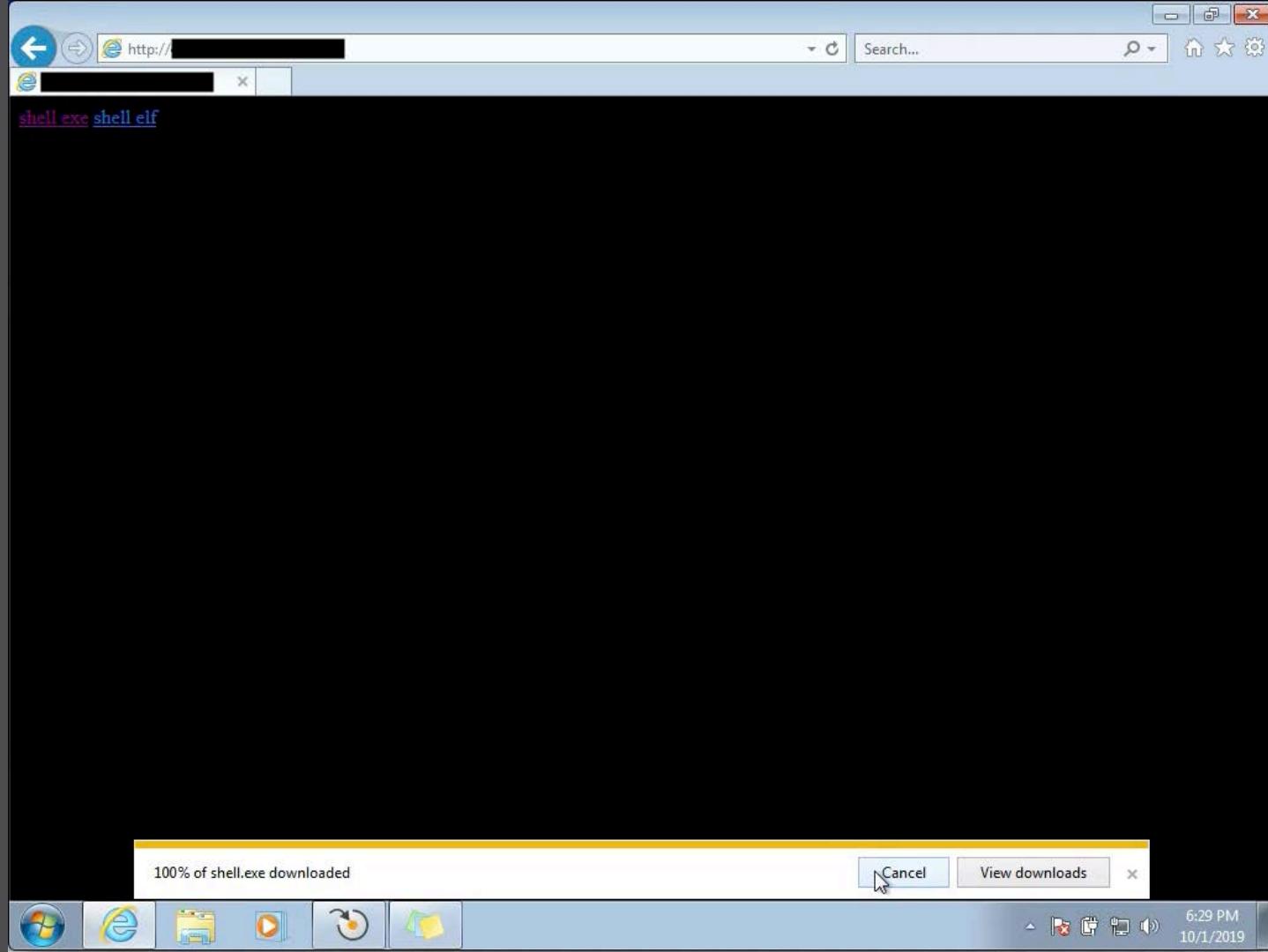
2:27 PM
9/22/2019

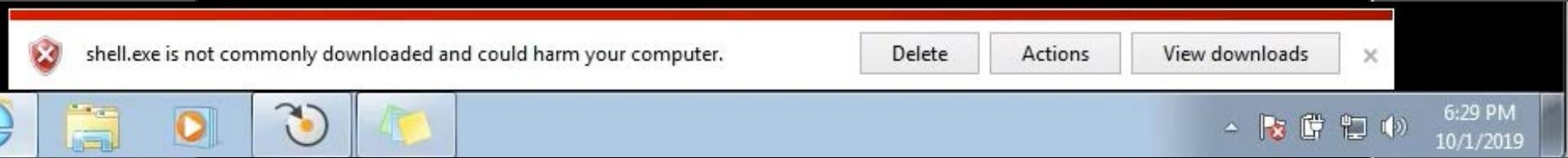
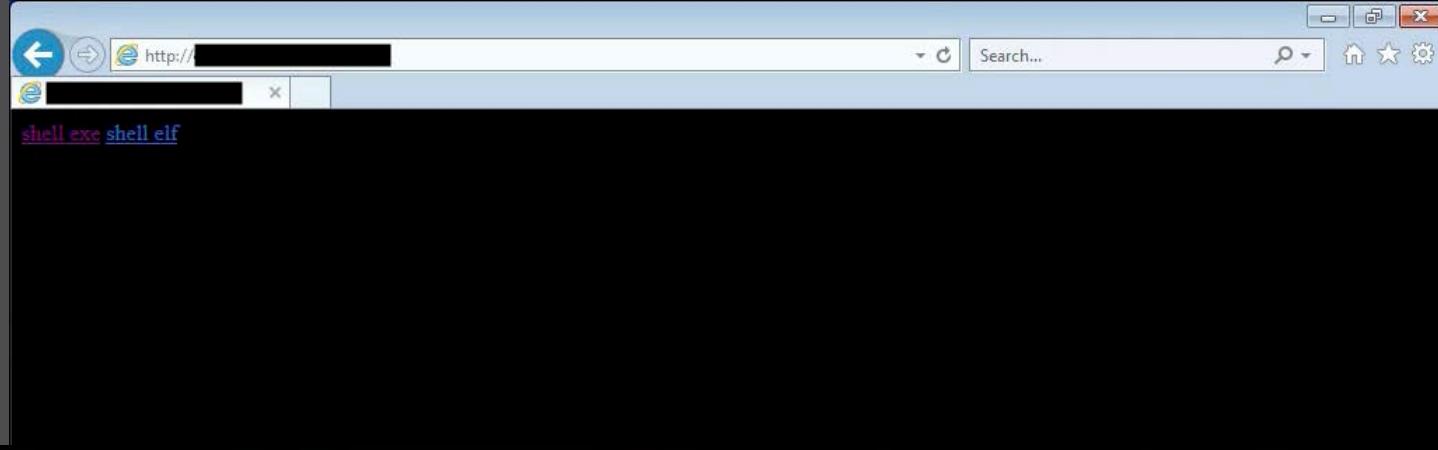
What Happened

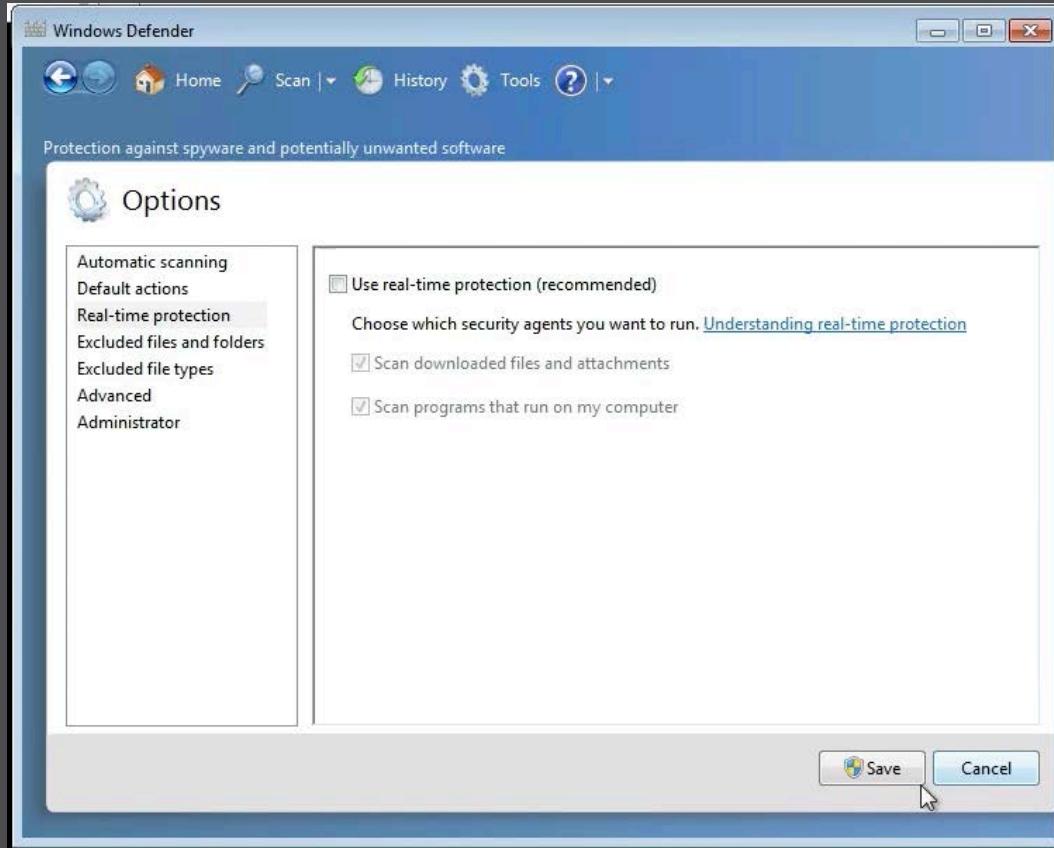


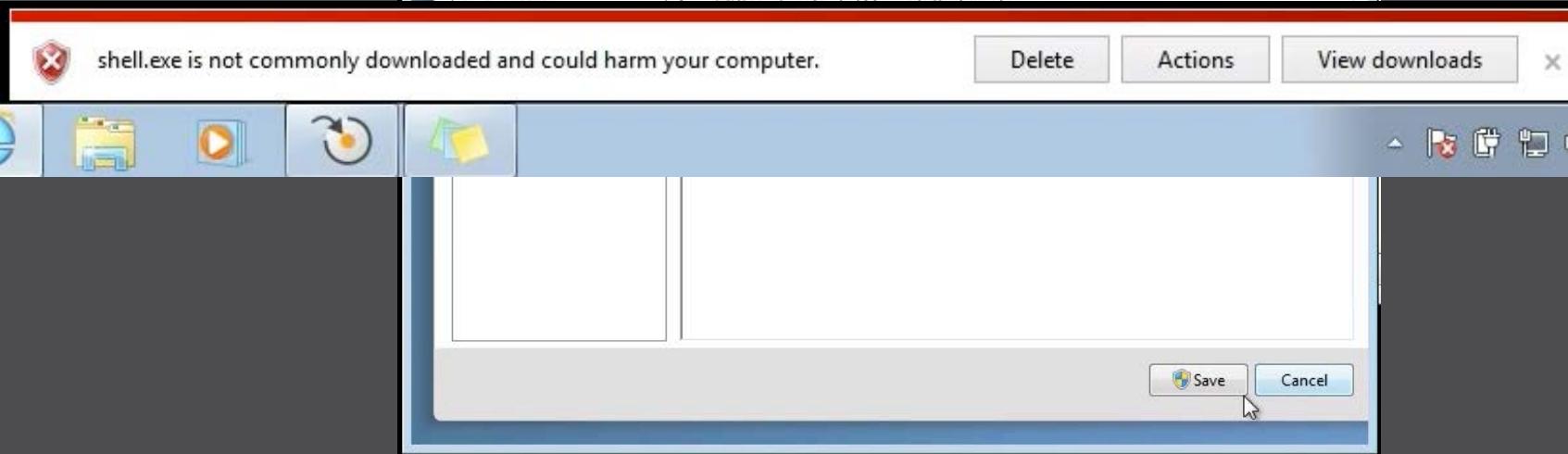
What Happened

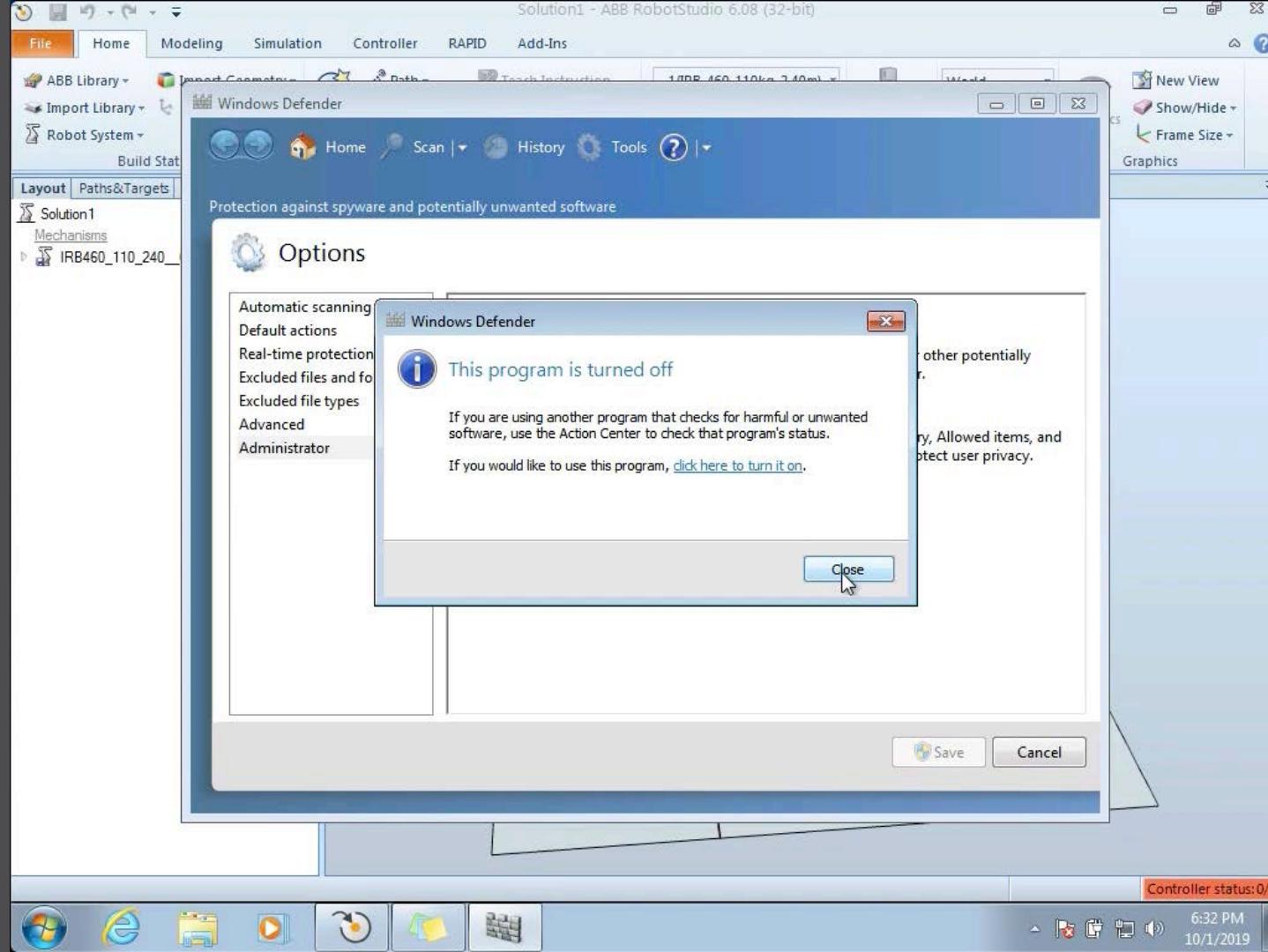


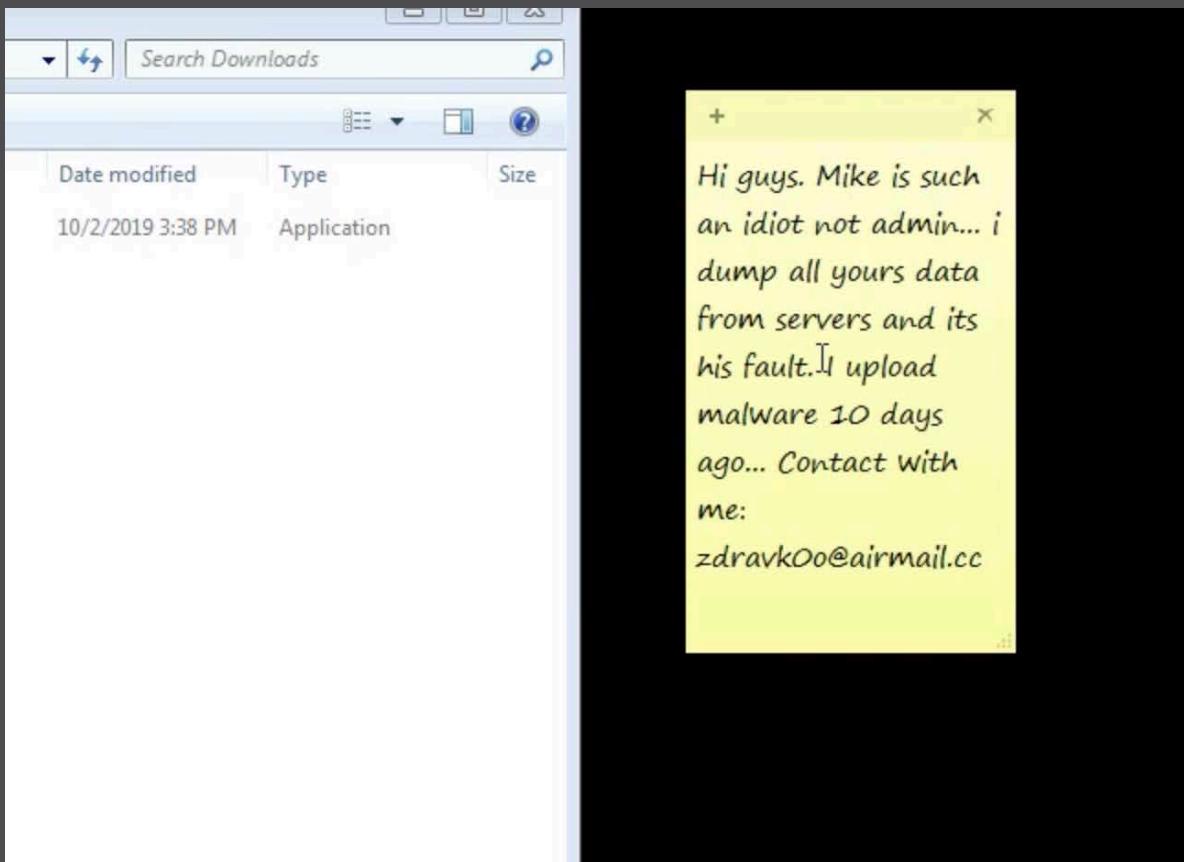




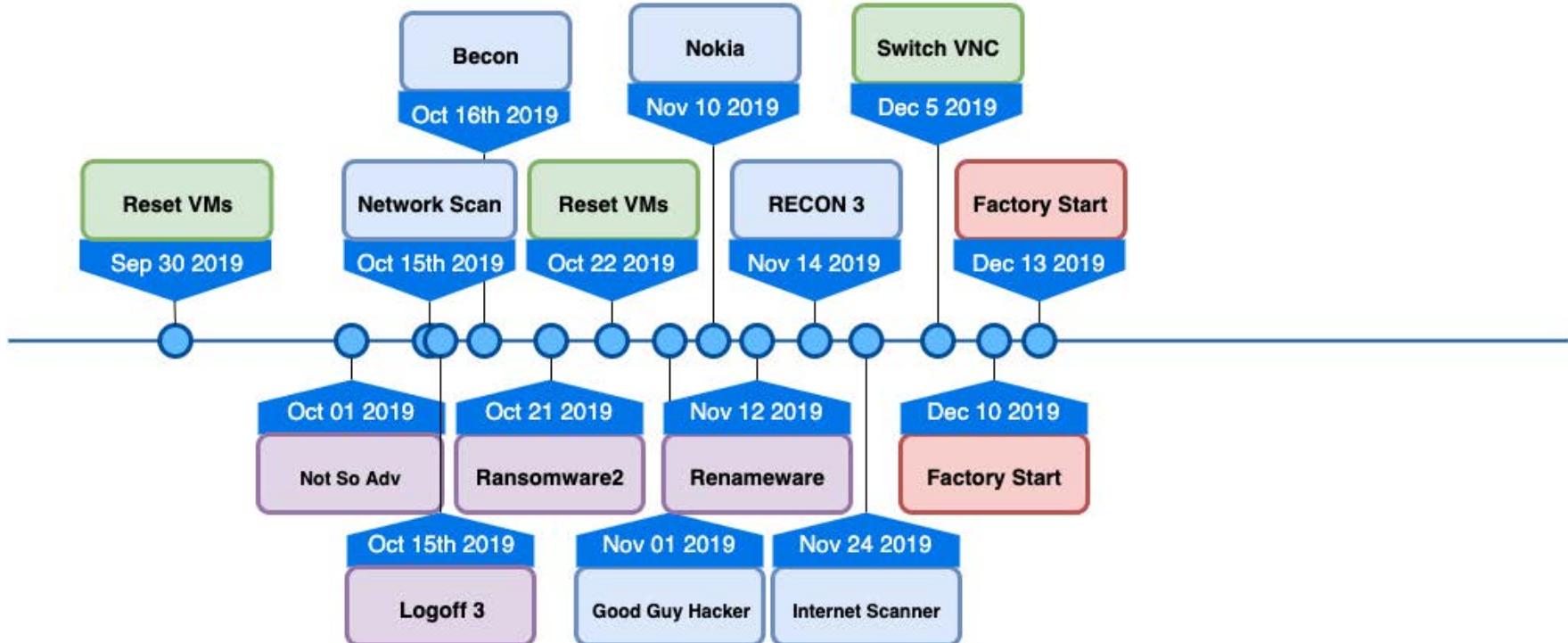




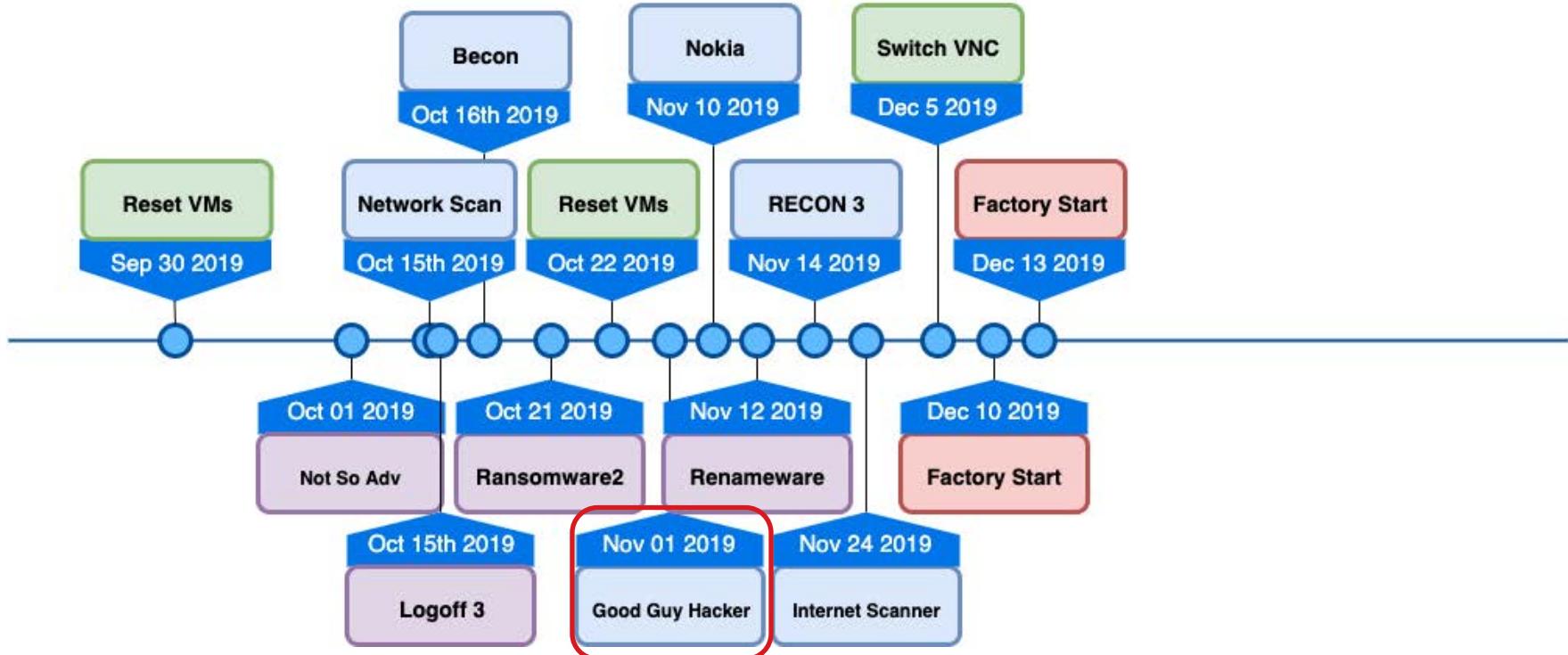




What Happened



What Happened



File Home Modeling Simulation Controller RAPID Add-Ins

Simulation Setup Station Logic Activate Mechanical Units

Create Collision Set Configure

Play Pause Stop Reset

I/O Simulator Trace Stopwatch

Enabled Signal Analyzer Signal Setup History

Record Record Application Record Graphics

Layout Paths&Targets Tags

Solution1 Mechanisms

IRB460_110_240_01

Links

- Base
- Link1
- Link2
- Link3
- LinkD1
- LinkD2
- LinkS1
- LinkS2
- Link4
- LinkS3
- Link6

Controller Status

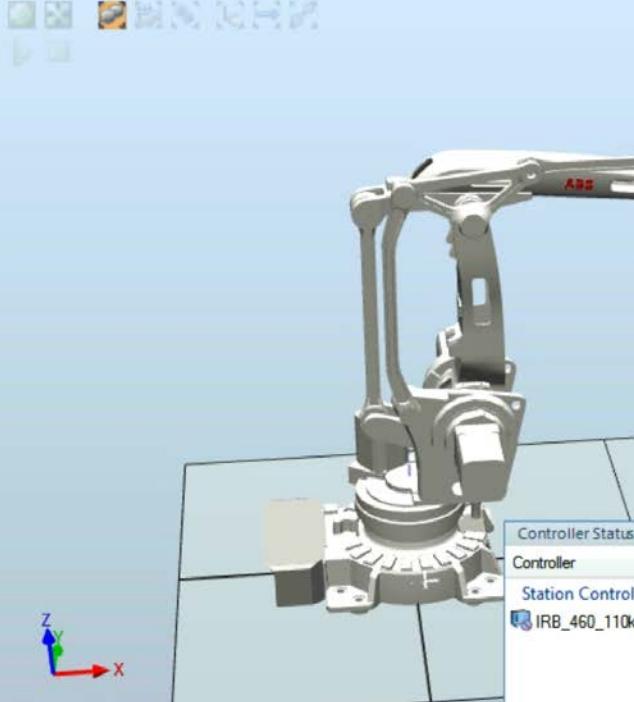
Controller	State	Mode
Station Controllers		
IRB_460_110kg_2.40m	Stopped	

Controller status: 0/1

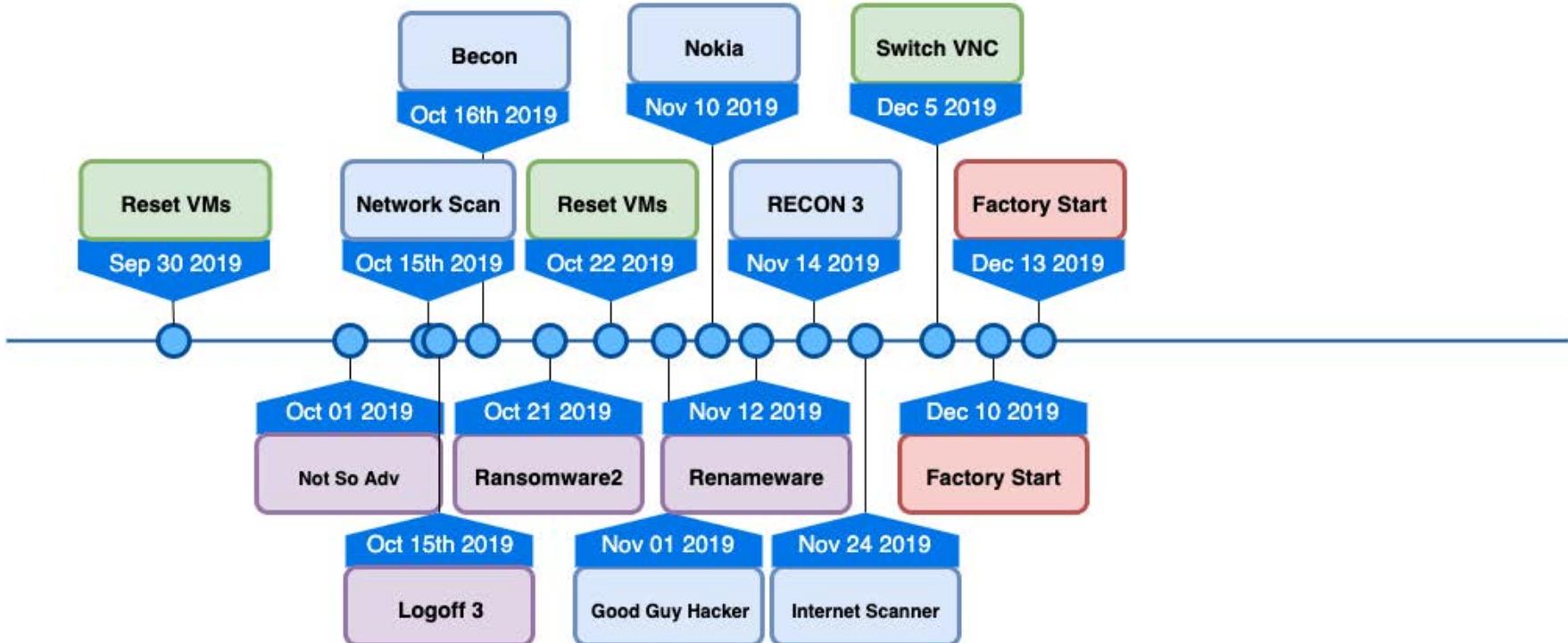
12:36 PM 11/1/2019

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

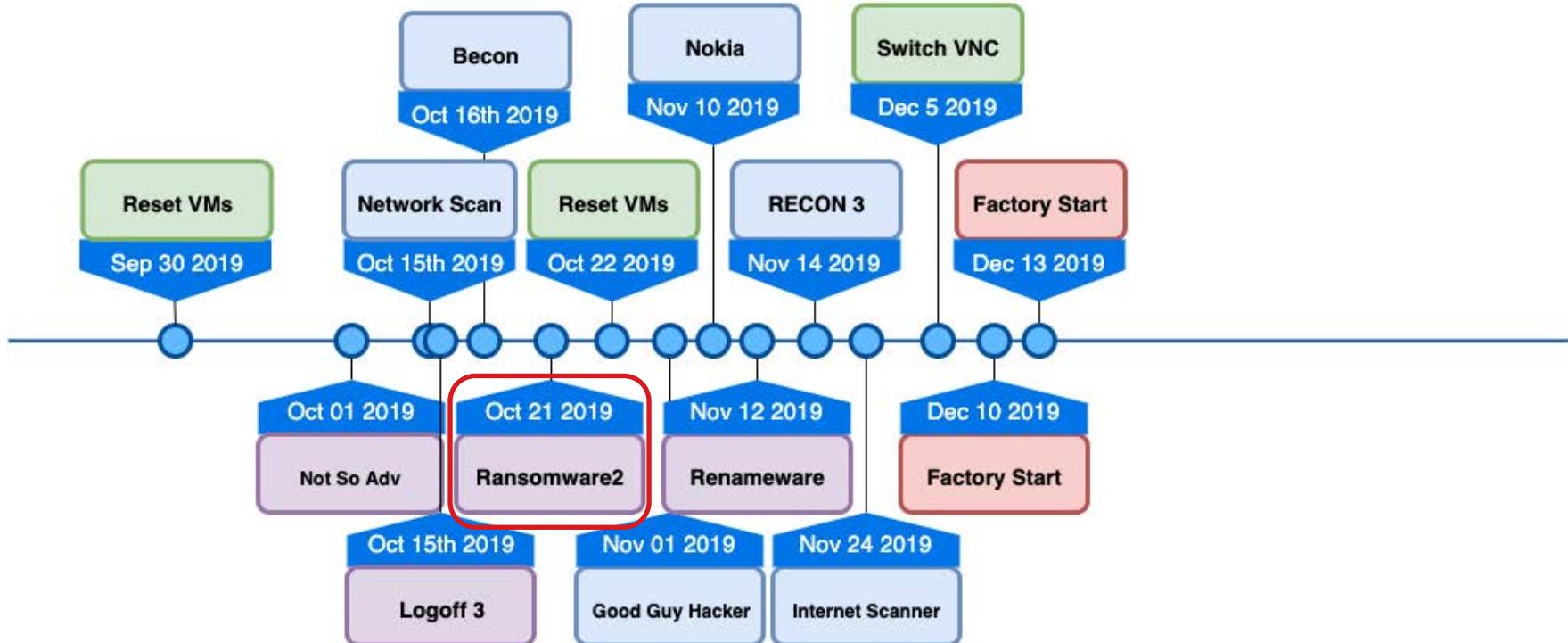
Hi i found out that your PC have an opened port 5901 that allow hackers (like me) to break into your pc so, i want to tell you to set a password to your VNC. m3trà



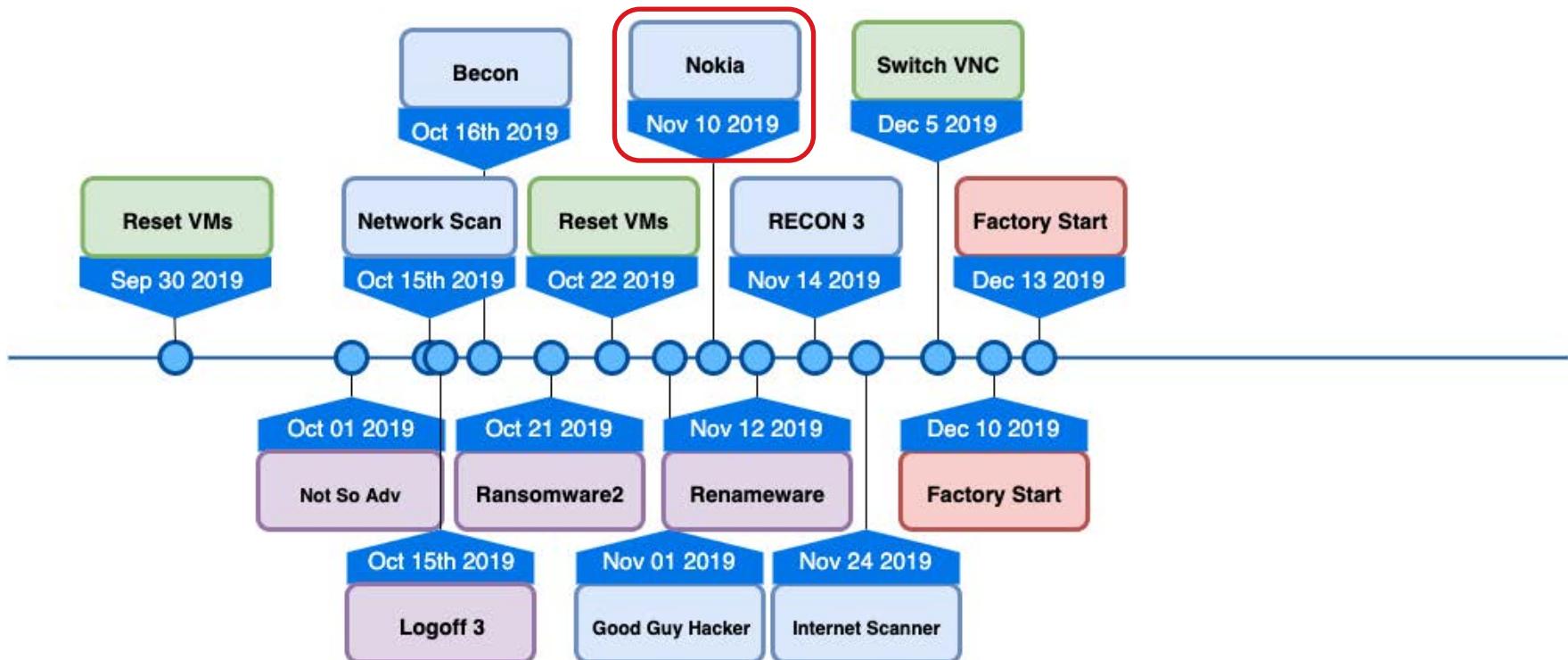
What Happened



What Happened



What Happened





Acrobat
Reader DC

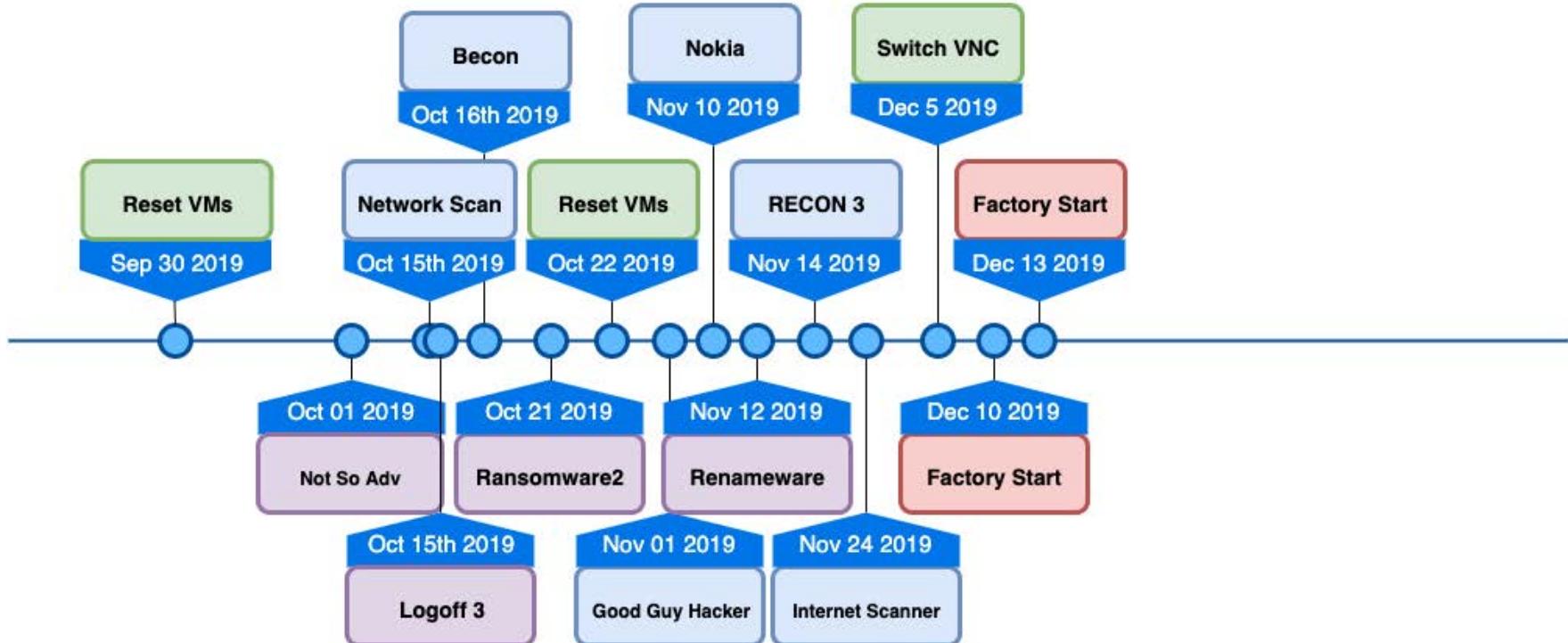


RobotStudio
6.08 (32-bit)

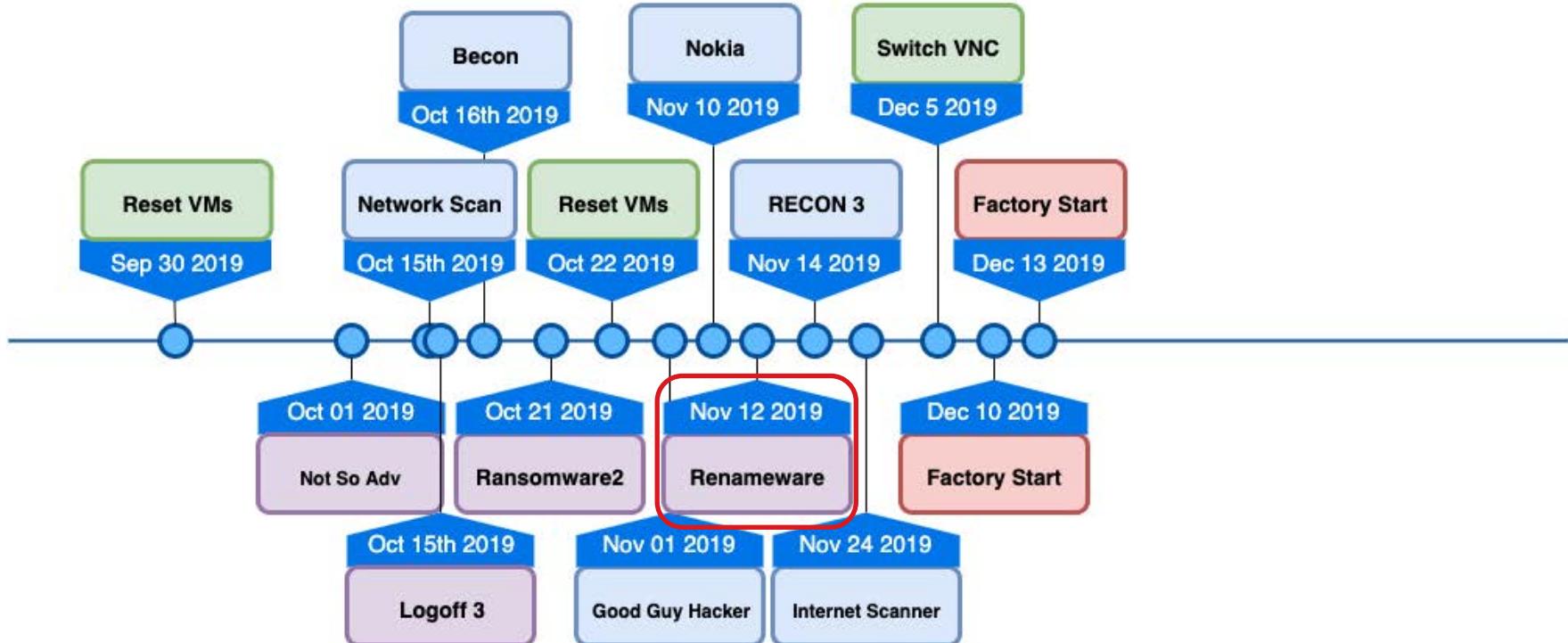


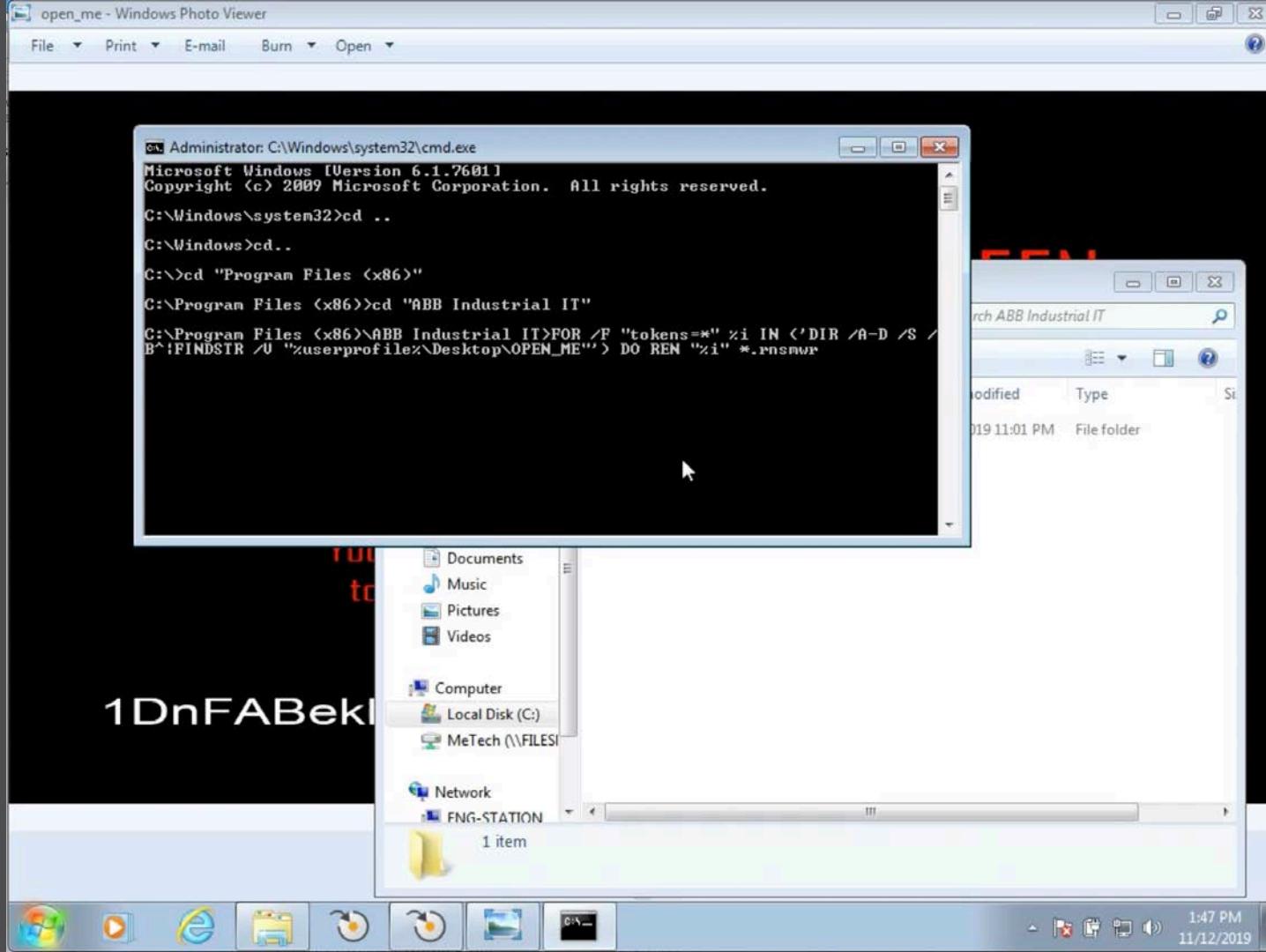
RobotStudio
6.08

What Happened

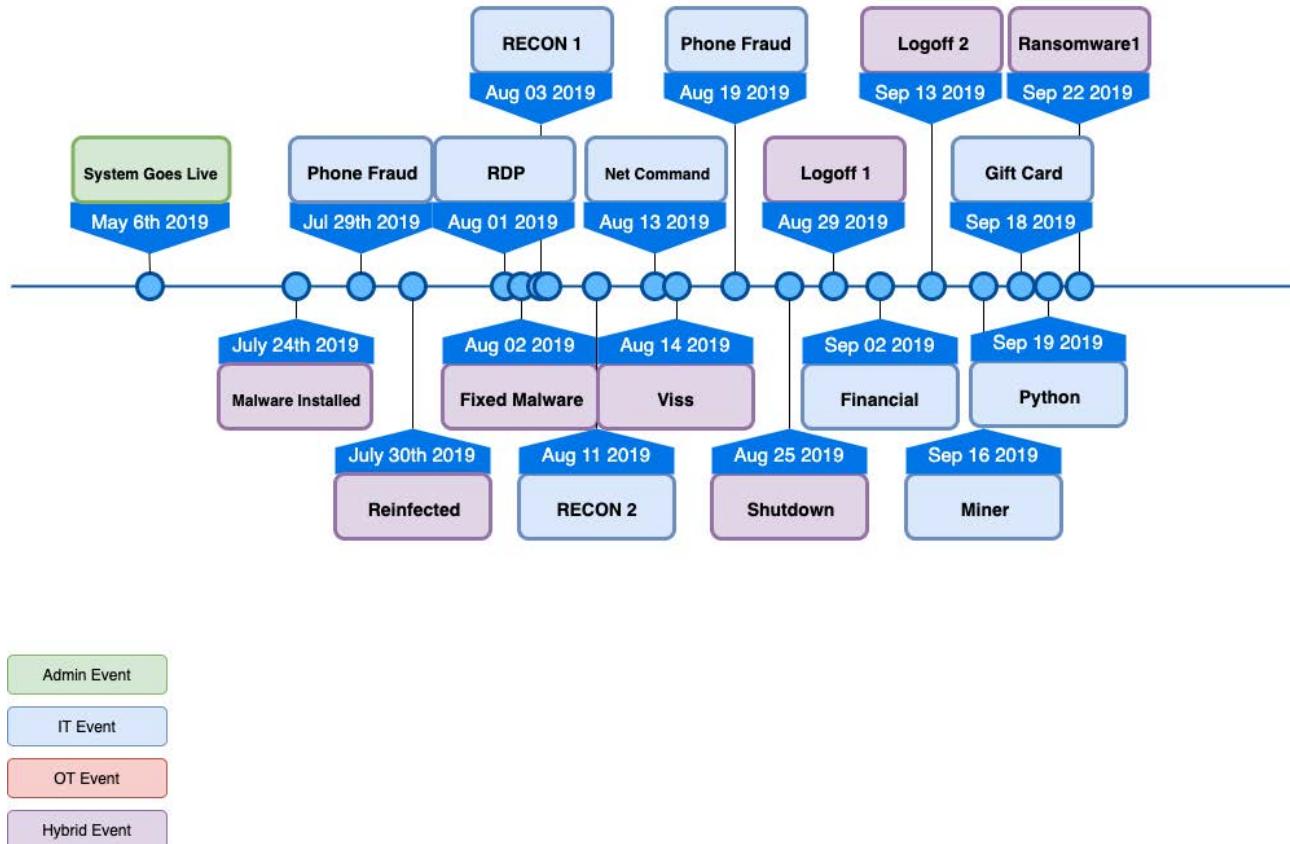


What Happened

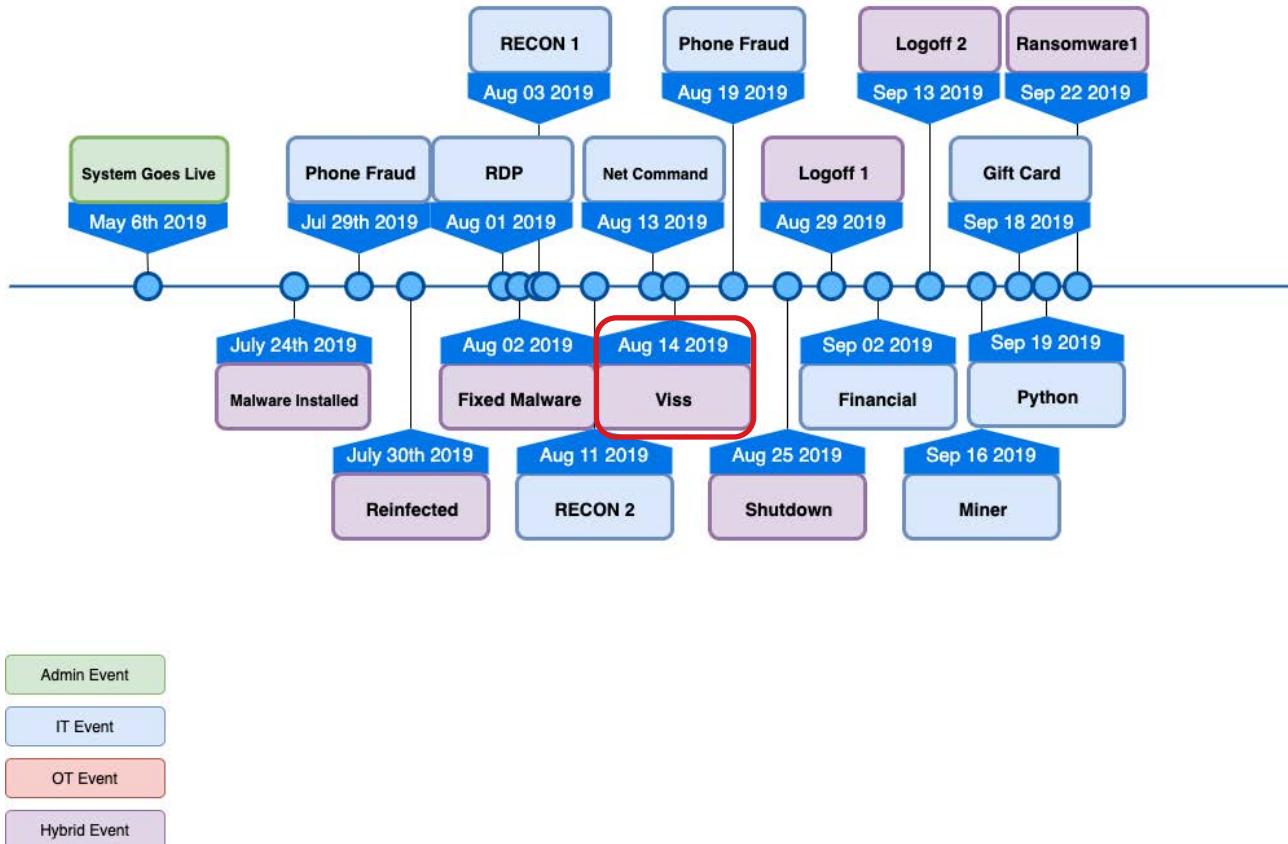


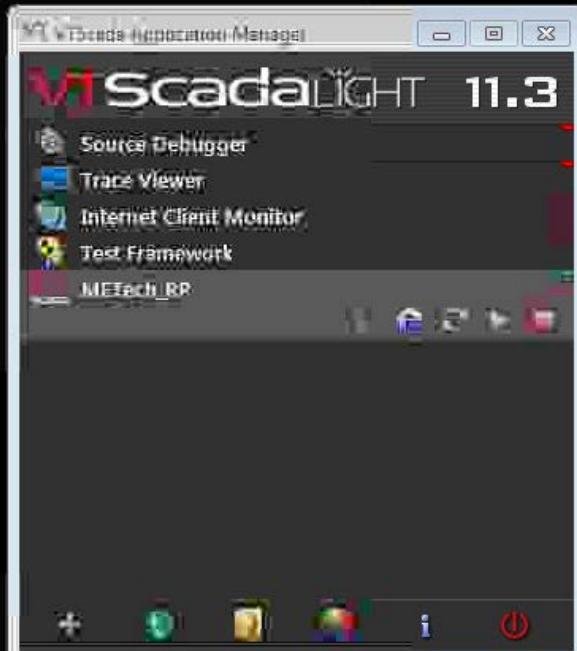


What Happened



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:



Dān Tentler @Viss

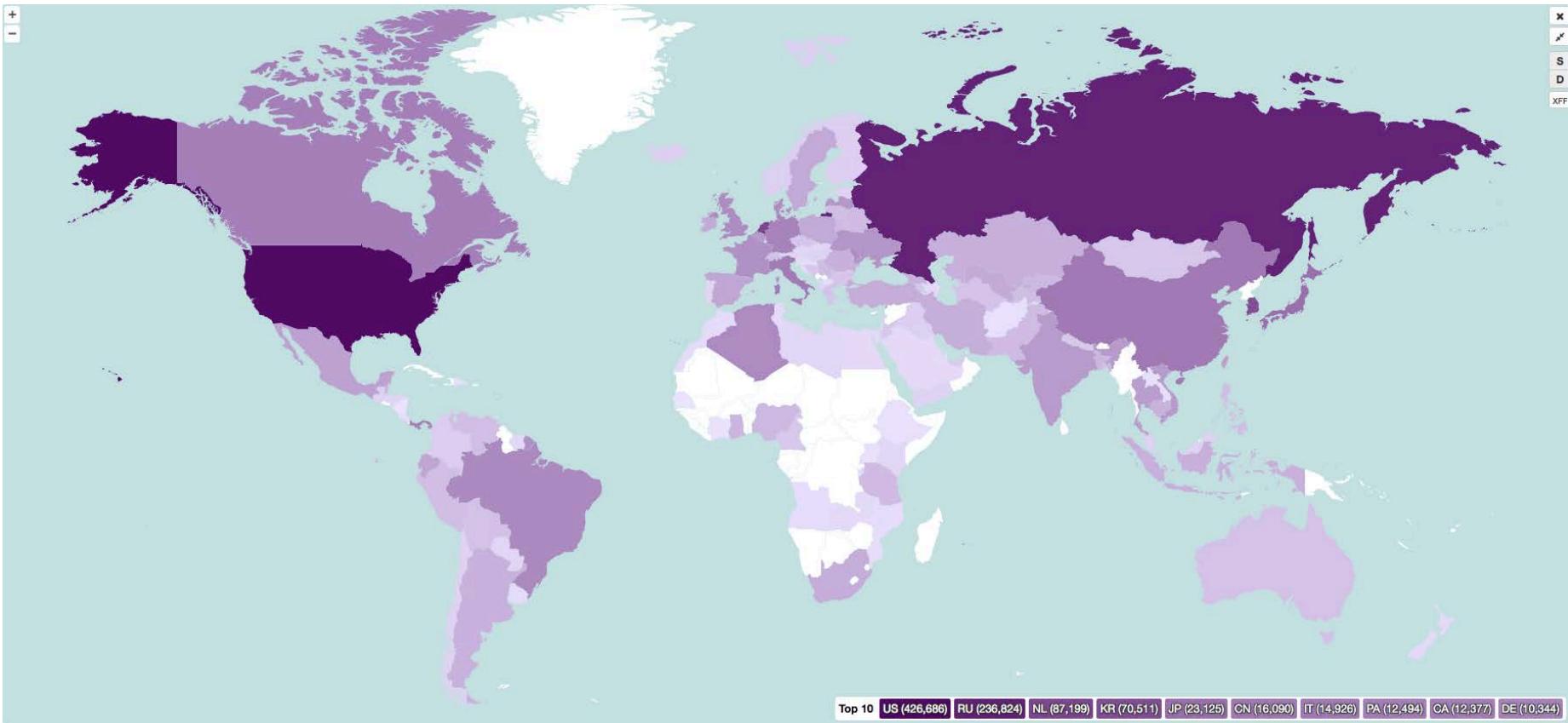
[Follow](#)



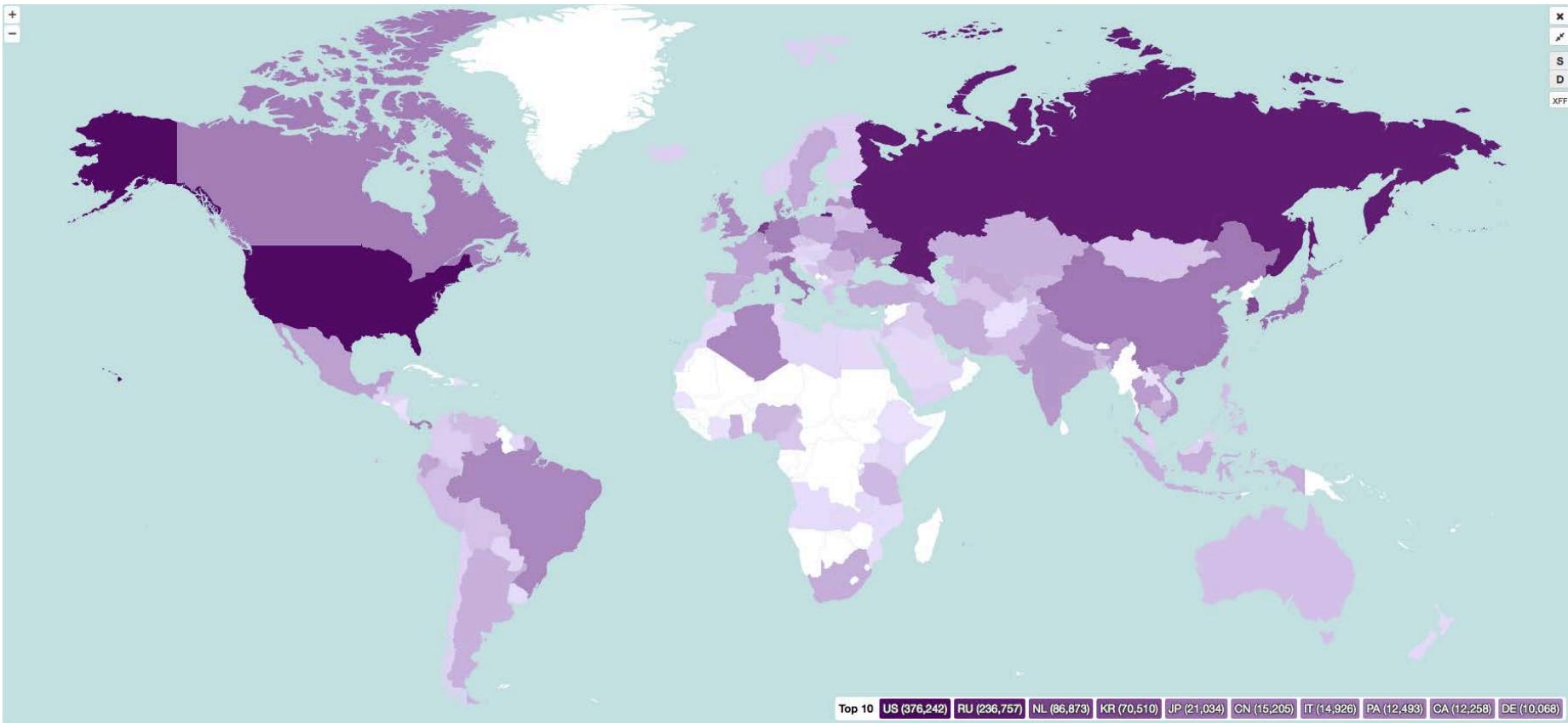
have you ever learned a thing, where the immediate outcome of that thing has been "i need rum. like right now"?

11:36 AM - 16 Aug 2019

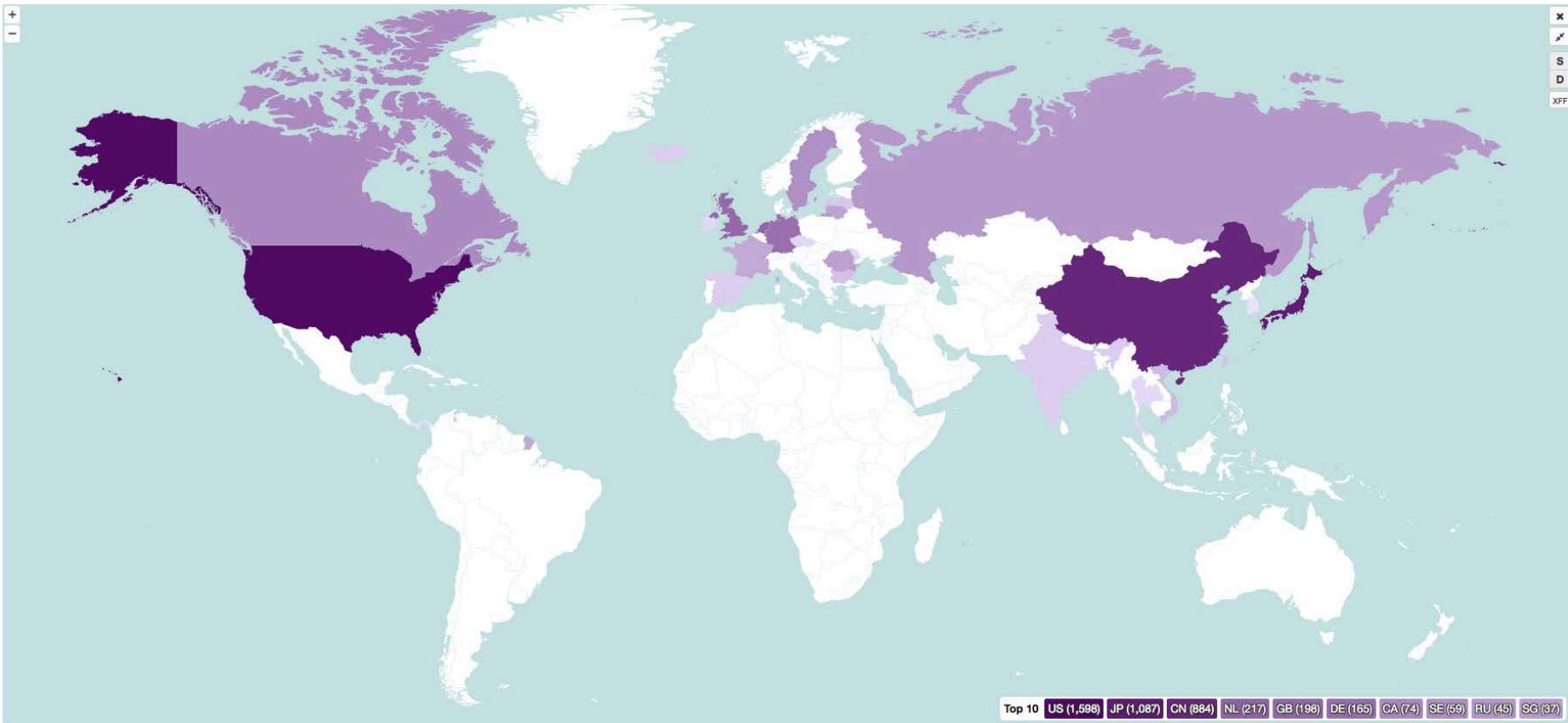
But WHO!?



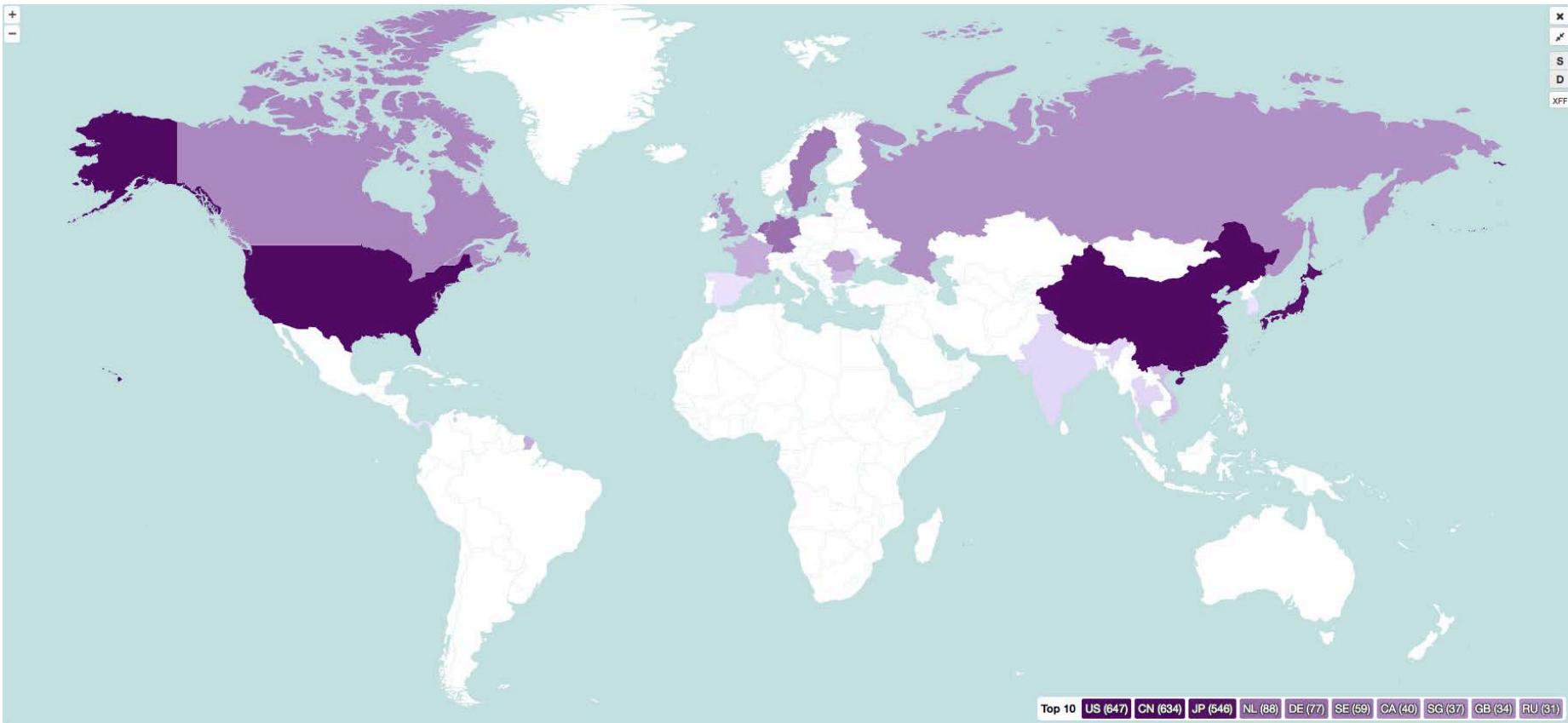
But WHO!?



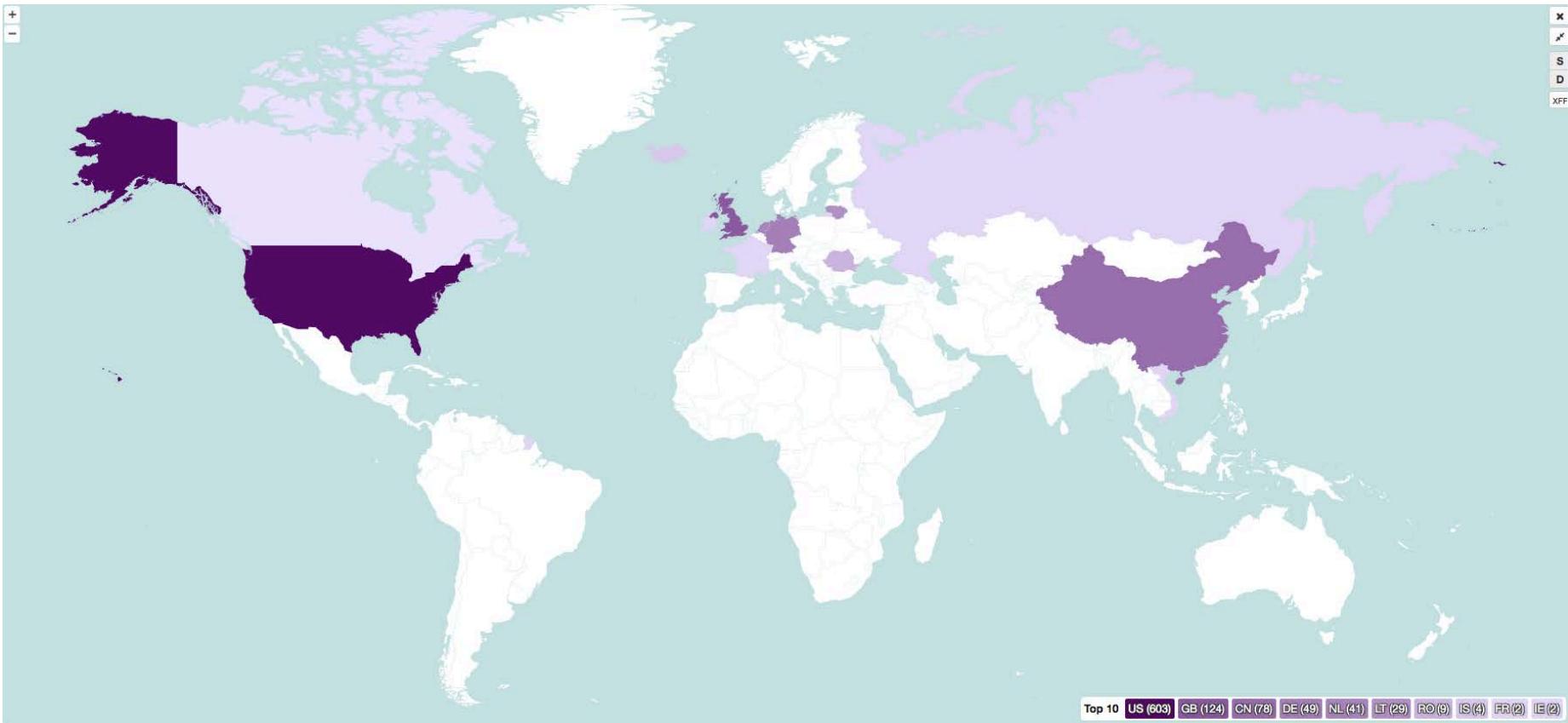
But WHO!?



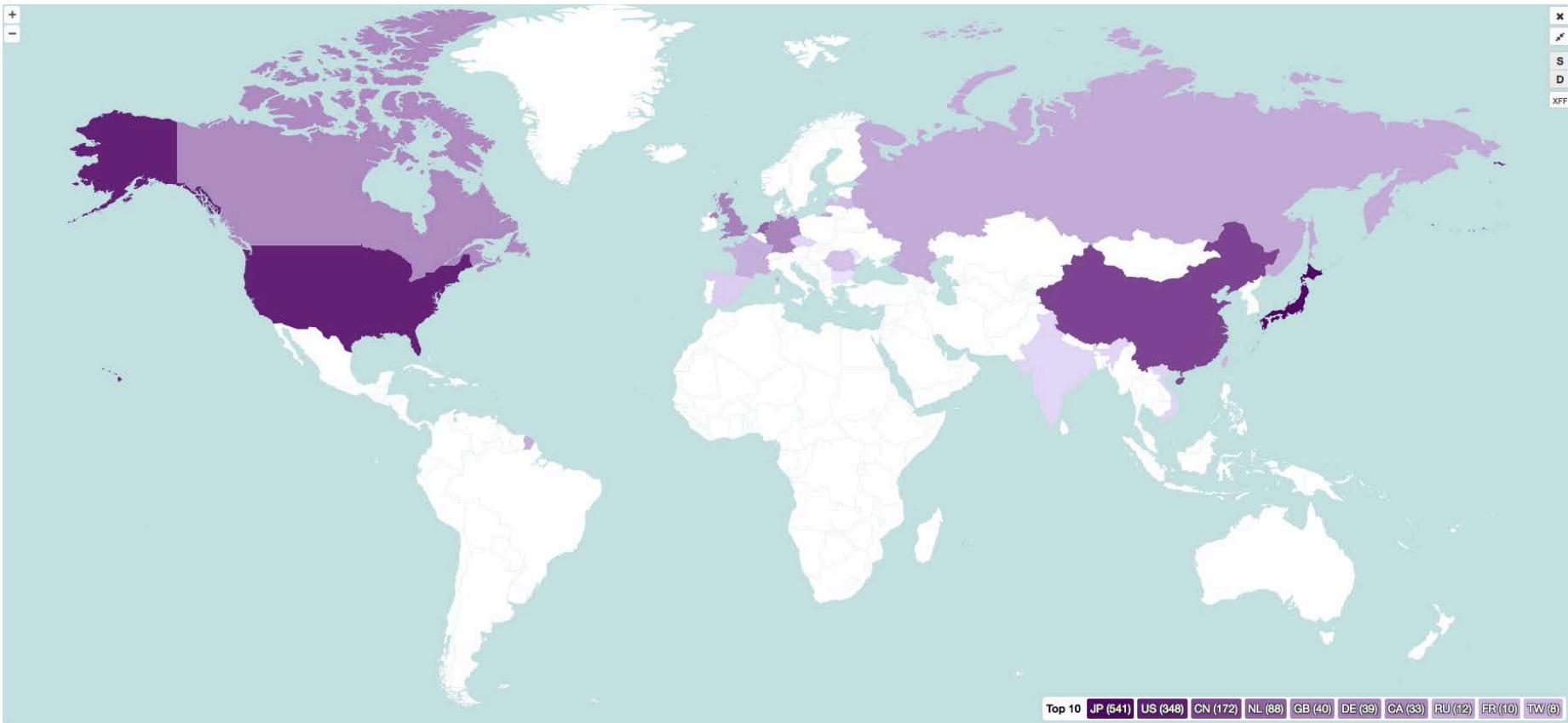
But WHO!?



But WHO!?

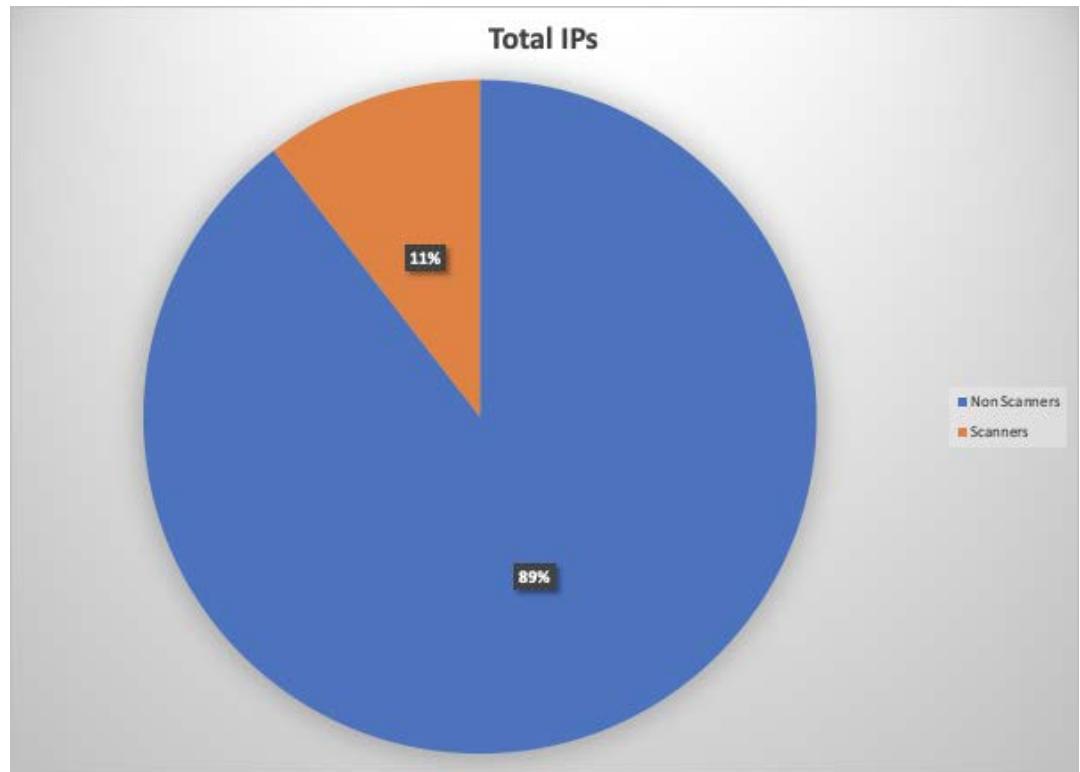


But WHO!?



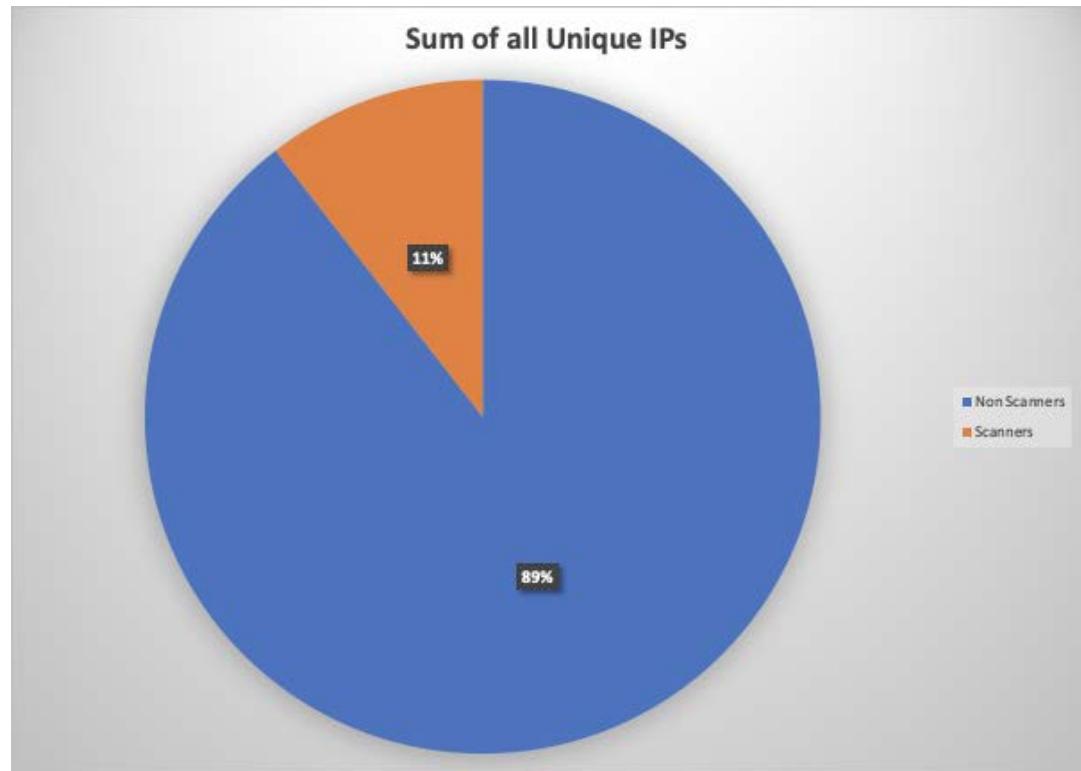
Stats: Total IPs Over Project

- 8905 Total IPs
- 592 Scanner IPs



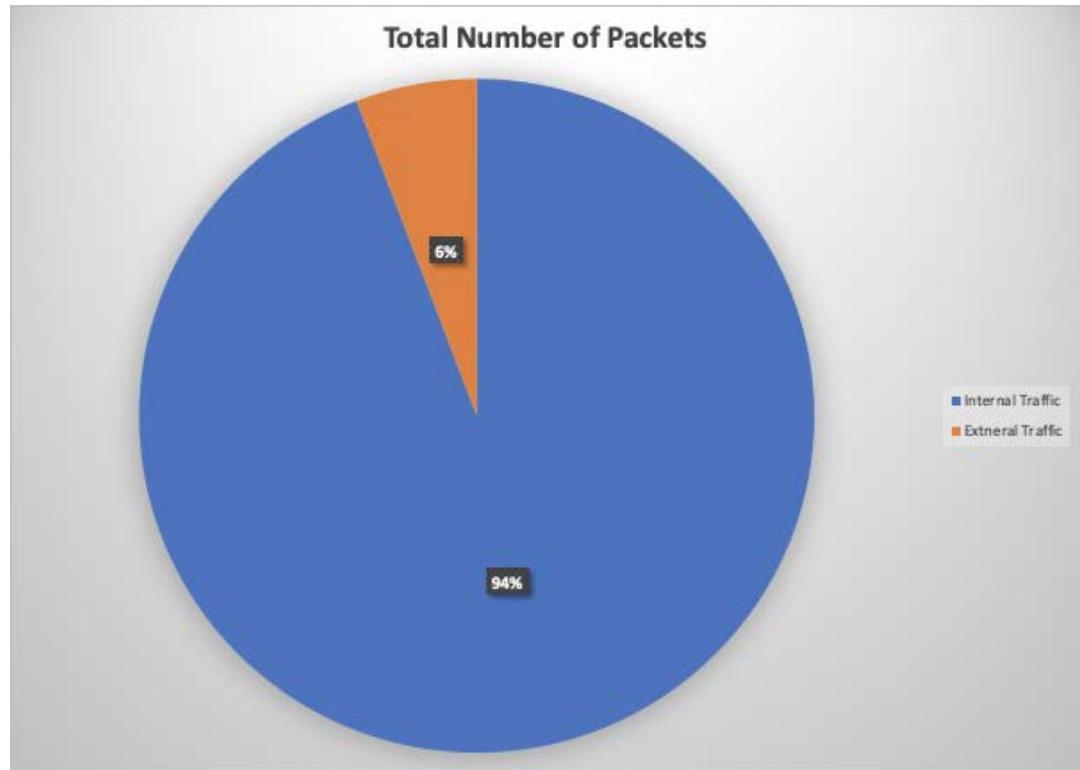
Stats: Sum of all unique IPs per day

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



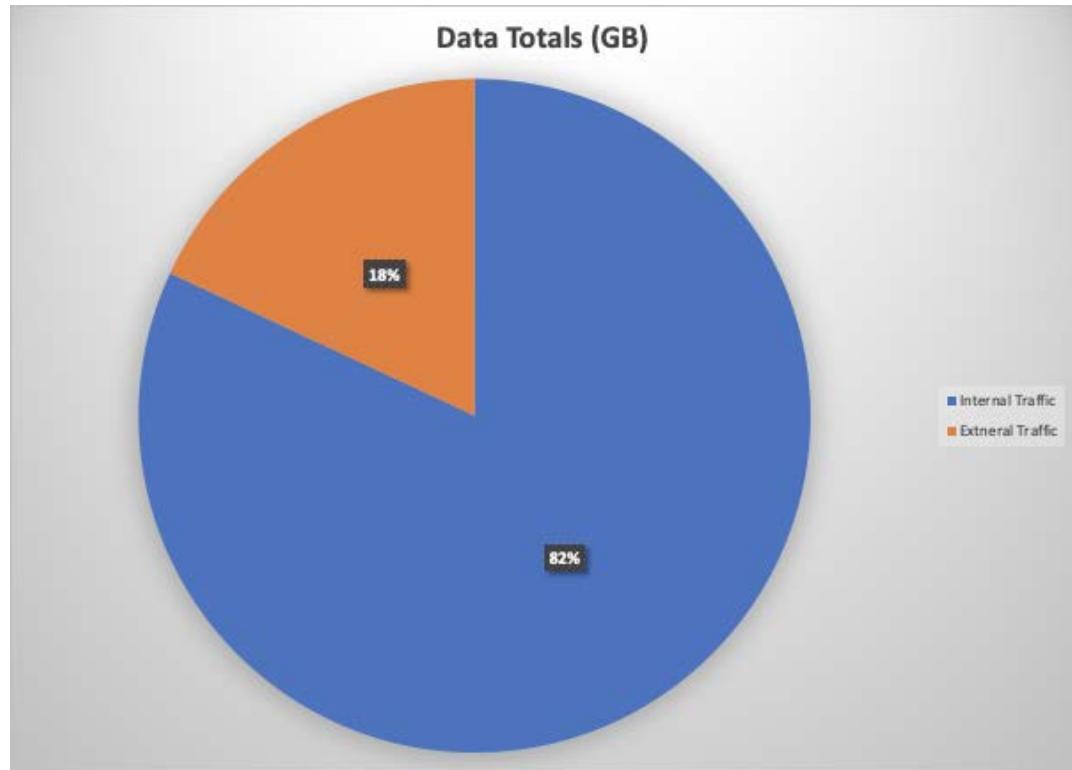
Stats: Total Packets/Bytes

- 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 Hilt, Federico Maggi, Charles Perine, Lord Remorin, Martin Rösler, and Rainer Vosseler

 research

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