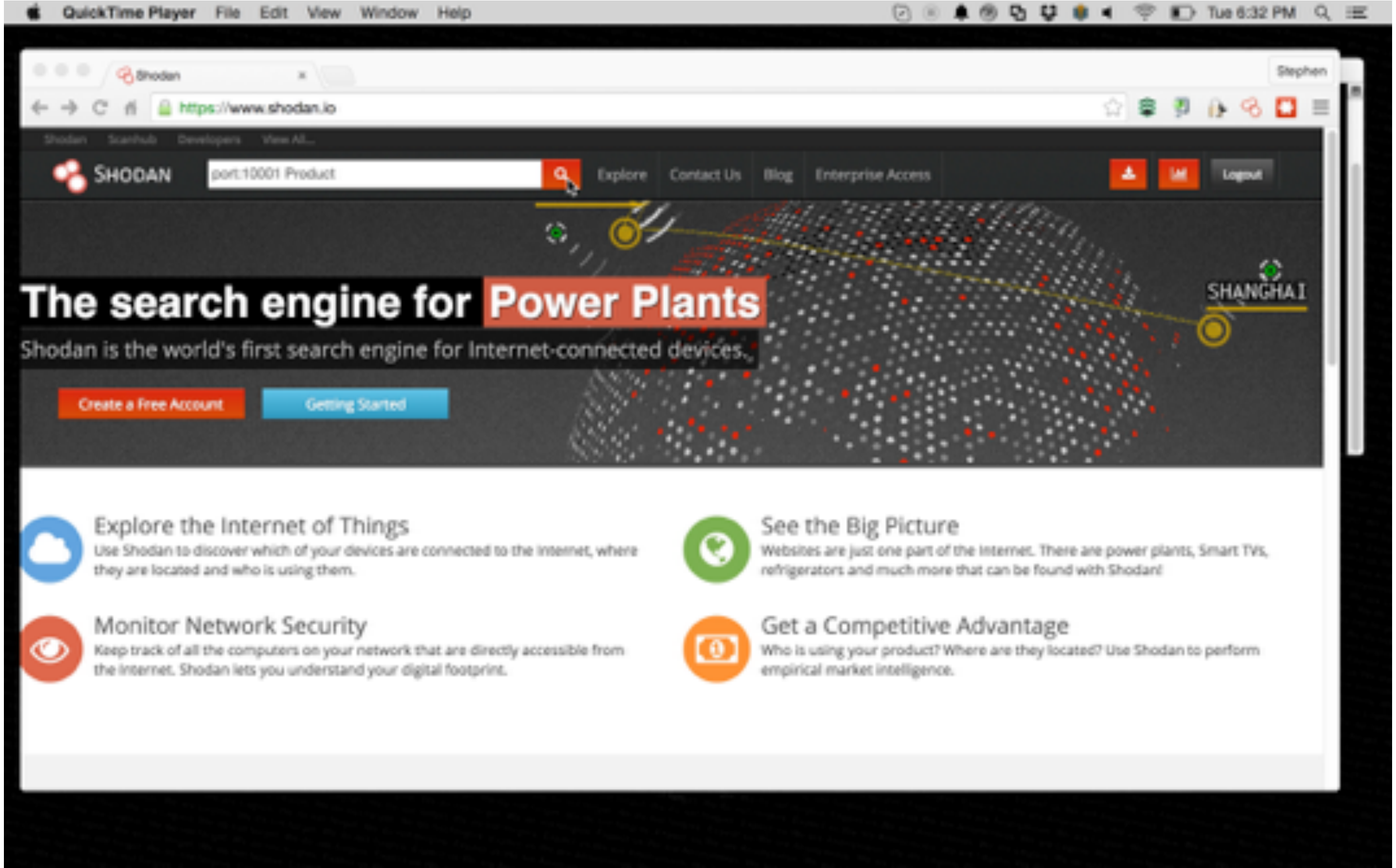
The Little Pump Gauge That Could: Attacks Against Gas Pump Monitoring Systems

Kyle **W**ilhoit
Sr. Threat Researcher
@lowcalspam

Stephen **H**ilt
Sr. Threat Researcher
@sjhilt

Where The “Industry” Is…

SCADA Became Popular.



The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

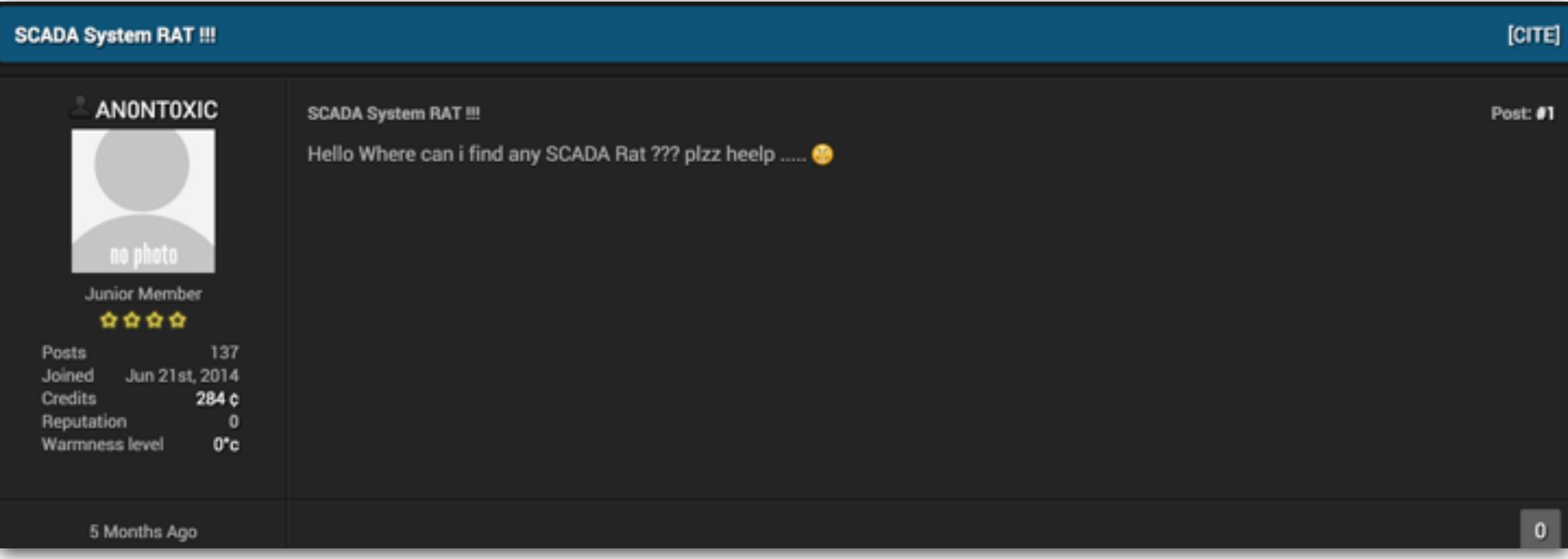
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Threats Began Adapting & Changing.

SCADA Started



SCADA System RAT !!!

[CITE]

ANONTOXIC

Junior Member

☆☆☆☆

Posts	137
Joined	Jun 21st, 2014
Credits	284 ¢
Reputation	0
Warmness level	0°c

SCADA System RAT !!!

Post: #1

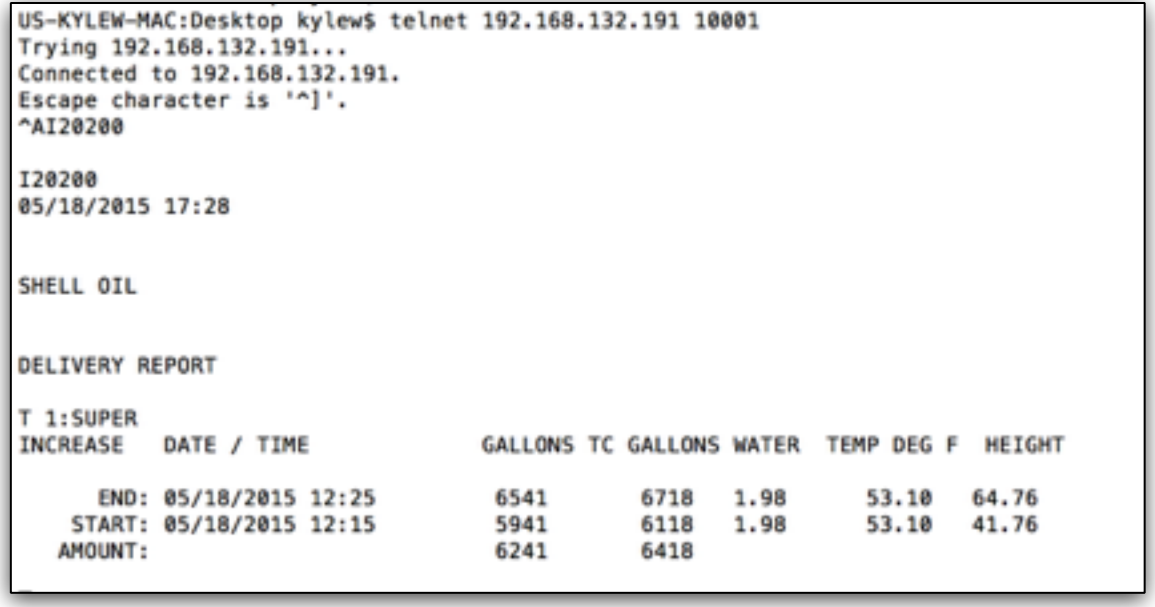
Hello Where can i find any SCADA Rat ??? plzz heelp ..... 😐

5 Months Ago

0

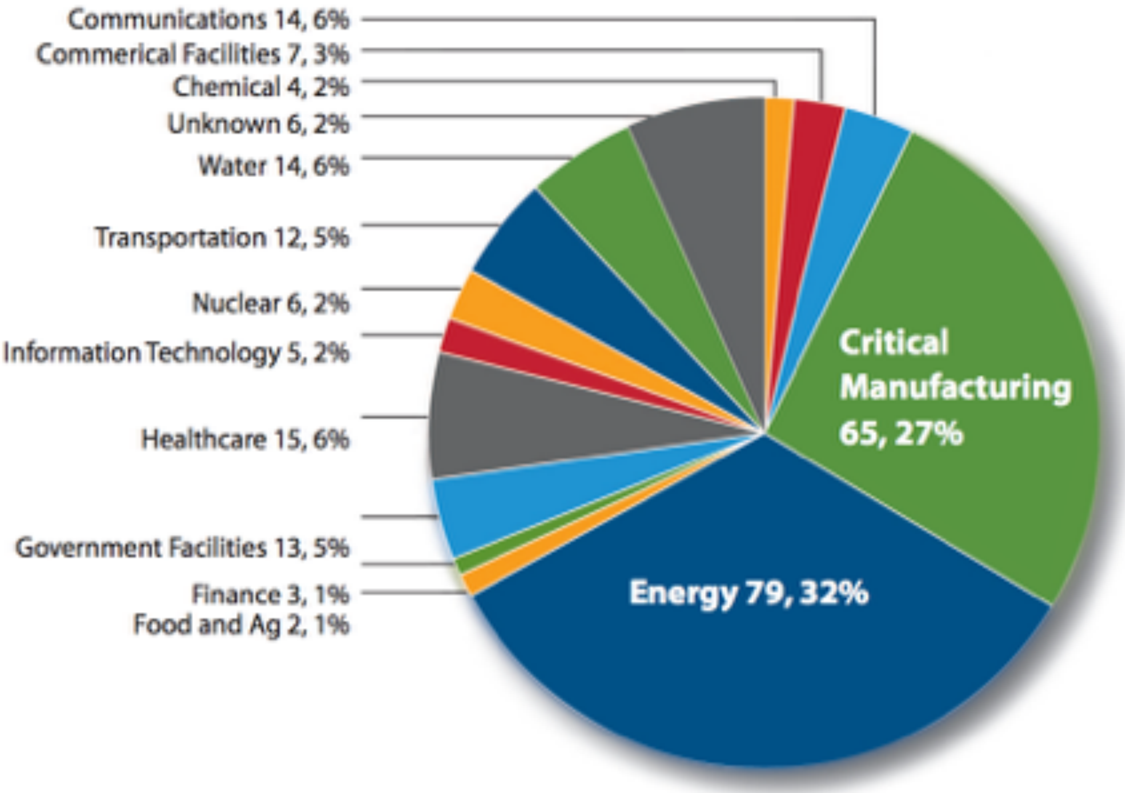
Trading in Dark Corners…

Vulnerabilities Continued…

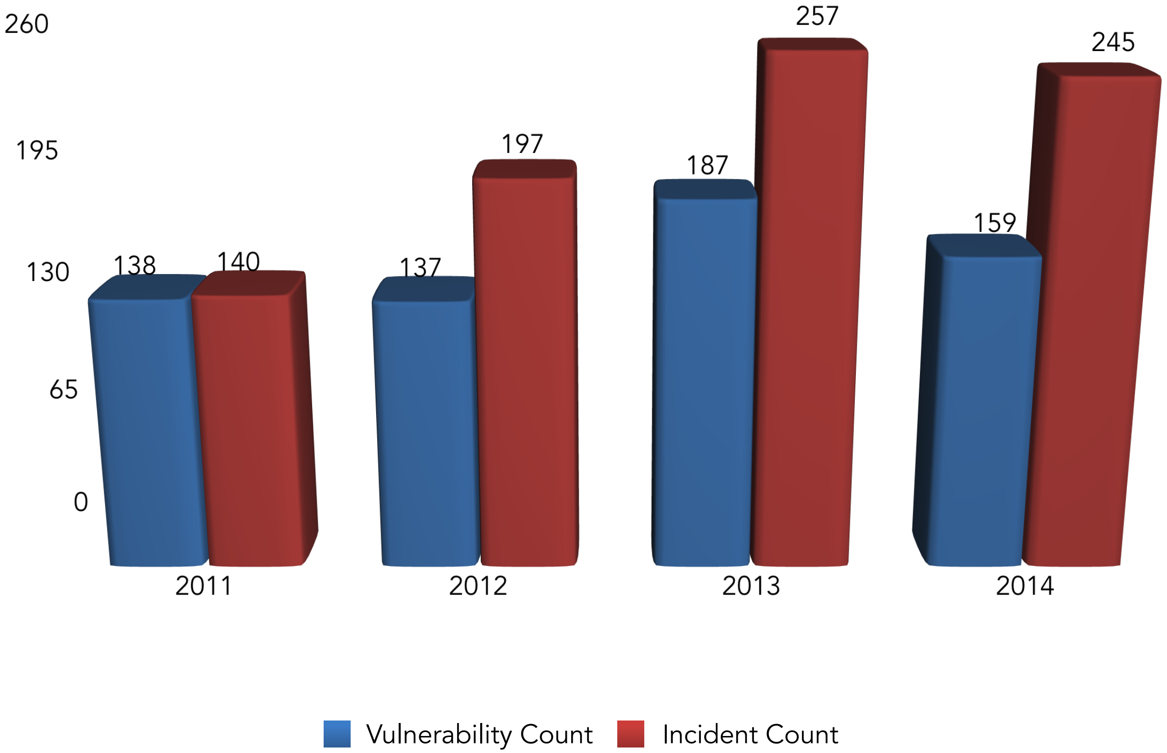


```
US-KYLEW-MAC:Desktop kylew$ telnet 192.168.132.191 10001
Trying 192.168.132.191...
Connected to 192.168.132.191.
Escape character is '^]'.
^AI20200

I20200
05/18/2015 17:28


SHELL OIL


DELIVERY REPORT

T 1:SUPER
INCREASE   DATE / TIME             GALLONS TC GALLONS WATER  TEMP DEG F  HEIGHT

      END: 05/18/2015 12:25         6541       6718   1.98      53.10   64.76
    START: 05/18/2015 12:15         5941       6118   1.98      53.10   41.76
   AMOUNT:                          6241       6418
```

Reported Incidents in US: 2014



SCADA Vulnerabilities and Incidents Per Year



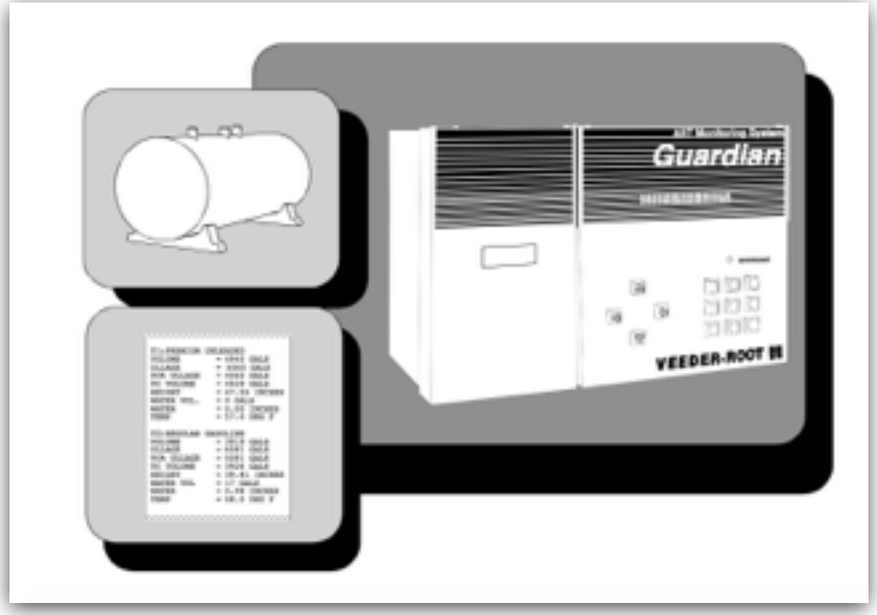
Why Attack SCADA?!

It's Easy

Criminal

Government

Guardian AST…dafuq is it?

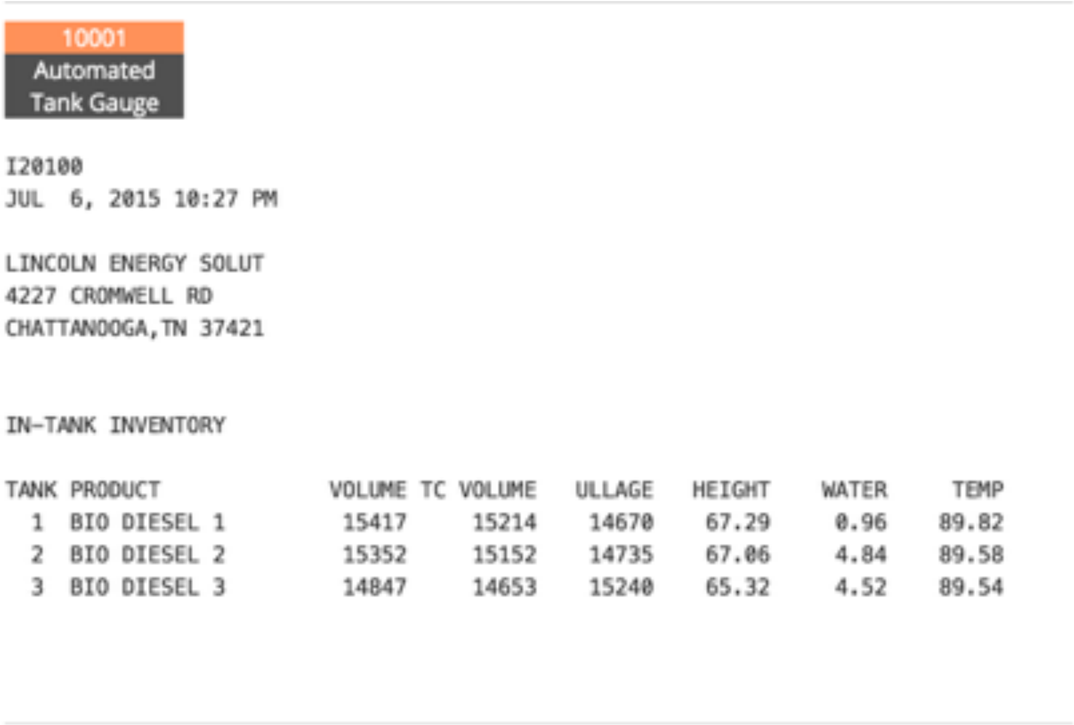


TREND MICRO

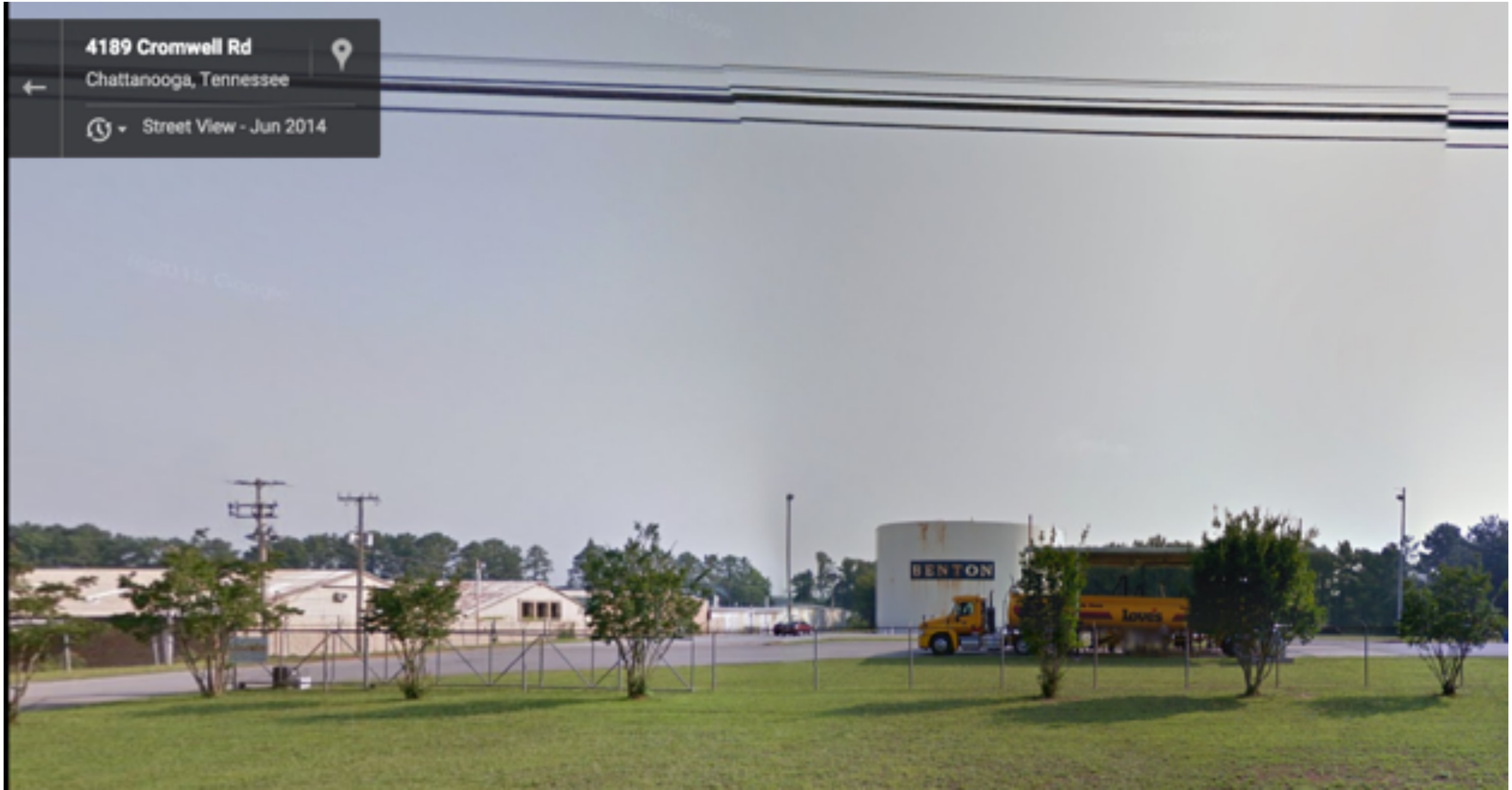
Gas station
Gas station
Gas station
Text

Not All Tanks Are Created Equal

- Gas Station Tanks
- Backup Generator Tanks
- Terminal Station Tanks
- Other Tanks?



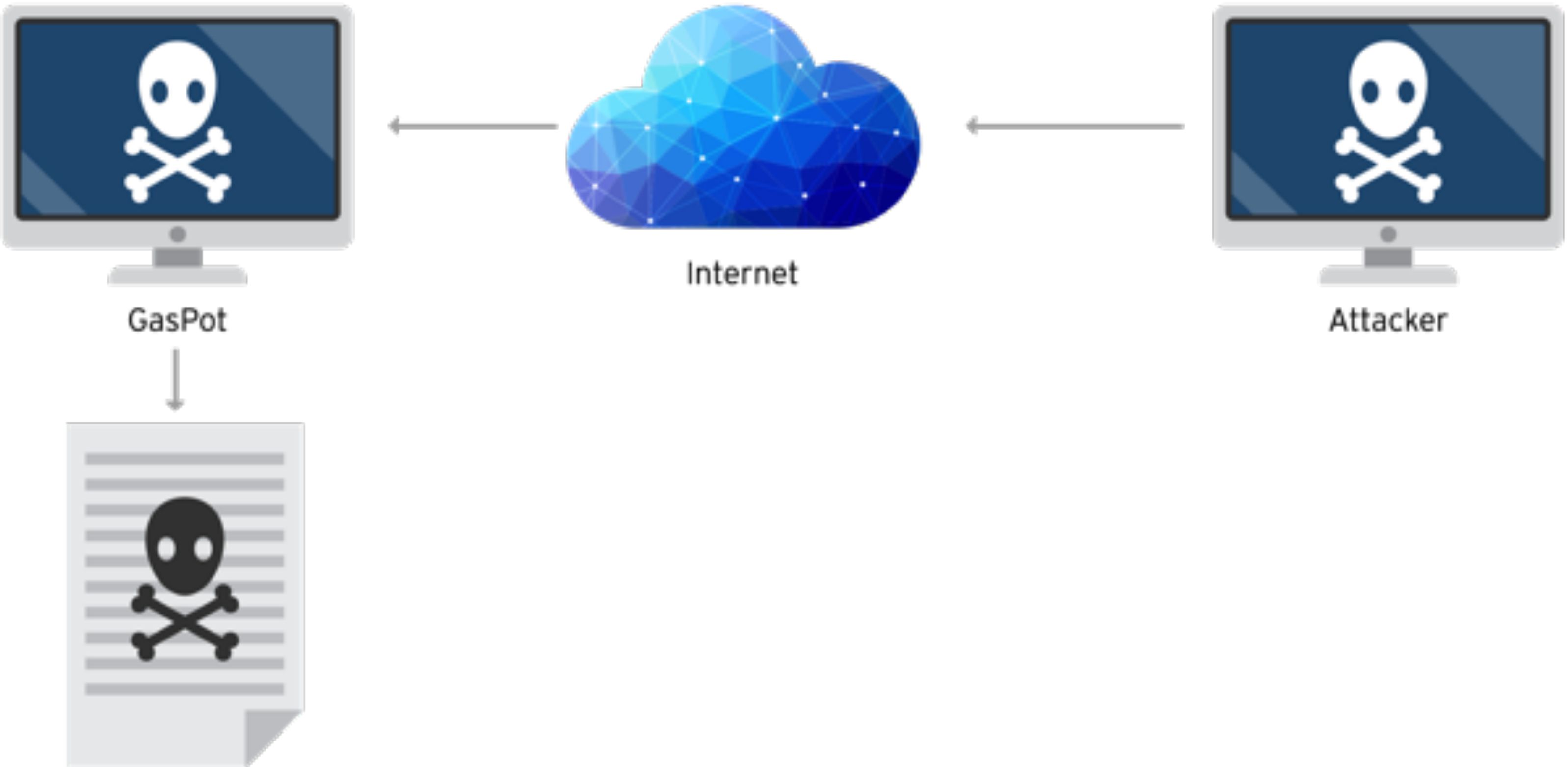
```
I20100
JUL  6, 2015 10:27 PM

LINCOLN ENERGY SOLUT
4227 CROMWELL RD
CHATTANOOGA,TN 37421


IN-TANK INVENTORY

TANK PRODUCT               VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  BIO DIESEL 1           15417      15214    14670    67.29     0.96    89.82
  2  BIO DIESEL 2           15352      15152    14735    67.06     4.84    89.58
  3  BIO DIESEL 3           14847      14653    15240    65.32     4.52    89.54
```


4189 Cromwell Rd
Chattanooga, Tennessee
Street View - Jun 2014
BENTON
Love's

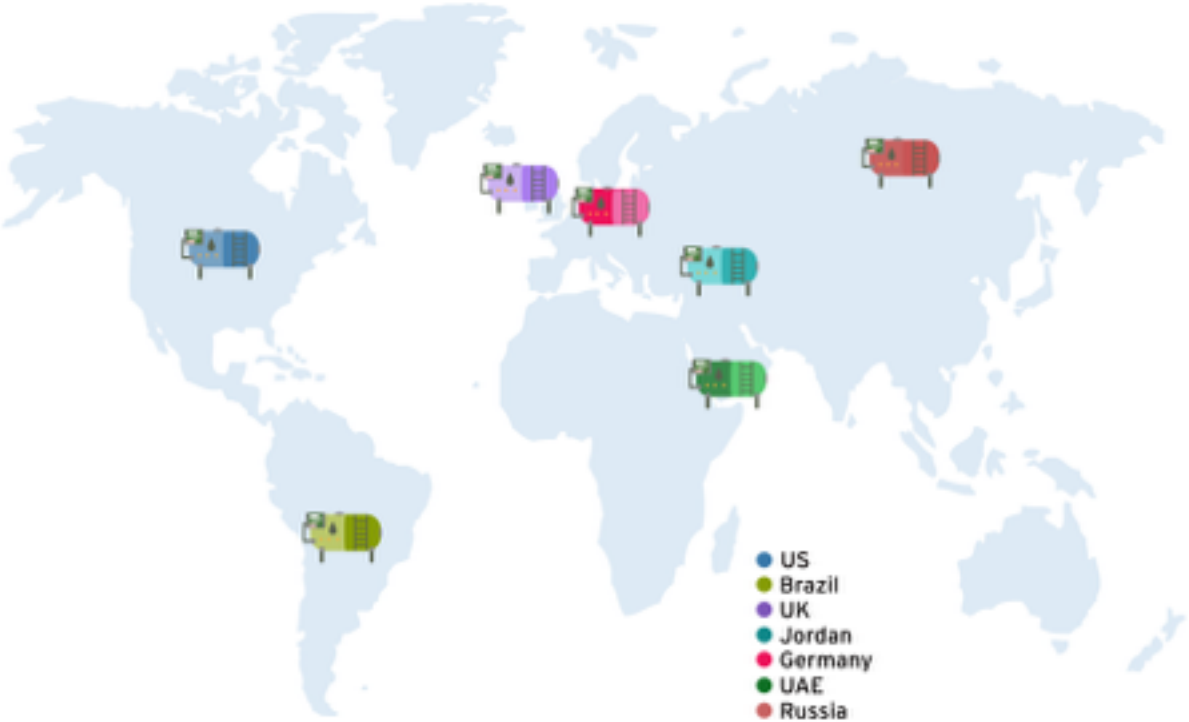
Introducing Gaspot

- HD Moore published his findings on Guardian's that are Internet facing
- Software based gas pump monitor honeypots
- Created to better understand attacks against gas pump monitor systems and non-critical infrastructure
- Derived from Anonymous' attacks against US based gas pumps
- Completely virtualized
- One Python script
- Accepts robust input/output
    - 6 commands

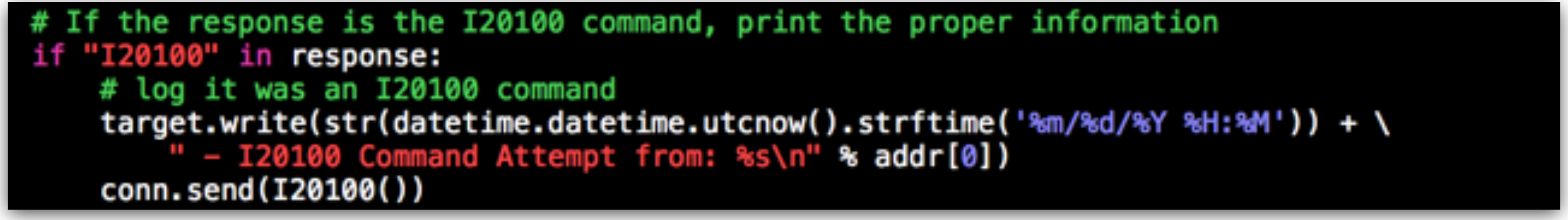
Architecture



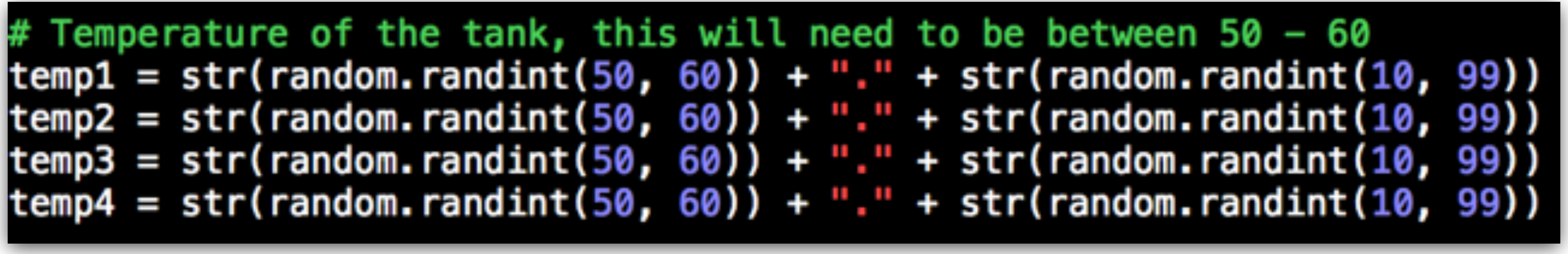
Deployment Locations



Code Considerations

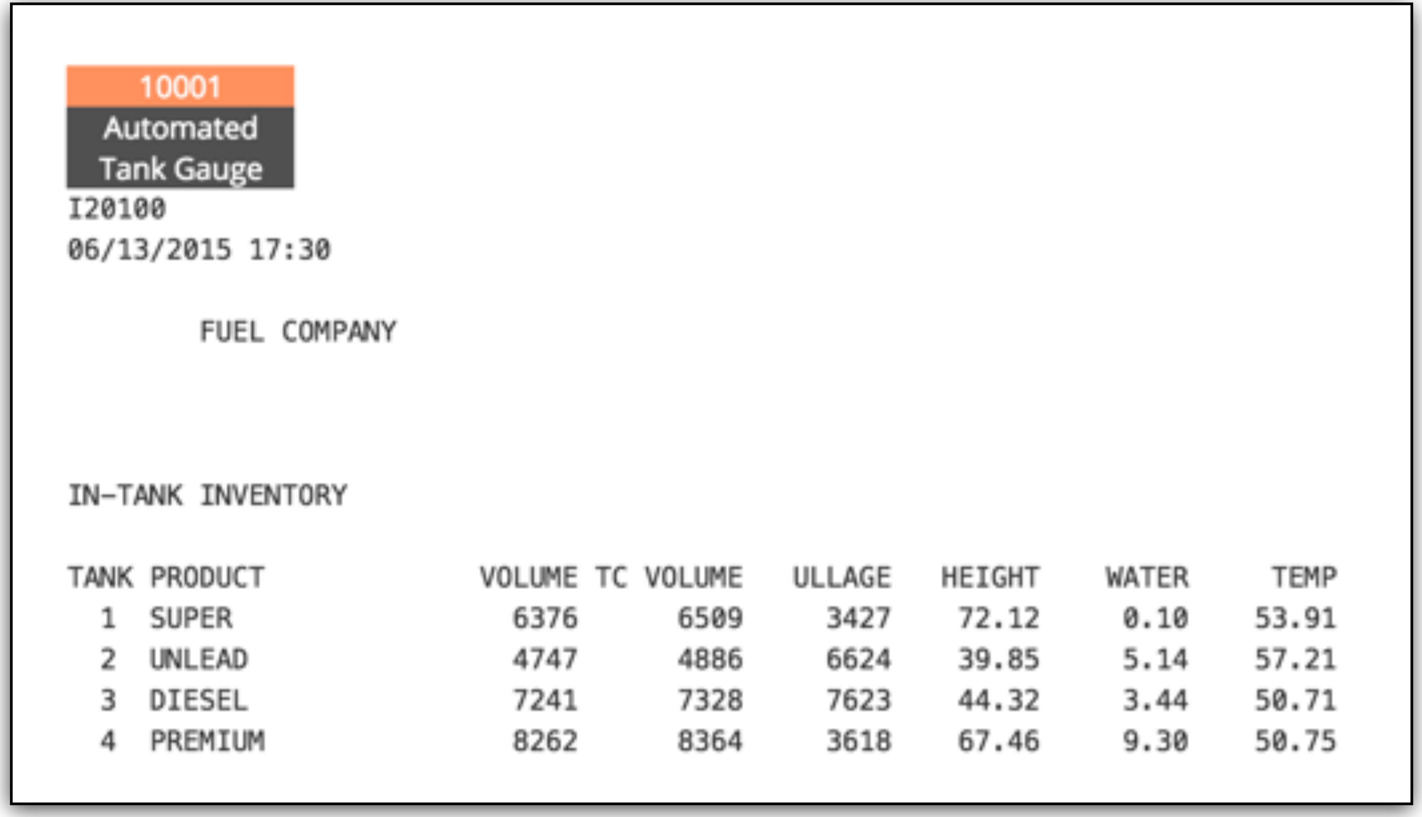


```
# If the response is the I20100 command, print the proper information
if "I20100" in response:
    # log it was an I20100 command
    target.write(str(datetime.datetime.utcnow().strftime('%m/%d/%Y %H:%M')) + \
        " - I20100 Command Attempt from: %s\n" % addr[0])
    conn.send(I20100())
```



```
# Temperature of the tank, this will need to be between 50 - 60
temp1 = str(random.randint(50, 60)) + "." + str(random.randint(10, 99))
temp2 = str(random.randint(50, 60)) + "." + str(random.randint(10, 99))
temp3 = str(random.randint(50, 60)) + "." + str(random.randint(10, 99))
temp4 = str(random.randint(50, 60)) + "." + str(random.randint(10, 99))
```

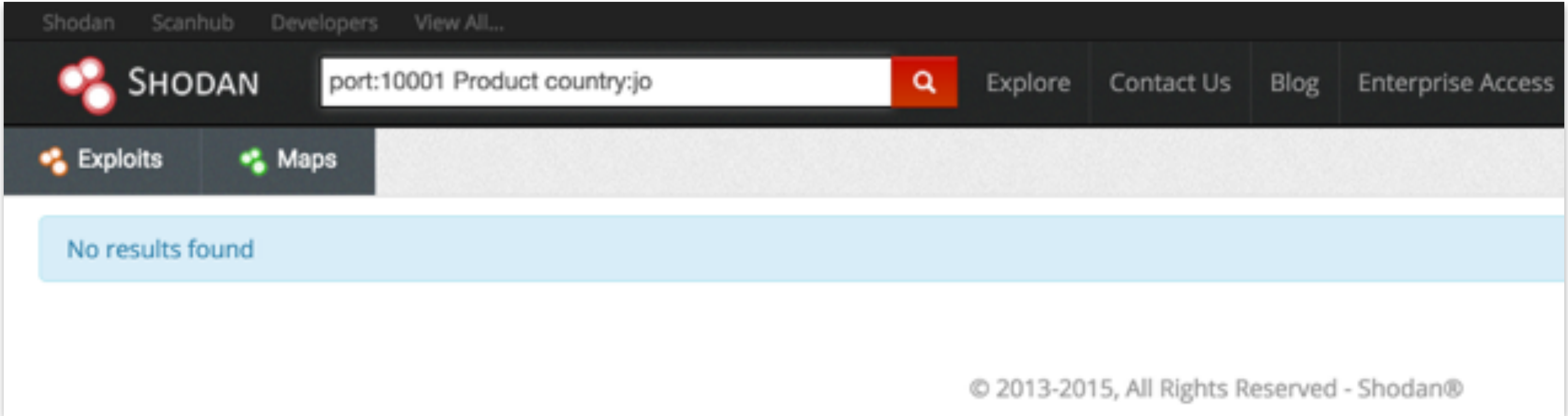
Gaspot on Shodan



```
I20100
06/13/2015 17:30

        FUEL COMPANY



IN-TANK INVENTORY

TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  SUPER                 6376      6509     3427    72.12     0.10    53.91
  2  UNLEAD                4747      4886     6624    39.85     5.14    57.21
  3  DIESEL                7241      7328     7623    44.32     3.44    50.71
  4  PREMIUM               8262      8364     3618    67.46     9.30    50.75
```

Shodan and Gaspot Consideration

- Not all Gaspot instances are on Shodan
- Able to see “organic” growth



port:10001 Product country:jo

No results found

© 2013-2015, All Rights Reserved - Shodan®

Attack Scenarios

- DDoS, bringing inventory control/distribution to a standstill.
- Change of pump names, resulting in incorrect fill of petrol into the tank. (eg: change unleaded to diesel)
- Change in pumping volume, resulting in over or under fill. (For instance, putting the volume as full, when it is empty)
- State sponsored, meaning a pump compromise to siphon off data for possible espionage during a business deal?

Classification of attacks

What They're Not…

- Portscans
- Successful telnet, then nothing
- Server fingerprinting
- Banner grabbing (HTTP GET)

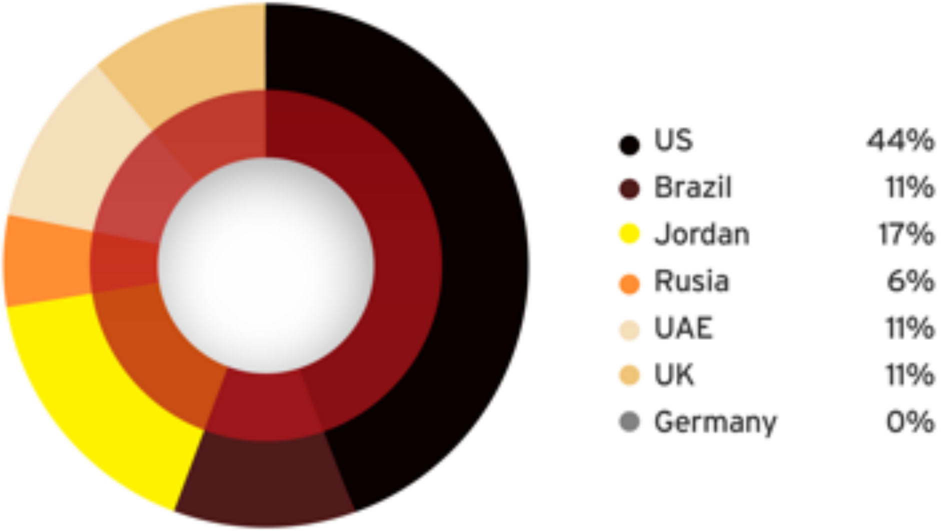
What They Are…

- Successful commands resulting in possible failure
- Fat fingering after telnetting
- Targeted malware
- DoS and DDoS

Attacks…

Attack Breakdown

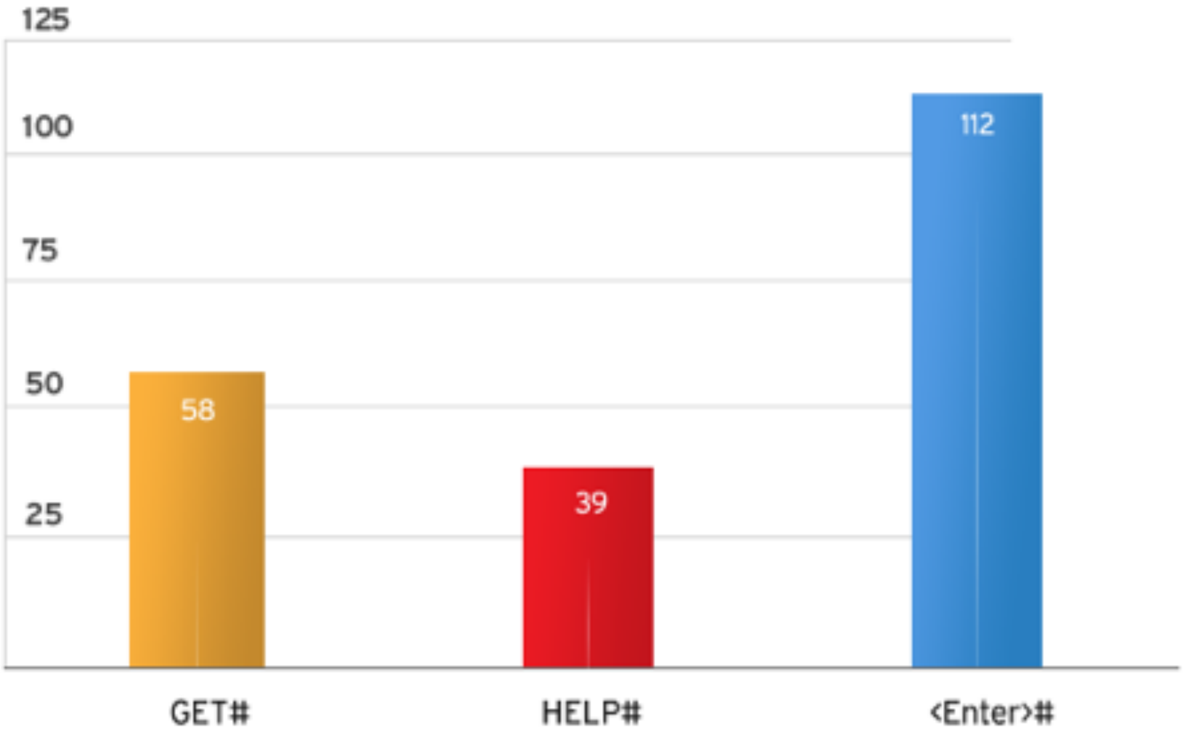
- 4 Pump Modifications
- 12 Pump Queries
- 2 DDoS/DoS Attacks



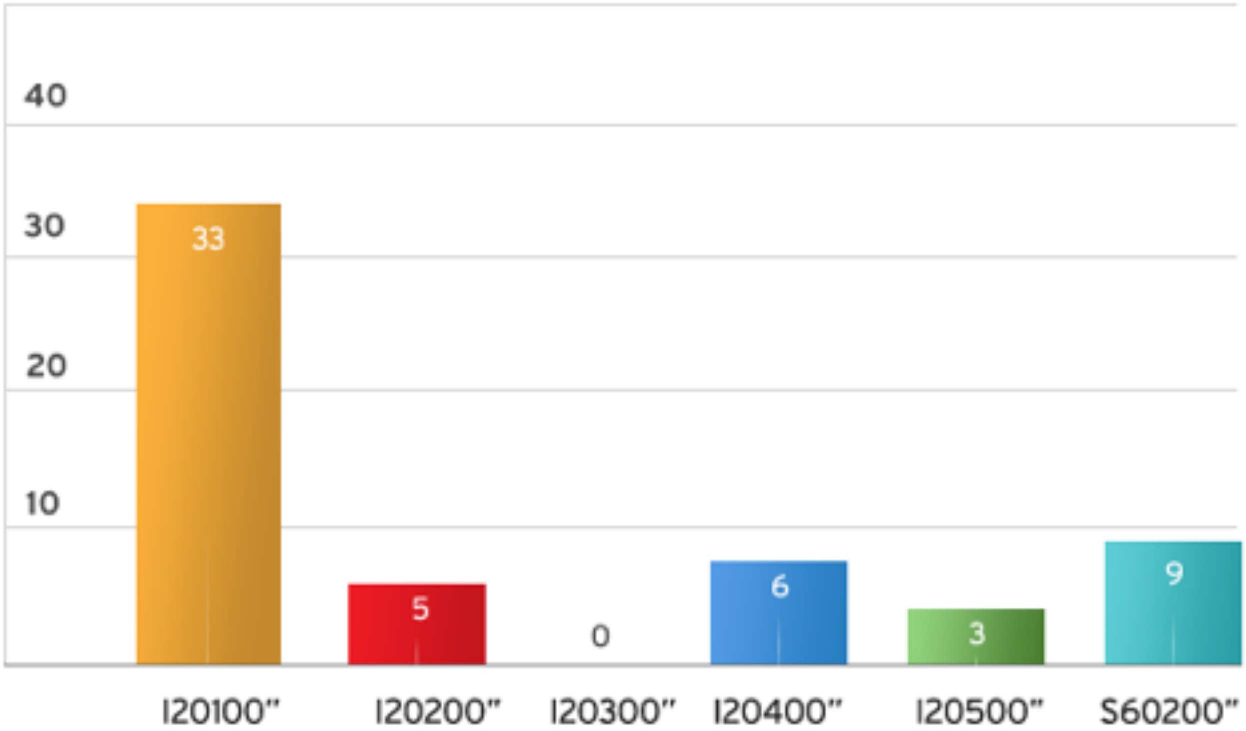
Attack Breakdown

Deployment / Attacker	US	RO	CN	RU	IR	SY	MX	CA
US	3		2				1	2
BR	1		1					
GB				2				
JO					2	1		
DE								
AE		1		1				
RU	1							

Connection Attempts



Valid Commands



Critical **vs.** Non-Critical Infrastructure

- Had a case study from 2013 showing attacks against critical infrastructure
- Wanted to find out if attacks happen to non-critical infrastructure

Attacks- Critical Vs. Non-Critical

- **Critical Infrastructure Honeypots 2013**
  - Deployed in 8 countries
  - 12 total deployments
  - 74 Attacks in total

- **Non- Critical Infrastructure Honeypots 2015**
  - Deployed in 7 countries
  - 10 total deployments
  - 18 Attacks in total

```
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
root@kali:/usr/share/dirbuster/wordlists#
```

Intelligence…?

Syrian Electronic Army

- Came about in 2011
- Supports President Bashar al-Assad
- Performs DDoS, Defacements, malware distribution, spamming, and general mischief
- Defaced CBS, AP, NPR, BBC, Al Jazeera, etc.

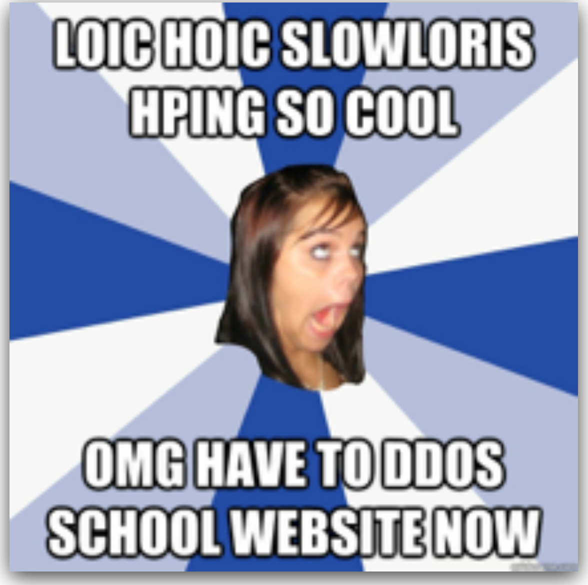
DDoS “Attack”

- DDoS performed for two days
    - Volume based attacks (UDP floods, etc.)
    - Protocol attack (Fragmented packets)
    - Roughly 2Gbps
- Performed on Gaspot in US
- Utilized what appears to be LOIC

GET /app/?
id=**17783745**&msg=**SEAcannn**
GO HTTP/
1.1Host:OBFUSCATED-Agent:
Mozilla/5.0 (Macintosh; U; Intel
Mac OS X 10.5; en-US; rv:
1.9.2.12) Gecko/20101026
Firefox/3.6.12Accept: text/
html,application/xhtml
+xml,application/xml;q=0.9,*/
*;q=0.8Accept-Language: en-
us,en;q=0.5Accept-Encoding:
gzip,deflateAccept

Attribution

- Possibly Syrian Electronic Army
    - 213.178.225.248
    - 213.178.225.232
    - 213.178.225.212
    - Etc.
  - DDoS against Gaspot in US
  - No public disclosure by SEA?
    - dafuq?
    - False flag?


LOIC HOIC SLOWLORIS HPING SO COOL
OMG HAVE TO DDOS SCHOOL WEBSITE NOW

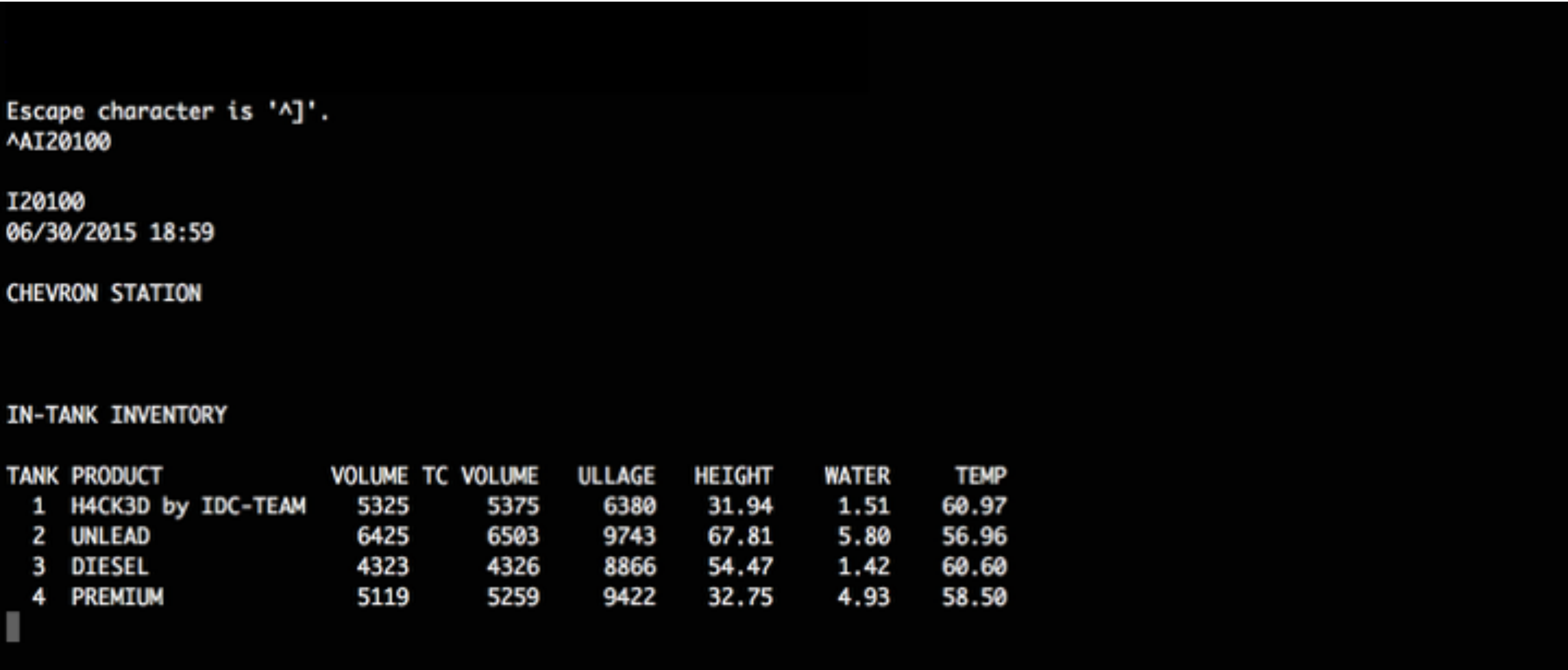
Iranian Dark Coders

- Group operating out of Iran
- Pro-Iranian group
- Website defacements, information sharing, malware distribution, and hacktivism

Modification "Attacks"

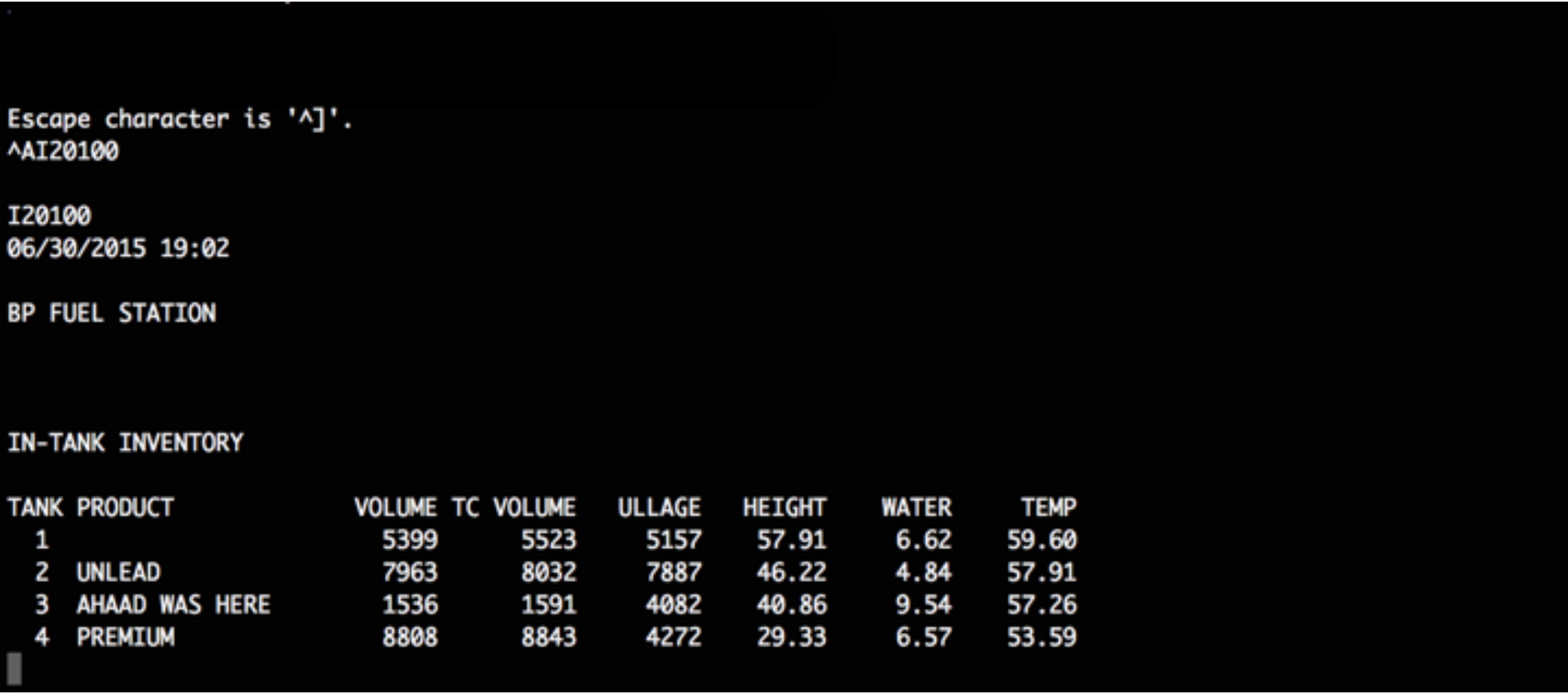
- Iranian Dark Coders?
  - 5.106.221.208
  - 2.147.147.123
  - 5.219.58.67
  - 31.14.94.33
- Modification of pump names
- Attacked two honeypots in Jordan
- Possible false flag?

"H4CK3D by IDC-TEAM"

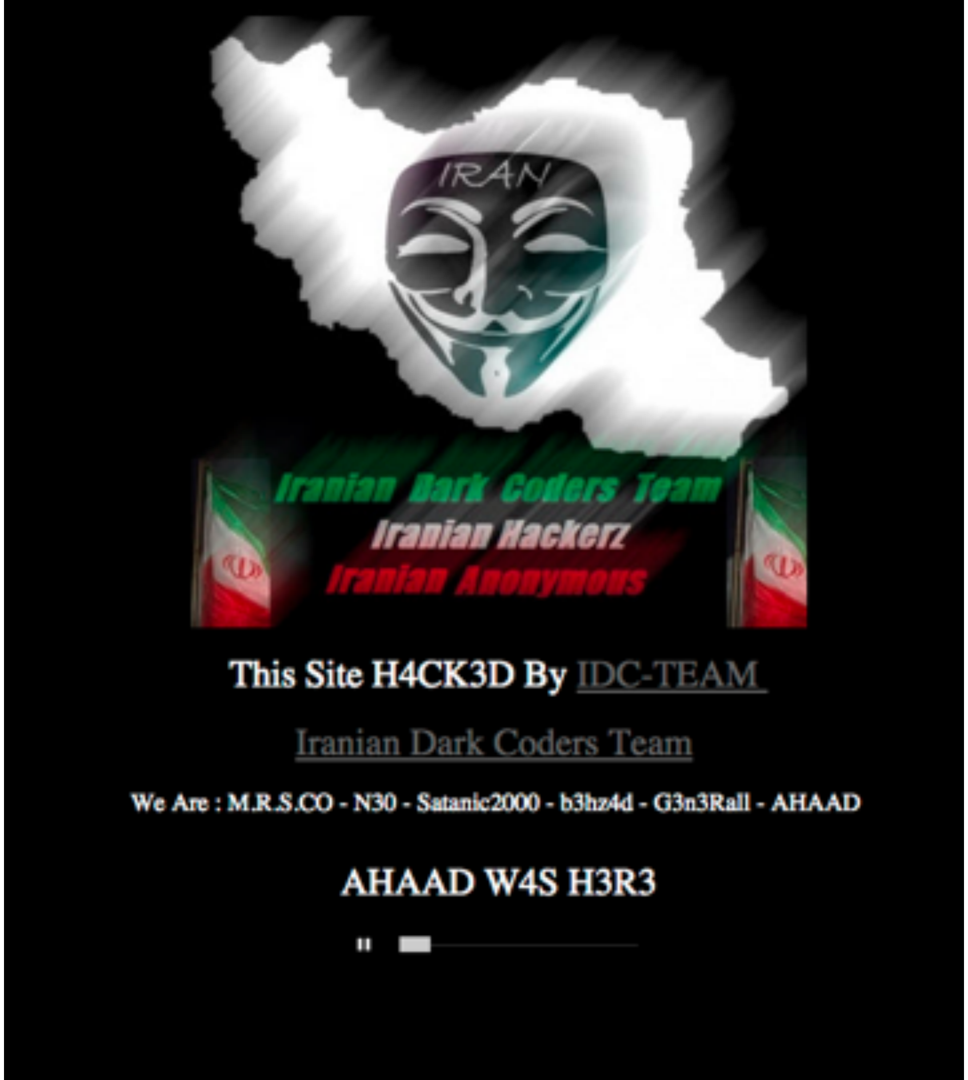


```
Escape character is '^]'.
^AI20100

I20100
06/30/2015 18:59

CHEVRON STATION



IN-TANK INVENTORY

TANK PRODUCT              VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  H4CK3D by IDC-TEAM     5325      5375     6380    31.94     1.51    60.97
  2  UNLEAD                 6425      6503     9743    67.81     5.80    56.96
  3  DIESEL                 4323      4326     8866    54.47     1.42    60.60
  4  PREMIUM                5119      5259     9422    32.75     4.93    58.50
```

"AHAAD WAS HERE"



```
Escape character is '^]'.
^AI20100

I20100
06/30/2015 19:02

BP FUEL STATION



IN-TANK INVENTORY

TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1                        5399      5523     5157    57.91     6.62    59.60
  2  UNLEAD                7963      8032     7887    46.22     4.84    57.91
  3  AHAAD WAS HERE        1536      1591     4082    40.86     9.54    57.26
  4  PREMIUM               8808      8843     4272    29.33     6.57    53.59
```

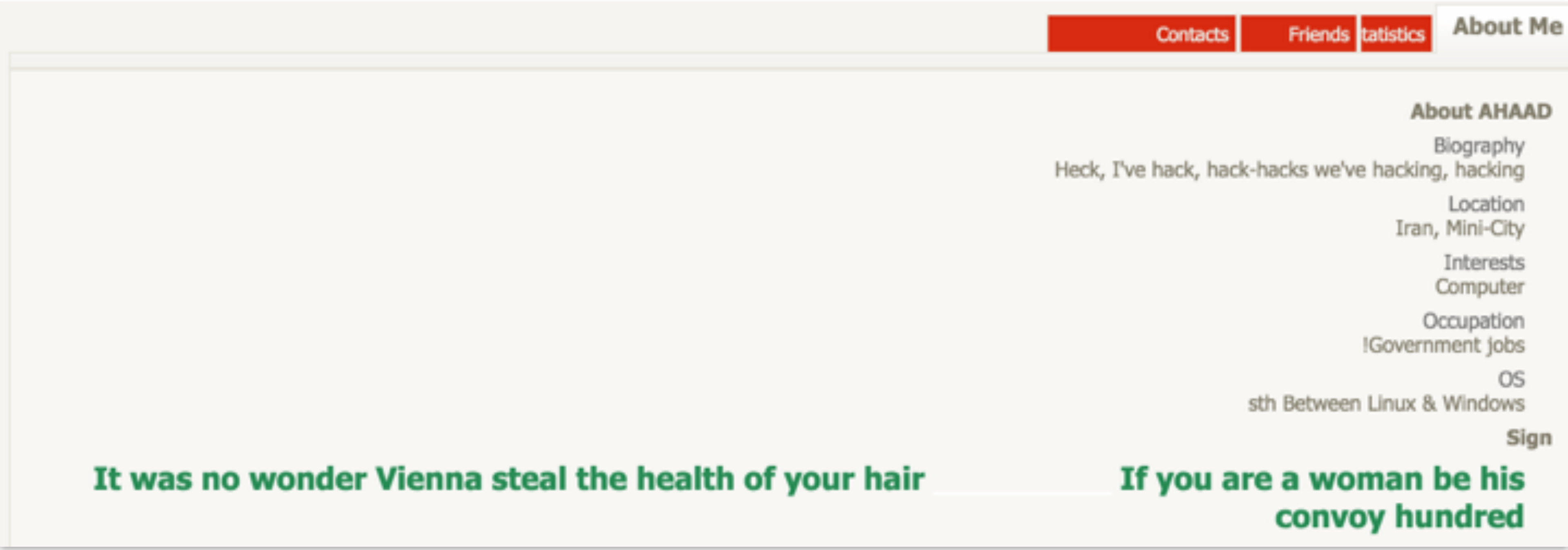


This Site H4CK3D By IDC-TEAM

Iranian Dark Coders Team

We Are : M.R.S.CO - N30 - Satanic2000 - b3hz4d - G3n3Rall - AHAAD

AHAAD W4S H3R3



About AHAAD

Biography
Heck, I've hack, hack-hacks we've hacking, hacking

Location
Iran, Mini-City

Interests
Computer

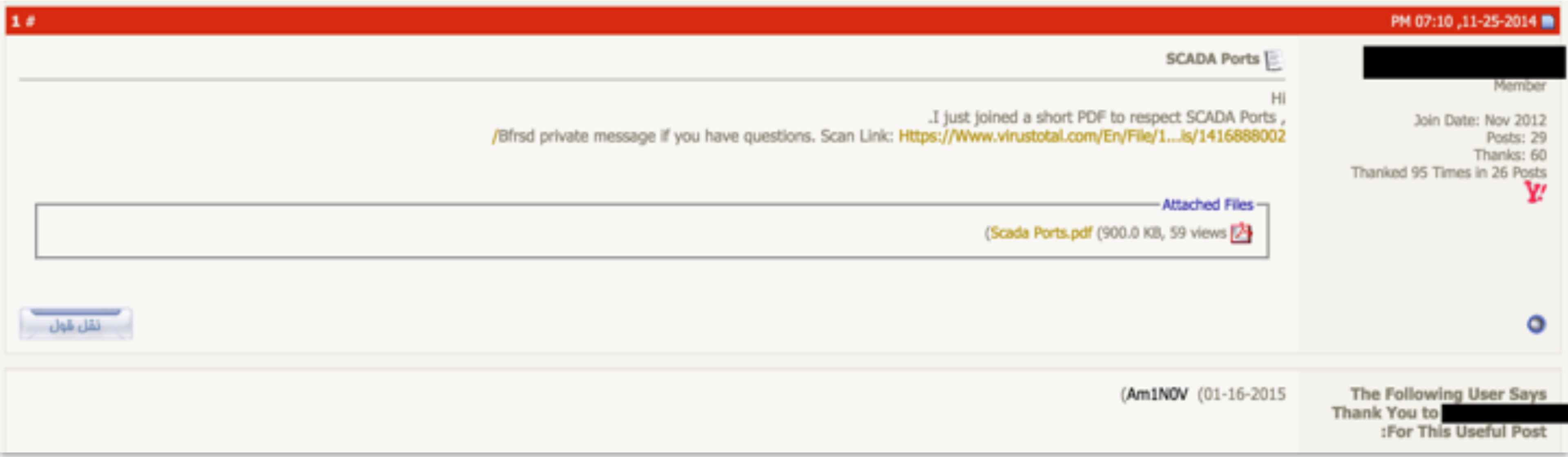
Occupation
!Government jobs

OS
sth Between Linux & Windows

Sign

It was no wonder Vienna steal the health of your hair

If you are a woman be his convoy hundred



1 # PM 07:10 ,11-25-2014

SCADA Ports

[redacted]
Member

Join Date: Nov 2012
Posts: 29
Thanks: 60
Thanked 95 Times in 26 Posts

Hi
.I just joined a short PDF to respect SCADA Ports ,
/Bfrsd private message if you have questions. Scan Link: Https://Www.virustotal.com/En/File/1...is/1416888002

Attached Files
(Scada Ports.pdf (900.0 KB, 59 views

The Following User Says Thank You to [redacted] :For This Useful Post

(Am1N0V (01-16-2015

Fin.

lowcalspam

sjhilt