RSAC Studio

Connect to Protect

Doomsday: A Probabilistic Analysis of Cyber-Dominance and Implications on Life

Jay Kaplan
CEO & Co-Founder
Synack
@JayKaplan

Julia Yrani
Strategic Alliances Lead
Synack
@Julia_Yrani

#RSAC


EMERGENCY
GOTHAM GENERAL HOSPITAL
Blu-ray.com
Source: http://moviepilot.com/posts/2277931

Source: http://www.therockatbc.com/wp-content/uploads/2013/12/Die-Hard-Wallpaper-1.jp

Source: https://www.pinterest.com/pin/390616967652102306/

Source: http://www.businesskorea.co.kr/english/news/industry/3585-power-station-mexgen-abengoa-builds-gas-combined-cycle-power-station-mexico-25-year

73%

Do not adequately protect their sensitive internal network

1/5

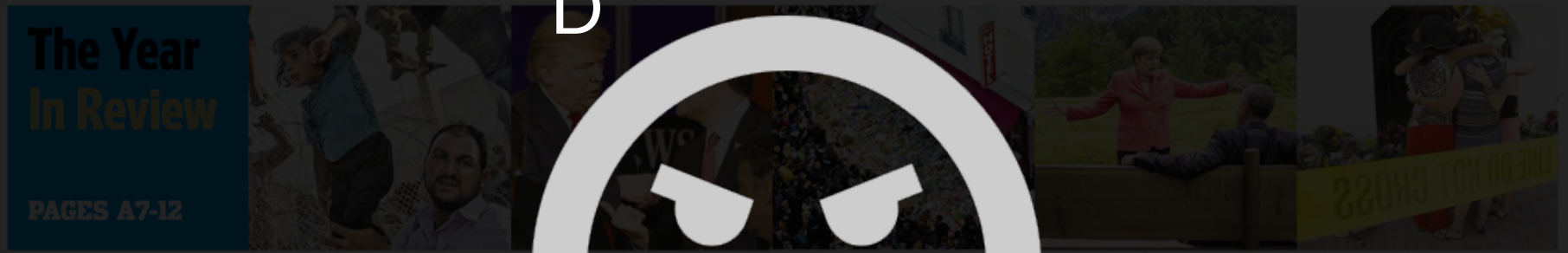
Are not confident in their ability to detect and respond to an attack

+50%

Do not have a dedicated security team

THE WALL STREET JOURNAL.

UNEXPECTE
D



DOW JONES | News Corp ★★★★★★ MO DECEMBER 21, 2015 ~ VOL. CCLXVI 46 WSJ.com ★★★★ $3.00

Last week: DJIA 17128.55 ▼ 136.66 0.8% NASDAQ 4923.08 ▼ 0.2% OXX 600 RY ▼ 1 eld 2.197% OIL $34.73 ▼ $0.89 EURO $1.0868 YEN 121.15

What's News

Business & Finance

Redstone's daughter last year rejected his $1 billion offer for her 20% stake in

DAM

Continued from Page One

against the advice of hacking gurus, increasingly brought them online in the past decade as a way to add "smarts" to U.S. infrastructure. Often, they are connected directly to office computer networks, which are notoriously easy to breach.

These systems control the flow in pipelines, the movements of drawbridges and water

ste d caused
dam last furnac

Th other govern
ments i pons, too. In
the early dent Ba-
rack Obama Israel used a so puter program to d fuges at Iran's nuclear facil Natanz, according to former U.S. officials.

The Department of Homeland Security has publicly warned industrial companies since 2011 to be more judicious in how they connect these systems to the In-

challen
digital defen
of cyberwar. Ami
three-letter agen ar
Internet add ules
governi urveil-
at first
to determine
e hackers had infiltrated, three of the people familiar with the incident said.

Hackers are believed to have gained access to the dam through a cellular modem, according to an unclassified Homeland Security summary

net, looking for vulnerable U.S. industrial-control systems. The hackers appeared to be focusing on certain Internet addresses, according to the people.

Analysts at the National Security Agency relayed these addresses to Homeland Security, the people said.

Eventually, investigators linked one address to a "Bowman" dam. But there are 31 dams in the U.S. that include the word "Bowman" in their name, according to U.S. Army

Iranian Hacking Raises U.S. Alarm

By Danny Yadron

Source: http://www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779/op-1

Source: http://obrazky.4ever.sk/umenie/film-a-serial/jaws-186381

0 Regulation

Source: http://quotesgram.com/the-office-michael-scott-quotes/

04.01.2016

THE FOLLOWING PREVIEW HAS BEEN APPROVED TO

ACCOMPANY THIS FEATURE

NERC CRITICAL INFRASTRUCTURE PROTECTION (CIP) -014 / CIP VERSION 5

www.filmratings.com

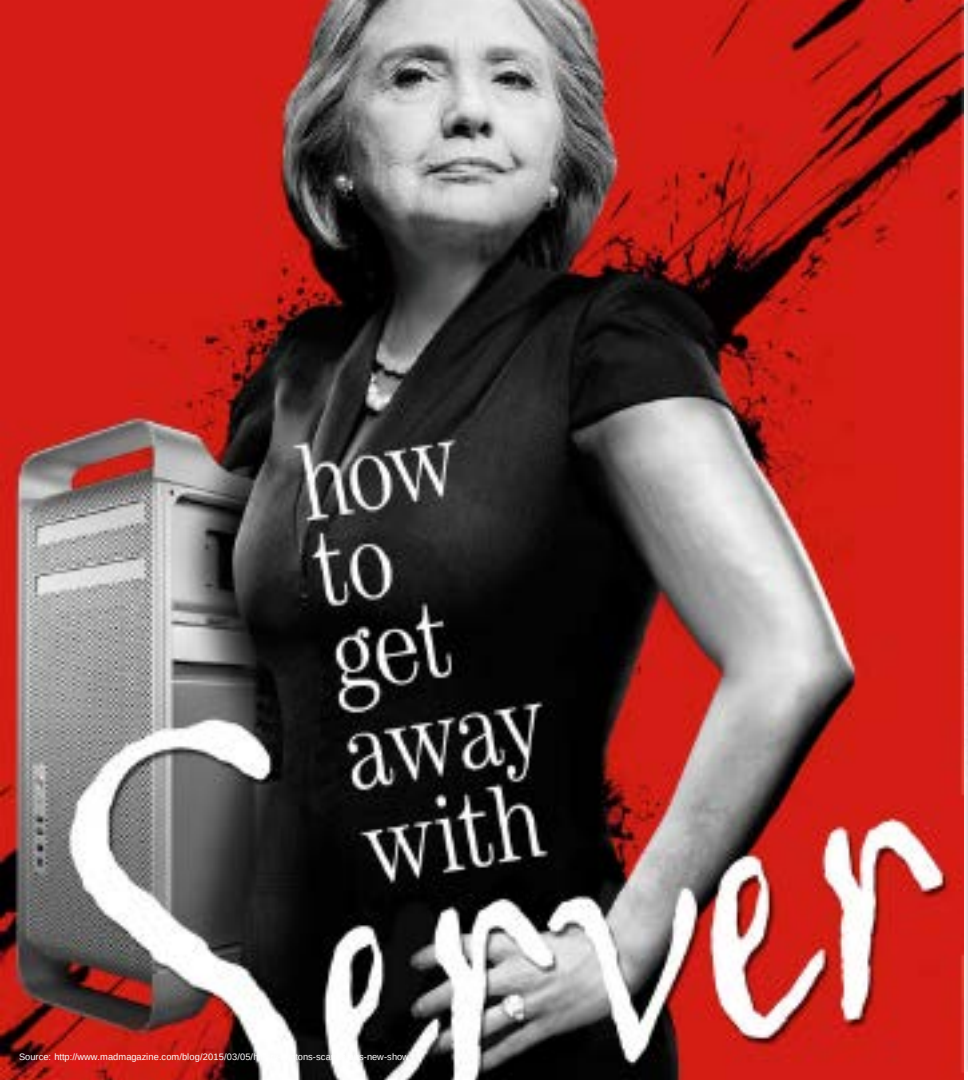
www.mpaa.org

Cyber Profile

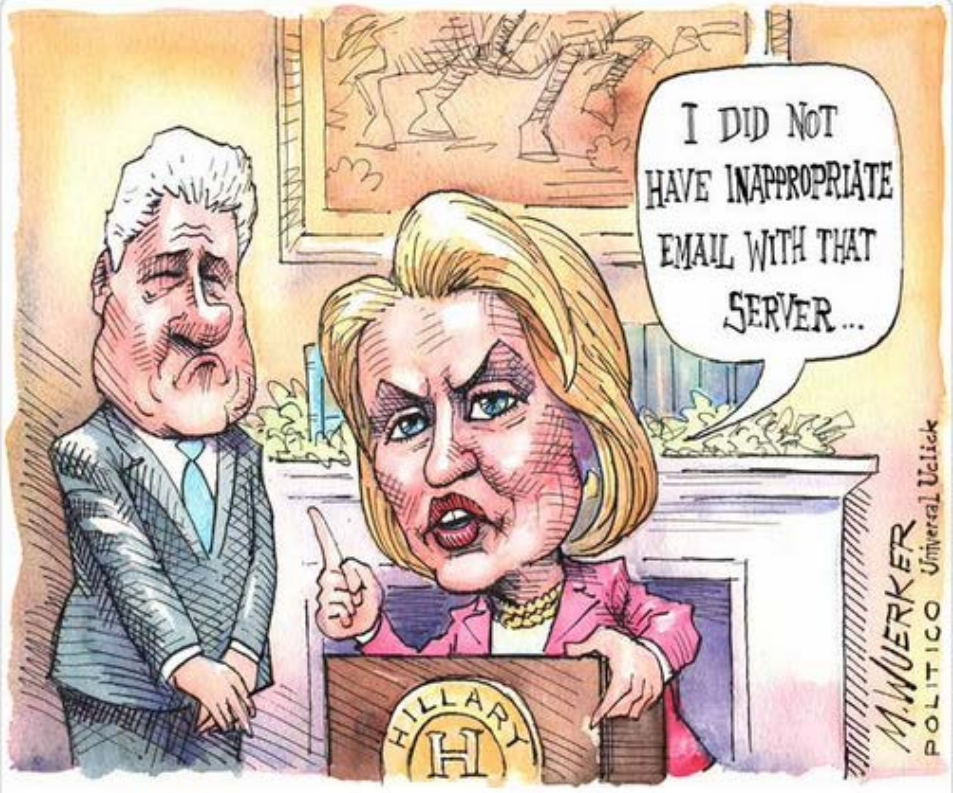
Kyrz Liberation Army (KLA) – Cyber Unit

- 215 Officers, Specialization in SCADA
- Motive: Prepositioning for International Conflict
- Capabilities: Stockpile of 0-Day Exploits,
- Home-grown Stealth Implants


55%
No Dedicated Security Team
98%
Dedicated Security Teams in the F500



Source: http://www.madmagazine.com/blog/2015/03/05/[illegible]ons-sca[illegible]e-new-show



POLITICO
@politico

Follow

.@wuerker's latest cartoon on Hillary Clinton's email controversy: politi.co/1BtyFZp

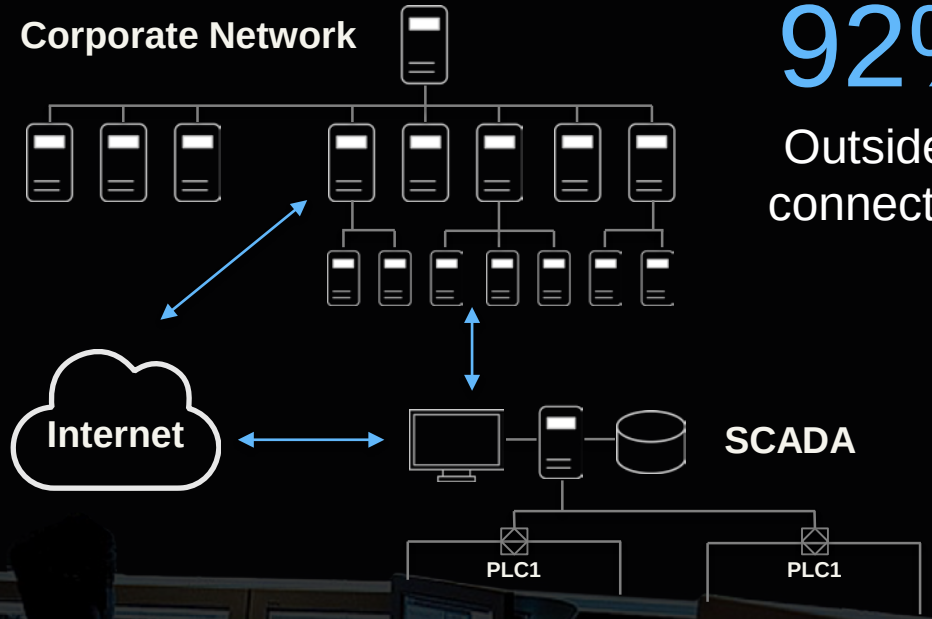
1:19 PM - 10 Mar 2015

239 RETWEETS 160 FAVORITES

Target Profile

Energy Utility Company

- Powers 50% of Tri-State Area
- Over 200 Employees
- Security Team: 2
- Network Diagram



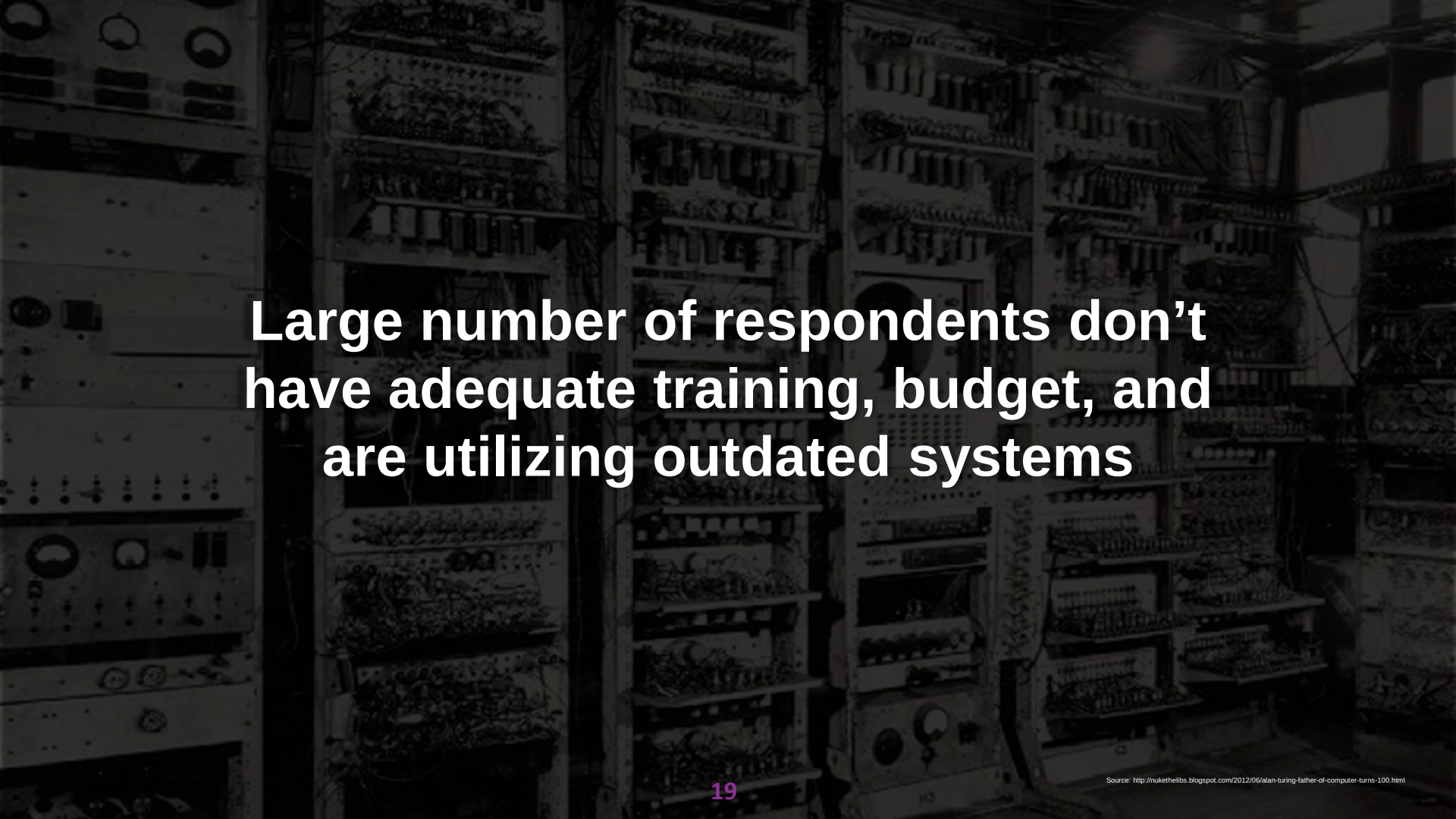
92%

Outside-in connectivity

82% admit to requiring manual intervention to stop an attack

Source: http://www.wnd.com/2014/08/expert-imminent-isis-threat-to-u-s-power-grid/

Source: http://www.fastcoexist.com/tag/nuclear-power



Large number of respondents don’t have adequate training, budget, and are utilizing outdated systems

Source: http://nukethelibs.blogspot.com/2012/06/alan-turing-father-of-computer-turns-100.html

50% agree that process control network are vulnerable to cyber threats

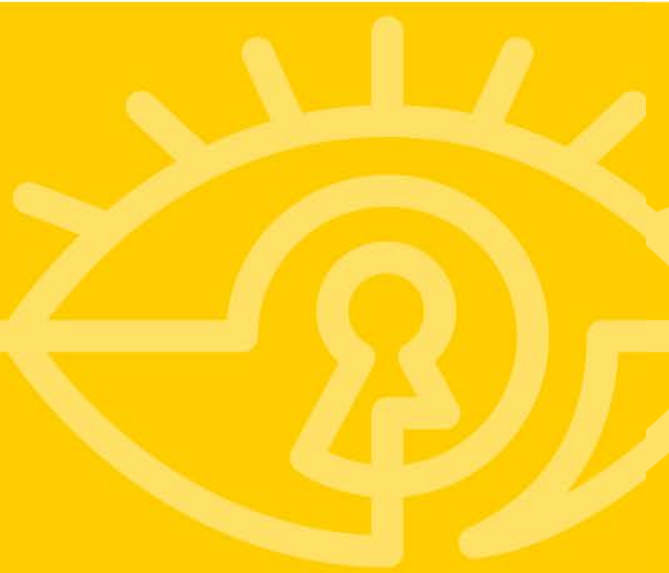
75% are allocating little to no budget on information security initiatives in 2016

Source: https://www.youtube.com/watch?v=6SOluodeJ7s

Source: http://yournewswire.com/nuclear-war-was-averted-in-1999-by-clintons-national-security-adviser/

Source: http://www.myspecialneedsnetwork.com/profiles/blogs/spring-roars-into-summer-with

Source: http://Source: http://www.zdnet.com/article/isps-and-rights-holders-release-draft-anti-piracy-code/



Thank You

RSAC Studio

Connect to Protect

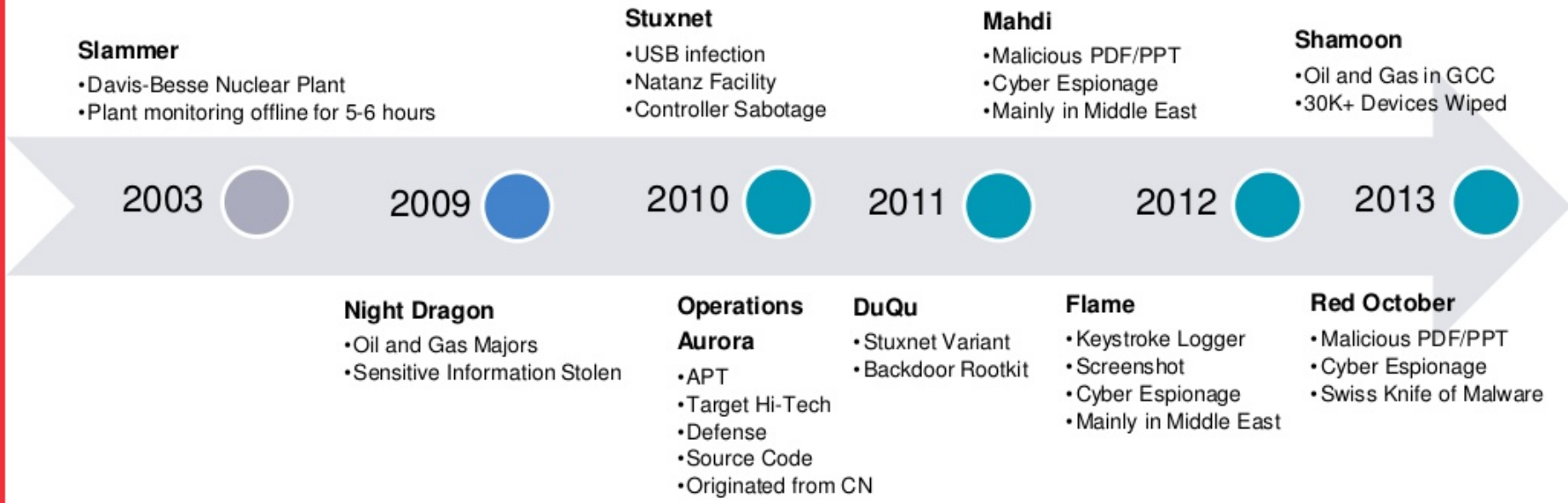
Honey, I Hacked the SCADA!: Industrial CONTROLLED Systems!

James Heyen
Systems Engineer
ViaSat - Secure Network Systems
@jlheyen

#RSAC

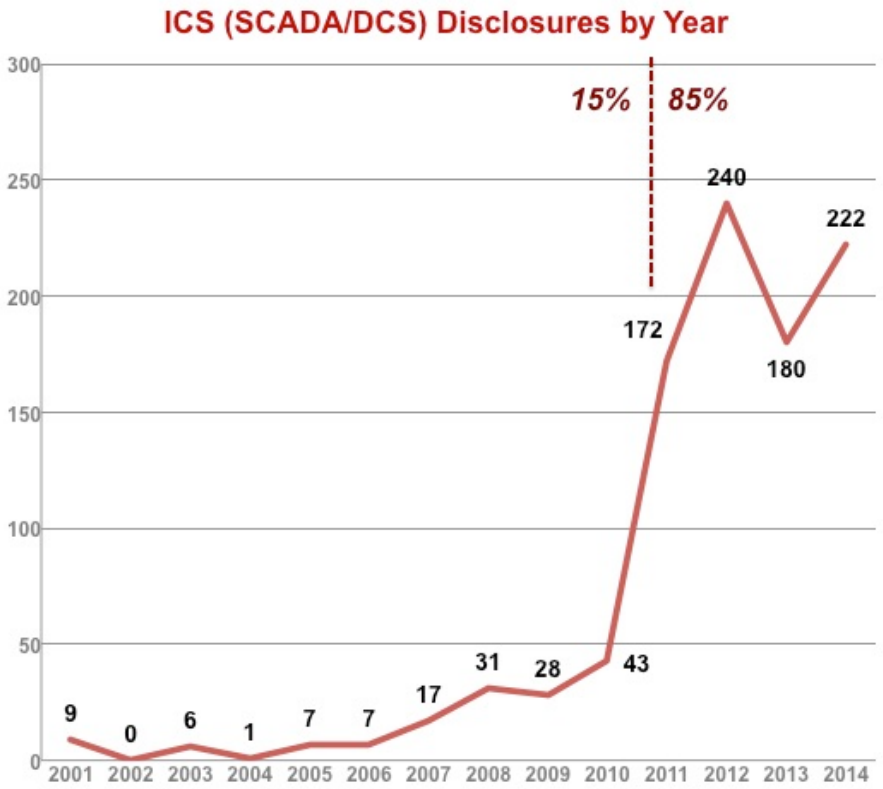
August 14, 2003 - The Saga begins…..

Timeline – Industrial Malware



National Oil Company Conference 2014 - Evolving Cyber Security - A Wake Up Call....

Full Disclosure



http://www.scadahacker.com

SCADA/ICS System Vulnerabilities

- What's connected?
- Few testing environments
- Compliance ≠ protection
- Legacy equipment
- Hacker highways
- Goodbye 'security by obscurity'

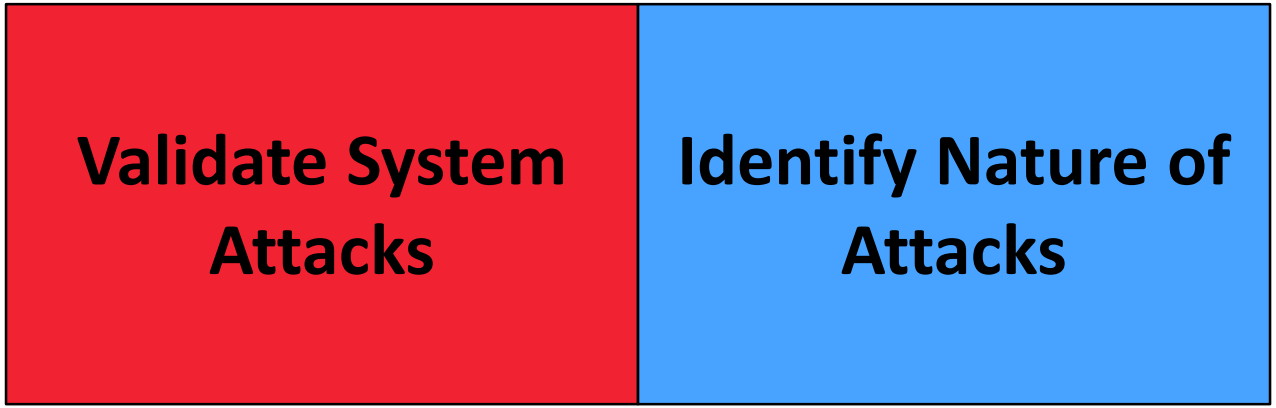
SCADA Operational Intelligence Program 2014-2015

ViaSat

SCADA Operational Intelligence Program 2014-2015

Validate System Attacks

SCADA Operational Intelligence Program 2014-2015



SCADA Operational Intelligence Program 2014-2015

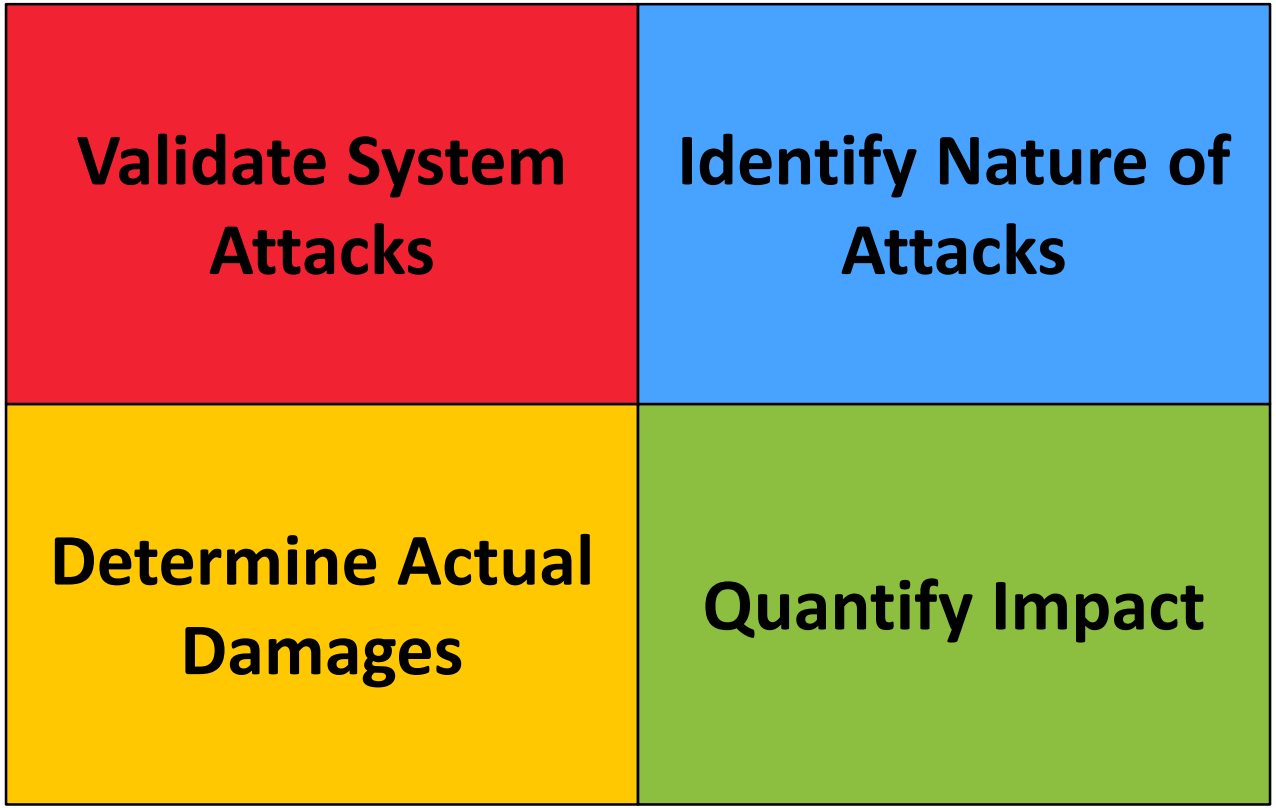
Validate System Attacks

Identify Nature of Attacks

Determine Actual Damages

ViaSat

SCADA Operational Intelligence Program 2014-2015



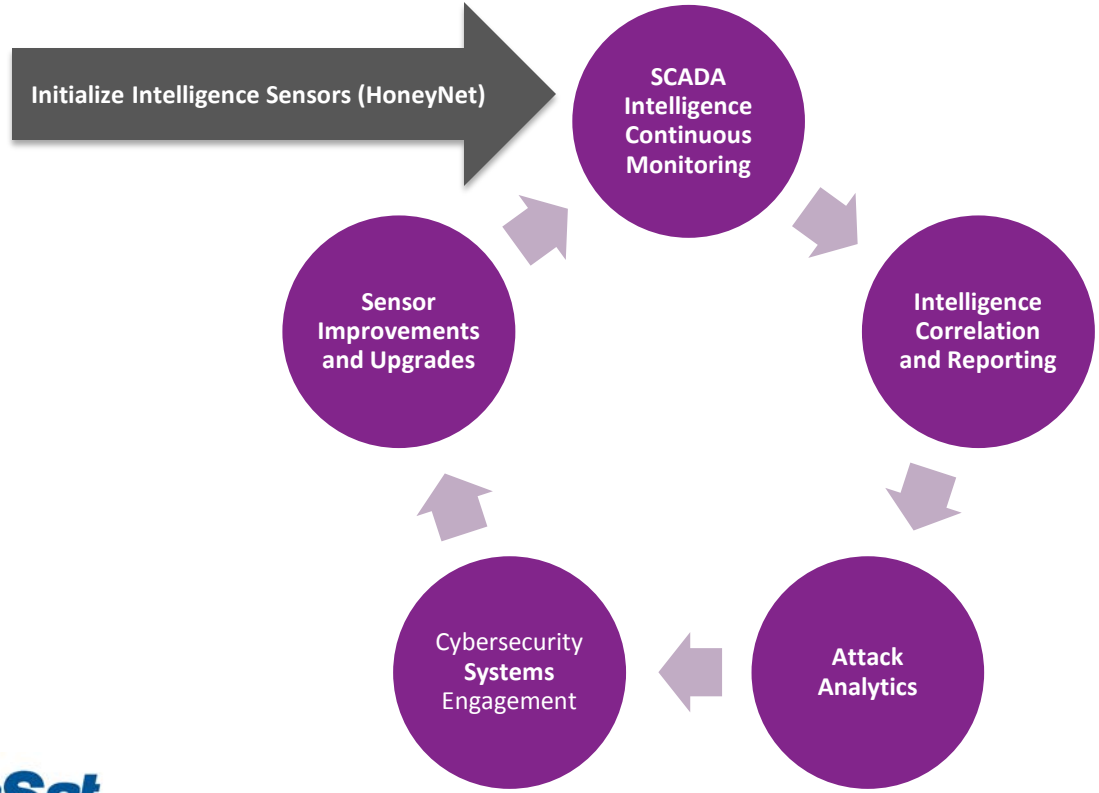
Requirements

- Real system appearance
- Interaction levels
- Attacker profile information
- FPC
- Tor or Not to Tor?

PASTEBIN

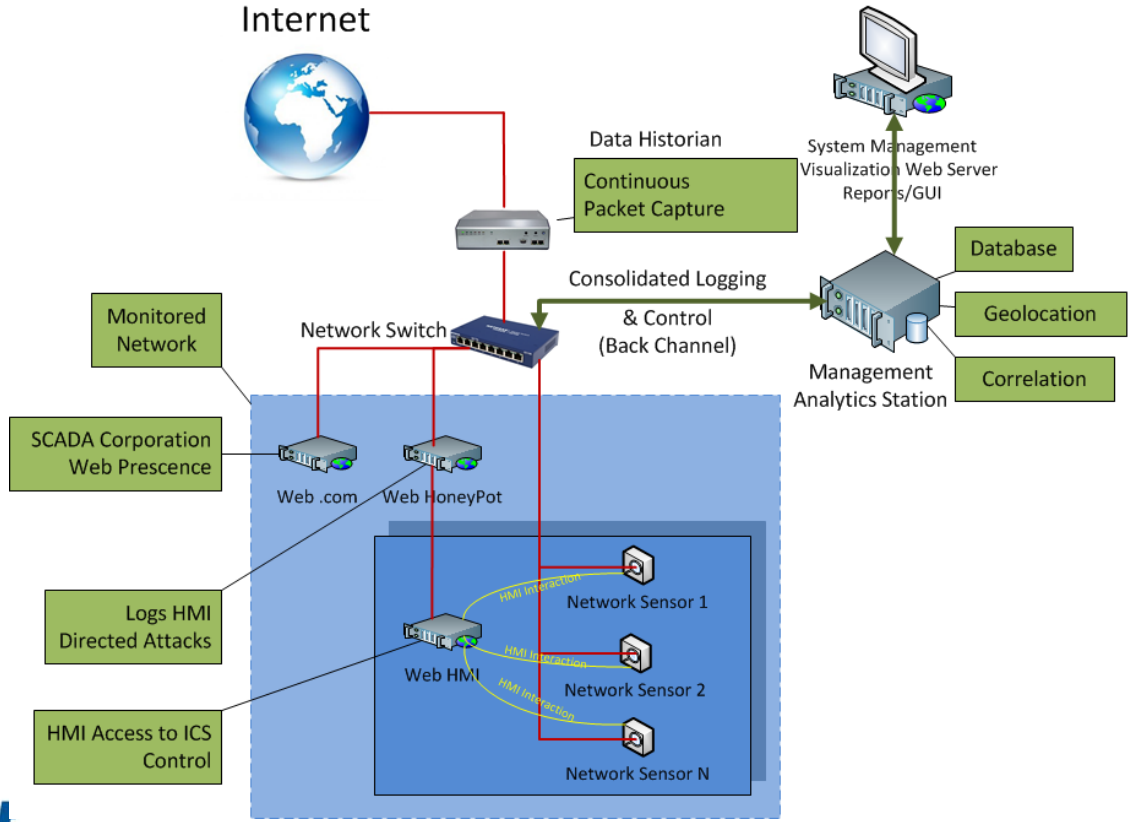
Tor

SCADA Intelligence Gathering Cycle



Myth or Reality?

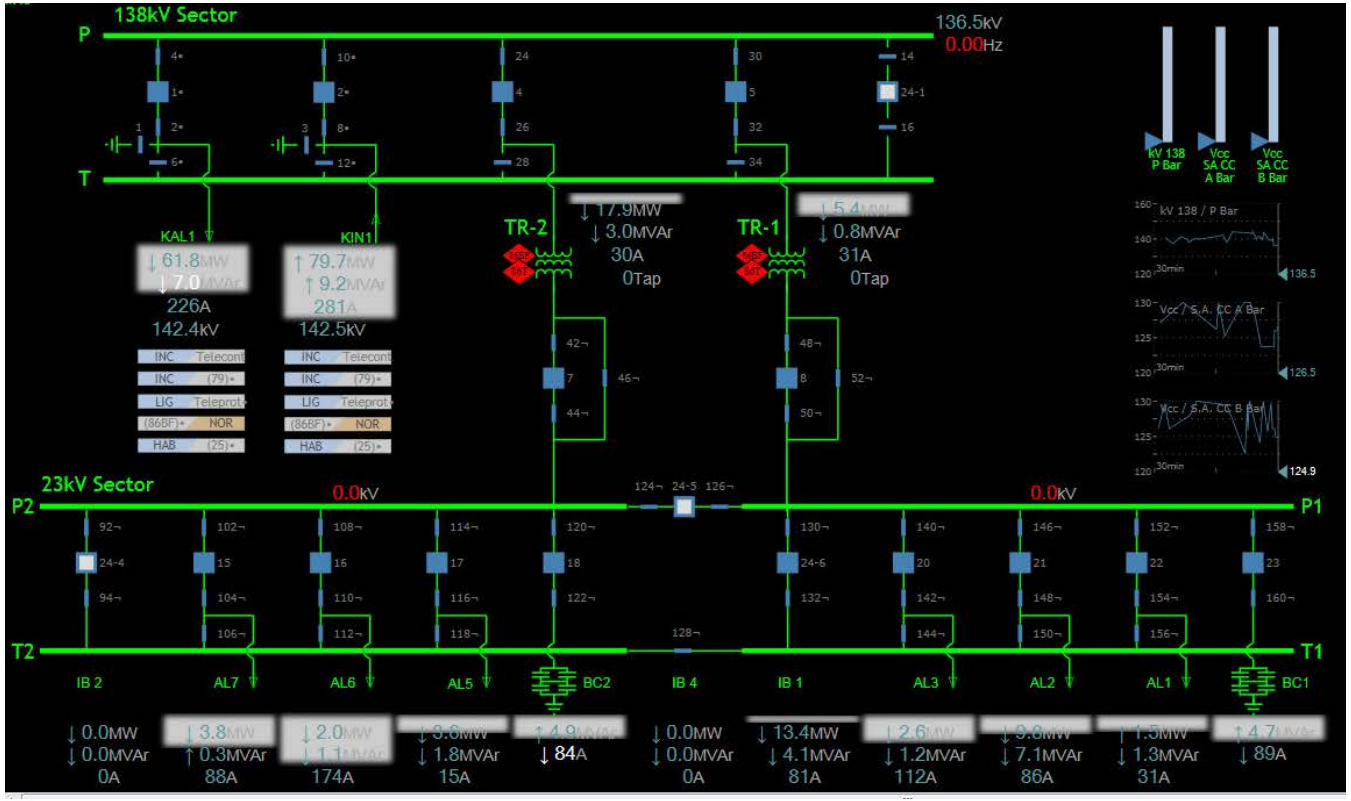
SCADA Intelligence System Architecture



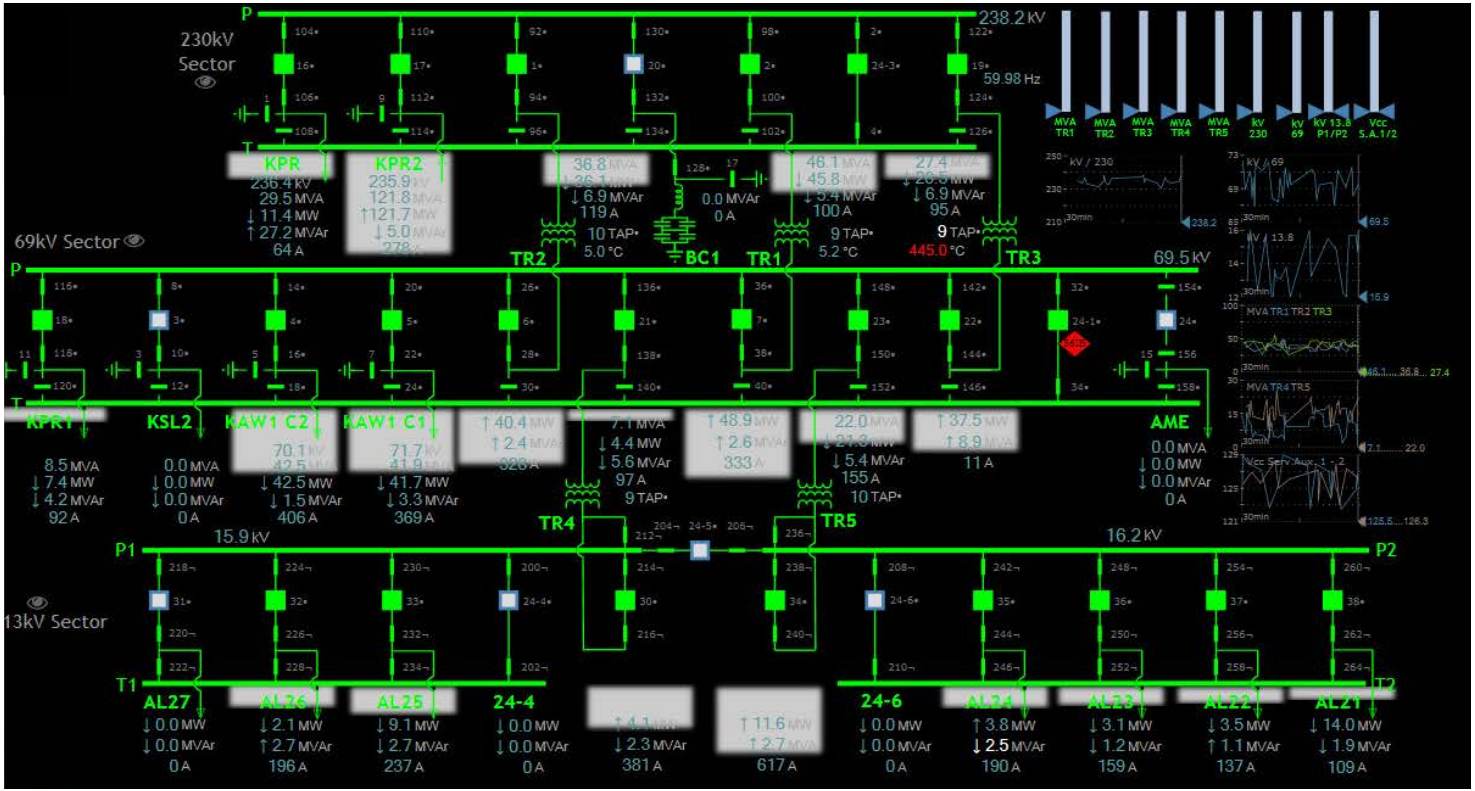
Low Interaction – plcscan.py


```
Scan start...
       .31.114:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                    :  v.0.0                    (00000000000000000000000000000000000000000000000000)
  Name of the PLC           : Power Grid 2              (506f7765722047726964203200000000000000000000000000000000000000000000)
  Name of the module        : Siemens, SIMANTIC S7-300  (5369656d656e732c2053494d414e5449432053372d33303000000000000000000000)
  Plant identification      :                           (43616c69666f726e69612053636164610000000000000000000000000000000000000000)
  Copyright                 : Original Siemens Equipment (4f726967696e616c205369656d656e732045717569706d656e74000000000000)
  Serial number of module   : 94233102                  (39343233333130320000000000000000000000000000000000000000000000000000)
  Module type name          : IM351-8 PN/DP CPU         (494d3335312d3820504e2f445020435055000000000000000000000000000000)
  OEM ID of a module        :                           (00000000000000000000000000000000000000000000000000000000000000000000)
  Location designation of a module:                                 (00000000000000000000000000000000000000000000000000000000000000000000)
       .31.114:502 Modbus/TCP
  Unit ID: 0
    Device:
  Unit ID: 255
    Device:
Scan complete
```

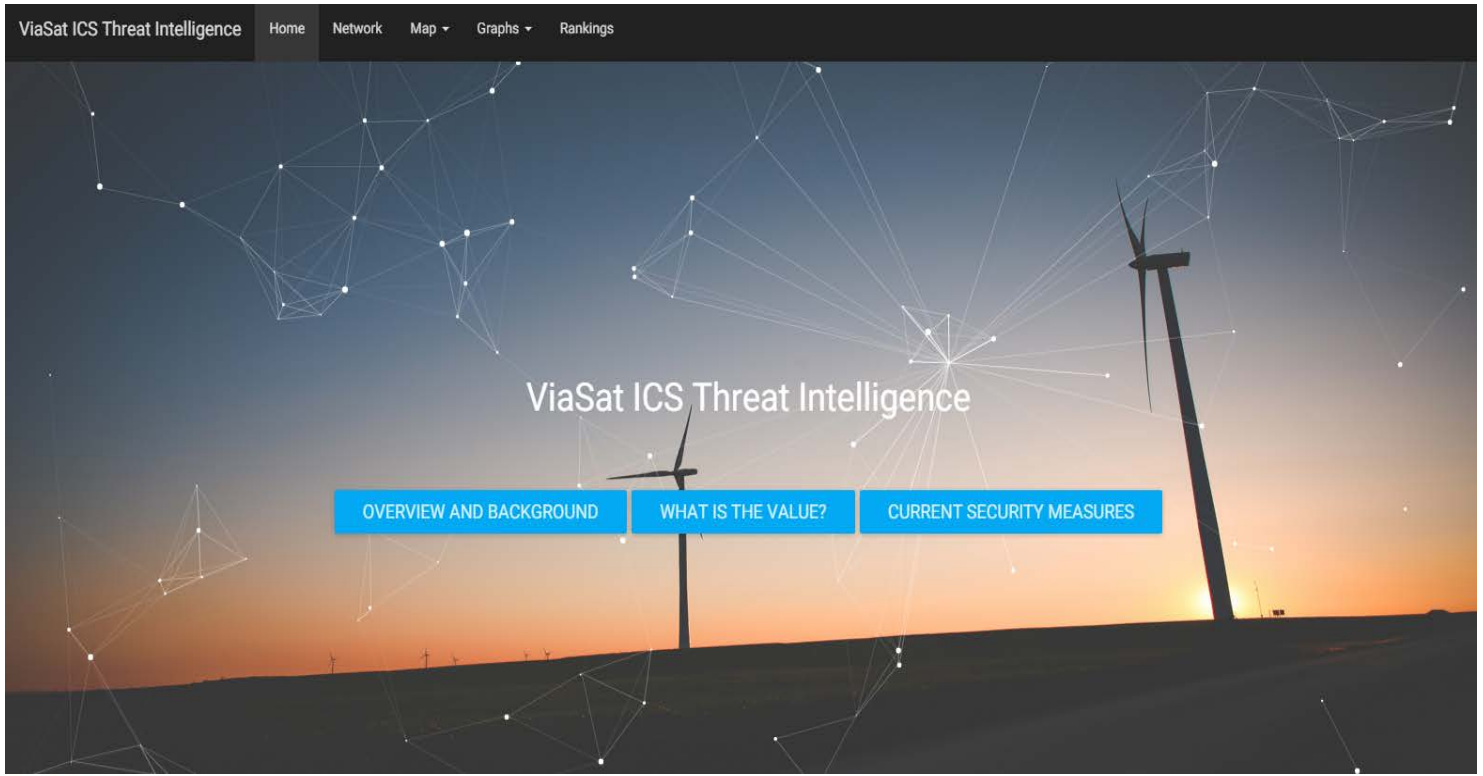
Medium and High Interaction



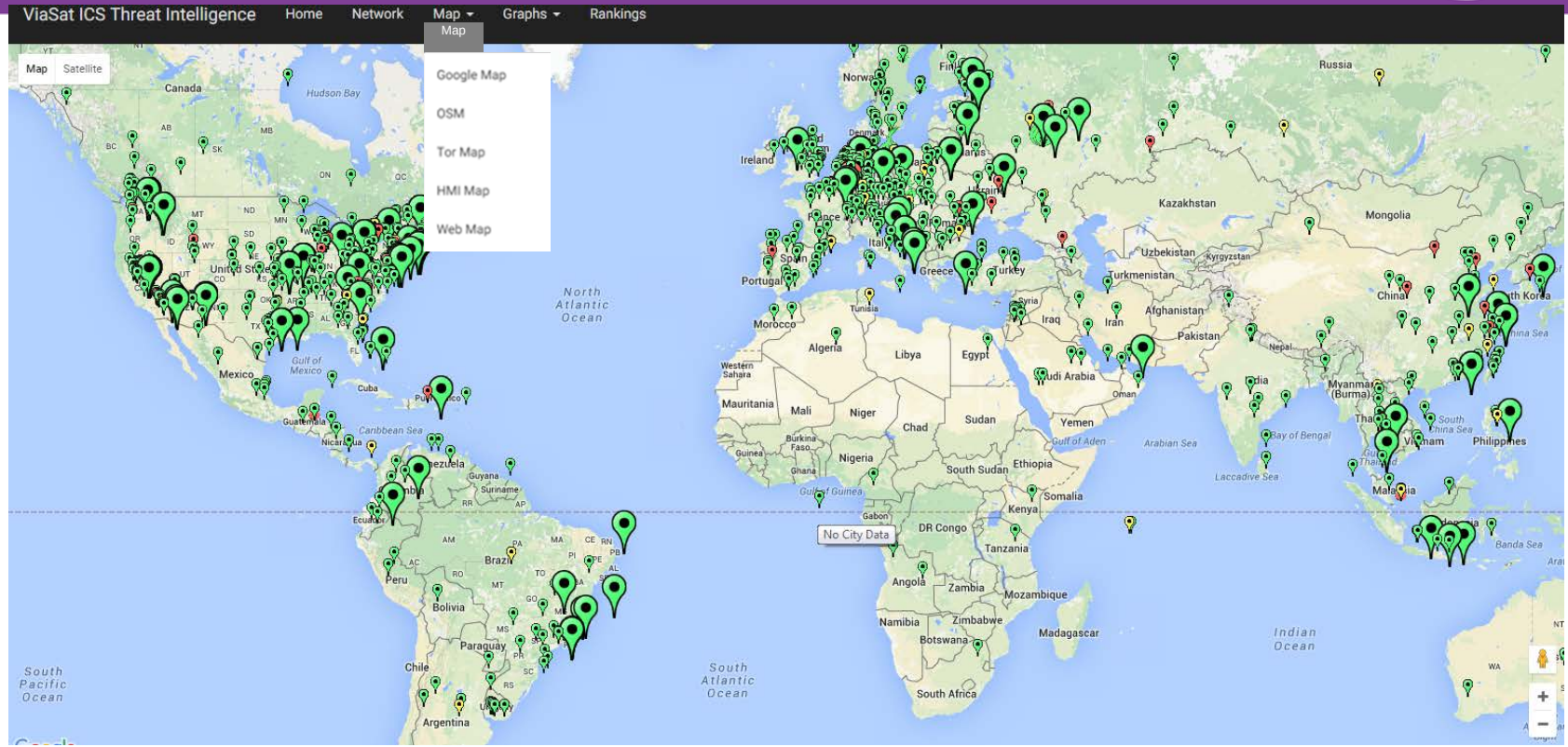
Medium and High Interaction



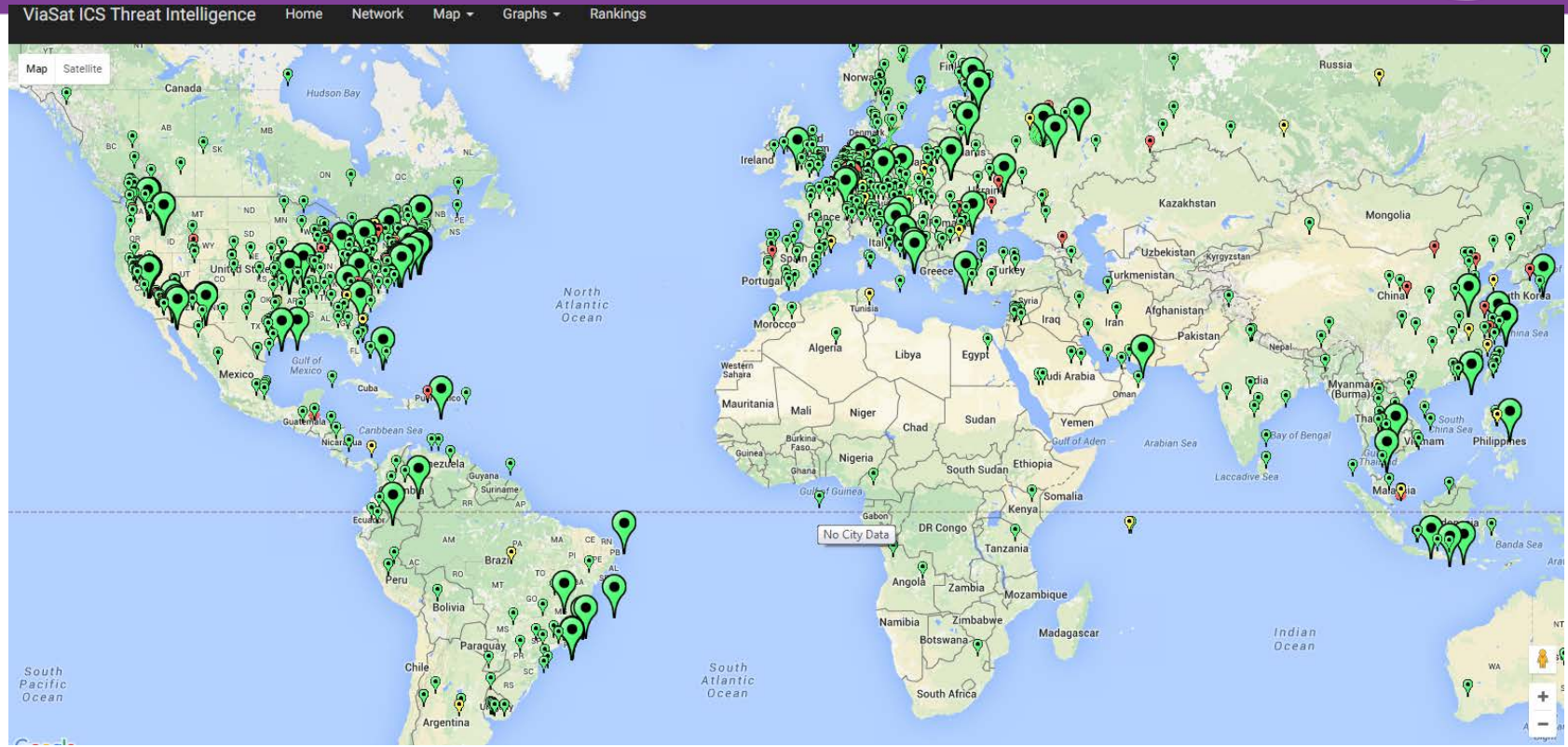
And we have liftoff....



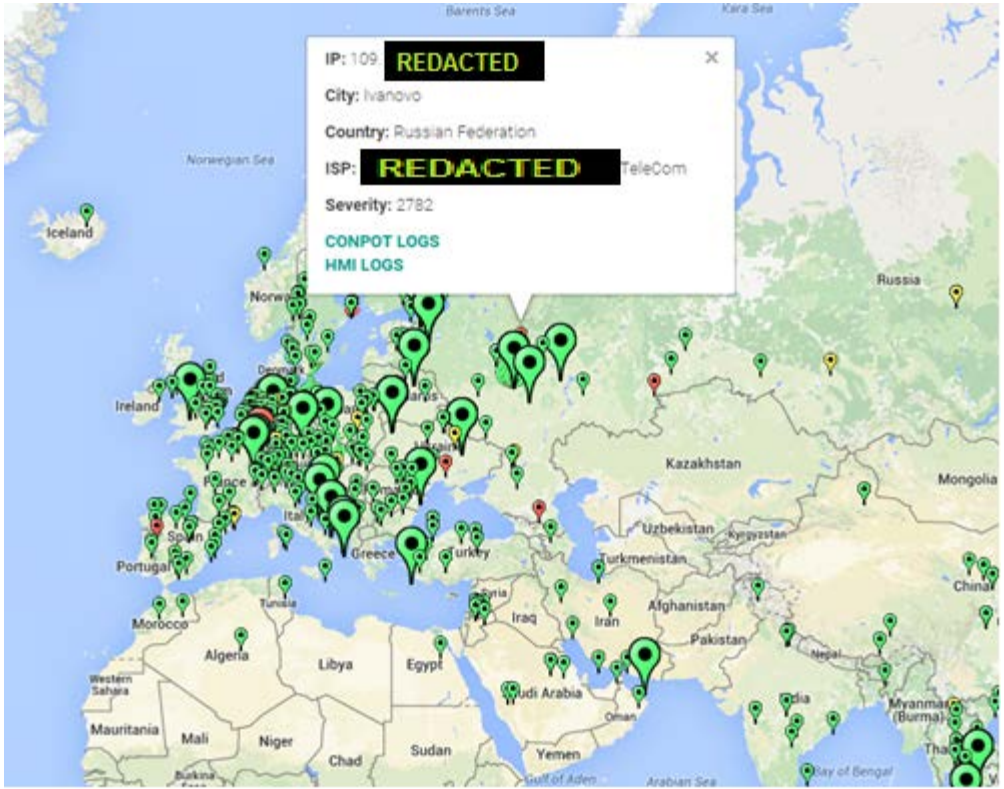
GeoLocation, GeoLocation, GeoLocation!



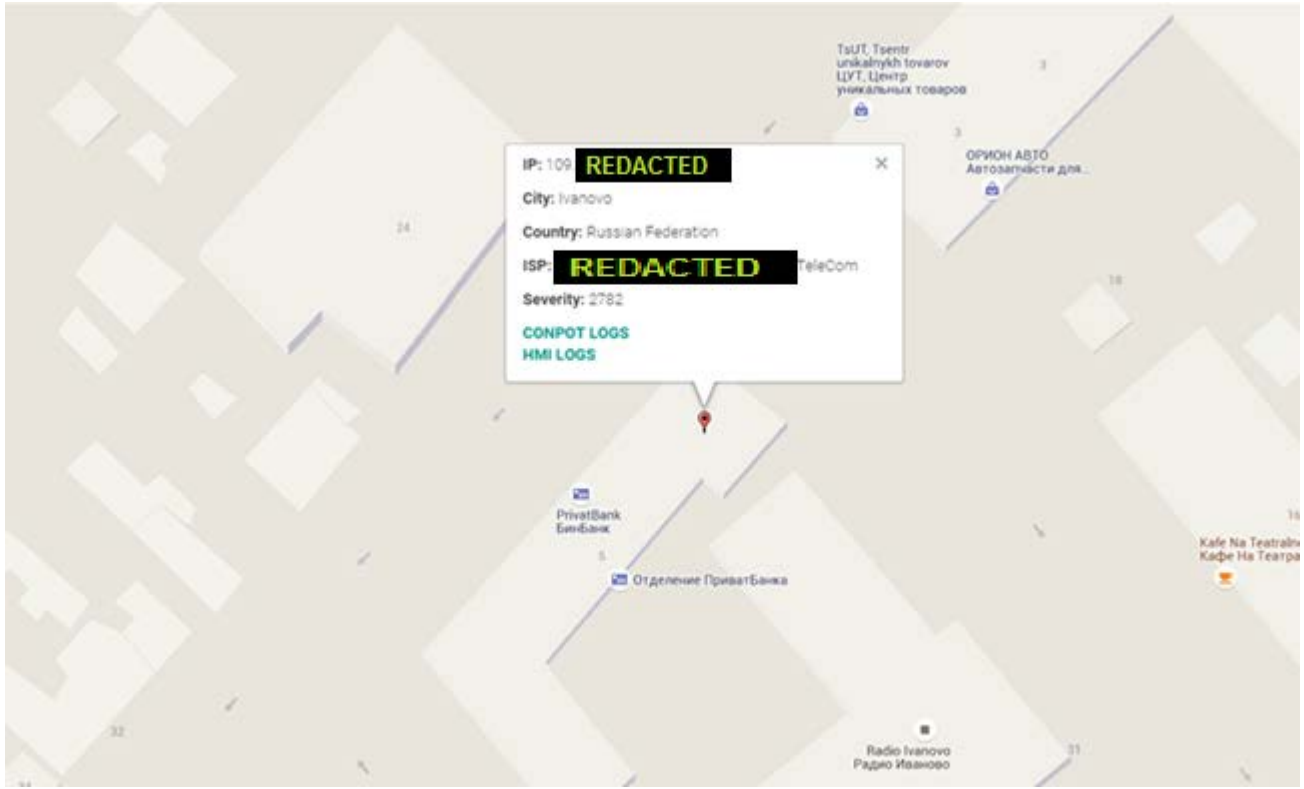
GeoLocation, GeoLocation, GeoLocation!



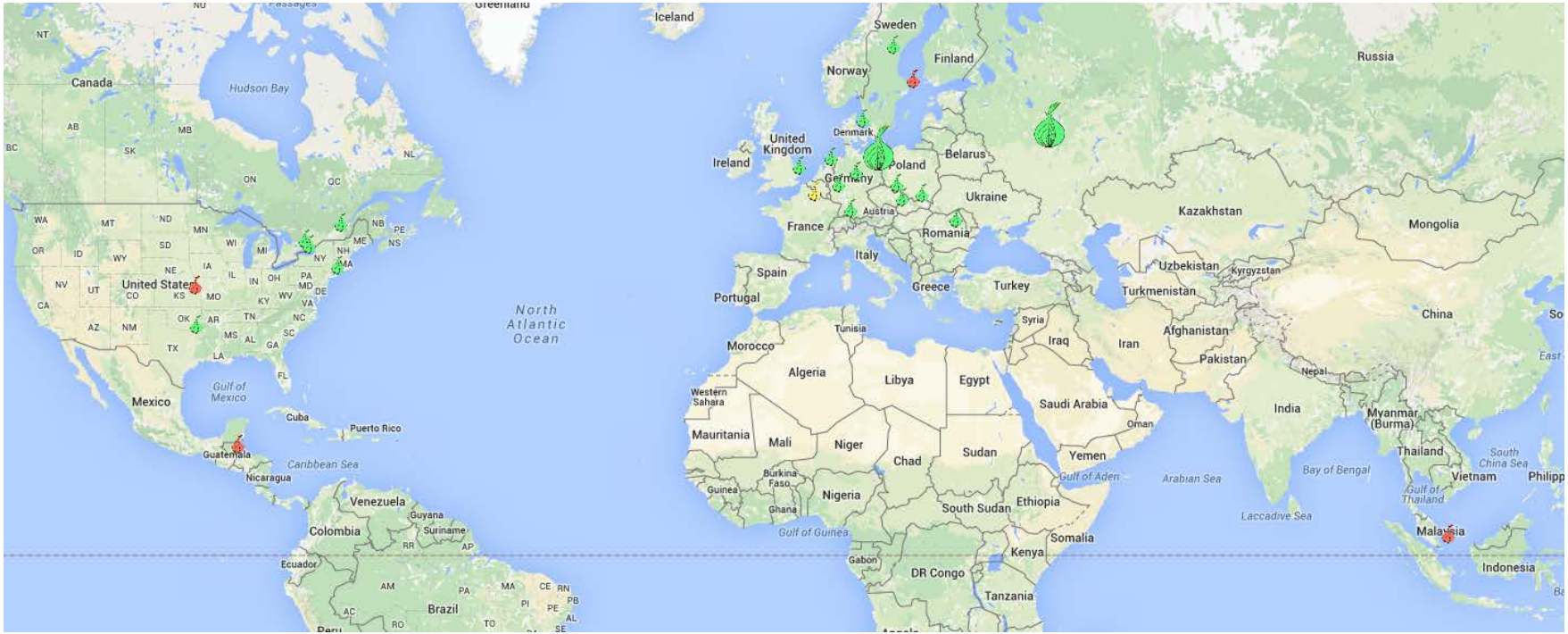
Attack Profile - Russian Federation – SEV 2782



Anybody Home?



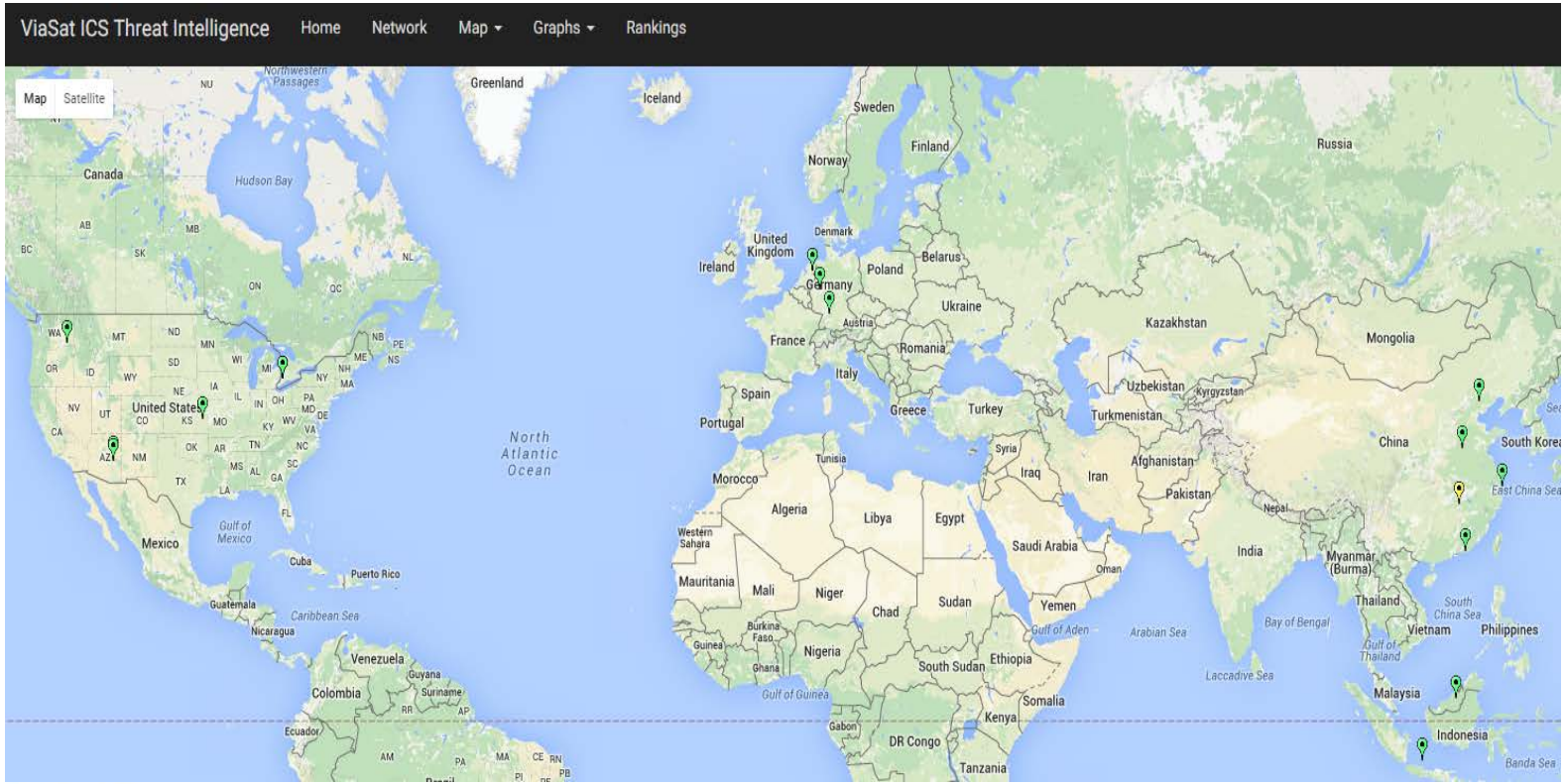
TOR (The Onion Router) Evasion?



ViaSat

RSAConference2016

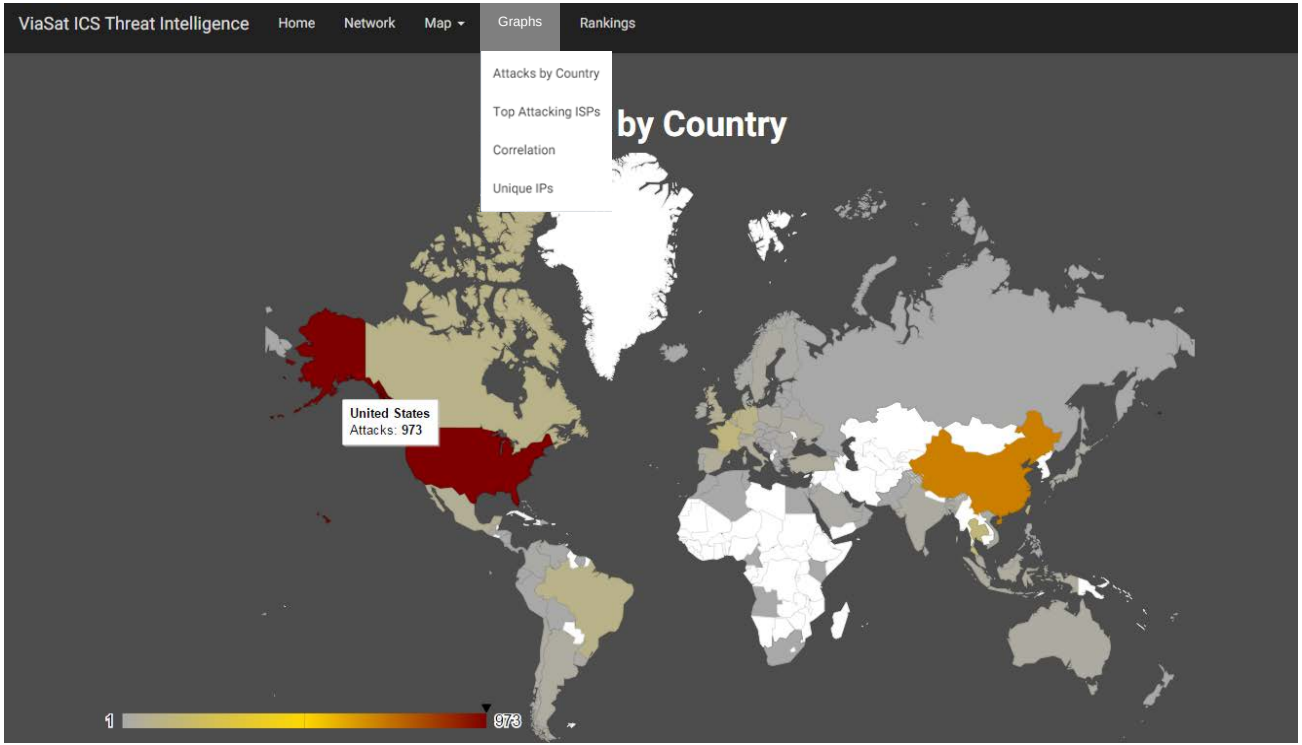
Attacks against HMIs?



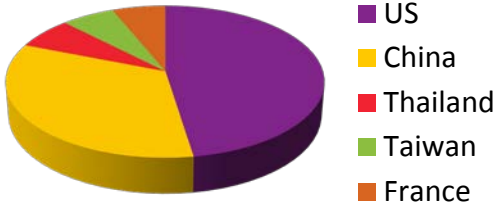
ViaSat

RSAConference2016

Not that we're keeping score…



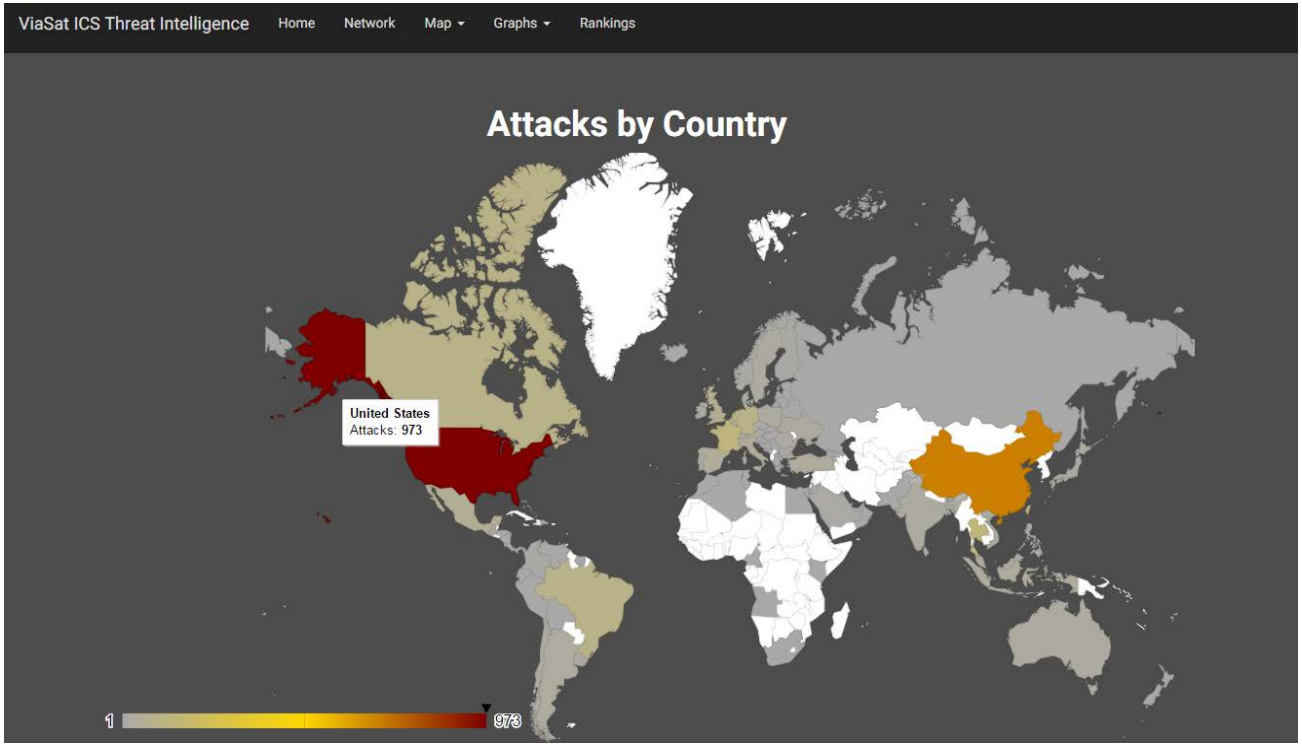
Attacks



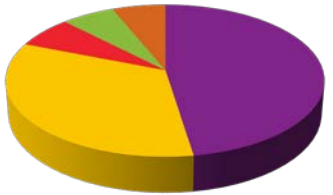
US	973
China	685
Thailand	137
Taiwan	126
France	126
Netherlands	125

ViaSat

Not that we're keeping score…



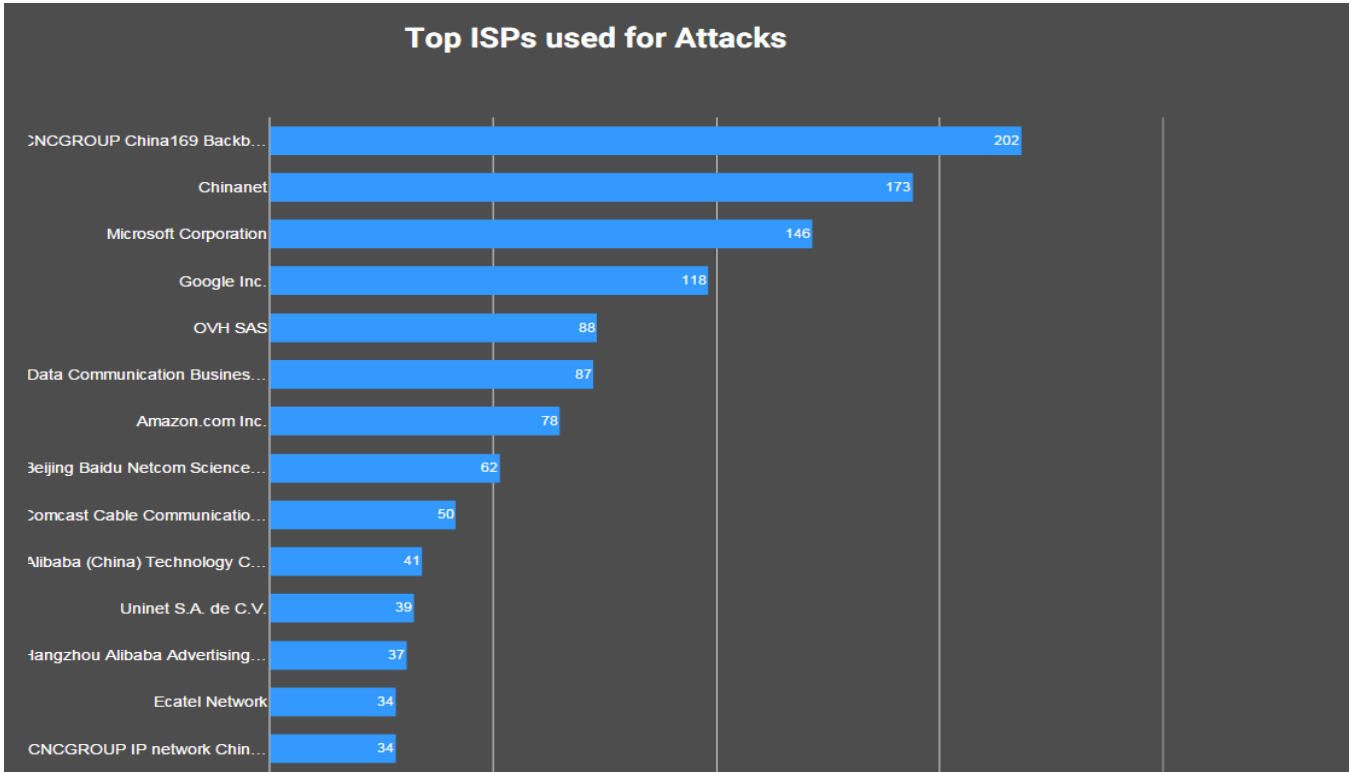
Attacks



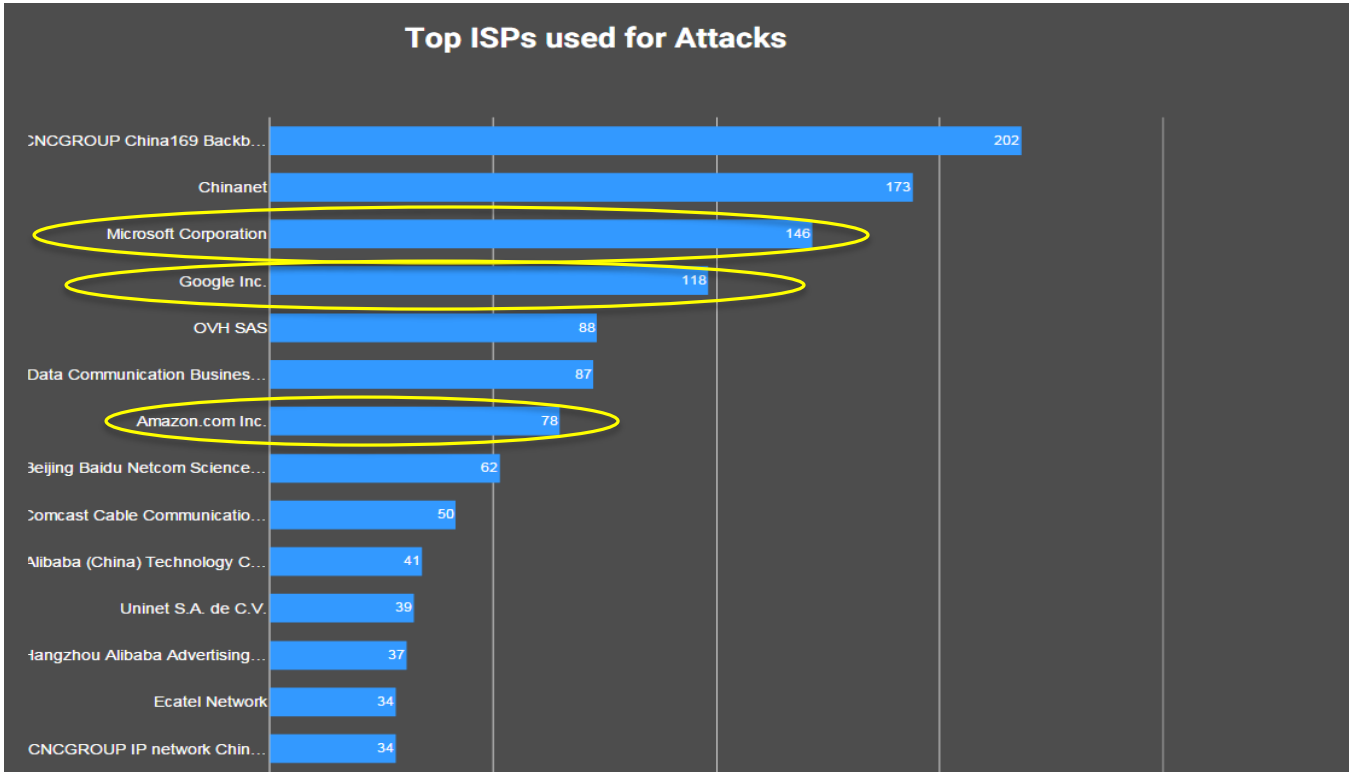
US	973
China	685
Thailand	137
Taiwan	126
France	126
Netherlands	125

ViaSat

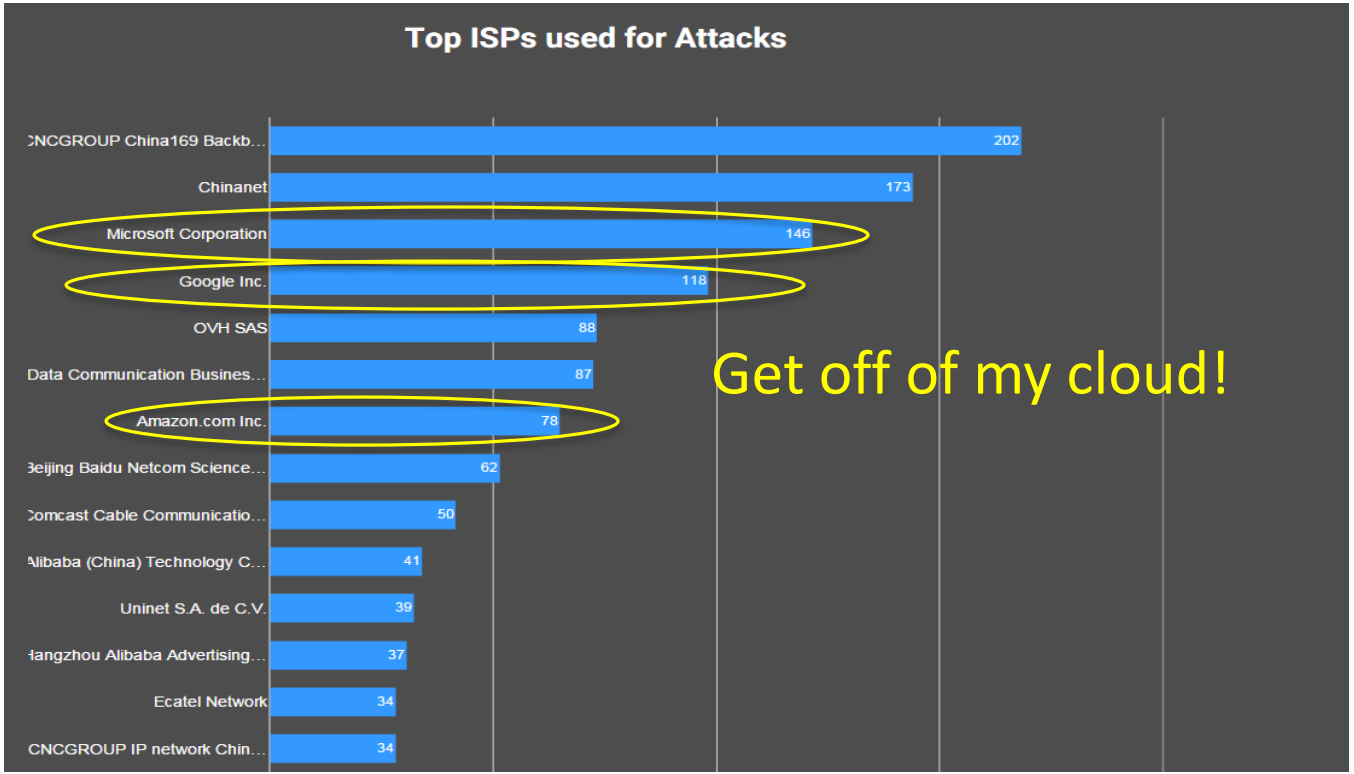
Top Internet Service Providers



Top Internet Service Providers



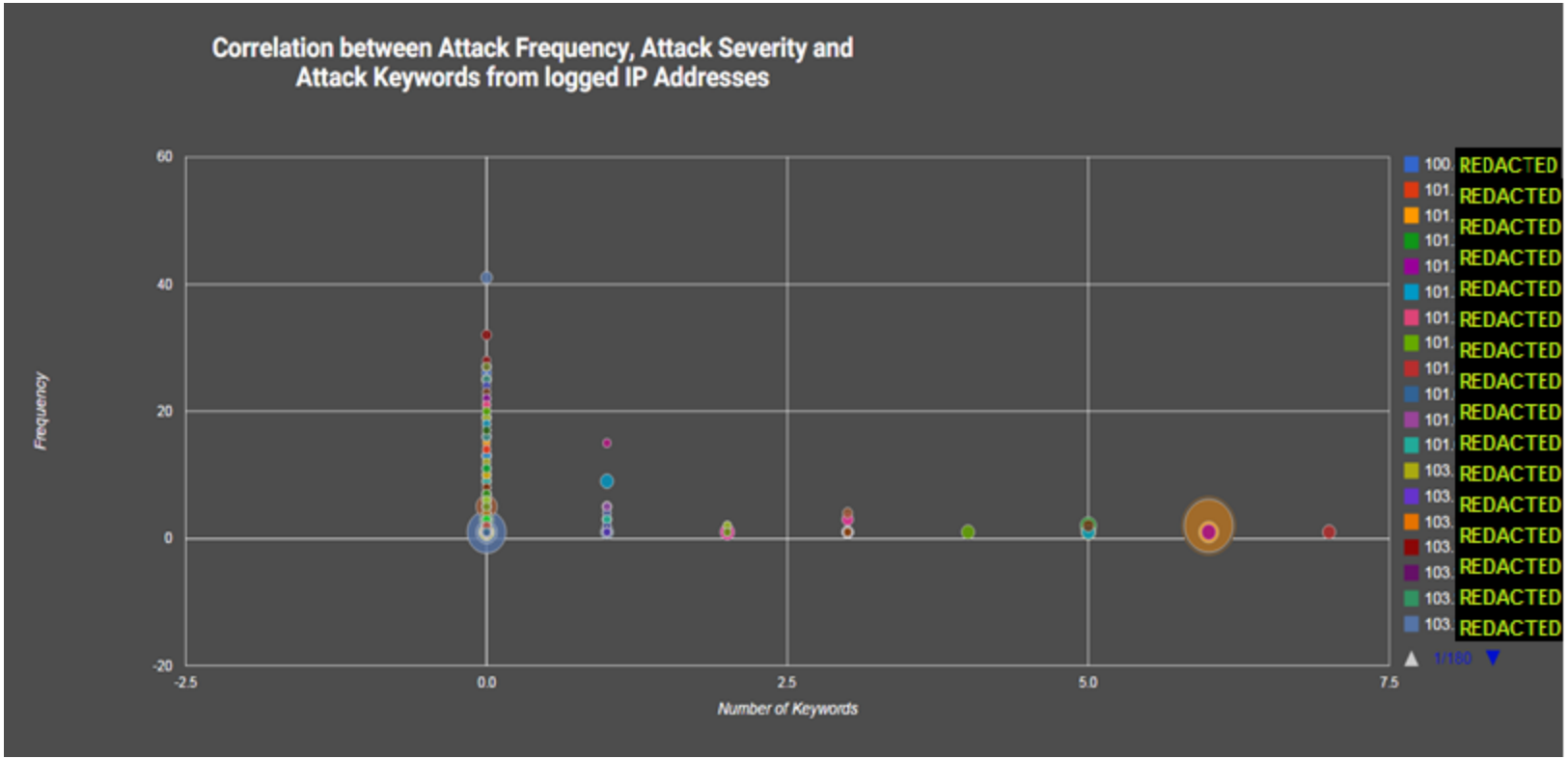
Top Internet Service Providers



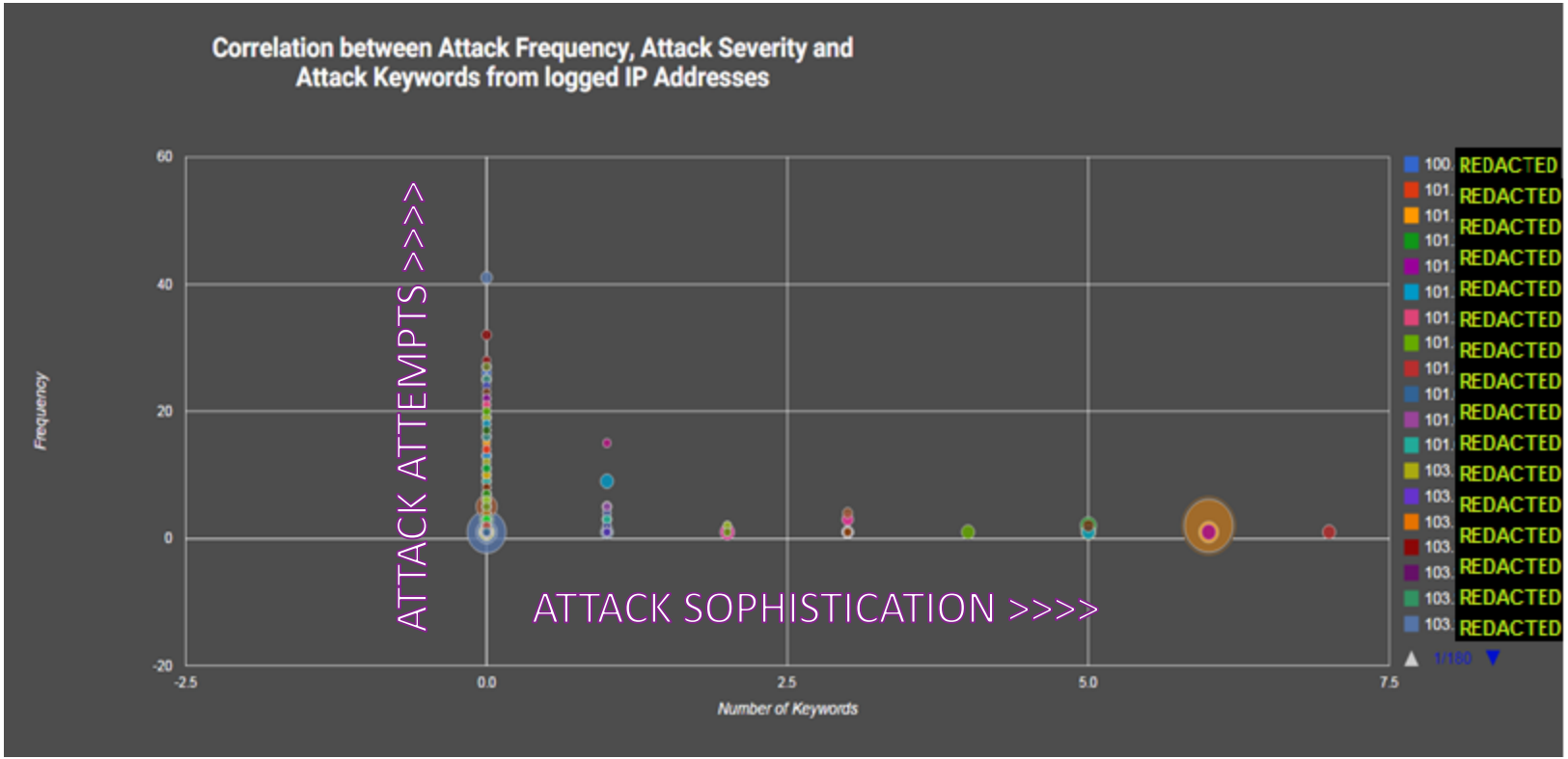
Get off of my cloud!

ViaSat

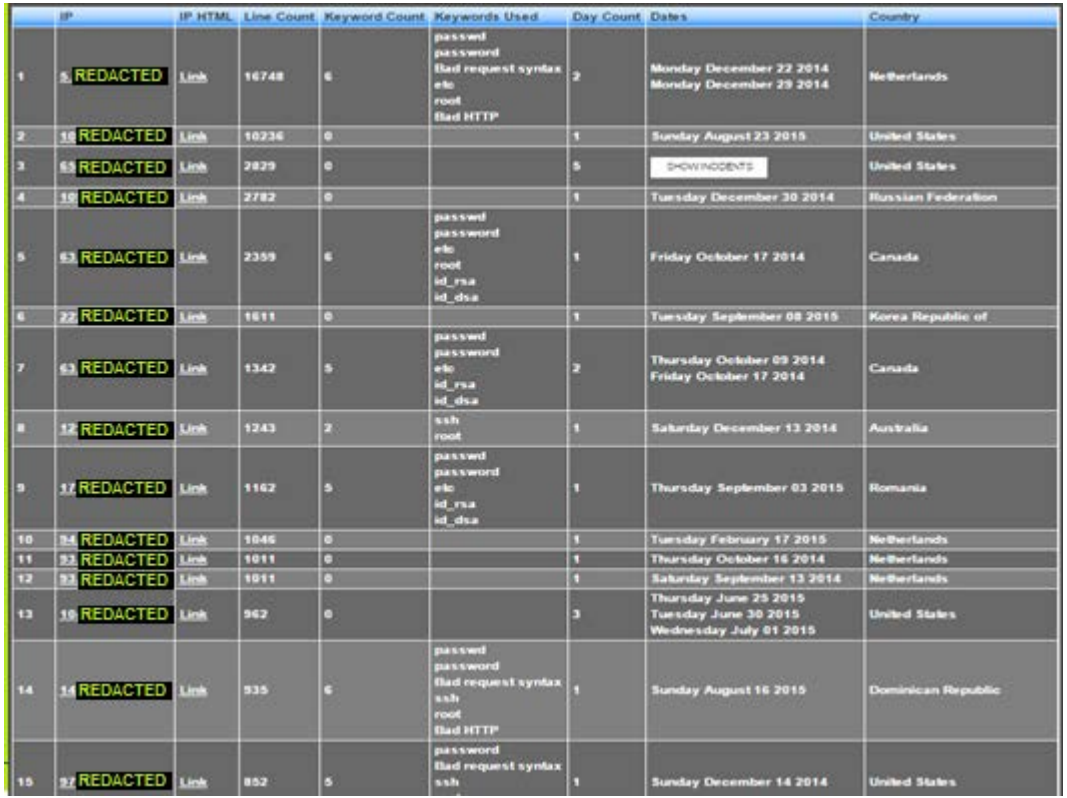
Correlation



Correlation

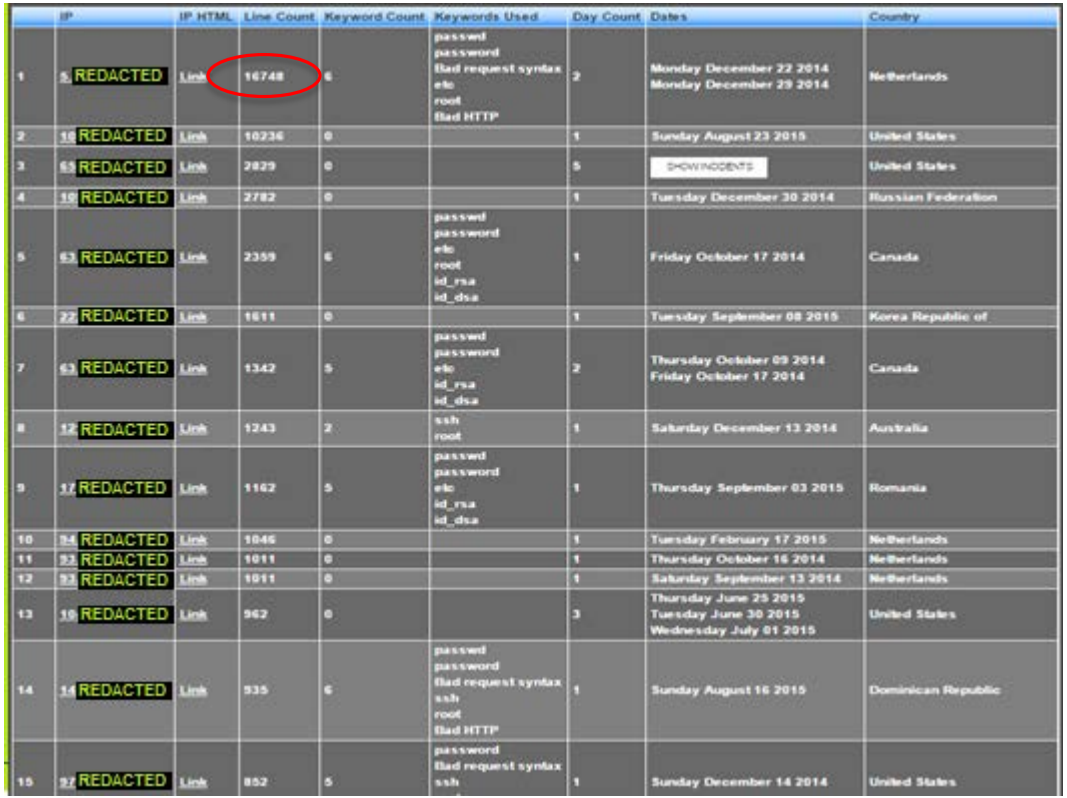


Rankings



	IP	IP HTML	Line Count	Keyword Count	Keywords Used	Day Count	Dates	Country
1	5. REDACTED	Link	16748	6	passwd password Bad request syntax etc root Bad HTTP	2	Monday December 22 2014 Monday December 29 2014	Netherlands
2	16 REDACTED	Link	10236	0		1	Sunday August 23 2015	United States
3	65 REDACTED	Link	2829	0		5	SHOW INCIDENTS	United States
4	10 REDACTED	Link	2782	0		1	Tuesday December 30 2014	Russian Federation
5	63 REDACTED	Link	2359	6	passwd password etc root id_rsa id_dsa	1	Friday October 17 2014	Canada
6	22 REDACTED	Link	1611	0		1	Tuesday September 08 2015	Korea Republic of
7	63 REDACTED	Link	1342	5	passwd password etc id_rsa id_dsa	2	Thursday October 09 2014 Friday October 17 2014	Canada
8	12 REDACTED	Link	1243	2	ssh root	1	Saturday December 13 2014	Australia
9	17 REDACTED	Link	1162	5	passwd password etc id_rsa id_dsa	1	Thursday September 03 2015	Romania
10	94 REDACTED	Link	1046	0		1	Tuesday February 17 2015	Netherlands
11	93 REDACTED	Link	1011	0		1	Thursday October 16 2014	Netherlands
12	93 REDACTED	Link	1011	0		1	Saturday September 13 2014	Netherlands
13	19 REDACTED	Link	962	0		3	Thursday June 25 2015 Tuesday June 30 2015 Wednesday July 01 2015	United States
14	14 REDACTED	Link	935	6	passwd password Bad request syntax ssh root Bad HTTP	1	Sunday August 16 2015	Dominican Republic
15	97 REDACTED	Link	852	5	password Bad request syntax ssh	1	Sunday December 14 2014	United States

Rankings



	IP	IP HTML	Line Count	Keyword Count	Keywords Used	Day Count	Dates	Country
1	5 REDACTED	Link	16748	6	passwd password Bad request syntax etc root Bad HTTP	2	Monday December 22 2014 Monday December 29 2014	Netherlands
2	10 REDACTED	Link	10236	0		1	Sunday August 23 2015	United States
3	65 REDACTED	Link	2829	0		5	SHOW INCIDENTS	United States
4	10 REDACTED	Link	2782	0		1	Tuesday December 30 2014	Russian Federation
5	63 REDACTED	Link	2359	6	passwd password etc root id_rsa id_dsa	1	Friday October 17 2014	Canada
6	22 REDACTED	Link	1611	0		1	Tuesday September 08 2015	Korea Republic of
7	63 REDACTED	Link	1342	5	passwd password etc id_rsa id_dsa	2	Thursday October 09 2014 Friday October 17 2014	Canada
8	12 REDACTED	Link	1243	2	ssh root	1	Saturday December 13 2014	Australia
9	17 REDACTED	Link	1162	5	passwd password etc id_rsa id_dsa	1	Thursday September 03 2015	Romania
10	94 REDACTED	Link	1046	0		1	Tuesday February 17 2015	Netherlands
11	93 REDACTED	Link	1011	0		1	Thursday October 16 2014	Netherlands
12	93 REDACTED	Link	1011	0		1	Saturday September 13 2014	Netherlands
13	19 REDACTED	Link	962	0		3	Thursday June 25 2015 Tuesday June 30 2015 Wednesday July 01 2015	United States
14	14 REDACTED	Link	935	6	passwd password Bad request syntax ssh root Bad HTTP	1	Sunday August 16 2015	Dominican Republic
15	97 REDACTED	Link	852	5	password Bad request syntax ssh	1	Sunday December 14 2014	United States

- 16748 Lines

Rankings

	IP	IP HTML	Line Count	Keyword Count	Keywords Used	Day Count	Dates	Country
1	5 REDACTED	Link	16748	4	passwd password Bad request syntax etc root Bad HTTP	2	Monday December 22 2014 Monday December 29 2014	Netherlands
2	16 REDACTED	Link	10236	0		1	Sunday August 23 2015	United States
3	65 REDACTED	Link	2829	0		5	SHOW INCIDENTS	United States
4	19 REDACTED	Link	2782	0		1	Tuesday December 30 2014	Russian Federation
5	63 REDACTED	Link	2359	6	passwd password etc root id_rsa id_dsa	1	Friday October 17 2014	Canada
6	22 REDACTED	Link	1611	0		1	Tuesday September 08 2015	Korea Republic of
7	63 REDACTED	Link	1342	5	passwd password etc id_rsa id_dsa	2	Thursday October 09 2014 Friday October 17 2014	Canada
8	12 REDACTED	Link	1243	2	ssh root	1	Saturday December 13 2014	Australia
9	17 REDACTED	Link	1162	5	passwd password etc id_rsa id_dsa	1	Thursday September 03 2015	Romania
10	94 REDACTED	Link	1046	0		1	Tuesday February 17 2015	Netherlands
11	93 REDACTED	Link	1011	0		1	Thursday October 16 2014	Netherlands
12	93 REDACTED	Link	1011	0		1	Saturday September 13 2014	Netherlands
13	19 REDACTED	Link	962	0		3	Thursday June 25 2015 Tuesday June 30 2015 Wednesday July 01 2015	United States
14	14 REDACTED	Link	935	6	passwd password Bad request syntax ssh root Bad HTTP	1	Sunday August 16 2015	Dominican Republic
15	97 REDACTED	Link	852	5	password Bad request syntax ssh	1	Sunday December 14 2014	United States

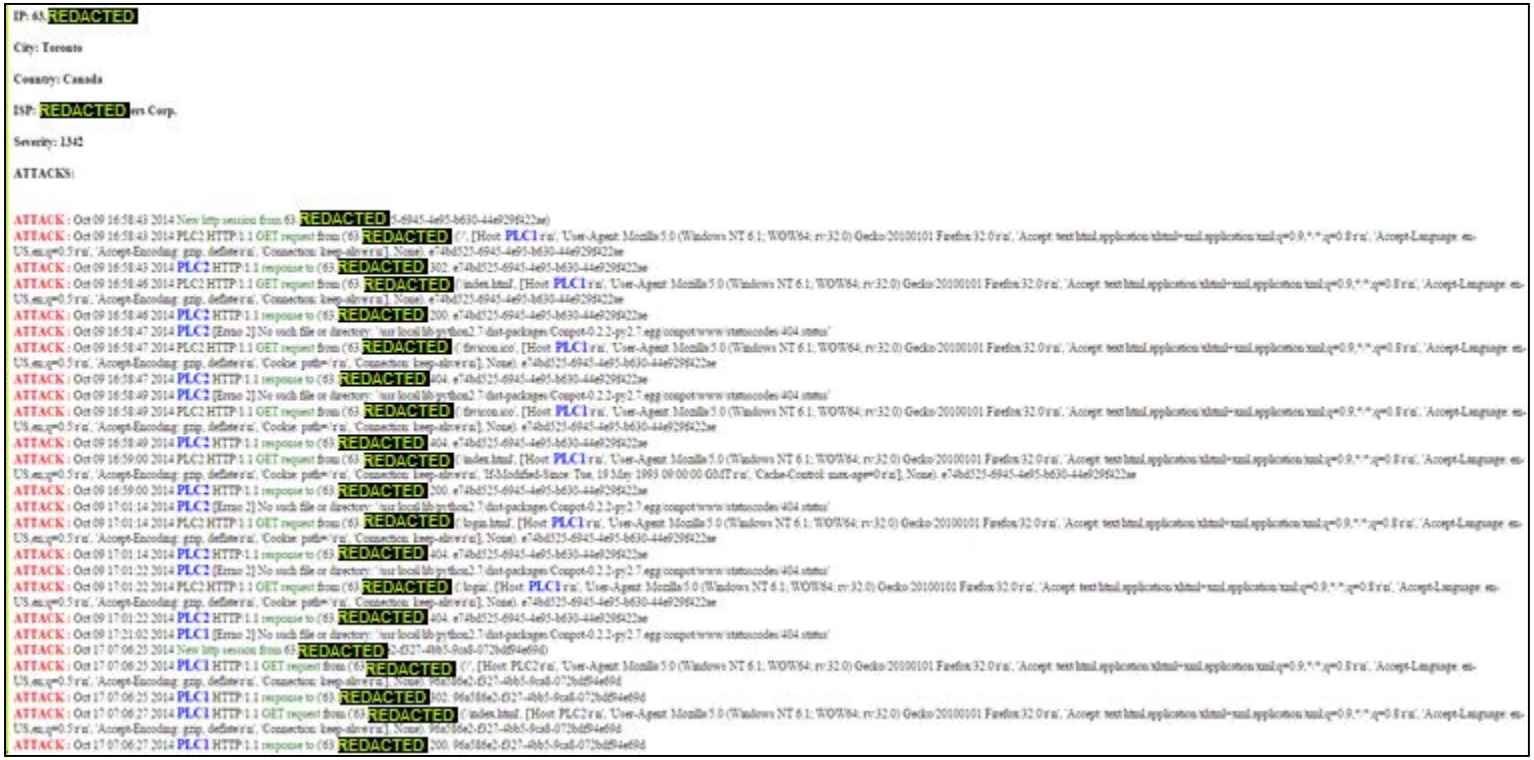
- 16748 Lines
- Recon

Rankings

	IP	IP HTML	Line Count	Keyword Count	Keywords Used	Day Count	Dates	Country
1	5 REDACTED	Link	16748	4	passwd password Bad request syntax etc root Bad HTTP	2	Monday December 22 2014 Monday December 29 2014	Netherlands
2	16 REDACTED	Link	10236	0		1	Sunday August 23 2015	United States
3	65 REDACTED	Link	2829	0		5	SHOW INCIDENTS	United States
4	19 REDACTED	Link	2782	0		1	Tuesday December 30 2014	Russian Federation
5	63 REDACTED	Link	2359	6	passwd password etc root id_rsa id_dsa	1	Friday October 17 2014	Canada
6	22 REDACTED	Link	1611	0		1	Tuesday September 08 2015	Korea Republic of
7	63 REDACTED	Link	1342	5	passwd password etc id_rsa id_dsa	2	Thursday October 09 2014 Friday October 17 2014	Canada
8	12 REDACTED	Link	1243	2	ssh root	1	Saturday December 13 2014	Australia
9	17 REDACTED	Link	1162	5	passwd password etc id_rsa id_dsa	1	Thursday September 03 2015	Romania
10	94 REDACTED	Link	1046	0		1	Tuesday February 17 2015	Netherlands
11	93 REDACTED	Link	1011	0		1	Thursday October 16 2014	Netherlands
12	93 REDACTED	Link	1011	0		1	Saturday September 13 2014	Netherlands
13	19 REDACTED	Link	962	0		3	Thursday June 25 2015 Tuesday June 30 2015 Wednesday July 01 2015	United States
14	14 REDACTED	Link	935	6	passwd password Bad request syntax ssh root Bad HTTP	1	Sunday August 16 2015	Dominican Republic
15	97 REDACTED	Link	852	5	password Bad request syntax ssh	1	Sunday December 14 2014	United States

- 16748 Lines
- Recon
- Coordinated Attack

Details, Evidence and Attacker Profiling



IP: 63.REDACTED

City: Toronto

Country: Canada

ISP: REDACTEDrs Corp.

Severity: 1342

ATTACKS:

ATTACK : Oct 09 16:58:43 2014 New http session from 63.REDACTED:5-6945-4e95-b630-44e029f422ae)
ATTACK : Oct 09 16:58:43 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Connection: keep-alive\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:43 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 302, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:46 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/index.html', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Connection: keep-alive\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:46 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 200, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:47 2014 PLC2 [Errno 2] No such file or directory: '/usr/local/lib/python2.7/dist-packages/Cowpot-0.2.2-py2.7.egg/cowpot/www/statuscodes/404.status'
ATTACK : Oct 09 16:58:47 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/favicon.ico', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Cookie: path=\'/\'\r\n', 'Connection: keep-alive\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:47 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 404, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:49 2014 PLC2 [Errno 2] No such file or directory: '/usr/local/lib/python2.7/dist-packages/Cowpot-0.2.2-py2.7.egg/cowpot/www/statuscodes/404.status'
ATTACK : Oct 09 16:58:49 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/favicon.ico', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Cookie: path=\'/\'\r\n', 'Connection: keep-alive\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:58:49 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 404, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:59:00 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/index.html', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Cookie: path=\'/\'\r\n', 'Connection: keep-alive\r\n', 'If-Modified-Since: Tue, 19 May 1993 09:00:00 GMT\r\n', 'Cache-Control: max-age=0\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 16:59:00 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 200, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 17:01:14 2014 PLC2 [Errno 2] No such file or directory: '/usr/local/lib/python2.7/dist-packages/Cowpot-0.2.2-py2.7.egg/cowpot/www/statuscodes/404.status'
ATTACK : Oct 09 17:01:14 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/login.html', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Cookie: path=\'/\'\r\n', 'Connection: keep-alive\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 17:01:14 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 404, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 17:01:22 2014 PLC2 [Errno 2] No such file or directory: '/usr/local/lib/python2.7/dist-packages/Cowpot-0.2.2-py2.7.egg/cowpot/www/statuscodes/404.status'
ATTACK : Oct 09 17:01:22 2014 PLC2 HTTP 1.1 GET request from (63.REDACTED) ('/login', [Host: PLC1\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Cookie: path=\'/\'\r\n', 'Connection: keep-alive\r\n'], None), e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 17:01:22 2014 PLC2 HTTP 1.1 response to (63.REDACTED) 404, e74bd525-6945-4e95-b630-44e029f422ae
ATTACK : Oct 09 17:21:02 2014 PLC1 [Errno 2] No such file or directory: '/usr/local/lib/python2.7/dist-packages/Cowpot-0.2.2-py2.7.egg/cowpot/www/statuscodes/404.status'
ATTACK : Oct 17 07:06:25 2014 New http session from 63.REDACTED:2-f327-49b5-9ca8-072bdf94e69d)
ATTACK : Oct 17 07:06:25 2014 PLC1 HTTP 1.1 GET request from (63.REDACTED) ('/', [Host: PLC2\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Connection: keep-alive\r\n'], None), 96a586e2-f327-49b5-9ca8-072bdf94e69d
ATTACK : Oct 17 07:06:25 2014 PLC1 HTTP 1.1 response to (63.REDACTED) 302, 96a586e2-f327-49b5-9ca8-072bdf94e69d
ATTACK : Oct 17 07:06:27 2014 PLC1 HTTP 1.1 GET request from (63.REDACTED) ('/index.html', [Host: PLC2\r\n', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0\r\n', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n', 'Accept-Language: en-US,en;q=0.5\r\n', 'Accept-Encoding: gzip, deflate\r\n', 'Connection: keep-alive\r\n'], None), 96a586e2-f327-49b5-9ca8-072bdf94e69d
ATTACK : Oct 17 07:06:27 2014 PLC1 HTTP 1.1 response to (63.REDACTED) 200, 96a586e2-f327-49b5-9ca8-072bdf94e69d

ViaSat

RSAConference2016

Findings - Attack Intelligence Correlation

- Real and malicious attacks directed at Critical Infrastructure
- Attack count and severity spiked on 9/11
- Legacy systems are extremely vulnerable
- Cloud provider sourcing rapidly increasing
- Only sophisticated attacks utilize evasion techniques (e.g. TOR)
- Diversity in attack tools (Simple scanners >>> Professional tools)

Apply ….An Ounce of Prevention

- Know your critical ICS devices AND their connections
- Use layered security AND defense-in-depth
- Maintain a proactive risk management program
- Regularly penetration test internally as well as the perimeter
- Remediate to mitigate vulnerabilities, exploits, and probing
- Consider HoneyNets as an early warning system
- Think “Purple”

RSAC Studio

Connect to Protect

Honey, I Hacked the SCADA!: Industrial CONTROLLED Systems!

James Heyen
Systems Engineer
ViaSat - RSA Booth #2915
@jlheyen
James.heyen@viasat.com
760.893.1134

#RSAC