

Snooping on Cellular Gateways and Their Critical Role in ICS

Justin Shattuck

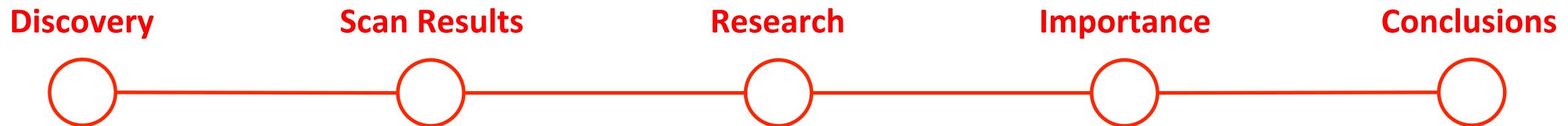
Principal Threat Researcher & Security Evangelist
F5 Networks, Inc. – F5 Labs

- Principal Threat Researcher, F5 Labs
- Mgr. of Services Engineering
 - F5 Silverline
 - Managed WAF and DDoS Scrubbing Services
- Security Product Developer
- 15+ years in InfoSec
- Author of “The Hunt for IOT” reports from F5 Labs.



@sh4t

Agenda





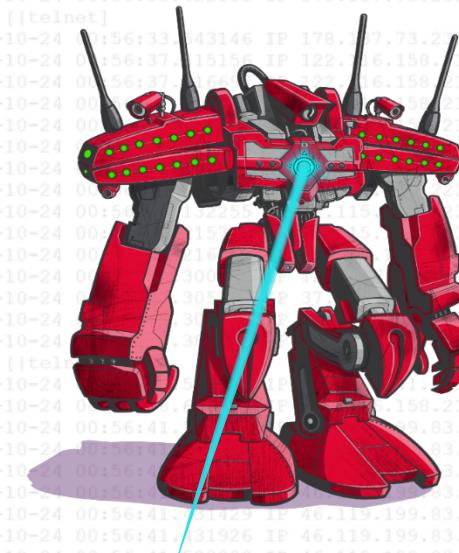
#BHUSA

How it began

October 22, 2016

In Belgium on vacation, DYN gets DDoS.

Investigating incident involving airport in Europe + BASHLITE



Discovery



How it began

October 22, 2016

In Belgium on vacation, DYN gets DDoS.

Investigating incident involving airport in Europe + BASHLITE

Discovery

How I fell in...

Observe packets being flung around internet

Scan networks

Find the results interesting

Repeat



Discovery

Scan Results



I'm a cellular gateway, Morty!

- Service and Host managed by 3rd party
- 39 active threat actors
- Numerous log entries clearly showing incoming attacks (mirai, shellshock attempts, bruteforce)

Sierra Wireless?

```
151.228.192.99
213.64.107.101
182.70.101.140
116.106.11.6
89.46.233.205
201.209.130.86
197.149.28.231
14.191.117.49
178.137.73.231
37.115.141.223
46.211.17.249
46.211.94.143
46.118.1.224
122.116.158.212
178.137.158.55
37.115.218.194
46.119.199.83
178.137.189.252
46.118.44.180
37.115.111.41
178.137.80.187
189.162.77.142
59.126.102.184
37.229.22.161
37.115.11.125
176.8.230.166
37.229.144.122
5.248.64.189
37.229.211.161
37.229.81.7
46.118.248.220
37.115.106.175
178.137.197.163
178.210.131.87
186.67.134.163
181.90.114.299
14.182.183.70
197.2.182.81
136.169.218.120
```

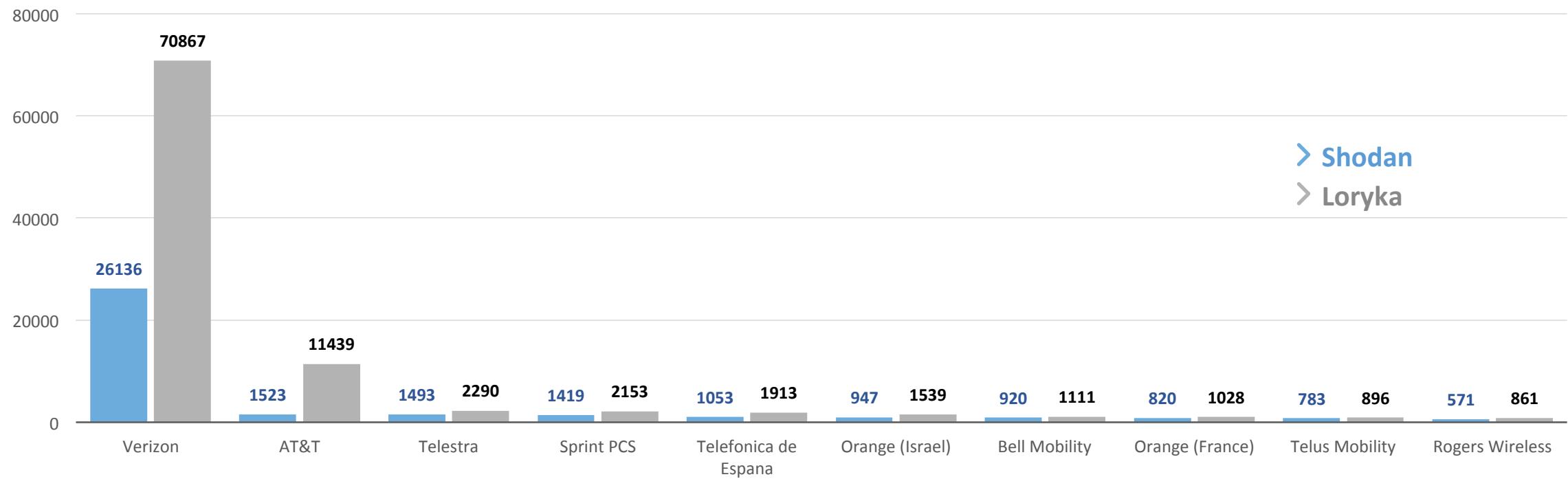


Discovery

Scan Results



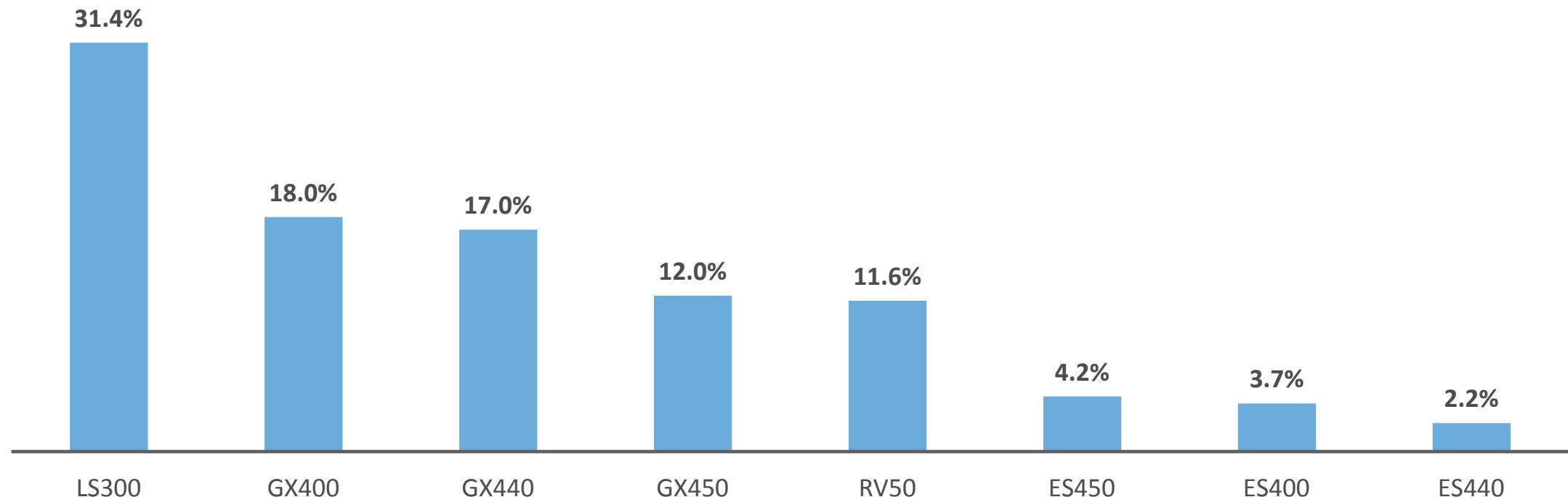
Scanning



Discovery

Scan Results

Device Distribution (Models)



Discovery

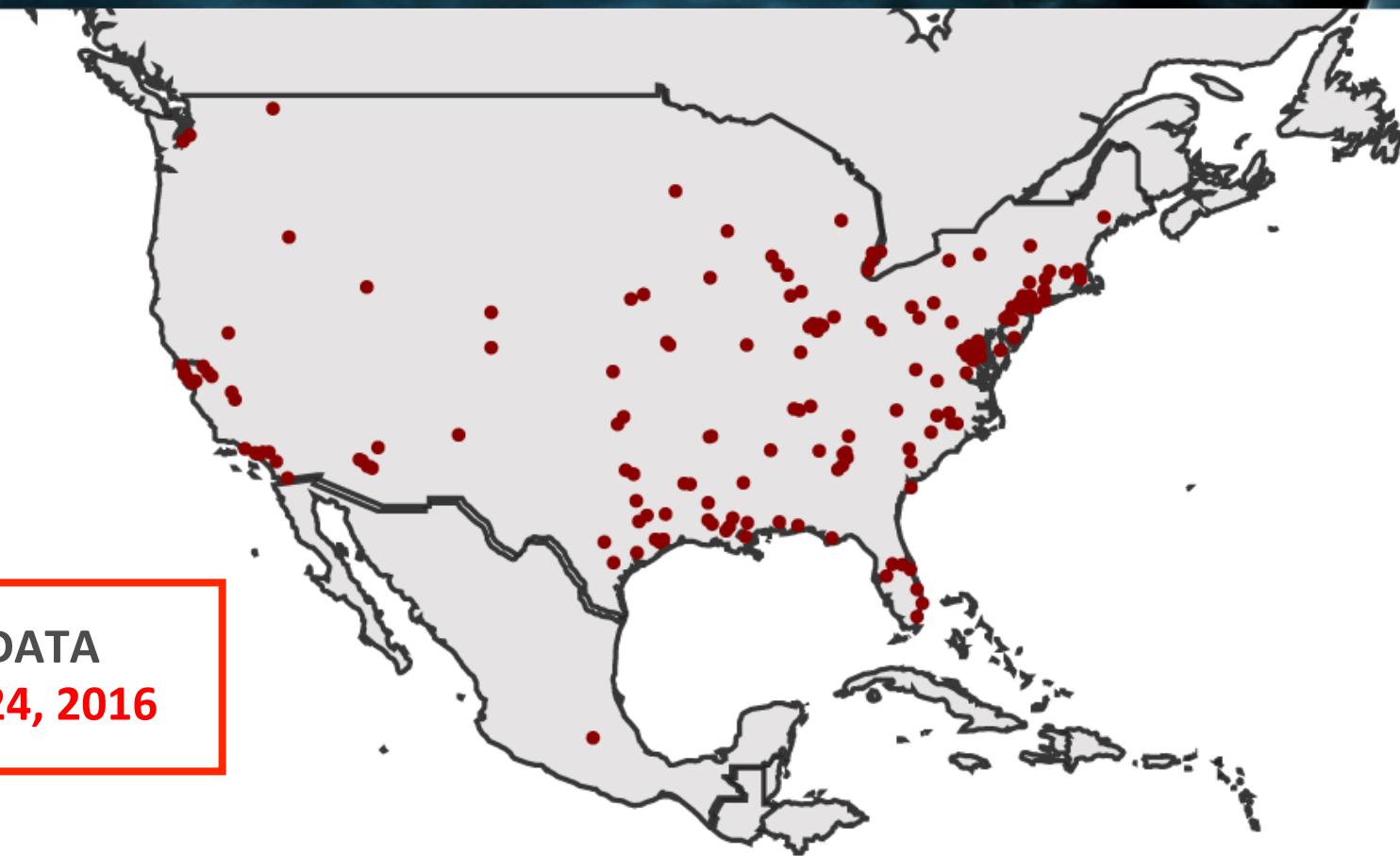
Scan Results

Device Distribution (United States)

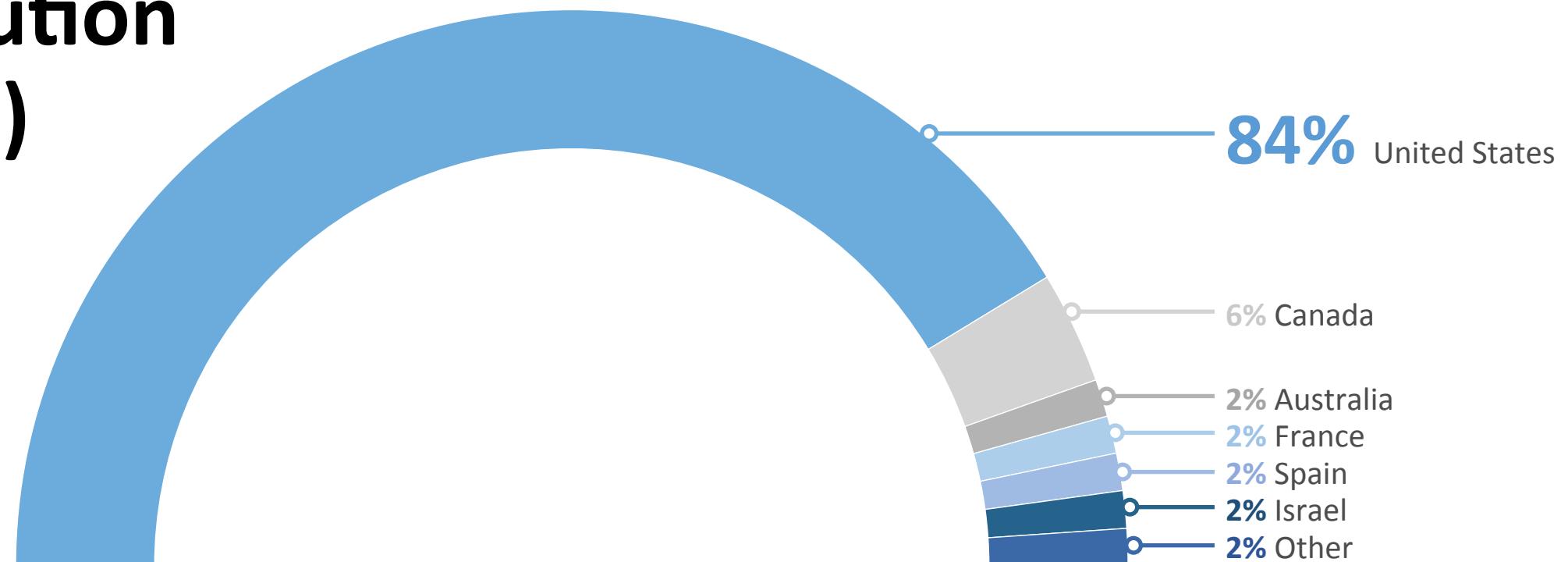


SCAN DATA
October 24, 2016

Scan Results



Device Distribution (Global)

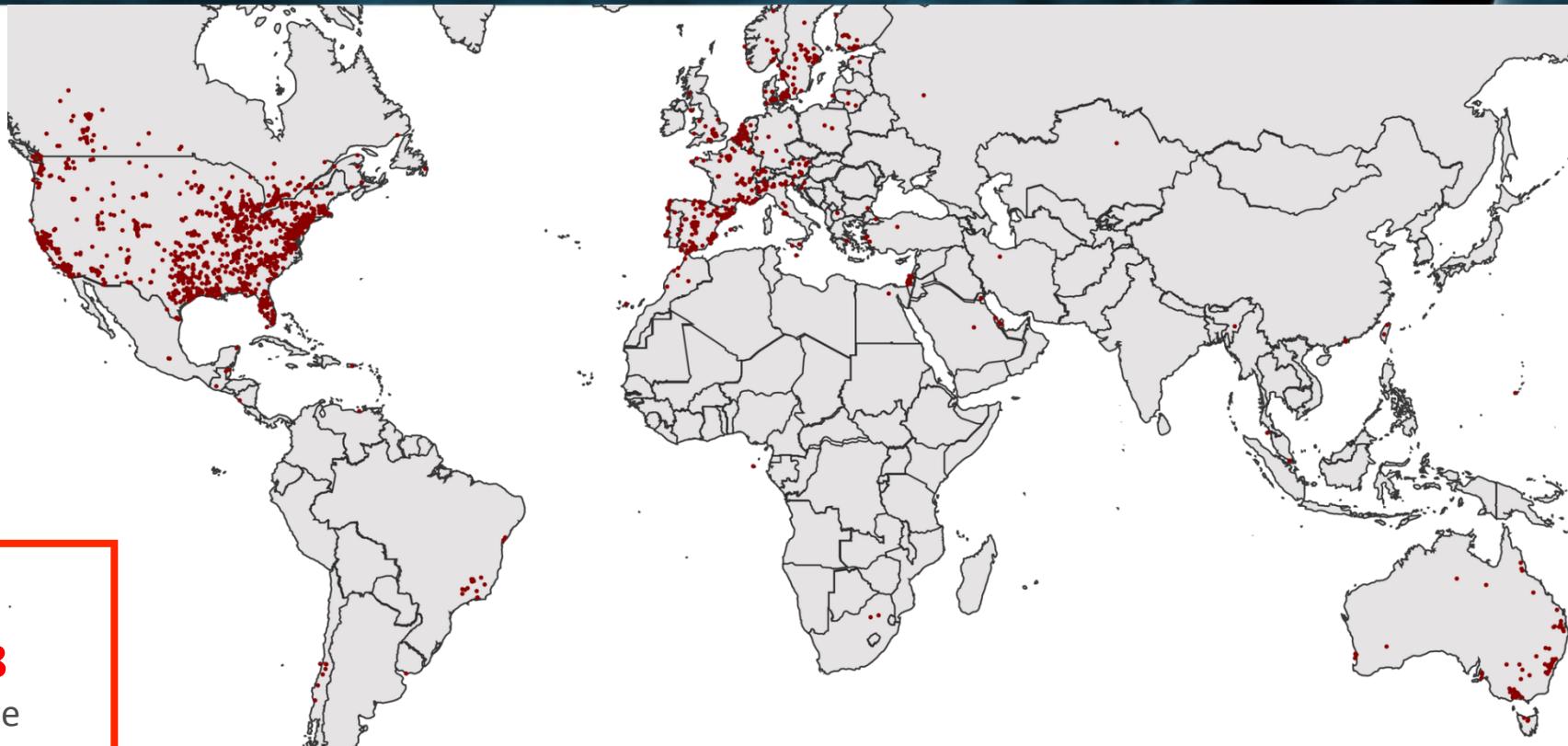


Discovery

Scan Results

Device Distribution (Global)

SCAN DATA
July 30, 2018
86237 in US alone



Discovery

Scan Results



Source

Sierra Wireless Technical Bulletin: Mirai

Oct 05, 2016 - Author: Sierra Wireless - 23551 Views

are reachable from the public internet. The attached technical bulletin provides information about Mirai along with instructions to protect your Sierra Wireless gateway and its local area network.

Sierra Wireless Technical Bulletin - Mirai - 4Oct2016

Sierra Wireless Technical Bulletin: Mirai Malware

Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

Based on currently available information, once the malware is running on the gateway it deletes itself and resides only in memory. The malware will then proceed to scan for vulnerable devices and report its findings back to a command and control server. The command and control server may also instruct the malware to participate in a Distributed Denial of Service (DDoS) attack on specified targets.

Source: Sierrawireless.com

Discovery

Scan Results

Alert (ICS-ALERT-16-286-01)

Sierra Wireless Mitigations Against Mirai Malware

[More Alerts](#)

Original release date: October 12, 2016 | Last revised: October 13, 2016

[Print](#) [Tweet](#) [Send](#) [Share](#)

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp>.

SUMMARY

NCCIC/ICS-CERT received a technical bulletin from the Sierra Wireless company, outlining mitigations to secure Airlink Cellular Gateway devices affected by (or at risk of) the "Mirai" malware. While the Sierra Wireless devices are not being targeted by the malware, unchanged default factory credentials, which are publicly available, could allow the devices to be compromised. Additionally, a lower security posture could lead to the device being used in Distributed Denial of Service (DDoS) attacks against Internet web sites. There is evidence that "Internet of Things"-type devices have been infected with the Linux malware Mirai, which attackers used in the recent DDoS attacks against the web site Krebs on Security [\[¶\]](#).

This alert is being produced to amplify mitigations outlined by Sierra Wireless, for users of the following products:

- LS300,
- GX400,
- GX/ES440,
- GX/ES450, and
- RV50

ICS-CERT would like to emphasize that there is no software or hardware vulnerability being exploited in the Sierra Wireless devices by the Mirai malware. The issue is configuration management of the device upon deployment.

Discovery

Scan Results



Scan Lessons

- Scanning cellular devices burns cellular bandwidth quickly.
- Initially, the United States was only focus.
- Fingerprinting devices can be tricky when they disappear often.
- Scanning became more targeted.

October 24, 2016

49692 Hosts

September 9, 2017

58670 Hosts

July 29, 2018

105400 Hosts

Discovery

Scan Results



Set up a lab...

- DYN DDoS Attack
- Sierra Wireless device discovered
- Research Begins



Discovery

Scan Results

Research



Lab Devices



SIERRA WIRELESS LS300
Weak Authentication



SIERRA WIRELESS GX450
Weak Authentication



SIERRA WIRELESS ES440
Weak Authentication



MOXA ONCELL G3xxx
No Authentication



DIGI TRANSPORT WR44
Weak Authentication

Scope

No Scope

Discovery

Scan Results

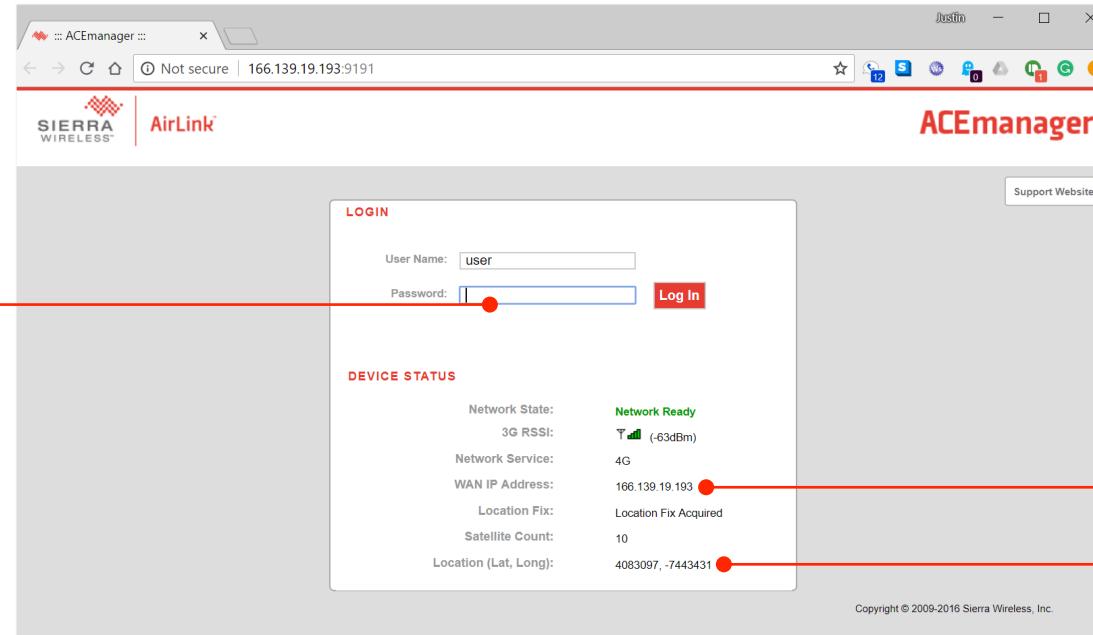
Research

“Exploiting” the Vulnerability

This is not dependent upon any vulnerability within the hardware or software.

DEFAULT
PASSWORD

Bruteforce attack(s)
are unnecessary.



WAN IP
166.139.19.193

PUBLIC GPS COORDINATES
40° 49' 51.5" N
47° 26' 03.5" W

Discovery

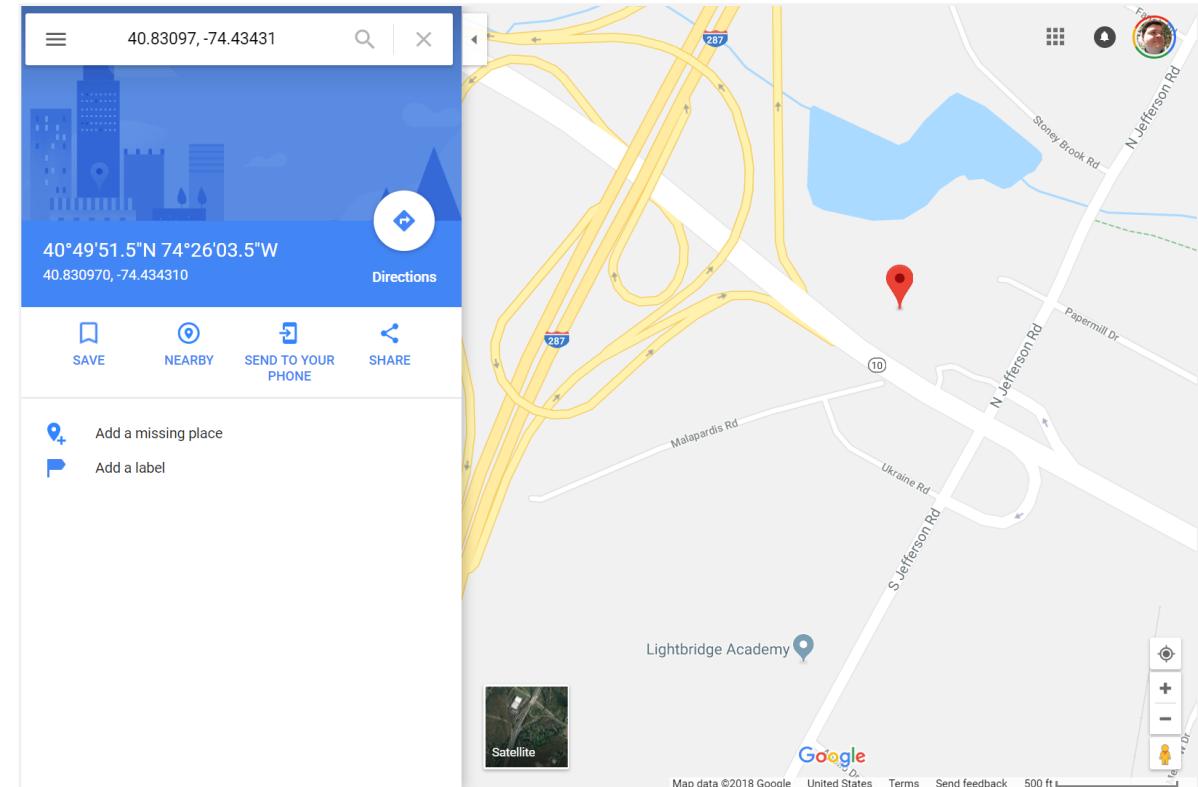
Scan Results

Research

Visualize

DEVICE STATUS

Network State:	Network Ready
3G RSSI:	桅杆 (-63dBm)
Network Service:	4G
WAN IP Address:	166.139.19.193
Location Fix:	Location Fix Acquired
Satellite Count:	10
Location (Lat, Long):	4083097, -7443431

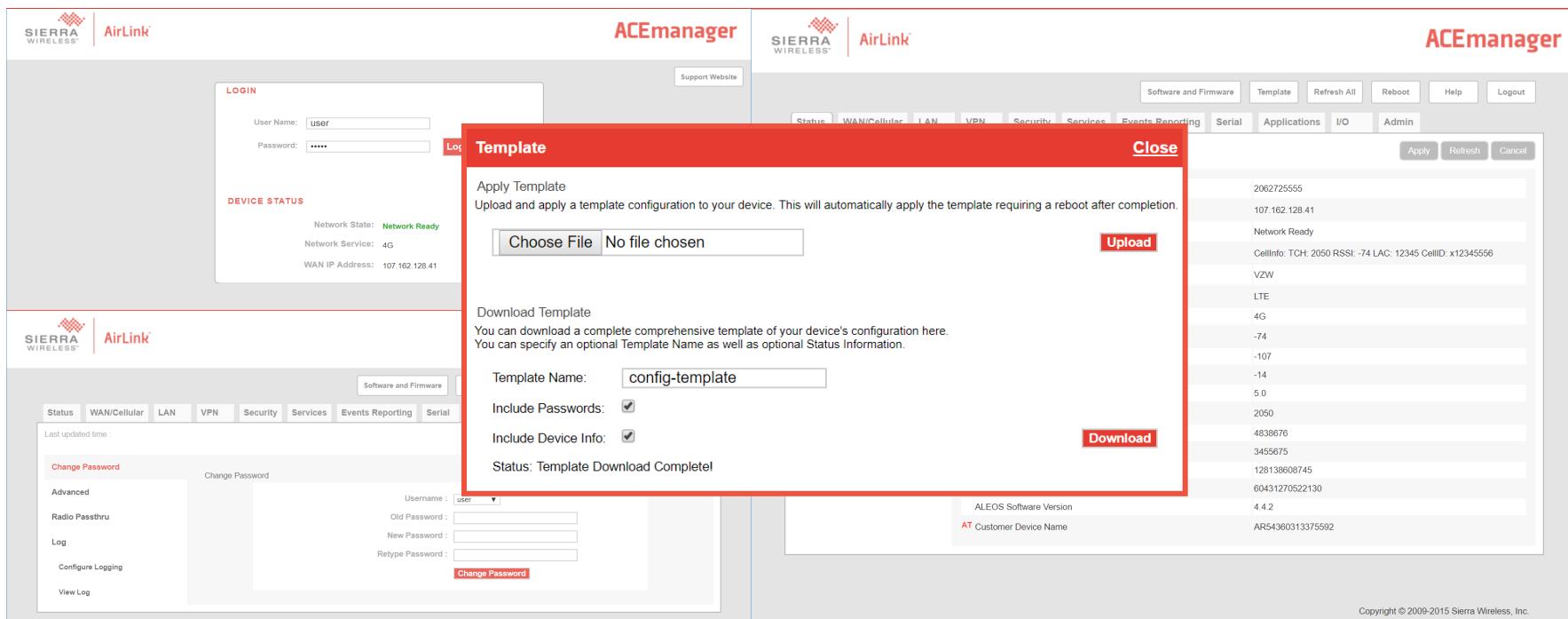


Discovery

Scan Results

Research

Lab Testing



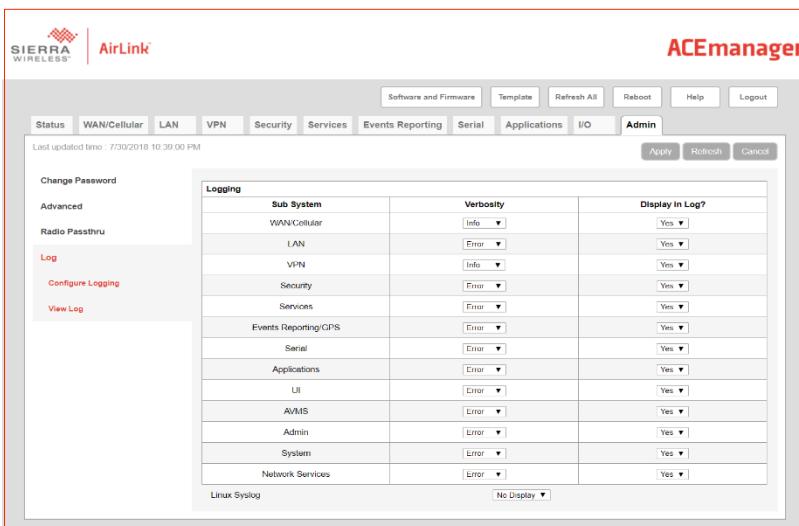
Discovery

Scan Results

Research

Lab Testing

Logging configuration



Discovery

Scan Results

Research



Logs
does not seem
to emit anything
useful about
auth.

Template Downloader

```

1 $ /usr/bin/env python
2 #encoding: utf-8
3 #
4 # Execute getthreads to stream connection requests to
5 # listed ip list file. Will attempt to authenticate
6 # using default credentials and then download the config
7 # template for each host.
8 #
9 # Usage:
10 #   crawler.py [ip list] [n threads]
11 #
12 import sys
13 import os
14 from selenium import webdriver
15 from selenium.webdriver.common import By
16 from selenium.webdriver.common.keys import Keys
17 from selenium.webdriver.support.ui import WebDriverWait
18 from selenium.webdriver.support import expected_conditions as EC
19
20 def usage():
21     print("Usage: python main.py ip_file num_threads")
22     exit(1)
23
24 def main():
25     if len(sys.argv) < 3 or not sys.argv[2].isdigit():
26         usage()
27     else:
28         ip_queue = []
29         num_threads = int(sys.argv[2])
30         ip_filename = sys.argv[1]
31         if not Path(ip_filename).exists():
32             usage()
33
34         with open(ip_filename) as ips:
35             for ip in ips:
36                 ip_queue.append(ip.strip())
37
38         # Spawn a worker pool and write the templates
39         pool = ThreadPool(num_threads)
40         res = pool.map_unordered(write_template, ip_queue)
41         pool.close()
42         pool.join()
43
44 def write_template(ip):
45     browser = get_chrome()
46     connect(browser, ip)
47     login(browser)
48     template = get_template(browser)
49     ip_bytes = ip.split('.')
50     file_name = ip_bytes[0] + ip_bytes[1] + '-' + template
51     with open(file_name, 'w') as output_file:
52         output_file.write(template)
53     return template
54
55

```

crawler.py – script to enumerate through a list of hosts, authenticate, and download the configuration template.

parse.py – script to analyze a path of configuration templates (XML), parse specific strings of interest, and output results to a file.

Lab test

Discovery

Scan Results

Research

```

<!-- Tracking Object -->
<item model-id="520000.d1" title="Tracking Object" value="0" />
<item model-id="520001.d1" title="Test IP Address" value="0.0.0.0" />
<item model-id="52003" title="Test IP Address" value="0.0.0.0" />
<item model-id="52004" title="Test Interval (seconds)" value="300" />
<item model-id="52005" title="Test Timeout (seconds)" value="0" />
<item model-id="52006" title="Maximum number of test retries" value="3" />
<item model-id="52007" title="Tracking Object" value="0" />
<item model-id="52008" title="Tracking Object" value="0" />

<!-- Dynamic Mobile Network Routing -->
<item model-id="530000" title="DMMR Enable" value="0" />
<item model-id="530001" title="DMMR Address" value="0.0.0.0" />
<item model-id="53002" title="N_MHAK_SPL" value="m" />
<item model-id="53020" title="N_MHAE_KEY" value="m" />
<item model-id="53003" title="Subset 1" value="0.0.0.0" />
<item model-id="53004" title="Subset 2" value="0.0.0.0" />
<item model-id="53005" title="Subset 3" value="0.0.0.0" />
<item model-id="53006" title="Subset 4" value="0.0.0.0" />
<item model-id="53007" title="Subset 5" value="0.0.0.0" />
<item model-id="53008" title="Subset 6" value="0.0.0.0" />
<item model-id="53009" title="Subset 7" value="0.0.0.0" />
<item model-id="53010" title="Subset 8" value="0.0.0.0" />
<item model-id="53011" title="Subset 1_NetMask" value="0.0.0.0" />
<item model-id="53012" title="Subset 2_NetMask" value="0.0.0.0" />
<item model-id="53013" title="Subset 3_NetMask" value="0.0.0.0" />
<item model-id="53014" title="Subset 4_NetMask" value="0.0.0.0" />
<item model-id="53015" title="Subset 5_NetMask" value="0.0.0.0" />
<item model-id="53016" title="Subset 6_NetMask" value="0.0.0.0" />
<item model-id="53017" title="Subset 7_NetMask" value="0.0.0.0" />
<item model-id="53018" title="Subset 8_NetMask" value="0.0.0.0" />

<!-- Forensic Agent -->
<item model-id="53107" title="Registration Timer (seconds)" value="60" />
<item model-id="53108" title="Retry Time Interval (seconds)" value="3" />
<item model-id="53104" title="Maximum Retry Count" value="5" />
<item model-id="53105" title="Registration Request Lifetime (seconds)" value="30" />

<!-- Reverse Tunneling Agent -->
<item model-id="53201" title="Maximum Transmission Unit . MTU (bytes)" value="1500" />
<item model-id="53204" title="Maximum Transmission Unit . MSS (bytes)" value="1460" />
<item model-id="53205" title="Force Fragmentation" value="0" />
<item model-id="53206" title="MTU (bytes)" value="1500" />

<!-- Addressing -->
<item model-id="53303" title="General" />
<item model-id="53304" title="Root Connection Mode" value="1" />
<item model-id="53305" title="Public Mode Channel Mask" value="255,255,255,255" />
<item model-id="53306" title="Power Tolerance (seconds)" value="16000" />

```

Found a funny pattern...

Devices would come and go...

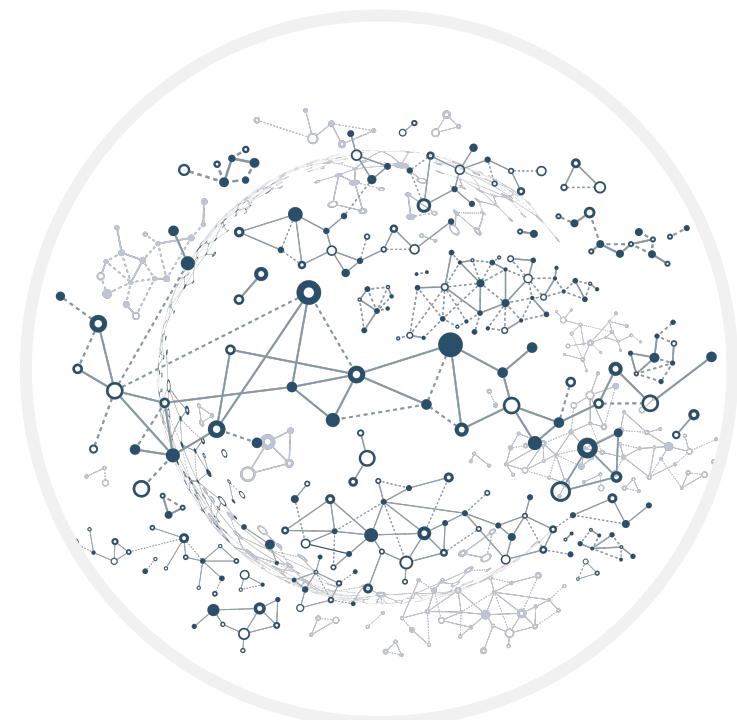
- DYN DDoS Attack
- Sierra Wireless device discovered
- Research Begins
- Setup a lab



Identifying Patterns

Devices would come and go...

- Public display of latitude and longitude.
- Scanning revealed hosts would go offline and return online at seemingly scheduled times.



Discovery

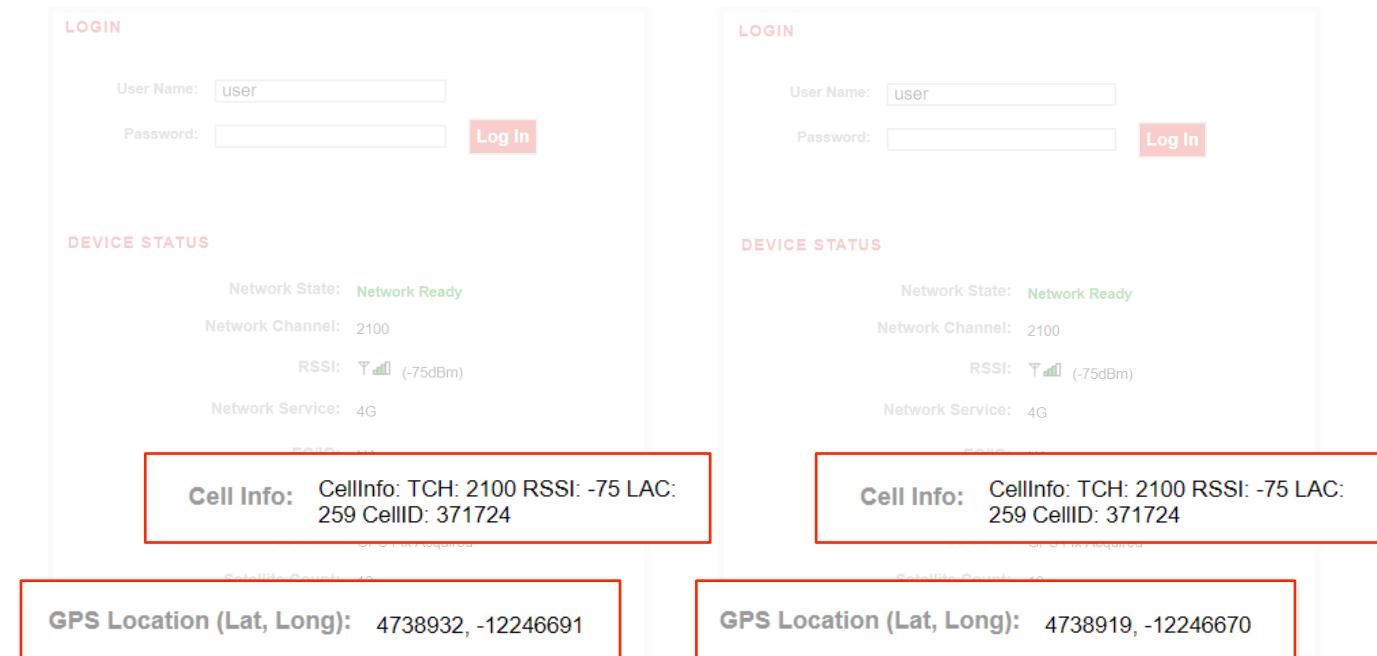
Scan Results

Research



Example

Oh, the places you shall go...
Can be observed by everyone...
And LAC/CELLID can give
ballpark location



The image shows two side-by-side screenshots of a mobile device's status screen. Both screens are identical, displaying the following information:

- LOGIN**: Fields for User Name (user) and Password, with a red "Log In" button.
- DEVICE STATUS**:
 - Network State: Network Ready
 - Network Channel: 2100
 - RSSI: -75dBm
 - Network Service: 4G
- Cell Info**: CellInfo: TCH: 2100 RSSI: -75 LAC: 259 CellID: 371724
- GPS Location (Lat, Long)**: 4738932, -12246691

Both screens have a red rectangular box highlighting the "Cell Info" and "GPS Location" sections.

Discovery

Scan Results

Research

Sierra Wireless case studies

St John Ambulance, Western Australia

California Highway Patrol, California

Ventura County Fire Department, California

South Bay Regional Public Communications Authority (SBRPCA), California

West Metro Fire Protection District, Colorado

Westminster Police Department, Colorado

Danish National Police, Denmark

Acadian Ambulance Service, Louisiana & Texas

East Baton Rouge Parish Emergency Medical Services (EMS), Louisiana

Mississippi Highway Safety Patrol

Gem Ambulance, New Jersey

City of Charlotte, North Carolina

Dickinson Police Department (DPD), Texas

Fairfax's Urban Search and Rescue Team, Virginia

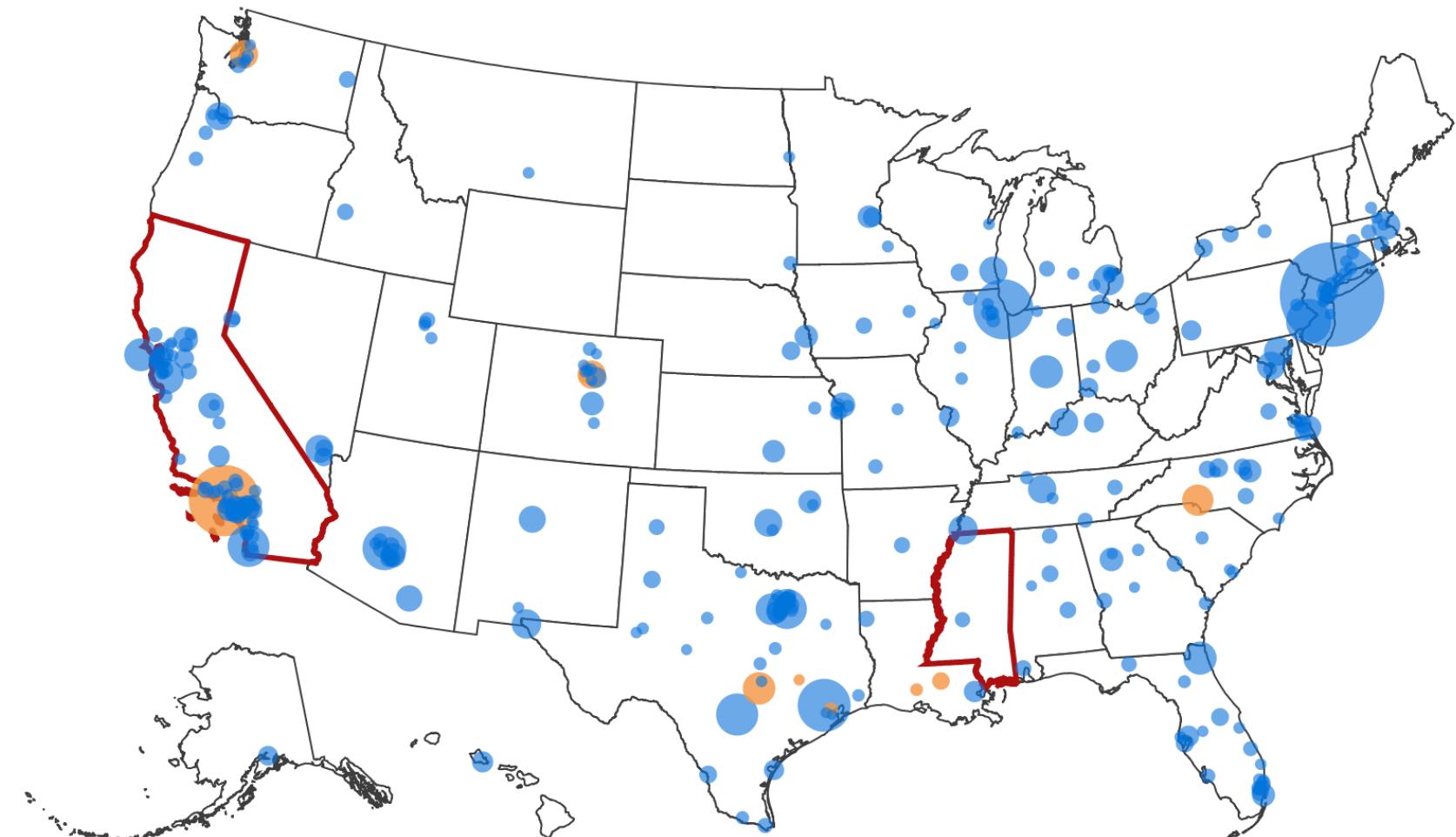
South Wales Police, Wales

City of Yakima, Washington

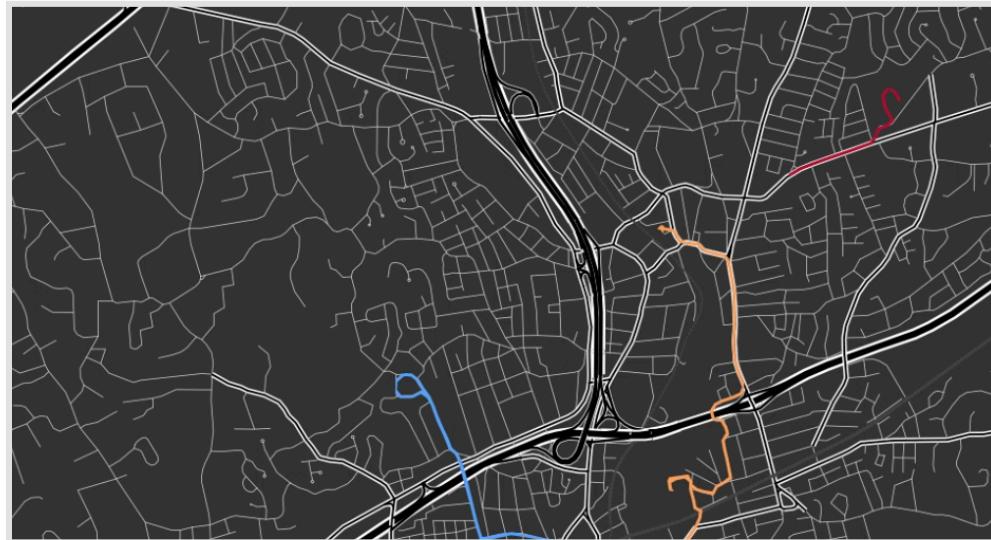
Seattle Fire Department, Washington



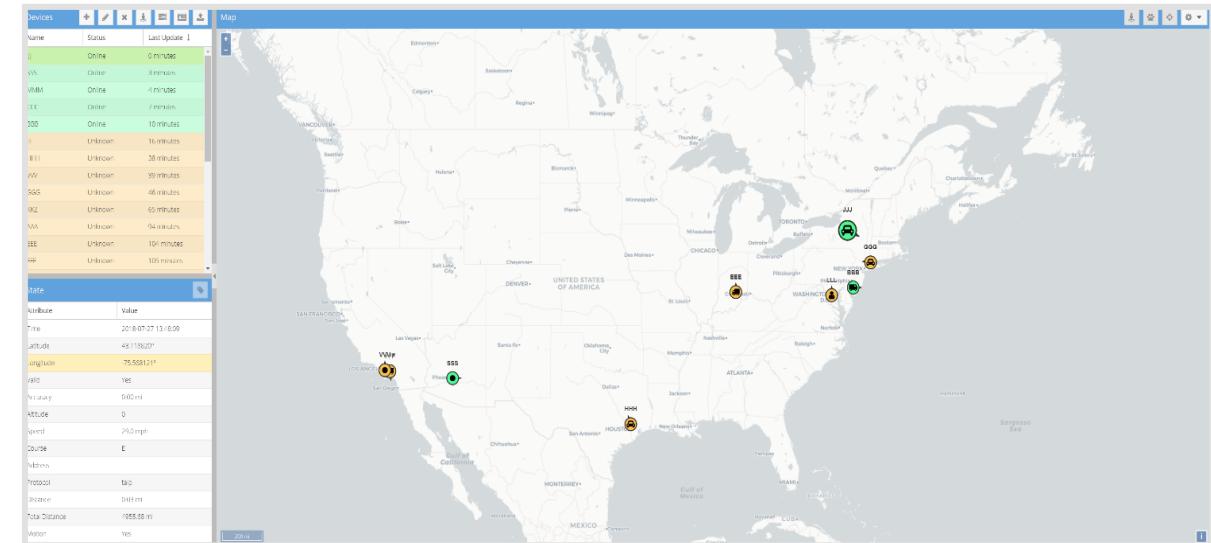
- Municipalities / Organizations Using Sierra Devices
- Top 300 Populous US Cities
- State Highway Patrol Use



Fleet / Vehicle Tracking



GPS Data Logging (TAIP)



TRACCAR – Open Source Fleet Software

Discovery

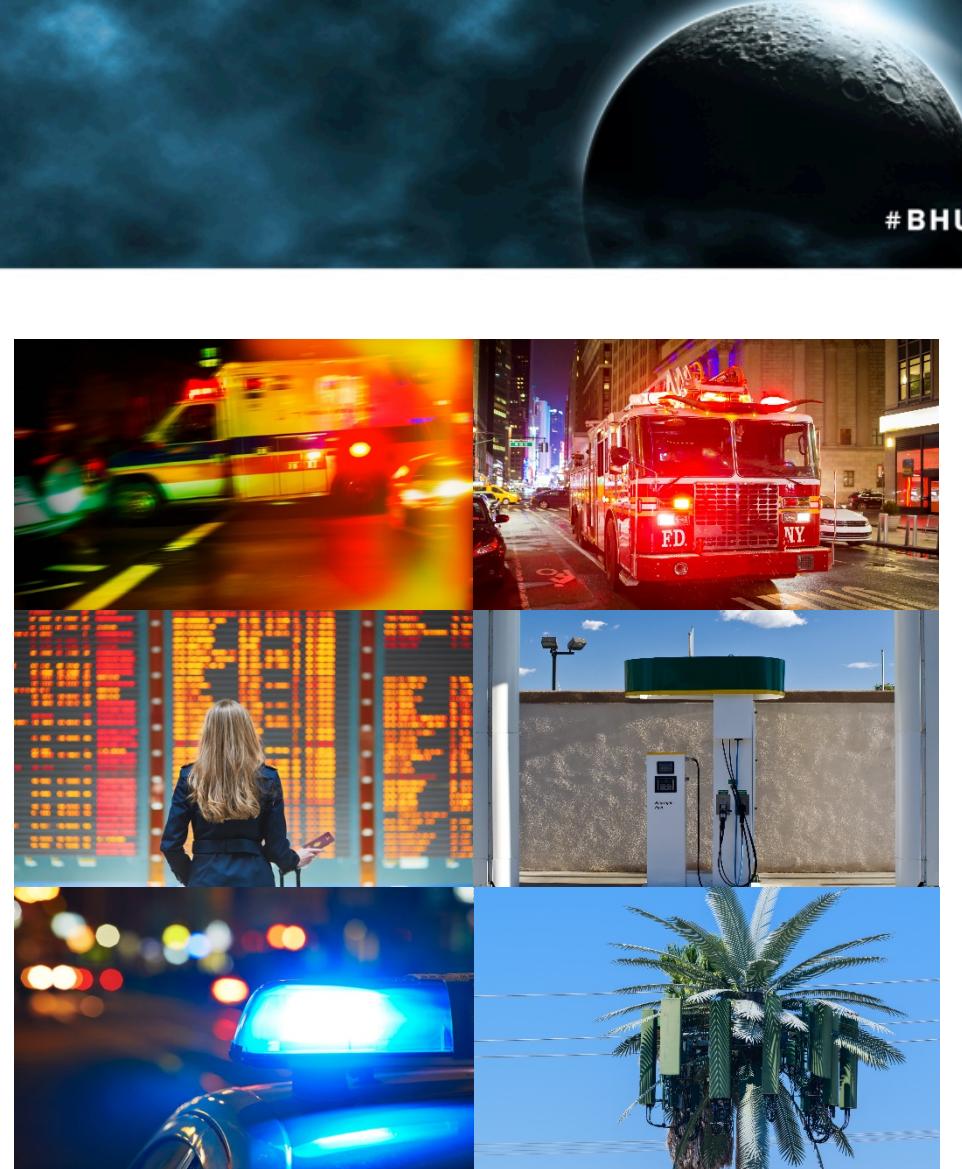
Scan Results

Research



This goes beyond cyber into life impact

- Re-route
- Monitor
- Listen
- Take offline
- Disrupt operations / communications
- Disrupt flow
- Disable
- Mess with data
- Did you know we have hydrogen cars?



Discovery

Scan Results

Research

Important

Conclusions

October 25, 2016

417

disclosures sent

0

responses

Discovery

Scan Results

Research

Important

Conclusions



Worst Case Scenarios

- Know where law enforcement officers are and are not to aid in crime
- More communications moving to encrypted means but GPS provides extreme accuracy.



Discovery

Scan Results

Research

Important

Conclusions

Worst Case Scenarios

- Targeted assassinations of LEOs
- GPS logging enables detailed pattern-of-life building, especially in areas where officers take their patrol cars home with them.



Discovery

Scan Results

Research

Important

Conclusions

Worst Case Scenarios

- Follow-on attacks on first responders
- Know when they are arriving and by which avenue. Enhances accuracy of remotely detonated IEDs.



Discovery

Scan Results

Research

Important

Conclusions

Out-of-band access, Retail,
Point of Sale, Kiosks, M2M, ATMs,
Mining, Fossil Fuels, Public Transit,
Public Safety, Law Enforcement

Use of cellular IoT (potential impact areas)

Government, Healthcare, Education,
Maritime, Utilities, Construction,
Hospitality, Robotics, Broadcasting

Unbreakable Cellular Bonding

**4x Service Providers.
100% Uptime.
1 Unbreakable Session.**



Bad Reception?

We understand the importance of staying connected wherever you are. Whether you're zooming around town or stationed in the middle of nowhere, roaming from network to network should not equate to downtime and more downtime.

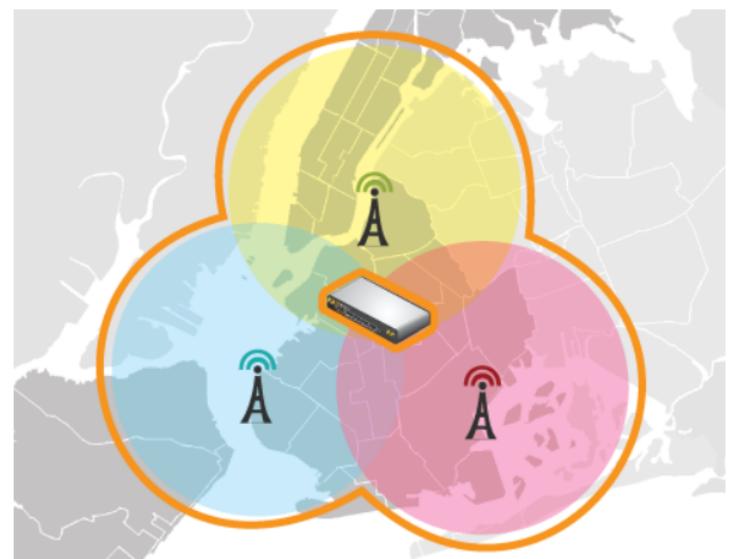
Which is why we believe in equipping our customers with best-in-class cellular routers to battle spotty coverage. Comprehensive [3G/4G LTE USB modem](#) support. Embedded SIM slots. Wi-Fi-powered WANs.

Wherever you go, whatever you do, our MAX Cellular Routers have you covered.

Speed & Reliability. Over Any Connection.

Of course, none of that means squat if your mission-critical connections disconnect when transitioning from one link to the next. So we go the extra mile and insist that our customers are protected by packet-level seamless failover and bandwidth bonding across all cellular connections.

No more re-establishing connections. No more skipped video frames. And no more waiting on file transfers. Simply put, your connection is unbreakable.



July 25, 2018

13,552

disclosures sent

2

responses

1

dialogue

Discovery

Scan Results

Research

Important

Conclusions

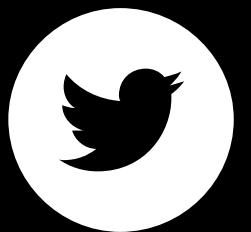


Conclusion



WE
CAN
FIX
THIS

- 1. Change password immediately!**
- 2. Upgrade firmware**
- 3. Configure management interface**
 - Stop using telnet and default port(s)
 - Maintain ACL to restrict access to management
 - Utilize VPN tunnel
 - Update log configuration to emit administrative events
 - Never enable login screen information details like GPS
- 4. Reach out to security@sierrawireless.com**



@sh4t



Questions

Acknowledgements

A sincere thank you to everyone who assisted in this work.

SARA BODDY

PAUL BURTON

PRESTON CROWE

