RSAC Studio

Connect to Protect

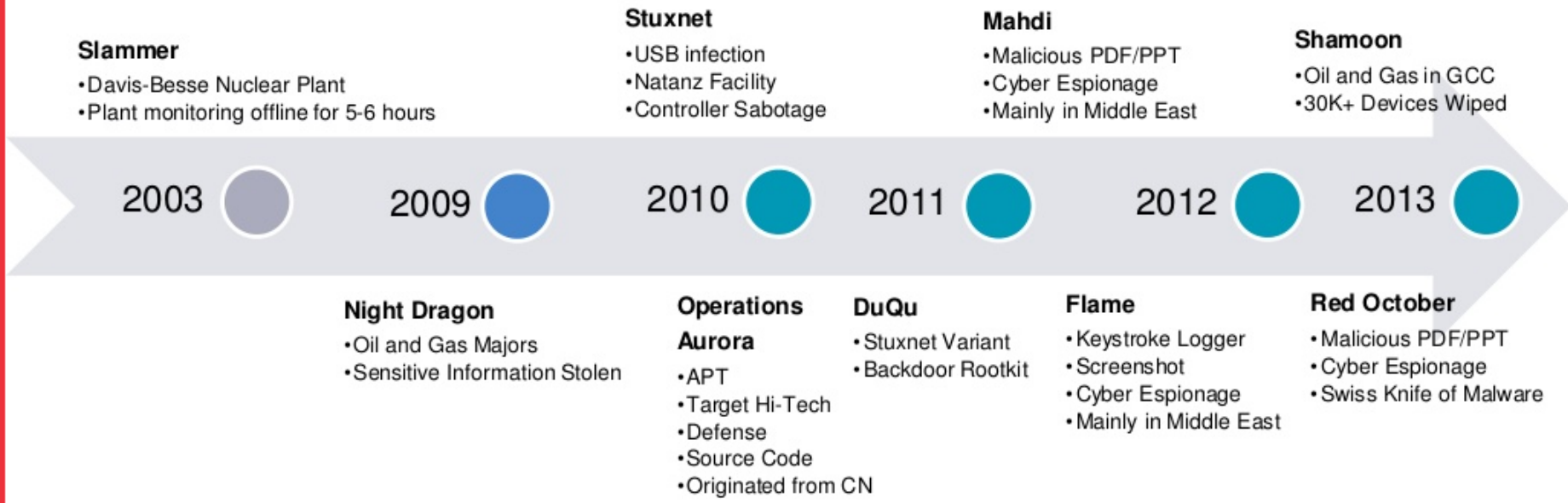
Honey, I Hacked the SCADA!: Industrial CONTROLLED Systems!

James Heyen
Systems Engineer
ViaSat - Secure Network Systems
@jlheyen

#RSAC

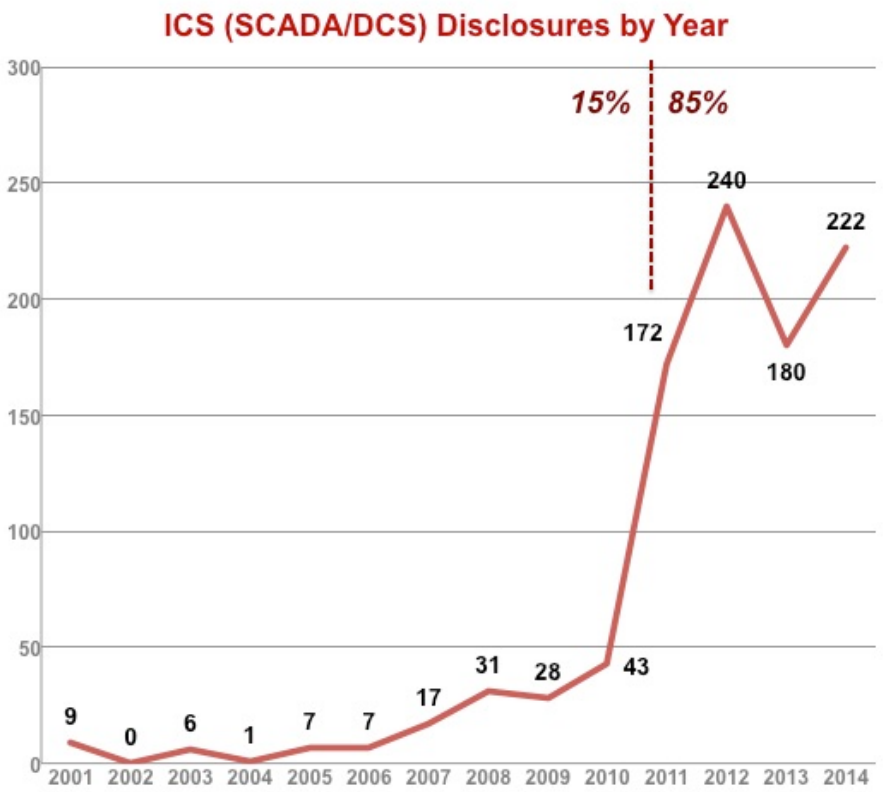
August 14, 2003 - The Saga begins…..

Timeline – Industrial Malware



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

Full Disclosure

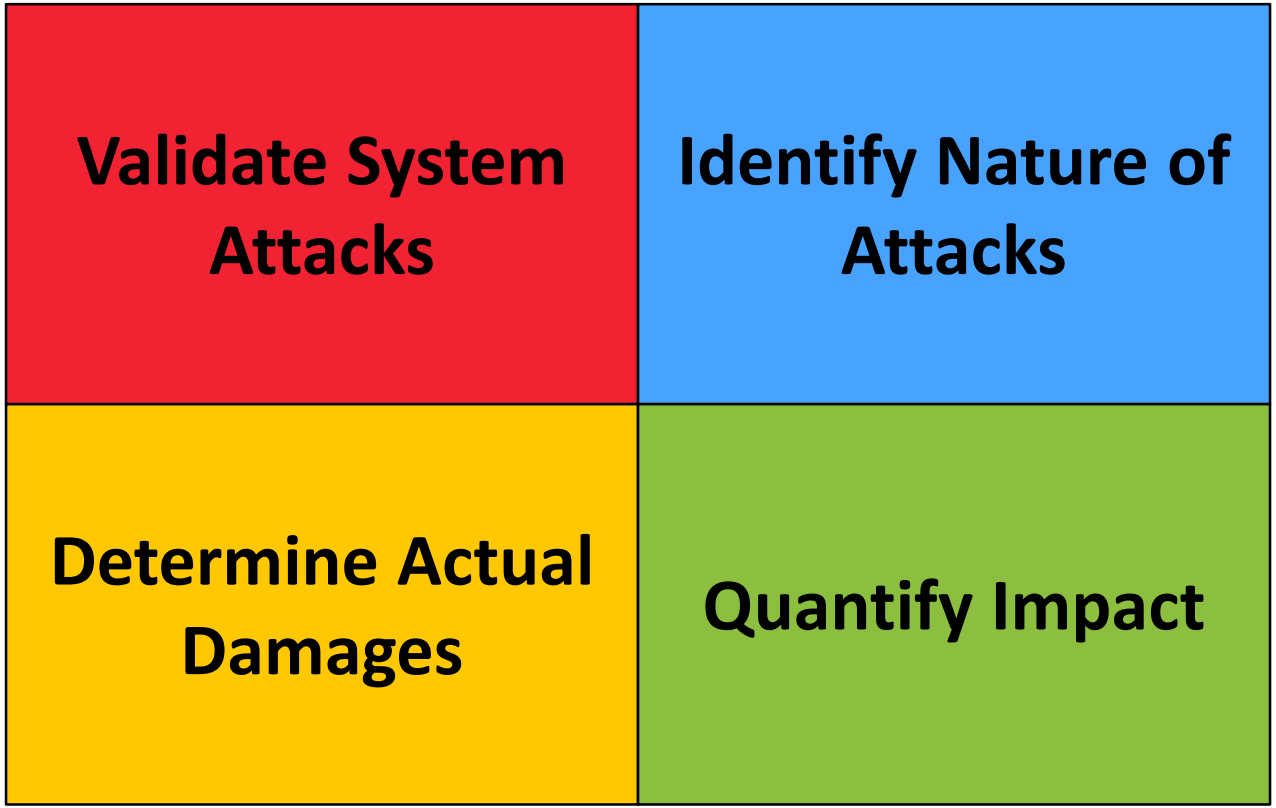


http://www.scadahacker.com

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



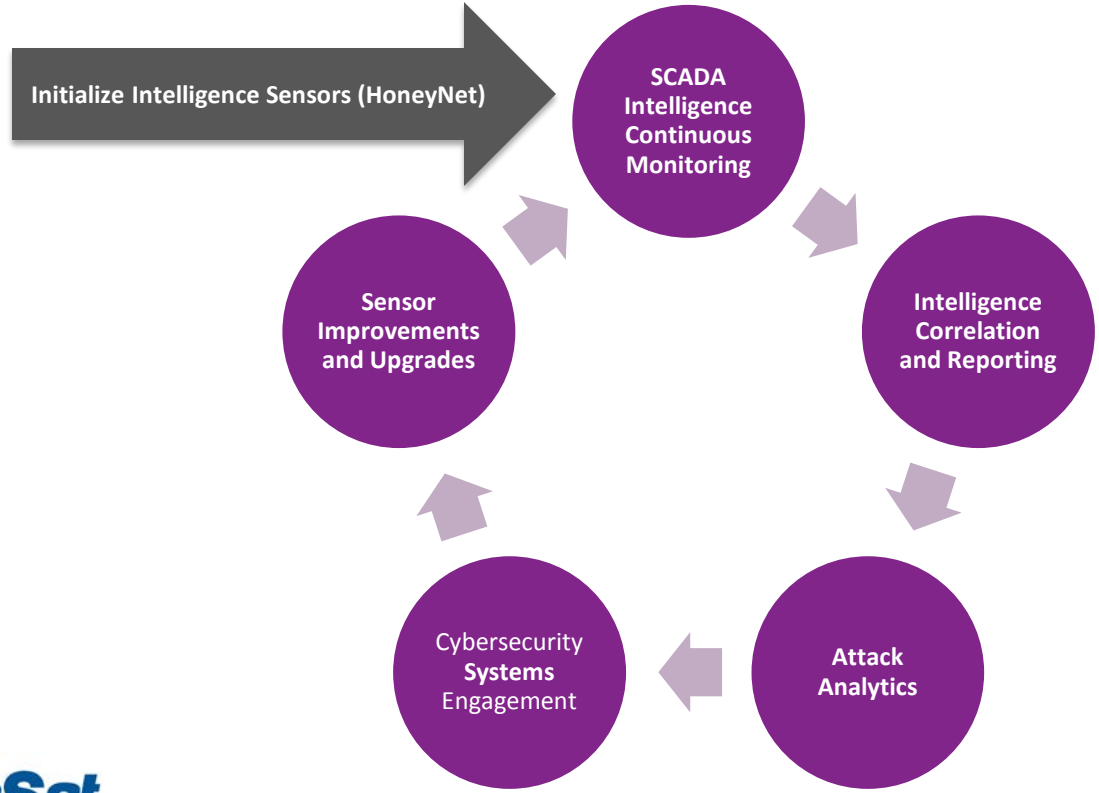
Requirements

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

PASTEBIN

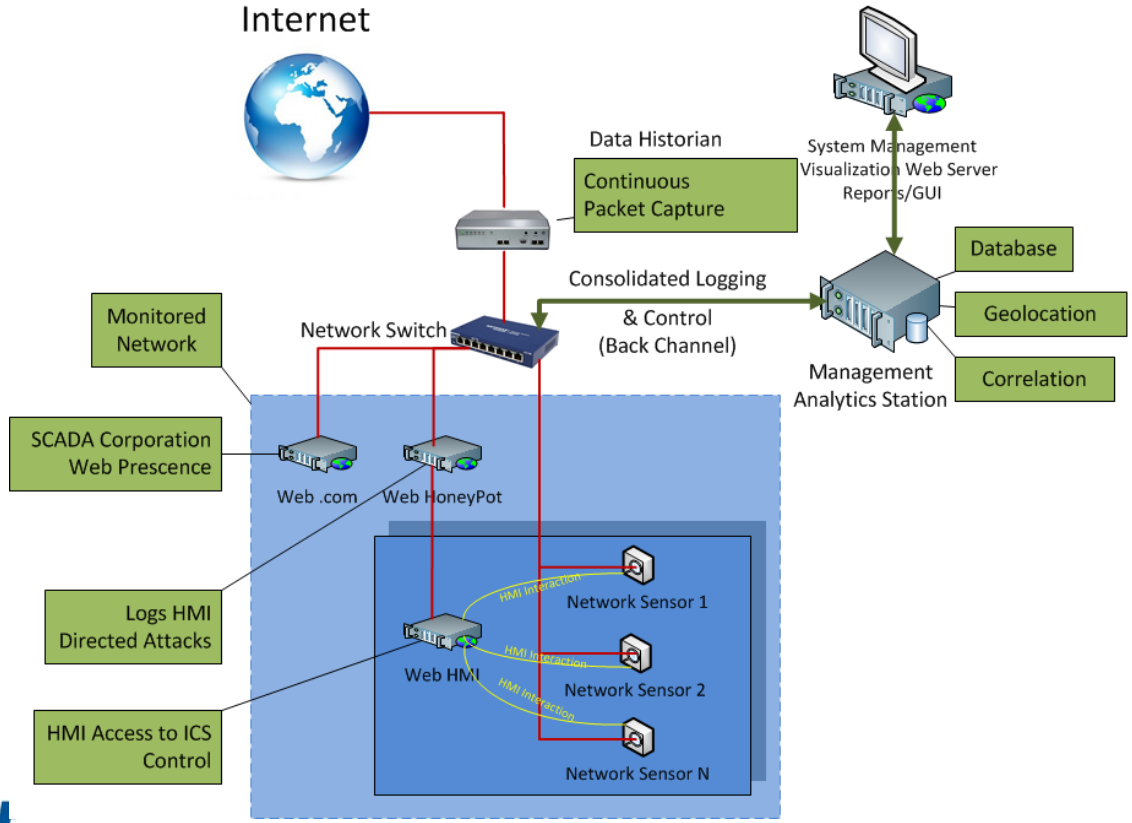
Tor

SCADA Intelligence Gathering Cycle



Myth or Reality?

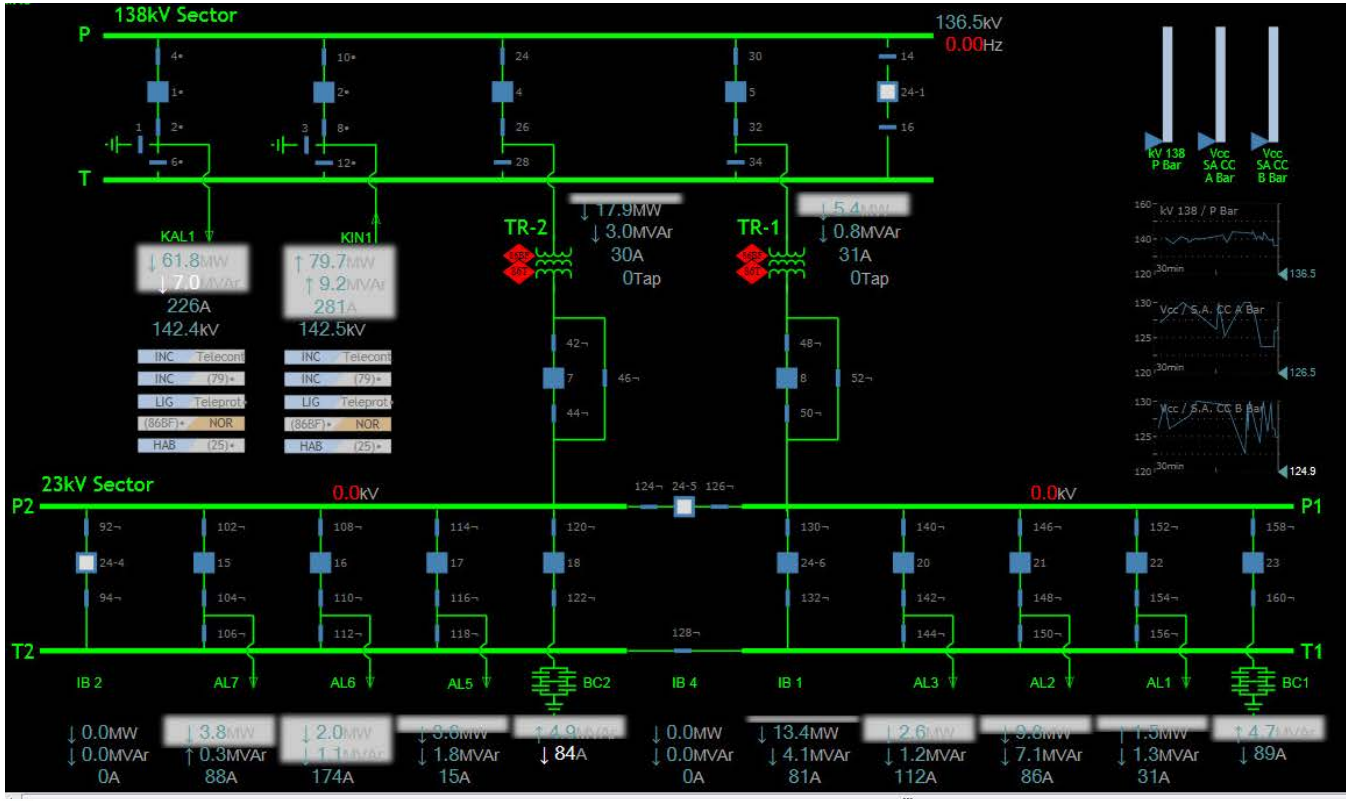
SCADA Intelligence System Architecture



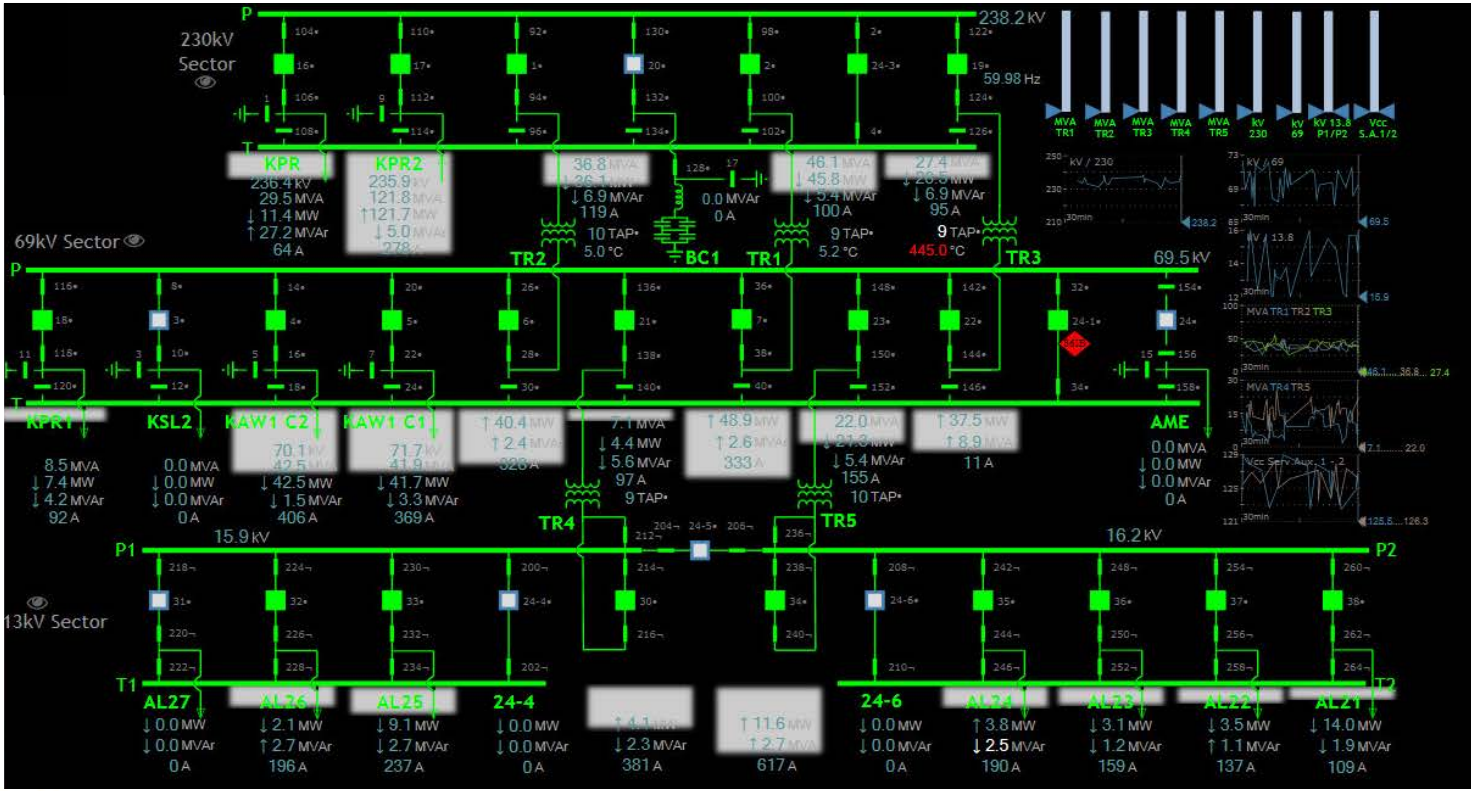
Low Interaction – plcscan.py


```
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  (5369656d656e732c2053494d414e5449432053372d333030000000000000000000)
  Plant identification      :                           (43616c69666f726e69612053636164610000000000000000000000000000000000)
  Copyright                 : Original Siemens Equipment (4f726967696e616c205369656d656e732045717569706d656e74000000000000)
  Serial number of module   : 94233102                  (393432333331303200000000000000000000000000000000000000000000000000)
  Module type name          : IM351-8 PN/DP CPU         (494d3335312d3820504e2f445020435055000000000000000000000000000000)
  OEM ID of a module        :                           (00000000000000000000000000000000000000000000000000000000000000)
  Location designation of a module:                           (000000000000000000000000000000000000000000000000000000000000000000)
       .31.114:502 Modbus/TCP
  Unit ID: 0
    Device:
  Unit ID: 255
    Device:
Scan complete
```

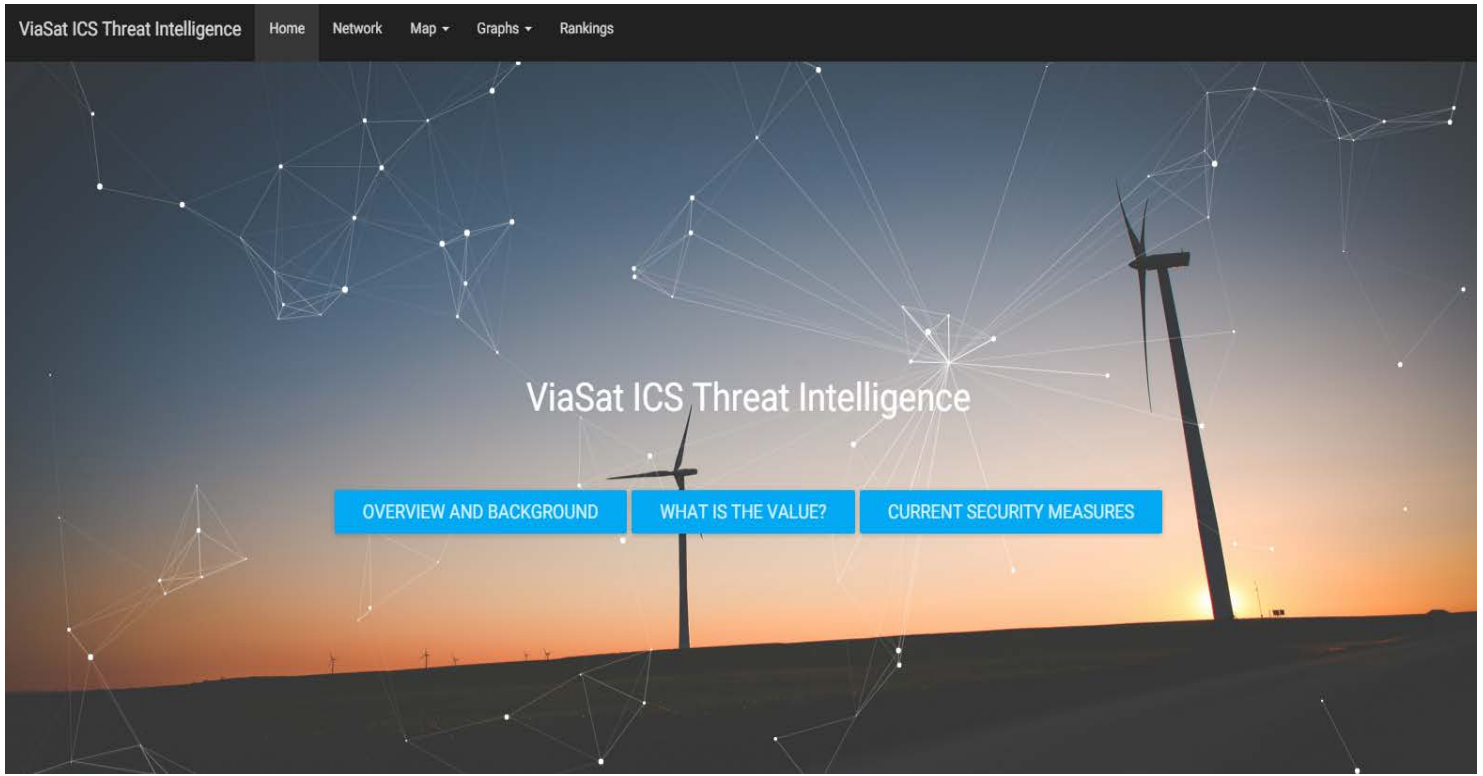
Medium and High Interaction



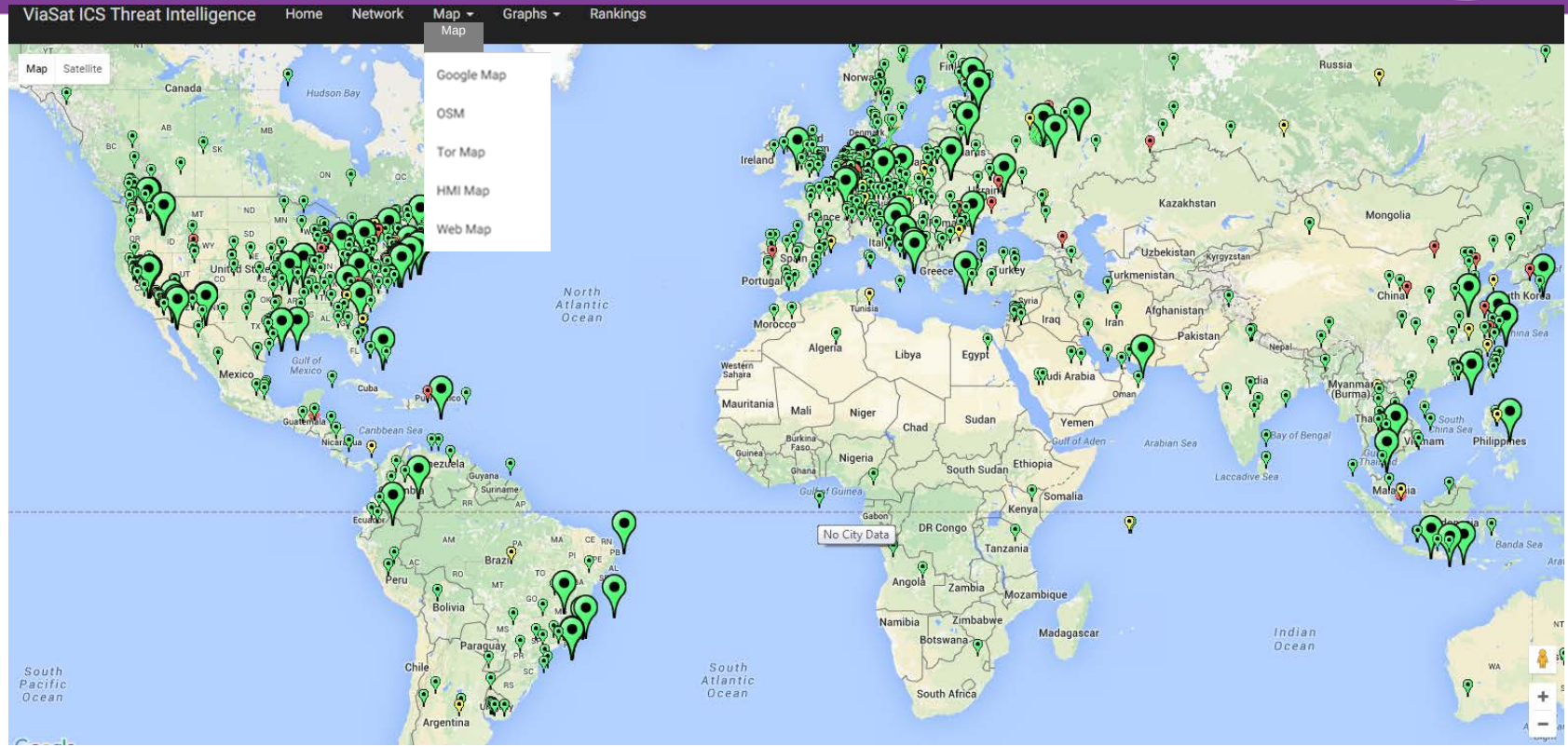
Medium and High Interaction



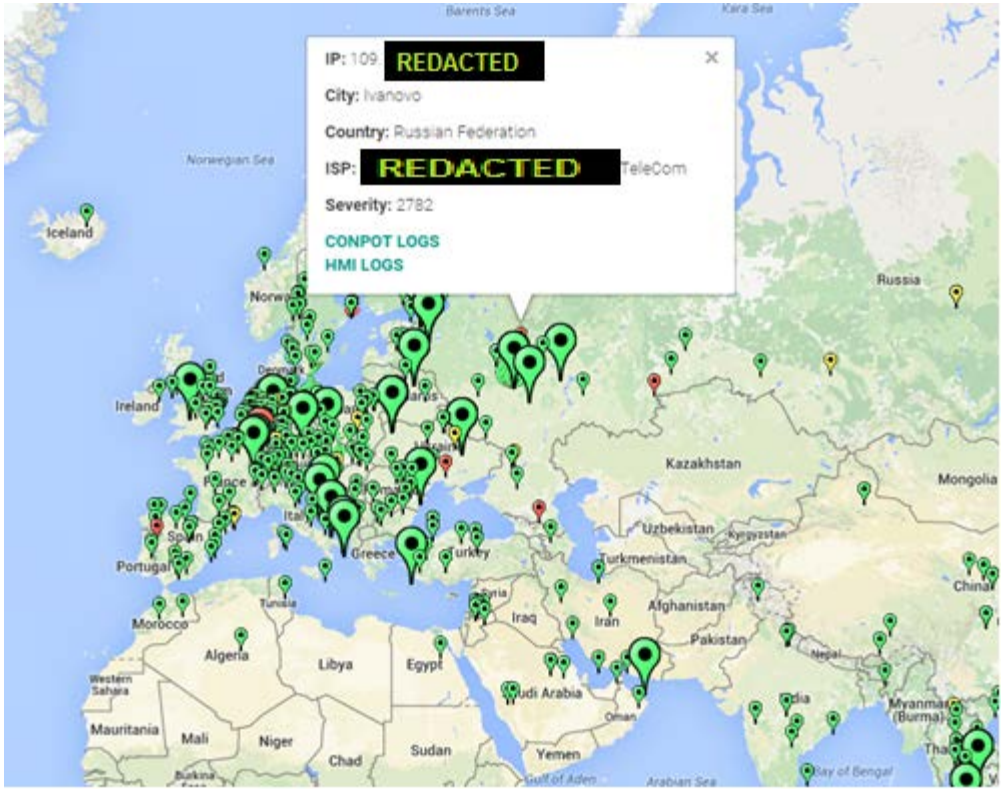
And we have liftoff....



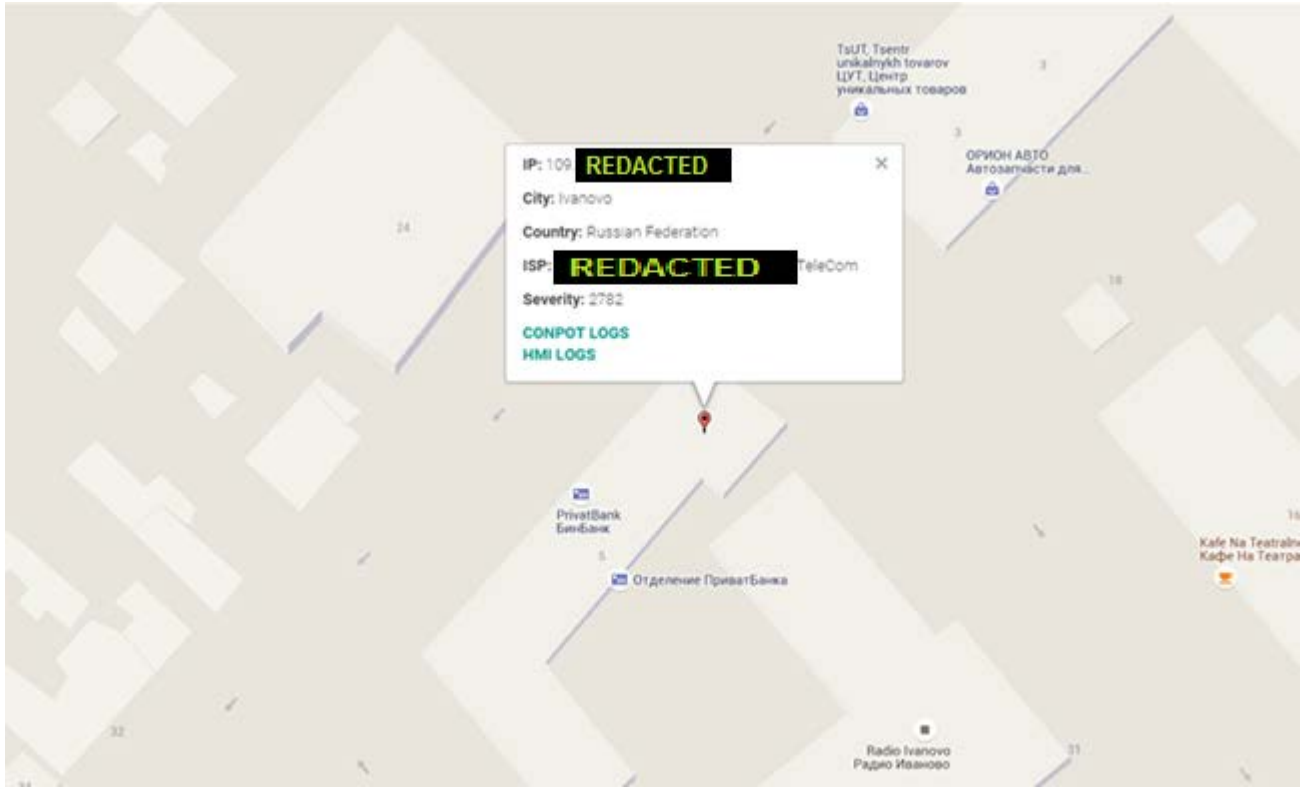
GeoLocation, GeoLocation, GeoLocation!



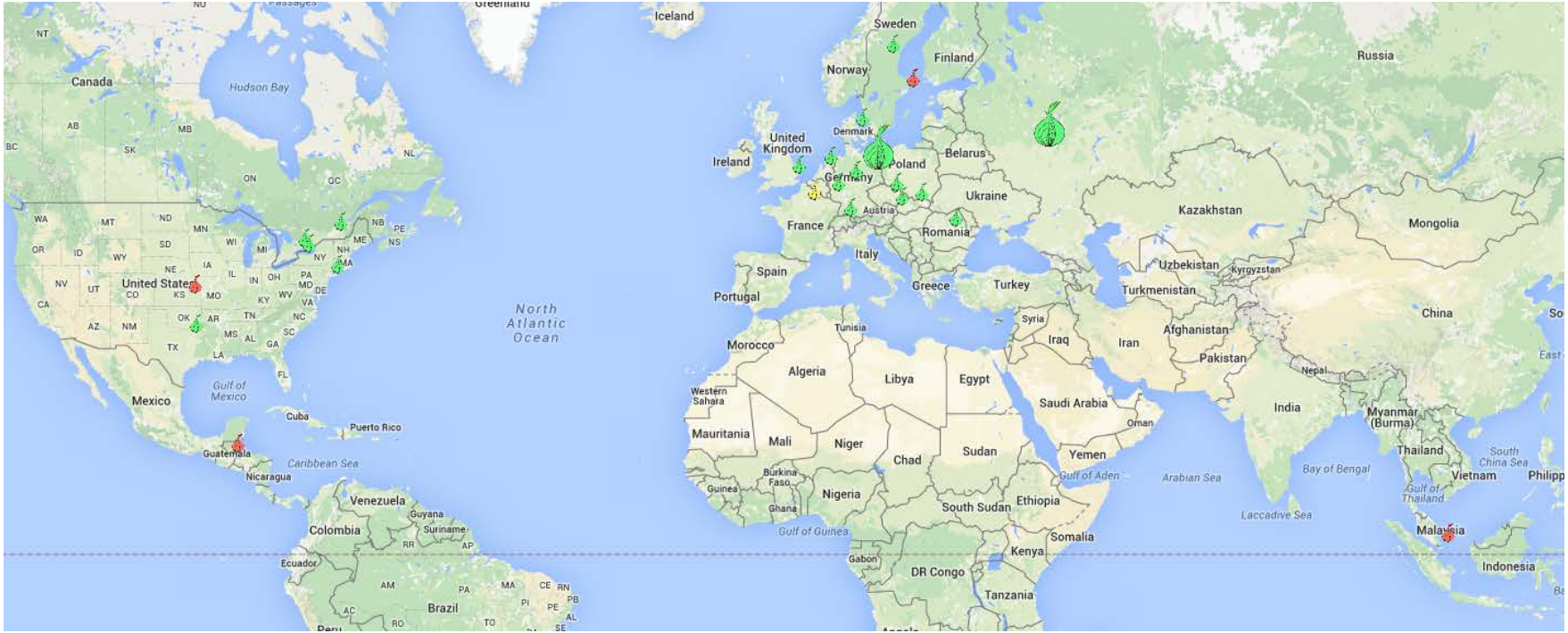
Attack Profile - Russian Federation – SEV 2782



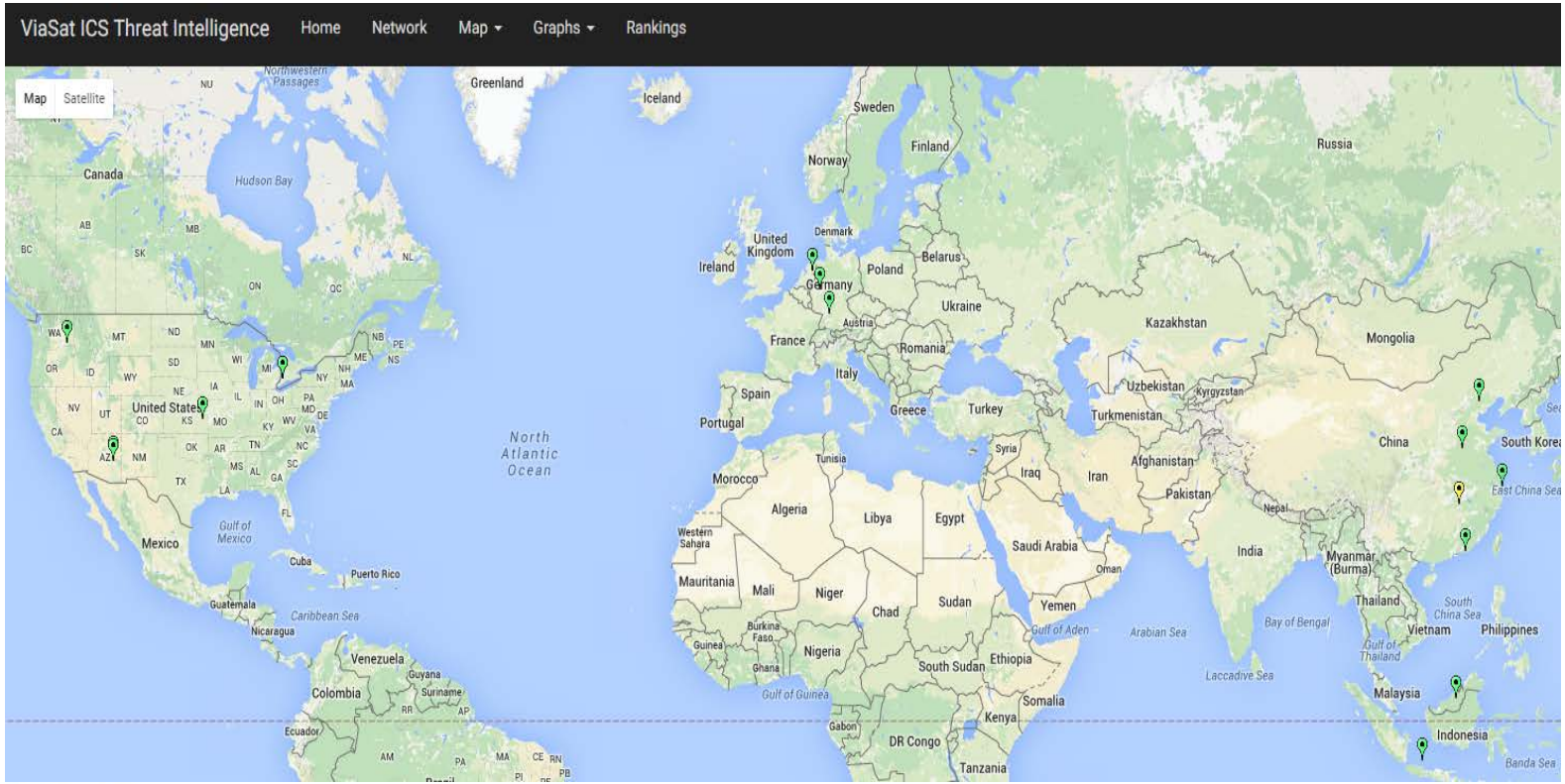
Anybody Home?



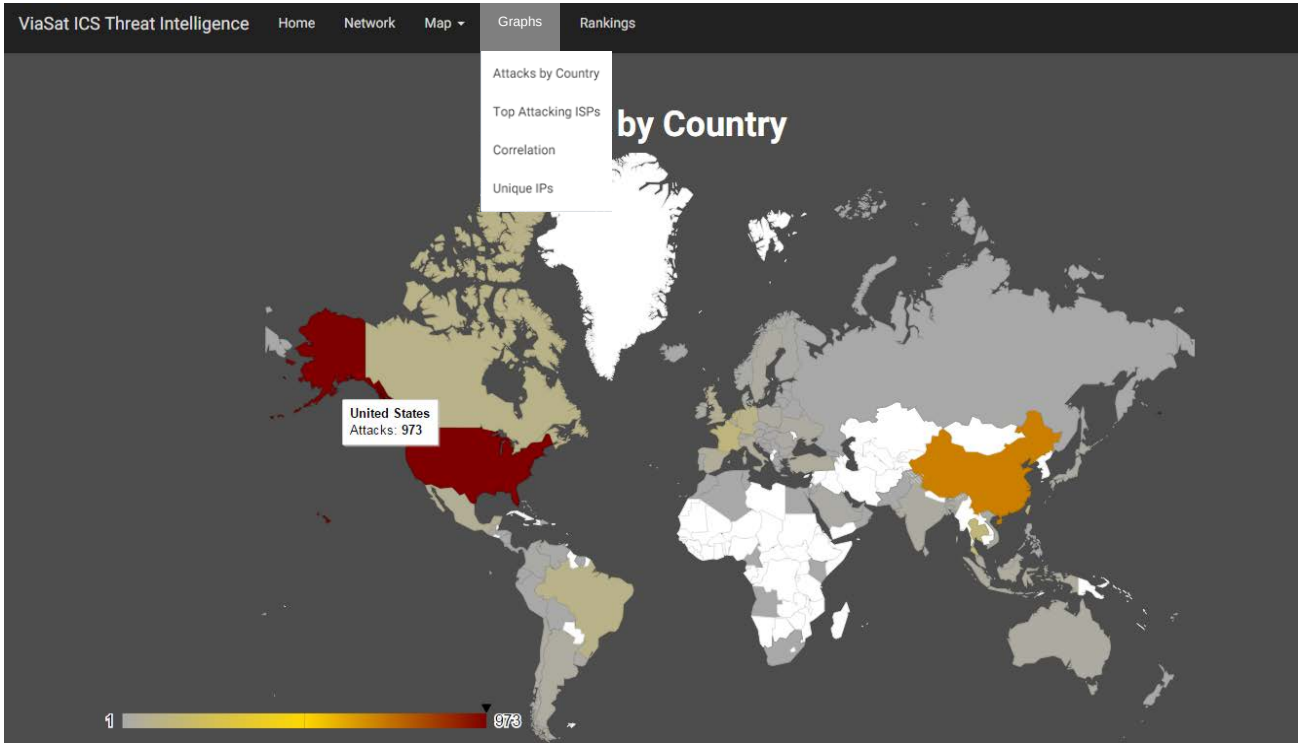
TOR (The Onion Router) Evasion?



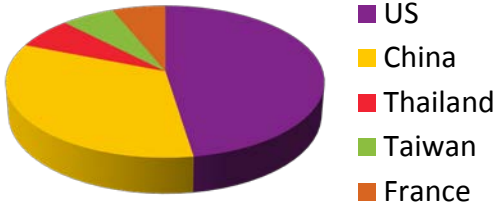
Attacks against HMIs?



Not that we're keeping score…

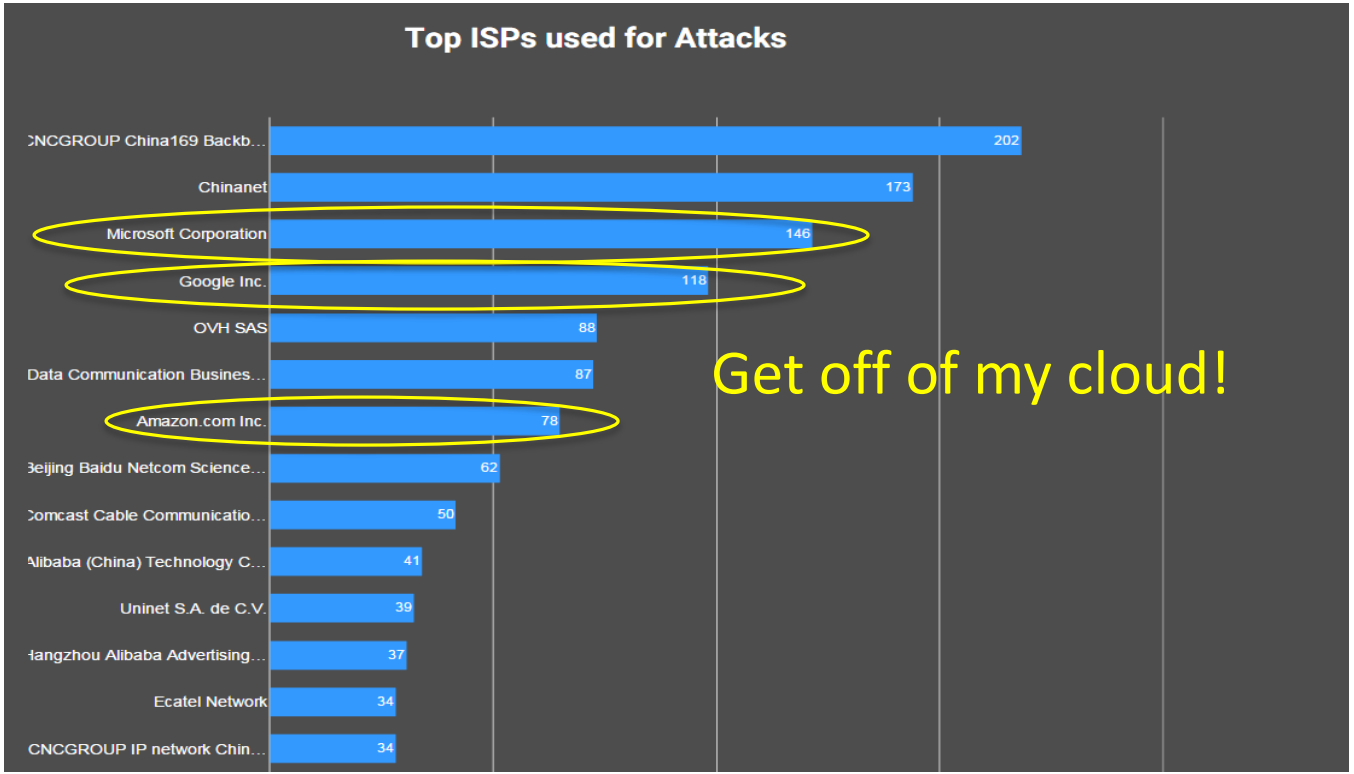


Attacks



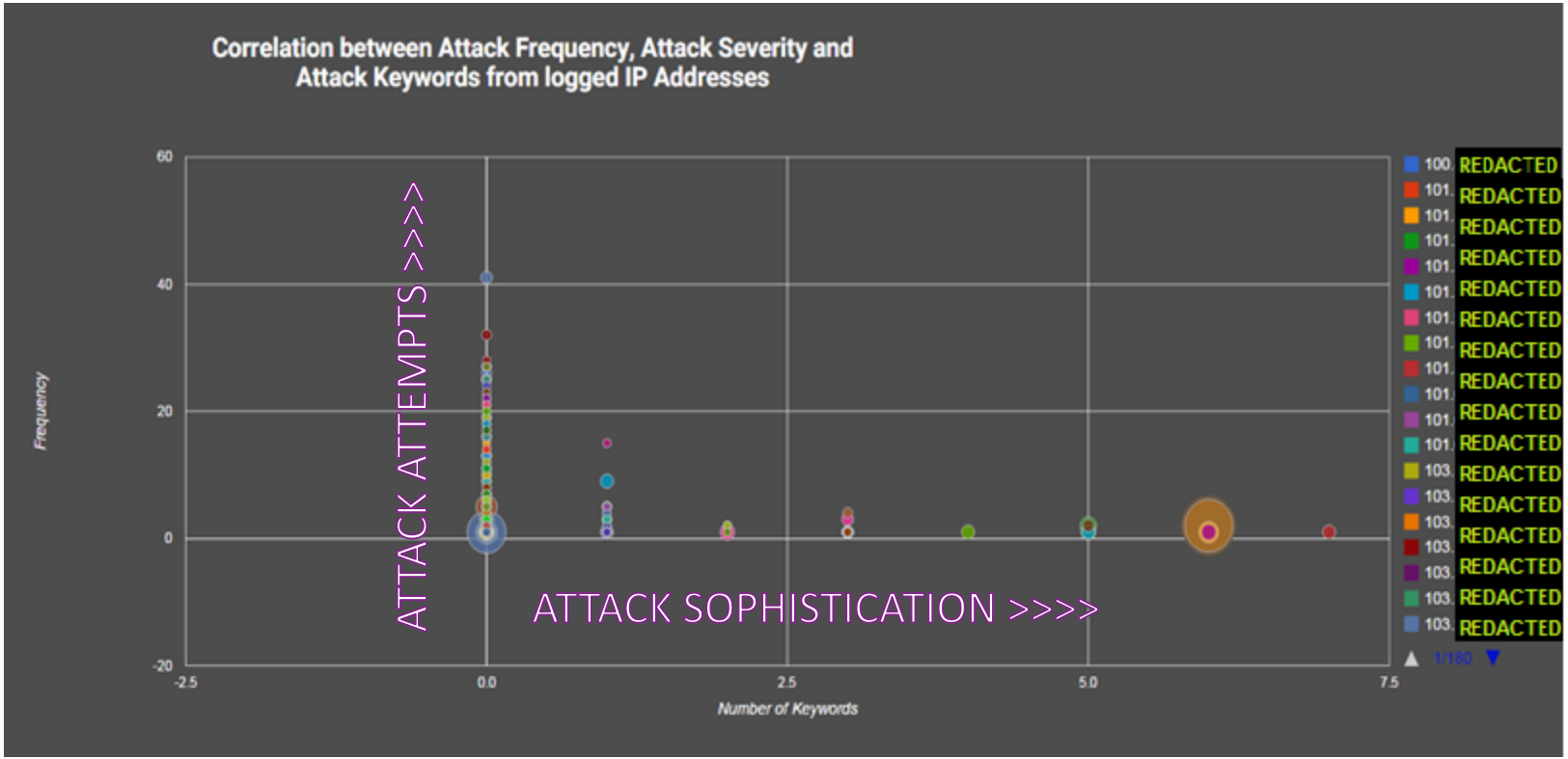
US	973
China	685
Thailand	137
Taiwan	126
France	126
Netherlands	125

Top Internet Service Providers



Get off of my cloud!

Correlation

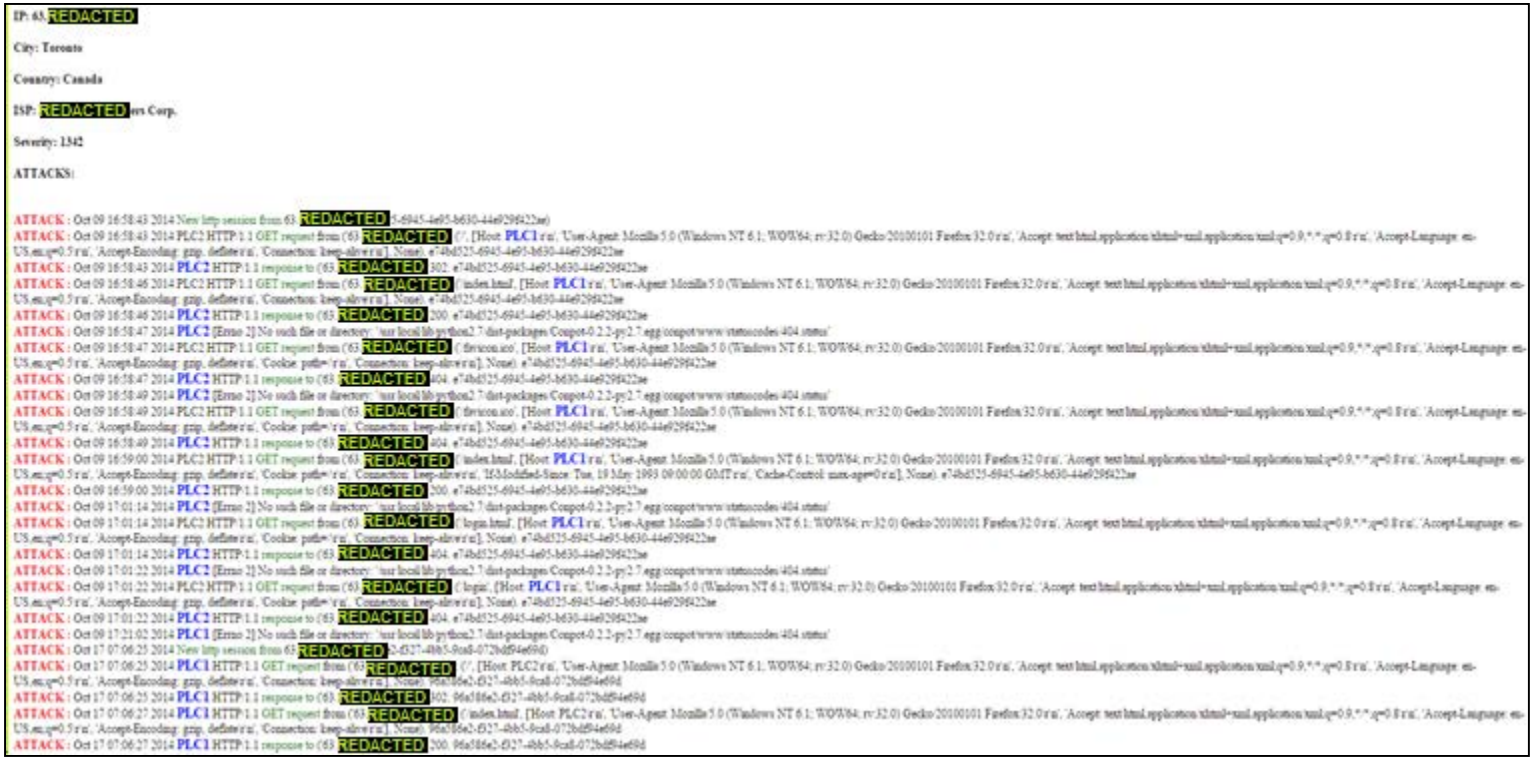


Rankings

	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: REDACTEDers 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Connection: keep-alive:rs'], 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Connection: keep-alive:rs'], 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Cookie: path=/:rs', 'Connection: keep-alive:rs'], 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Cookie: path=/:rs', 'Connection: keep-alive:rs'], 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Cookie: path=/:rs', 'Connection: keep-alive:rs', 'If-Modified-Since: Tue, 19 May 1993 09:00:00 GMT:rs', 'Cache-Control: max-age=0:rs'], 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Cookie: path=/:rs', 'Connection: keep-alive:rs'], 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:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Cookie: path=/:rs', 'Connection: keep-alive:rs'], 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-f327-4bb5-9ca8-072bdf94e69d)
ATTACK : Oct 17 07:06:25 2014 PLC1 HTTP 1.1 GET request from (63.REDACTED (/', [Host: PLC2:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Connection: keep-alive:rs'], None), 96a586e2-f327-4bb5-9ca8-072bdf94e69d
ATTACK : Oct 17 07:06:25 2014 PLC1 HTTP 1.1 response to (63.REDACTED:302, 96a586e2-f327-4bb5-9ca8-072bdf94e69d
ATTACK : Oct 17 07:06:27 2014 PLC1 HTTP 1.1 GET request from (63.REDACTED (/index.html', [Host: PLC2:rs', 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0:rs', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8:rs', 'Accept-Language: en-US,en;q=0.5:rs', 'Accept-Encoding: gzip, deflate:rs', 'Connection: keep-alive:rs'], None), 96a586e2-f327-4bb5-9ca8-072bdf94e69d
ATTACK : Oct 17 07:06:27 2014 PLC1 HTTP 1.1 response to (63.REDACTED:200, 96a586e2-f327-4bb5-9ca8-072bdf94e69d

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