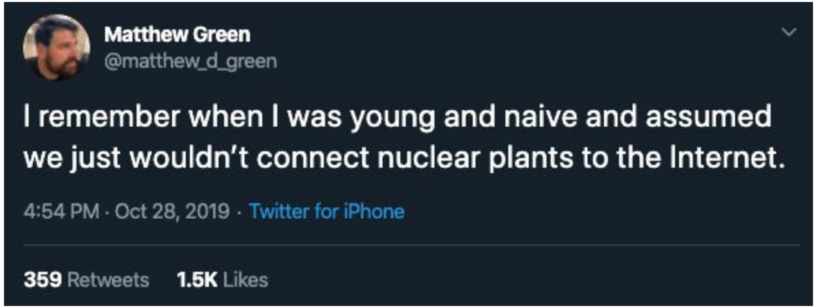
Gas What? I can see your GasPots.

Studying the fingerprintability of ICS honeypots in the wild

Mohammad-Reza Zamiri-Gourabi
ZD Research

Ali Razmjoo Qalaei
OWASP

Babak Amin Azad
Stony Brook University

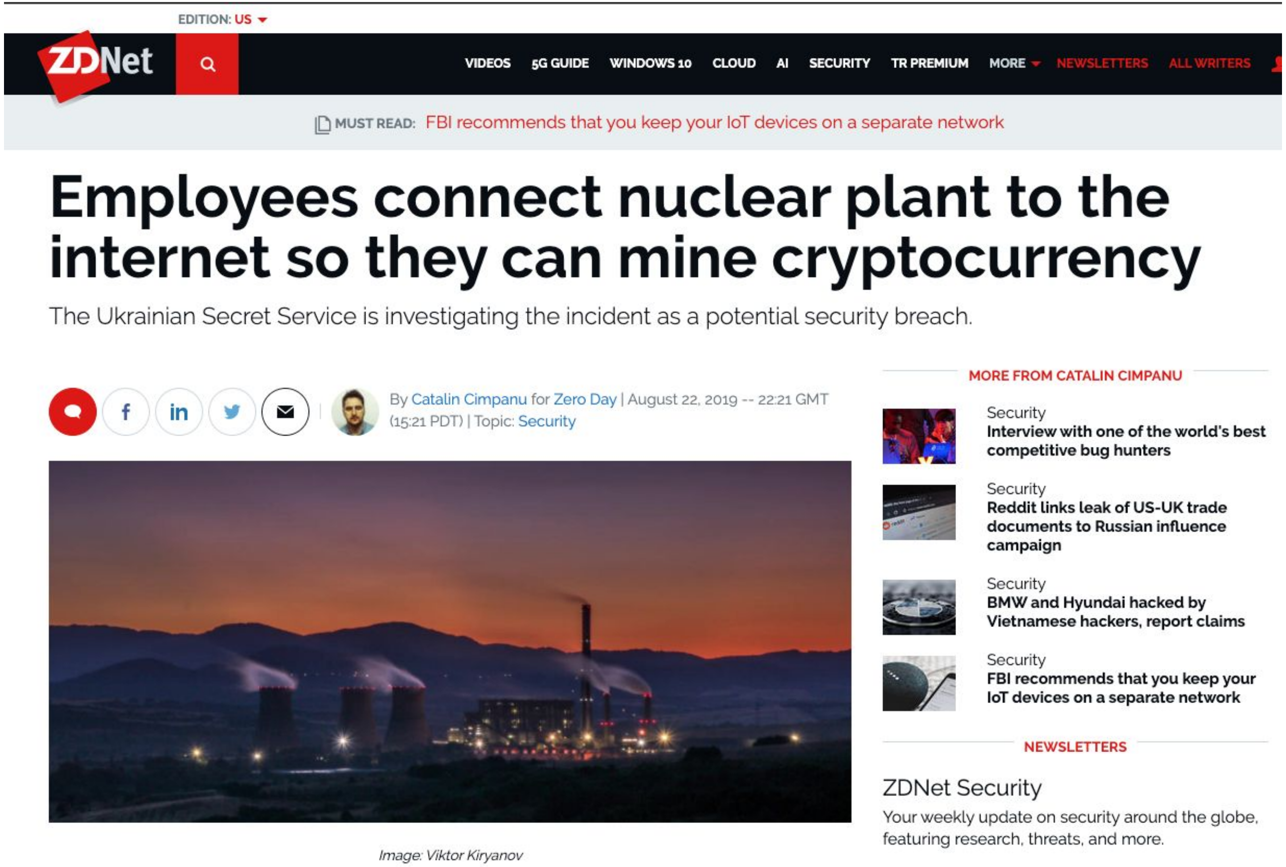


Matthew Green
@matthew_d_green

I remember when I was young and naive and assumed we just wouldn't connect nuclear plants to the Internet.

4:54 PM · Oct 28, 2019 · Twitter for iPhone

359 Retweets 1.5K Likes



EDITION: US

ZDNet

VIDEOS 5G GUIDE WINDOWS 10 CLOUD AI SECURITY TR PREMIUM MORE NEWSLETTERS ALL WRITERS

MUST READ: FBI recommends that you keep your IoT devices on a separate network

Employees connect nuclear plant to the internet so they can mine cryptocurrency

The Ukrainian Secret Service is investigating the incident as a potential security breach.

By Catalin Cimpanu for Zero Day | August 22, 2019 -- 22:21 GMT (15:21 PDT) | Topic: Security

Image: Viktor Kiryanov

MORE FROM CATALIN CIMPANU

Security
Interview with one of the world's best competitive bug hunters

Security
Reddit links leak of US-UK trade documents to Russian influence campaign

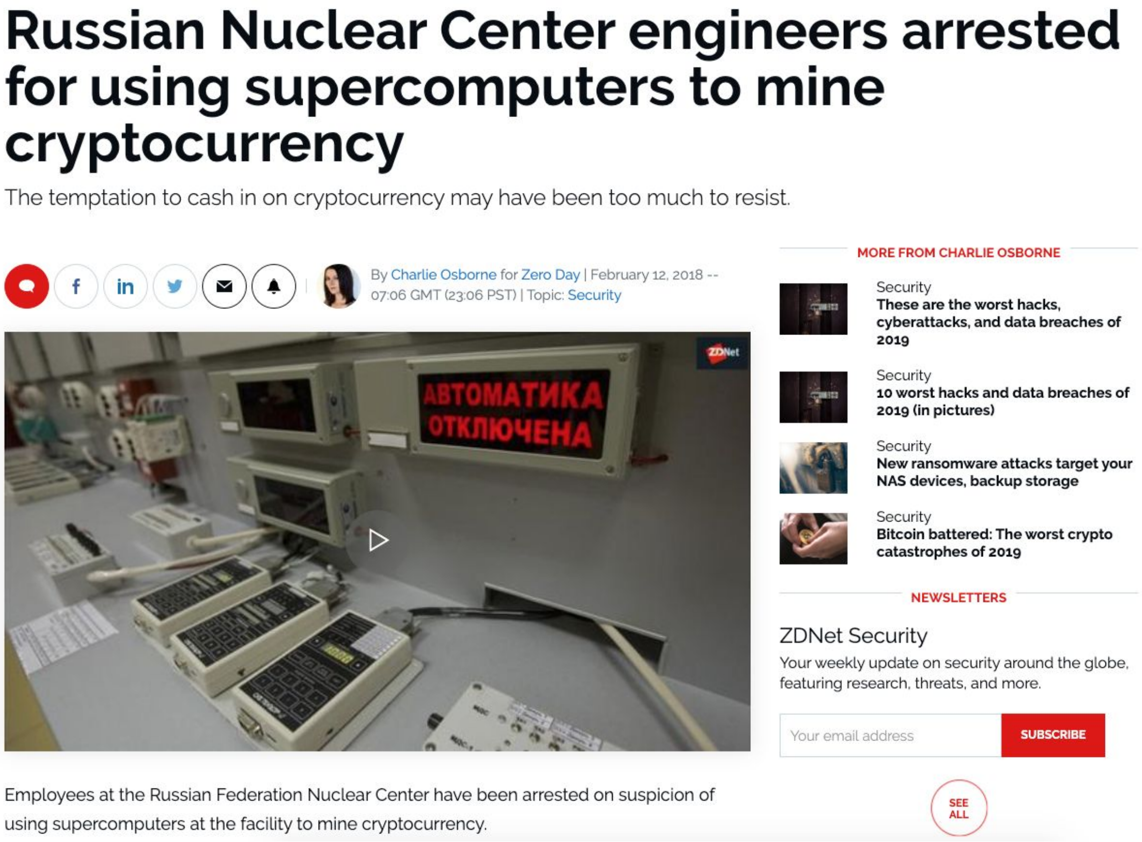
Security
BMW and Hyundai hacked by Vietnamese hackers, report claims

Security
FBI recommends that you keep your IoT devices on a separate network

NEWSLETTERS

ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.



Russian Nuclear Center engineers arrested for using supercomputers to mine cryptocurrency

The temptation to cash in on cryptocurrency may have been too much to resist.

By Charlie Osborne for Zero Day | February 12, 2018 -- 07:06 GMT (23:06 PST) | Topic: Security

Employees at the Russian Federation Nuclear Center have been arrested on suspicion of using supercomputers at the facility to mine cryptocurrency.

MORE FROM CHARLIE OSBORNE

Security
These are the worst hacks, cyberattacks, and data breaches of 2019

Security
10 worst hacks and data breaches of 2019 (in pictures)

Security
New ransomware attacks target your NAS devices, backup storage

Security
Bitcoin battered: The worst crypto catastrophes of 2019

NEWSLETTERS

ZDNet Security

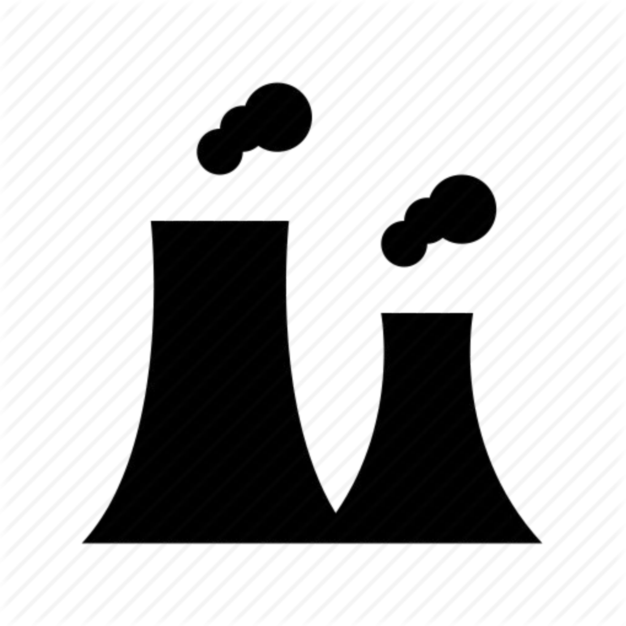
Your weekly update on security around the globe, featuring research, threats, and more.

Your email address | SUBSCRIBE

SEE ALL

ICS Attacks

- Stuxnet attacking Iran nuclear facilities
- Use of multiple zero day exploits
- Focus on specific PLC device
- ICS devices were not built to be published over internet
- Honeypots could help detect attacks

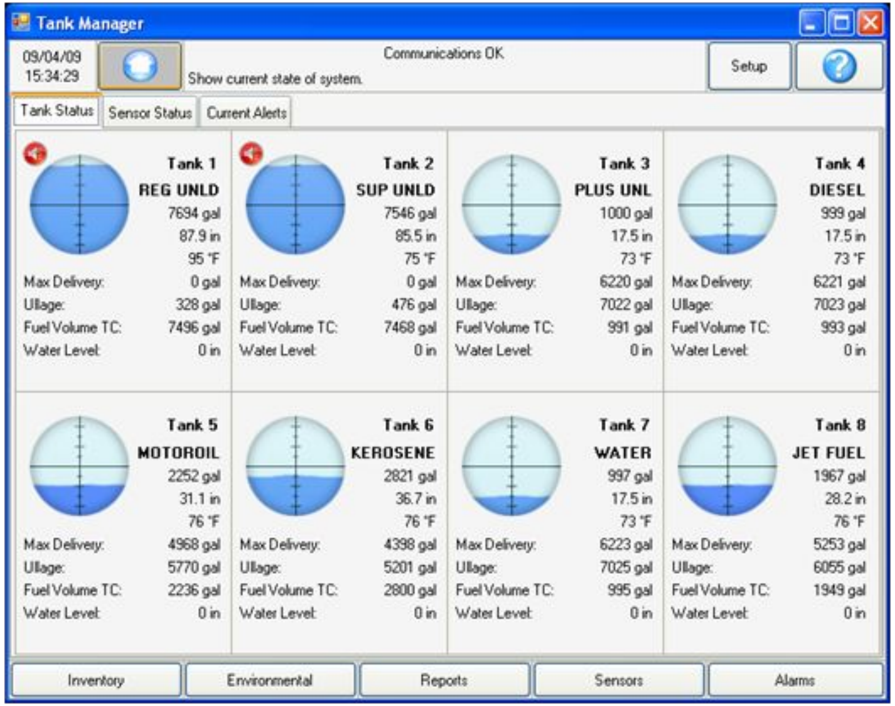


ICS Honeypots

- **ConPot:** Generic ICS Honeypot supports SFTP, FTP, Guardian AST, S7, Modbus, ...
- **GasPot**: Guardian AST Honeypot (Gas Tank Inventory)
- **Scada-Honeynet**: Simulated PLC TCP/IP Stack, Modbus, Telnet, ...
- **GridPot**: Combines ConPot with power distribution system simulator
- **iHoney**: Waste water treatment plant simulator
- They are all low interaction (obviously)

Challenges of designing ICS Honeypots

- It is inherently difficult to make a good ICS honeypot
- Proprietary protocols
- Sensors that collect data from real world



09/04/09
15:34:29

Communications OK

Show current state of system.

	Tank 1	Tank 2	Tank 3	Tank 4
	REG UNLD	SUP UNLD	PLUS UNL	DIESEL
	7694 gal	7546 gal	1000 gal	999 gal
	87.9 in	85.5 in	17.5 in	17.5 in
	95 °F	75 °F	73 °F	73 °F
Max Delivery:	0 gal	0 gal	6220 gal	6221 gal
Ullage:	328 gal	476 gal	7022 gal	7023 gal
Fuel Volume TC:	7496 gal	7468 gal	991 gal	993 gal
Water Level:	0 in	0 in	0 in	0 in

	Tank 5	Tank 6	Tank 7	Tank 8
	MOTOROIL	KEROSENE	WATER	JET FUEL
	2252 gal	2821 gal	997 gal	1967 gal
	31.1 in	36.7 in	17.5 in	28.2 in
	76 °F	76 °F	73 °F	76 °F
Max Delivery:	4968 gal	4398 gal	6223 gal	5253 gal
Ullage:	5770 gal	5201 gal	7025 gal	6055 gal
Fuel Volume TC:	2236 gal	2800 gal	995 gal	1949 gal
Water Level:	0 in	0 in	0 in	0 in

Attacks on Automatic Tank Gauges

- GasPot simulates Veeder Root's ATG devices.
- Historically hackers attacked these devices to:
  - Rename tank information
  - Resize tanks (Cause overflow)
  - Shutdown dispensing
  - Hide leaks by suppressing alerts

Fingerprinting categories

1. Default configuration
2. Missing protocol features
3. Unusual behavior
4. Fingerprinting the underlying OS

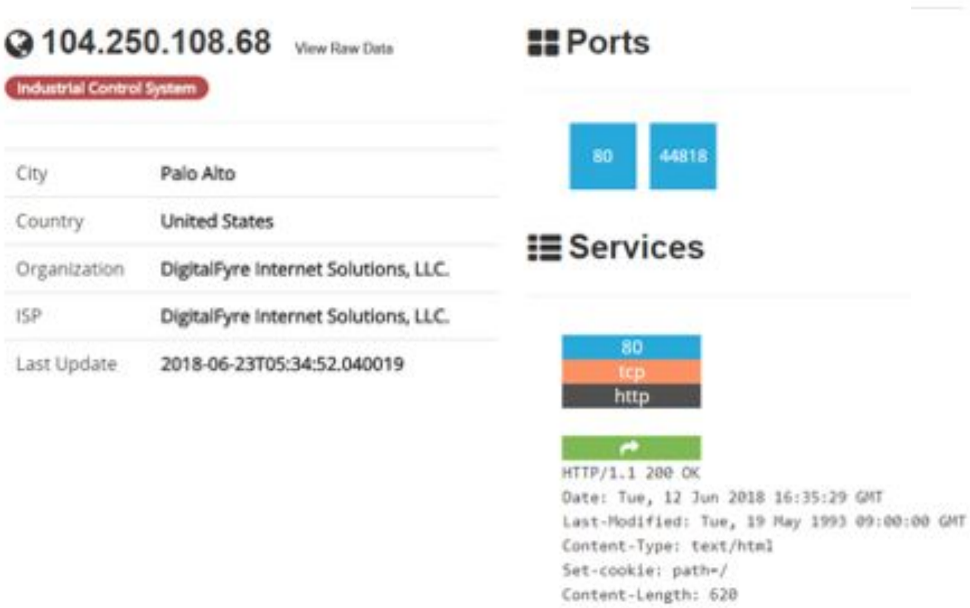
Default configuration (ConPot)

Protocol	Port	Signature	Shodan	Censys
Siemens S7	102	PLC name: Technodrome	214	185
		Plant identification: Mouser Factory	215	162
		Serial number of module: 88111222	182	92

Default configuration (ConPot)

Protocol	Port	Signature	Shodan	Censys
HTTP	80	Last-Modified: Tue, 19 May 1993 09:00:00 GMT	240	133
Telnet	50100	Connected to [00:13:EA:00:00:00]	31	-
IEC104	2404	Data Received: 680e00000000	13	-
Ethernet IP	4818	Product name: 1756-L61/B LOGIX5561	83	-

Default configuration (ConPot)



104.250.108.68 View Raw Data

Industrial Control System

City	Palo Alto
Country	United States
Organization	DigitalFyre Internet Solutions, LLC.
ISP	DigitalFyre Internet Solutions, LLC.
Last Update	2018-06-23T05:34:52.040019

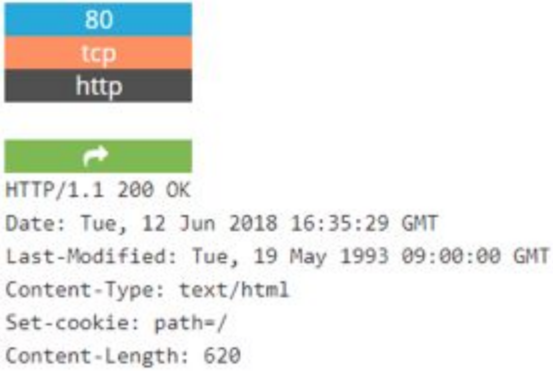
Ports

80 44818

Services

80
tcp
http

```
HTTP/1.1 200 OK
Date: Tue, 12 Jun 2018 16:35:29 GMT
Last-Modified: Tue, 19 May 1993 09:00:00 GMT
Content-Type: text/html
Set-cookie: path=/
Content-Length: 620
```

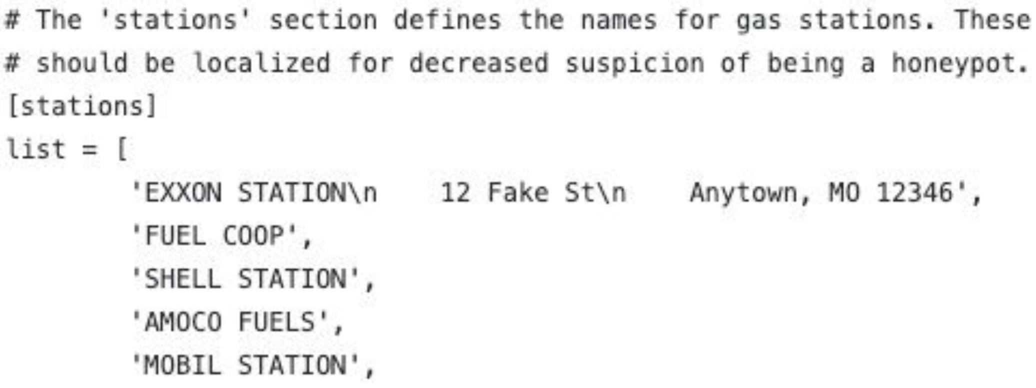


80
tcp
http

```
HTTP/1.1 200 OK
Date: Tue, 12 Jun 2018 16:35:29 GMT
Last-Modified: Tue, 19 May 1993 09:00:00 GMT
Content-Type: text/html
Set-cookie: path=/
Content-Length: 620
```

Default configuration (GasPot)

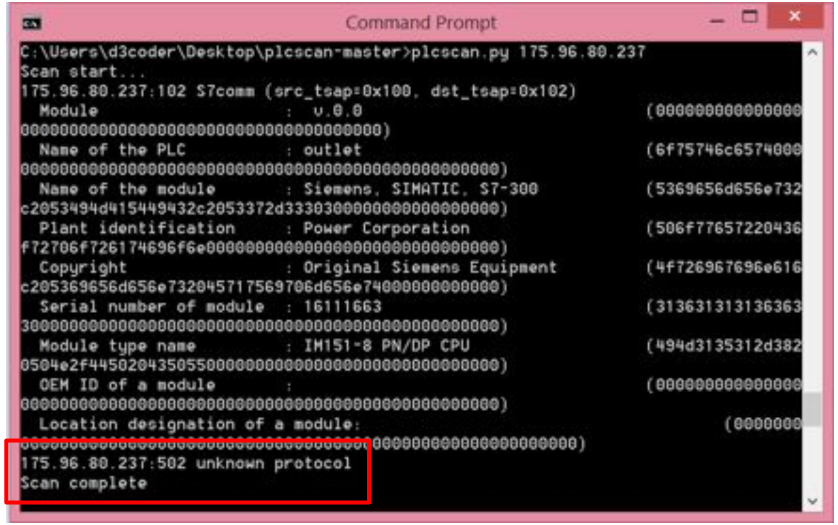
GasPot default station names



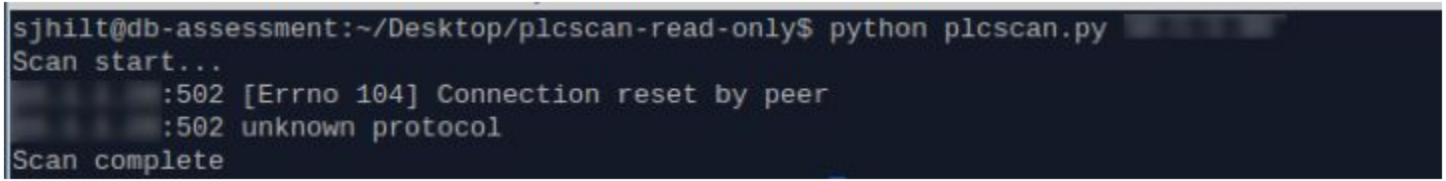
```
# The 'stations' section defines the names for gas stations. These
# should be localized for decreased suspicion of being a honeypot.
[stations]
list = [
        'EXXON STATION\n    12 Fake St\n    Anytown, MO 12346',
        'FUEL COOP',
        'SHELL STATION',
        'AMOCO FUELS',
        'MOBIL STATION',
```

Missing protocol features (ConPot and Scada Honeynet)

- Plcscan shows unknown protocol for Modbus on ConPot
- Similar results on Scada Honeynet



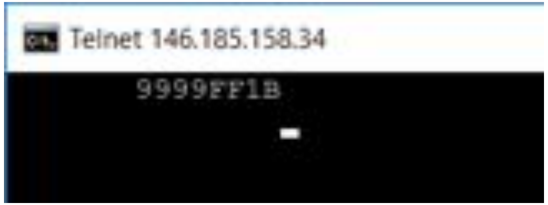
```
C:\Users\d3coder\Desktop\plcscan-master>plcscan.py 175.96.80.237
Scan start...
175.96.80.237:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                   :  v.0.0                    (0000000000000000
0000000000000000000000000000000000000)
  Name of the PLC          : outlet                    (6f75746c65740000
0000000000000000000000000000000000000000000000000)
  Name of the module       : Siemens, SIMATIC, S7-300  (5369656d656e732
c2053494d415449432c2053372d3330300000000000000000)
  Plant identification     : Power Corporation         (506f776572204306
f72706f726174696f6e000000000000000000000000000000)
  Copyright                : Original Siemens Equipment (4f726967696e616
c205369656d656e732045717569706d656e74000000000000)
  Serial number of module  : 16111663                  (3136313131363633
3000000000000000000000000000000000000000000000000)
  Module type name         : IM151-8 PN/DP CPU         (494d3135312d382
0504e2f445020435055000000000000000000000000000000)
  OEM ID of a module       :                           (0000000000000000
0000000000000000000000000000000000000000000000000)
  Location designation of a module:                            (0000000
000000000000000000000000000000000000000000000000000000000)
175.96.80.237:502 unknown protocol
Scan complete
```



```
sjhilt@db-assessment:~/Desktop/plcscan-read-only$ python plcscan.py [redacted]
Scan start...
[redacted]:502 [Errno 104] Connection reset by peer
[redacted]:502 unknown protocol
Scan complete
```

Missing protocol features (GasPot)

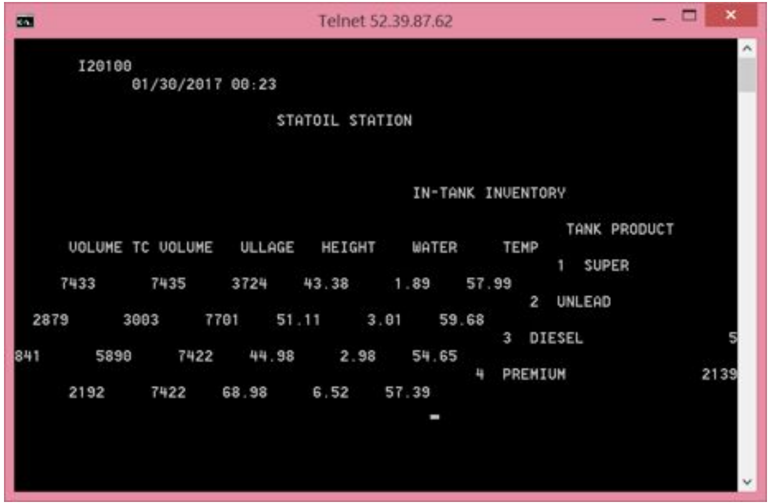
- Guardian AST, Automatic Tank Gauges support a variety of commands.
- I20100 query returns in tank inventory information. (Supported by GasPot)
- I30100 returns sensor status report. (Not supported, returns 9999FF1B)



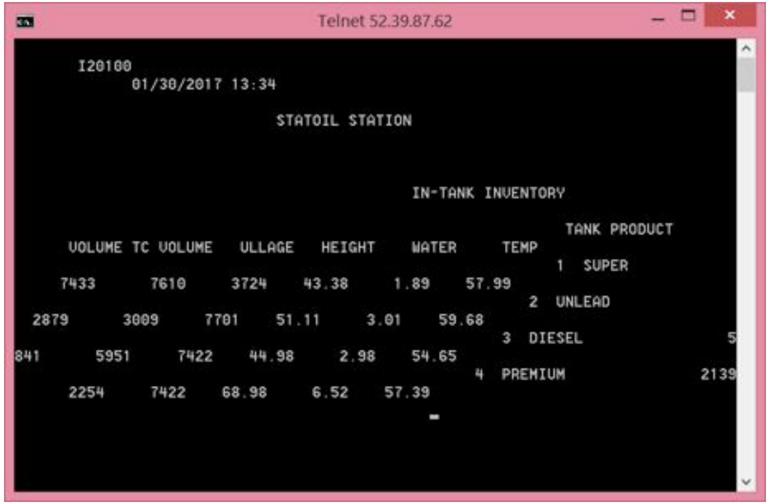
```
9999FF1B
```

Unusual behavior

On a normal ATG device, the temperature, oil level and other features are going to change over time.



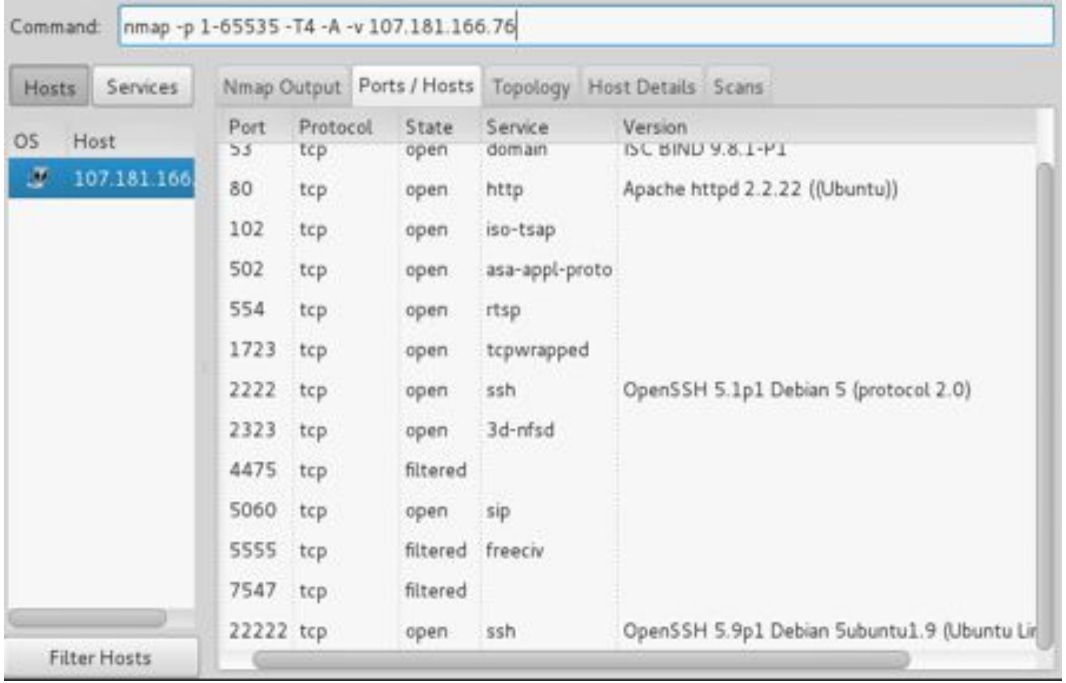
```
       I20100
             01/30/2017 00:23

                             STATOIL STATION



                                            IN-TANK INVENTORY

                                                              TANK PRODUCT
      VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER      TEMP
                                                             1  SUPER
     7433      7435     3724    43.38     1.89    57.99
                                                          2  UNLEAD
  2879      3003     7701    51.11     3.01    59.68
                                                       3  DIESEL                5
841      5890     7422    44.98     2.98    54.65
                                                    4  PREMIUM               2139
      2192     7422    68.98     6.52    57.39
```



```
       I20100
             01/30/2017 13:34

                             STATOIL STATION



                                            IN-TANK INVENTORY

                                                              TANK PRODUCT
      VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER      TEMP
                                                             1  SUPER
     7433      7610     3724    43.38     1.89    57.99
                                                          2  UNLEAD
  2879      3009     7701    51.11     3.01    59.68
                                                       3  DIESEL                5
841      5951     7422    44.98     2.98    54.65
                                                    4  PREMIUM               2139
      2254     7422    68.98     6.52    57.39
```

Platform fingerprinting

- The operating system
- List of open ports



Command: `nmap -p 1-65535 -T4 -A -v 107.181.166.76`

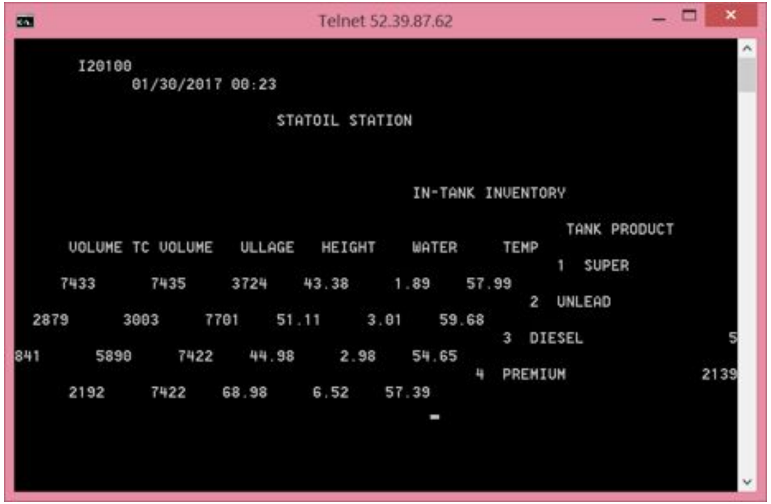
Port	Protocol	State	Service	Version
53	tcp	open	domain	ISC BIND 9.8.1-P1
80	tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))
102	tcp	open	iso-tsap	
502	tcp	open	asa-appl-proto	
554	tcp	open	rtsp	
1723	tcp	open	tcpwrapped	
2222	tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (protocol 2.0)
2323	tcp	open	3d-nfsd	
4475	tcp	filtered		
5060	tcp	open	sip	
5555	tcp	filtered	freeciv	
7547	tcp	filtered		
22222	tcp	open	ssh	OpenSSH 5.9p1 Debian 5ubuntu1.9 (Ubuntu Lir

Specific fingerprints for GasPot

- These features are not inherently different
- Use these for validation

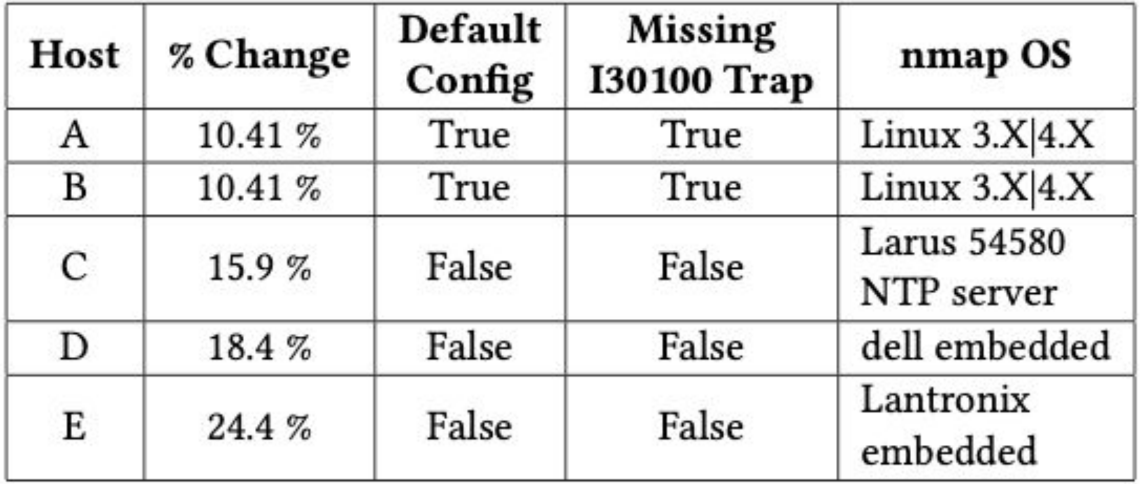
Extra features

- Response time (GasPot returns instantly, Real ATGs take longer to respond)
- Output text formatting (Only \n instead of \r\n)



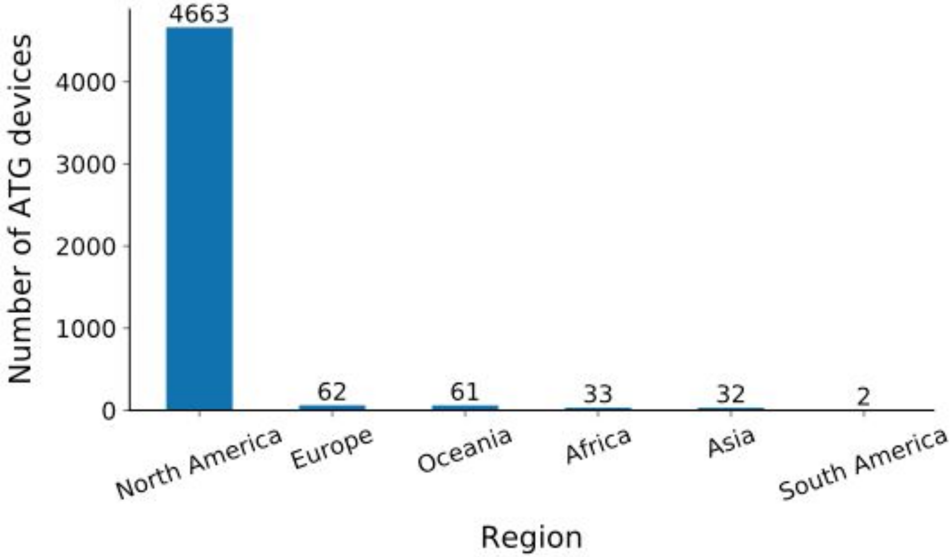
```
     I20100
           01/30/2017 00:23

                              STATOIL STATION



                                             IN-TANK INVENTORY

                                                      TANK PRODUCT
      VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
                                                     1   SUPER
     7433      7435     3724    43.38     1.89    57.99
                                                   2  UNLEAD
  2879      3003      7701    51.11      3.01    59.68
                                                 3  DIESEL                5
841      5890      7422    44.98      2.98    54.65
                                               4  PREMIUM              2139
      2192      7422    68.98      6.52    57.39
                                      -
```

Results: Example hosts in our dataset

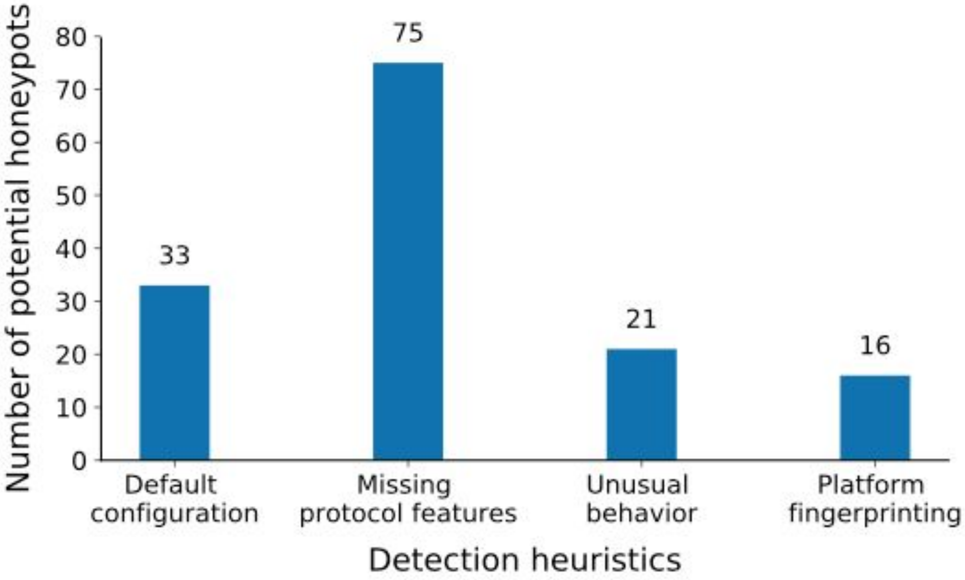


Host	% Change	Default Config	Missing I30100 Trap	nmap OS
A	10.41 %	True	True	Linux 3.X|4.X
B	10.41 %	True	True	Linux 3.X|4.X
C	15.9 %	False	False	Larus 54580 NTP server
D	18.4 %	False	False	dell embedded
E	24.4 %	False	False	Lantronix embedded

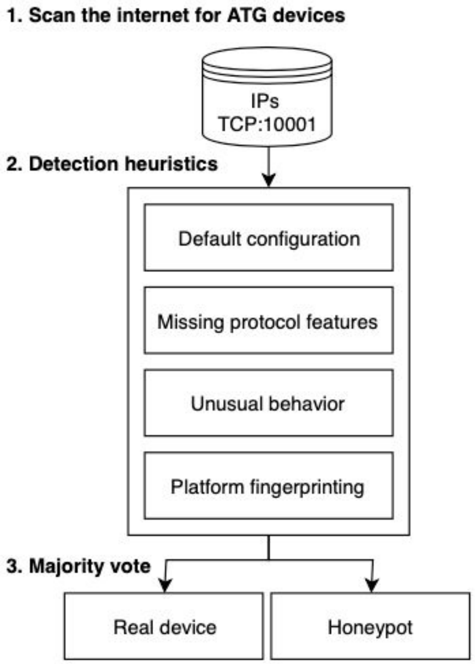
Results: ATG device locations



Results: ATG device detected by detection heuristics



Deciding if a host is a honeypot

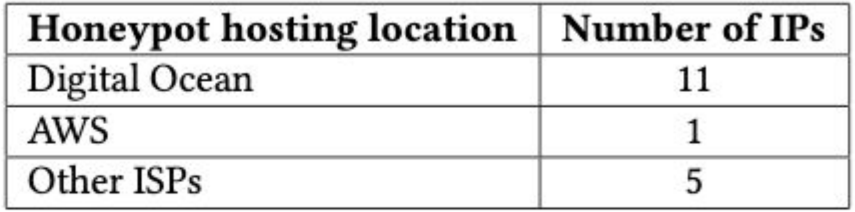


1. **Scan the internet for ATG devices**

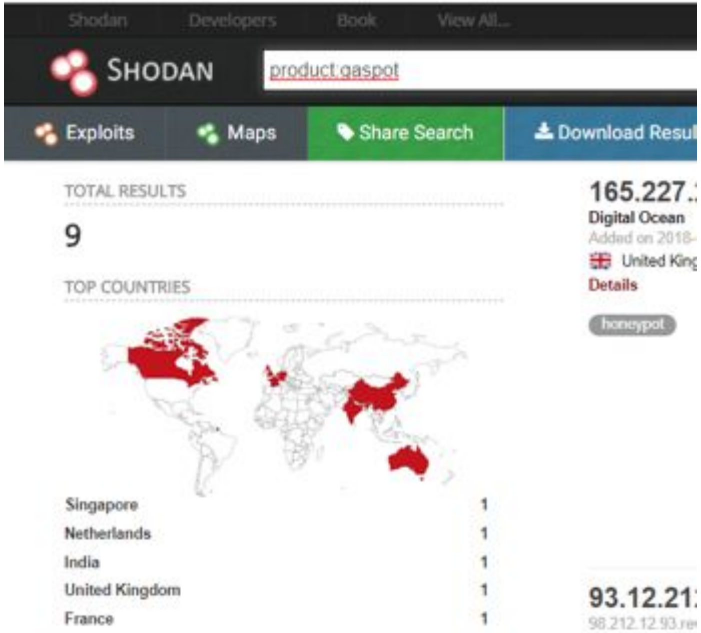
2. **Detection heuristics**

3. **Majority vote**

Result: Geolocation of detected GasPots



Honeypot hosting location	Number of IPs
Digital Ocean	11
AWS	1
Other ISPs	5



product:gaspot

TOTAL RESULTS

9

TOP COUNTRIES

Singapore	1
Netherlands	1
India	1
United Kingdom	1
France	1

165.227.

Digital Ocean

Added on 2018-

United King

Details

93.12.21

98.212.12.93.re

Source code is publicly available

- ICS scanner module:

  OWASP Nettacker project (Automated penetration testing tool)

  https://github.com/zdresearch/OWASP-Nettacker/blob/master/lib/payload/scanner/ics_honeypot/ics.py
- Guardian AST Honeypot module:

  OWASP Honeypot project

  https://github.com/zdresearch/OWASP-Honeypot/tree/master/lib/modules/ics

  - Dynamic response to queries
  - Added support for missing commands
  - Added delay to responses to simulate behavior of real devices
  - Fixed line breaks

Conclusion

- Honeypots provide an invaluable tool for detecting ICS attacks
- Creating ICS honeypots is challenging by its nature
- Existing ICS honeypots can easily be fingerprinted
- Case study on fingerprinting GasPots on the internet
- Providing the ICS scanner module & the Guardian AST honeypot that is more resilient to fingerprinting