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

Kyle Wilhoit
Sr. Threat Researcher
@lowcalspam

Stephen Hilt
Sr. Threat Researcher
@sjhilt
Where The “Industry” Is...
SCADA Became Popular.
Threats Began Adapting & Changing.
SCADA Started

Trading in Dark Corners...
Vulnerabilities Continued…
Reported Incidents in US: 2014

Critical Manufacturing 65, 27%

Energy 79, 32%

Communications 14, 6%
Commercial Facilities 7, 3%
Chemical 4, 2%
Unknown 6, 2%
Water 14, 6%
Transportation 12, 5%
Nuclear 6, 2%
Information Technology 5, 2%
Healthcare 15, 6%
Government Facilities 13, 5%
Finance 3, 1%
Food and Ag 2, 1%
SCADA Vulnerabilities and Incidents Per Year

- **2011**
  - Vulnerability Count: 138
  - Incident Count: 140

- **2012**
  - Vulnerability Count: 137
  - Incident Count: 197

- **2013**
  - Vulnerability Count: 187
  - Incident Count: 257

- **2014**
  - Vulnerability Count: 159
  - Incident Count: 245

Legend:
- Blue: Vulnerability Count
- Red: Incident Count
Why Attack SCADA?!

It’s Easy

Government

Criminal
Guardian AST...dafuq is it?
Not All Tanks Are Created Equal

- Gas Station Tanks
- Backup Generator Tanks
- Terminal Station Tanks
- Other Tanks?
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
Architectural Diagram:

- GasPot
- Internet
- Attacker
Deployment Locations
Code Considerations

```python
# 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())
```

```python
# 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

---

### Tank Gauge

<table>
<thead>
<tr>
<th>TANK</th>
<th>PRODUCT</th>
<th>VOLUME</th>
<th>TC VOLUME</th>
<th>ULLAGE</th>
<th>HEIGHT</th>
<th>WATER</th>
<th>TEMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SUPER</td>
<td>6376</td>
<td>6509</td>
<td>3427</td>
<td>72.12</td>
<td>0.10</td>
<td>53.91</td>
</tr>
<tr>
<td>2</td>
<td>UNLEAD</td>
<td>4747</td>
<td>4886</td>
<td>6624</td>
<td>39.85</td>
<td>5.14</td>
<td>57.21</td>
</tr>
<tr>
<td>3</td>
<td>DIESEL</td>
<td>7241</td>
<td>7328</td>
<td>7623</td>
<td>44.32</td>
<td>3.44</td>
<td>50.71</td>
</tr>
<tr>
<td>4</td>
<td>PREMIUM</td>
<td>8262</td>
<td>8364</td>
<td>3618</td>
<td>67.46</td>
<td>9.30</td>
<td>50.75</td>
</tr>
</tbody>
</table>
Shodan and Gaspot Consideration

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

<table>
<thead>
<tr>
<th>Deployment / Attacker</th>
<th>US</th>
<th>RO</th>
<th>CN</th>
<th>RU</th>
<th>IR</th>
<th>SY</th>
<th>MX</th>
<th>CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>BR</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JO</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AE</td>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RU</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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?
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?
Escape character is '^['.

^AI20100

I20100
06/30/2015 18:59

CHEVRON STATION

IN-TANK INVENTORY

<table>
<thead>
<tr>
<th>TANK</th>
<th>PRODUCT</th>
<th>VOLUME</th>
<th>TC VOLUME</th>
<th>ULLAGE</th>
<th>HEIGHT</th>
<th>WATER</th>
<th>TEMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>H4CK3D by IDC-TEAM</td>
<td>5325</td>
<td>5375</td>
<td>6380</td>
<td>31.94</td>
<td>1.51</td>
<td>60.97</td>
</tr>
<tr>
<td>2</td>
<td>UNLEAD</td>
<td>6425</td>
<td>6503</td>
<td>9743</td>
<td>67.81</td>
<td>5.80</td>
<td>56.96</td>
</tr>
<tr>
<td>3</td>
<td>DIESEL</td>
<td>4323</td>
<td>4326</td>
<td>8866</td>
<td>54.47</td>
<td>1.42</td>
<td>60.60</td>
</tr>
<tr>
<td>4</td>
<td>PREMIUM</td>
<td>5119</td>
<td>5259</td>
<td>9422</td>
<td>32.75</td>
<td>4.93</td>
<td>58.50</td>
</tr>
</tbody>
</table>
"AHAAD WAS HERE"

---

**Escape character is '^J'.**

^AI20100

I20100

06/30/2015 19:02

BP FUEL STATION

---

**IN-TANK INVENTORY**

<table>
<thead>
<tr>
<th>TANK</th>
<th>PRODUCT</th>
<th>VOLUME</th>
<th>TC VOLUME</th>
<th>ULLAGE</th>
<th>HEIGHT</th>
<th>WATER</th>
<th>TEMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UNLEAD</td>
<td>5399</td>
<td>5523</td>
<td>5157</td>
<td>57.91</td>
<td>6.62</td>
<td>59.60</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>7963</td>
<td>8032</td>
<td>7887</td>
<td>46.22</td>
<td>4.84</td>
<td>57.91</td>
</tr>
<tr>
<td>3</td>
<td>AHAAD WAS HERE</td>
<td>1536</td>
<td>1591</td>
<td>4082</td>
<td>40.86</td>
<td>9.54</td>
<td>57.26</td>
</tr>
<tr>
<td>4</td>
<td>PREMIUM</td>
<td>8808</td>
<td>8843</td>
<td>4272</td>
<td>29.33</td>
<td>6.57</td>
<td>53.59</td>
</tr>
</tbody>
</table>
This Site H4CK3D By IDC-TEAM

Iranian Dark Coders Team

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

AHAAD W4S H3R3
It was no wonder Vienna steal the health of your hair

If you are a woman be his convoy hundred
I just joined a short PDF to respect SCADA Ports. Send a 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: For This Useful Post