## RSAC Studio



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

#### **James Heyen**

Systems Engineer
ViaSat - Secure Network Systems
@jlheyen



## August 14, 2003 - The Saga begins.....







#### **Timeline – Industrial Malware**



#### Slammer

- Davis-Besse Nuclear Plant
- ·Plant monitoring offline for 5-6 hours

#### Stuxnet

- USB infection
- Natanz Facility
- · Controller Sabotage

#### Mahdi

- Malicious PDF/PPT
- Cyber Espionage
- Mainly in Middle East

#### Shamoon

- ·Oil and Gas in GCC
- •30K+ Devices Wiped

2003



2009



2010



2011



2012



2013



#### **Night Dragon**

- Oil and Gas Majors
- Sensitive Information Stolen

#### Operations

#### Aurora

- APT
- Target Hi-Tech
- Defense
- Source Code
- Originated from CN

#### DuQu

- Stuxnet Variant
- Backdoor Rootkit

#### Flame

- Keystroke Logger
- Screenshot
- Cyber Espionage
- Mainly in Middle East

#### Red October

- Malicious PDF/PPT
- Cyber Espionage
- Swiss Knife of Malware

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

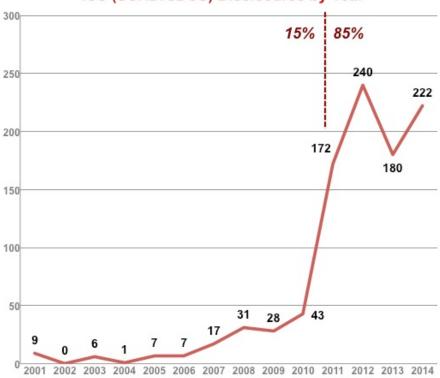




#### **Full Disclosure**









## **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



Validate System
Attacks

Identify Nature of Attacks

Determine Actual Damages

**Quantify Impact** 



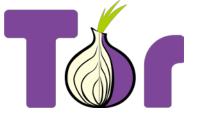
## Requirements



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



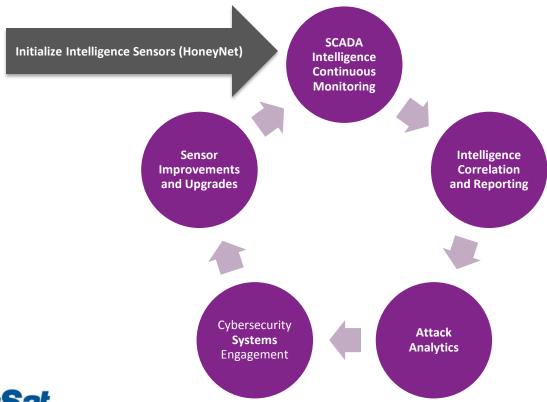






## **SCADA Intelligence Gathering Cycle**







### Myth or Reality?

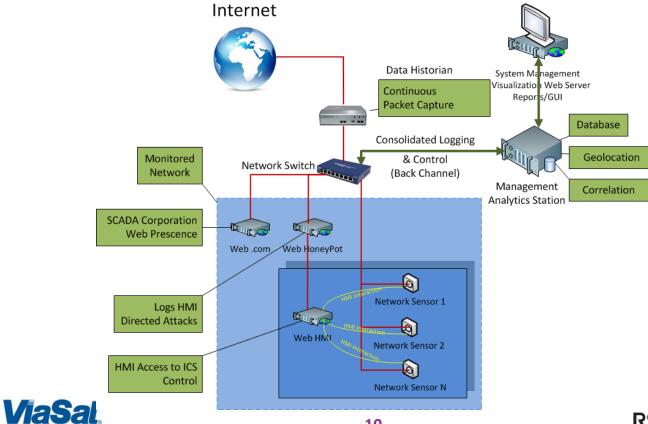






#### **SCADA Intelligence System Architecture**





#### **Low Interaction – plcscan.py**

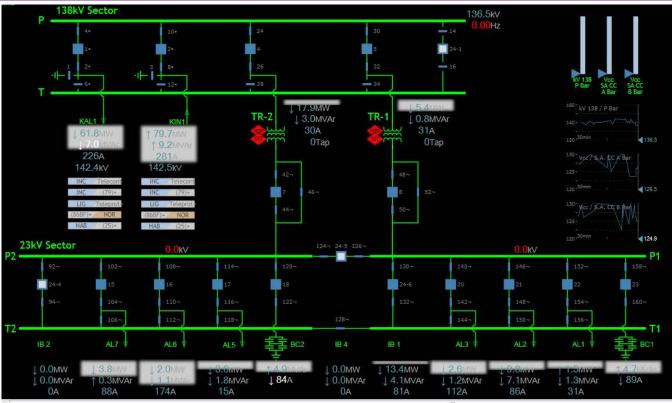


```
can start...
     .31.114:102 S7comm (src tsap=0x100, dst tsap=0x102)
                                            Module
                  : v.0.0
 Name of the PLC
                 : Power Grid 2
                                            Name of the module
                  : Siemens, SIMANTIC S7-300
                                            Plant identification
 Copyright : Original Siemens Equipment
                                            (4f726967696e616c205369656d656e732045717569706d656e74000A0000
 Serial number of module : 94233102
 Module type name : IM351-8 PN/DP CPU
 OEM ID of a module
 Location designation of a module:
     .31.114:502 Modbus/TCP
 Unit ID: 0
  Device:
 Unit ID: 255
  Device:
Scan complete
```



#### **Medium and High Interaction**

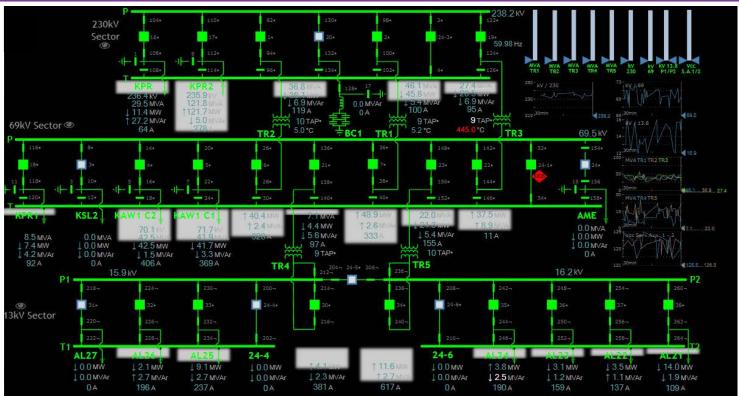






#### **Medium and High Interaction**

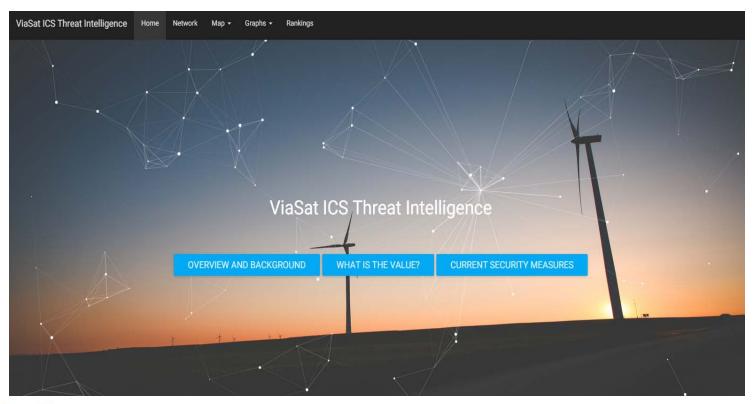






#### And we have liftoff....

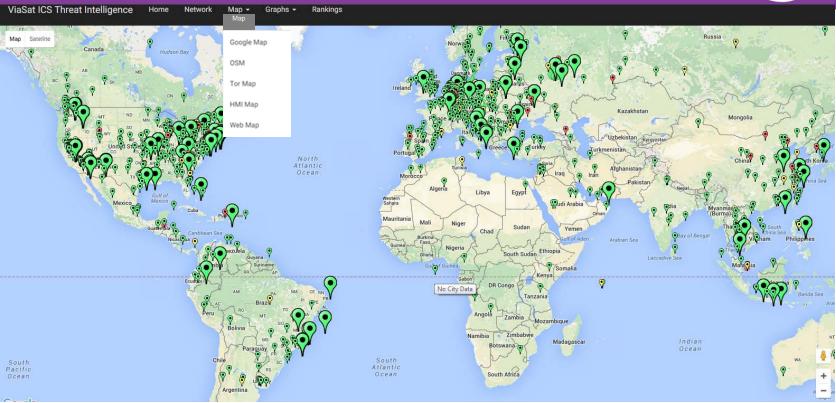






#### GeoLocation, GeoLocation!

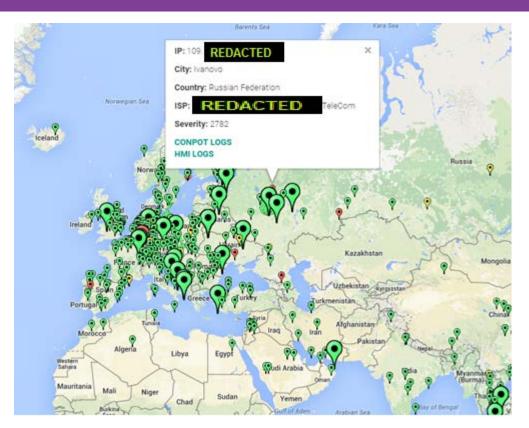






#### Attack Profile - Russian Federation - SEV 2782

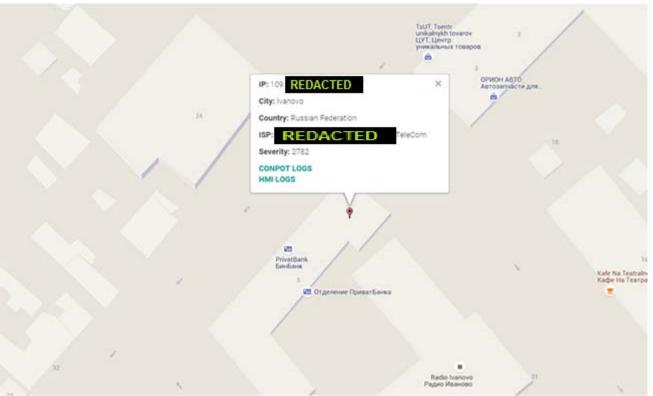






## **Anybody Home?**

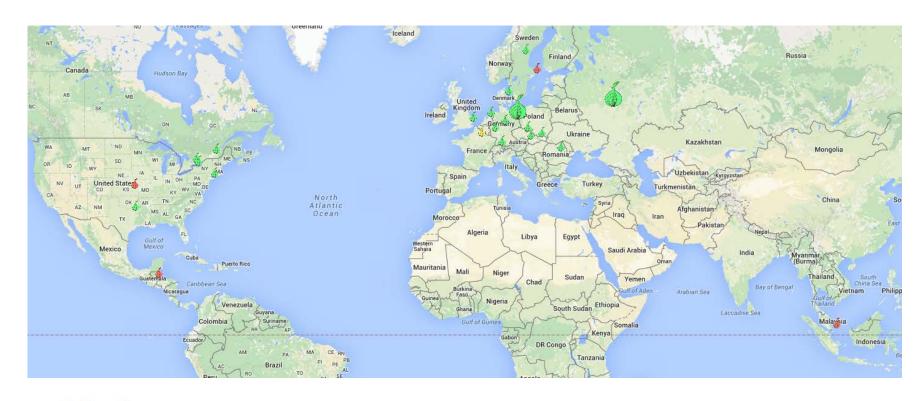






## **TOR (The Onion Router) Evasion?**

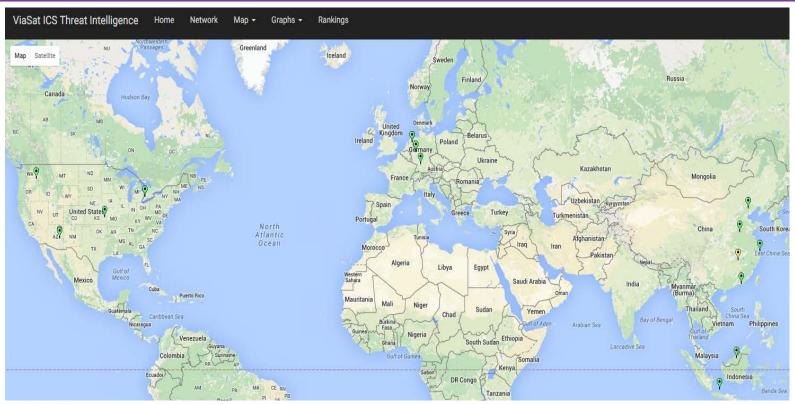






## **Attacks against HMIs?**





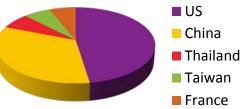


## Not that we're keeping score...





#### **Attacks**

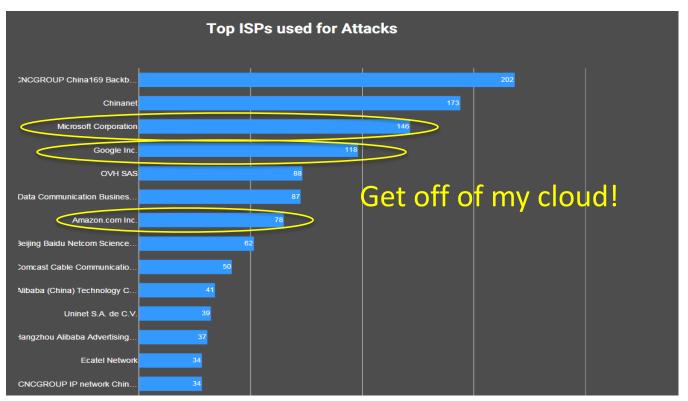


| US          | 973 |
|-------------|-----|
| China       | 685 |
| Thailand    | 137 |
| Taiwan      | 126 |
| France      | 126 |
| Netherlands | 125 |



#### **Top Internet Service Providers**

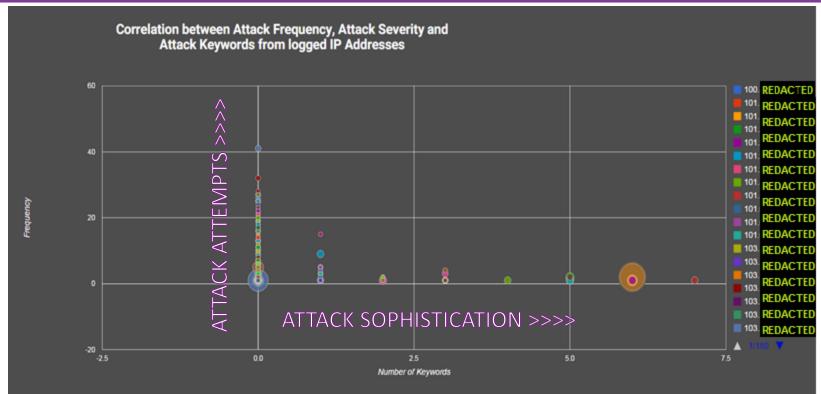






#### Correlation







## Rankings



|     | jp.         | IP HTML | Line Count | Keyword Count | Keywords Used   | Day Count  | Dates   | Country            |
|-----|-------------|---------|------------|---------------|---|------------|---|--------------------|
|     | s REDACTED  |         | 16748      |               | passwil<br>password<br>Bad request syntax<br>etc<br>root<br>Bad HTTP  | 2          | Monday December 22 2014<br>Monday December 29 2014                      | Netherlands        |
| 2   | 10 REDACTED | Link    | 10236      | •             |   | 5          | Suretay August 23 2015  | United States      |
| 2   | REDACTED    | Link    | 2829       | •             |   | •          | SHOWINGOENTS  | United States      |
| 3   | 19 REDACTED | Link    | 2782       | •             |   | .5         | Tuesday December 30 2014  | Russian Federation |
|     | REDACTED    |         | 2359       |               | grasswed grasswered edo root id_rsa id_dsa                            |            | Friday October 17 2014  | Canada             |
| 330 | REDACTED    | Link    | 1611       | 0             |   | 1          | Tuesday September 08 2015   | Korea Republic of  |
| 7   | 63 REDACTED | Link    | 1342       | •             | password<br>password<br>etc<br>id_rsa<br>id_dsa                       | <b>2</b> ( | Thursday October 09 2014<br>Friday October 17 2014                      | Carnarda           |
|     | 18 REDACTED | Unk     | 1243       | 2             | ssh<br>root   | 1          | Saturday December 13 2014   | Australia          |
| •   | 12 REDACTED | Link    | 1162       |               | password password elc id_rsa id_dsa                                   |            | Thursday September 03 2015  | Romania            |
| 10  | M REDACTED  | Link    | 1046       | •             |   | 1          | Tuesday February 17 2015  | Netherlands        |
| 11  | 32 REDACTED | Link    | 1011       | •             |   | 1          | Thursday October 15 2014  | Netherlands        |
| 12  | ■ REDACTED  | Link    | 1011       | •             |   | 1          | Saturday September 13 2014  | Netherlands        |
| 13  | 19 REDACTED | Link    | 962        | •             |   | 3          | Thursday June 25 2015<br>Tuesday June 30 2015<br>Wednesday July 01 2015 | United States      |
| 14  | ™ REDACTED  | Link    | 535        | •             | passwd<br>password<br>flud request syntax<br>sab<br>root<br>flud HTTP |            | Sunday August 16 2015   | Dominican Republic |
| 15  | az REDACTED | Link    | 852        | 5             | password<br>Bad request syntax<br>ssh                                 | ,          | Sunday December 14 2014   | United States      |

- 16748 Lines
- Recon
- Coordinated Attack



#### Details, Evidence and Attacker Profiling



```
IP: 63. REDACTED
 City: Toronto
 Country: Canada
 ISP: REDACTED ors Corp.
  Security: 1342
  ATTACKS
  ATTACK: Oct 09 16:58:43 2014 New littp seizion from 63 REDACTED 5:6945-4e95-8630-44e929822ae)
  ATTACK : Oct 09 16:58-83 2014 PLC2 HTTP 1.1 GET request from (6) REDACTED (*/. [Host PLC2 rs., Vast-Apast Monillo 5.0 (Windows NT 6.1; WOW64; rr 32 0) Gecko 20100101 Factor 32 0 rs., 'Accept test bind application tends—sun application tends—s
 US.emp=0.5 rm; Accept Encoding gap, define rm; Connection Resp. alove rm; None), e74bd525-6945-4e95-b690-44e929422be
 ATTACK: On 09 16:30:43 2014 PLC2 HTTP:1.1 response to (65 REDACTED 302: e74bb525-6945-4695-b630-4446/29525be
ATTACK 10:1916/3:49 2014 FLC2 HTTP-11 GET request from (6) REDACTED (modes hand, [Host PLC1 rat, United Agent Monitor's NT 61; WOW84; rv32.0) Godes 20100011 Faction 32.0 rat, Accept non-hand, application hand, application hand, published hand, published hand, application 
  ATTACK: Oct 09 16:59:47 2014 PLC2 (Erran 2) No such file or directory "sur local bit systems 7 dast-packages Coupot 0.2.2-pv2.7 egg coupot www.stemscodes 404 stems."
  ATTACK: On 99 16:39 47 2014 PLC2 HTTP 1.1 GET requirer from (65 REDACTED) (francous co., [Host PLC1 rs., User-Agent Monthly NT 61: WOW64; rv 32:00 Getics 20000001 Fastina 32 0 rs., 'Accept west little Japphoness which was a spin or a contract of the cont
 US.es.y=0.5 no. Accept Encoding grap, definence. Cookse potter (no. Connection beep-slivens), Note: e74bd325-6945-4e95-b630-44e9596322ee
  ATTACK: Oct 09 16:39:47 2014 PLC2 HTTP:1.1 response to (63 EVED/ACTIED 404 +745d525-6945-4-65-5630-44-6298422ae
  ATTACK: Oct 09 18:58:49 2014 PLC2 (Ermo 3) No such file or directors: "our local bit systems 7 dust speckages Compot 0.2.2-ps 2.1 egg compot www.statuscodes 404 status"
 ATTACK: On 99 16-58-49 2014 PLC2 HTTP 1 I GET request from (65 REDACTED) ( for some of the Control of the Contr
 ATTACK: Oct 09 16:33:49 2014 PLC: HTTP:1.1 response to (6): SEEDAGTED 404 e74bd325:4945-4e95-b630-44e925022se
  ATTACK: Ont 09:16:9:00 2014 PLC3 HTTP: 1 GET request from (6) (ED)ACTED (mides html, [Nort PLC1 rs. User-Agent Monitor's NT 61: WOWNE, rs 2:0) Gedo: 20:00101 Facility PLC3 HTTP: 1 GET request from (6) (ED)ACTED (mides html; Flority PLC1 rs. (Arrept Language en-
 US.m.; "O Sra", "Acopy Encoding, pap, deflewing, "Cockie path" ra", "Connection Leop-thewing, "HASOdified-Since Tox, 19 May 1993 09 00 00 OMTra", Cache Control max-aper0ral, None, e74b5131-5943-4495-5650-444929522he
  ATTACK: Oct 09 16:59:00 2014 PLC2 HTTP:1.1 response to (6) REDACTED 200, e745d525-6945-4e95-5630-44e929522ae
 ATTACK: Oct 09 17 01:14 2014 PLC2 (Error 2) No such file or directory "sur local bit probate." I dist quelanges Compot 0.2.3-pr.2.7 ear compot was status codes 404 status."
  ATTACK: Oct 09 17-01 14 2014 PLC2 HTTP 1 1 OET request from (6) REDACTED (logar lated, PLC2 res. Cores a Month of Olivations NT 61: WOWSE re 17-01 Gende 20100001 Forder 20 Orac Accept text bent application within variant polication within variant polication within variant polication.
  US en. p=0.5 rm. 'Accept Encoding grip, define rm.' Cookse point rm.' Connection, keep-sire rm.', Noon, e745d315-5945-4e95-5650-44e9295422as
  ATTACK: 0ct 09 17 01:14 2014 PLC2 HTTP-1.1 response to (6) REDACTED 404, e74b525-6945-4e95-b630-4be929922be
  ATTACK: Oct 09 17:01:22:2014 PLC2 (Erms 2) No such file or directors: "turn local life by those 2.7 dast-packages Compot-0.2.2-ps/2.7 egg compot terms statuscodes 404 status."
 ATTACK | Oct 09 17 01 22 2014 FLC2 HTTP 1 1 OET request from (6) TEDACTED (Inguis: [Not PLC1 rs. Uses Agent Monitor's Monitor's NT 61, WOWSH, ev 22 0) Octo 20100101 Factor's 2 0 rs. (Accept test familiapplication state) **mail: population state | mail: population state |
US.au.;=0.5 rs.', 'Accept Encoding: gap, definer is', Cookie petite' rs', Connection beep-almer is'], Nossi, e74bd225-6945-4e75-b630-44e9296922se
ATTACK: Oct 09 17:01:22 2014 PLC2 HTTP:1.1 response to (63 REDACTIED) 404, e74bd525-6945-4e95-b630-44e9296922se
  ATTACK: On 99 17 21 92 2014 PLC1 (Error 21 No such file or directory: Year local lib by those 2 7 day outcomes Compete 0.2.2-ey 2.7 agg compet wave instructed with status
 ATTACK: Oct 17 07:06:25 2014 New littly session from 65 REDACTED 2:6321-4965-9m8-072hd94e696)
 ATTACK: On 17 07:06 25 2014 PLC1 HTTP:1.1 GET: report from (6 TEDACTED) (*, [Host PLC2'ex, Voer-Agent. Monille 5 0 (Windows NT 6.1, WOW84; nr 32.0) Gecks 20100101 Factor 32.0 nr. Accept next html.application whitely wait application with the positive of a property of the contraction of the positive of a property of the contraction of the positive of a property of the contraction of the positive of the positive of the contraction of the positive of the positiv
 ATTACK: Oct 17 07:06:25:3014 PLC1 HTTP:1.1 response to (6). REDACTED 102:96x166x3:627-48b5-9cx8-072bd694e696
  ATTACK: On 17 07 06 27 2014 PLC1 HTTP 1.1 OET report from (6) Tengos from (6) 
US.en.p=0.5 rm. Accept Encoding grap, definition. Connection Even-alore rm.], Note: 96a186a1-611-6b5-6ca8-073bdf94e69d
  ATTACK: Oct 17 07 06:27 2014 PLC1 HTTP: 1 response to (63 REDACTED) 200. 96s/366c2-6327-4665-9cs8-0726d594e69d
```



## **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



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

760.893.1134

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

