IOT: EXPLORING THE THREAT SURFACE

Jason Ortiz
Sr. Integration Engineer
01 | INTRODUCTION
EVERYTHING I KNOW ABOUT IOT
EVERYTHING I KNOW ABOUT IOT SECURITY
QUESTIONS?

THANK YOU.
EVERYTHING I THINK SORT OF MAKES SENSE...

» IoT Ecosystem
  » The Edge

» The Fog/Mist

» The Cloud
WHAT IS THE BIG IDEA?

» Data

Technology

General Motors Watches You Listen To The Radio

» Data

Alphabet’s ‘smart city’ idea sparks concerns over data use, sharing of profits

» Data

» Simple
03 | SECURING THE EDGE
HARDWARE

» Physical Ports
  » uArt
  » JTAG

JTAGulator Kit

$170

ADD TO CART
FIRMWARE

» Vulnerabilities
  » Conventional
  » Stored keys?
  » Memory dump keys?

» Updates ... or NOT
AUTHENTICATION

» Sooooo many things!

» Based mostly in HTTP
AUTHENTICATION

» Elliptic Curve Crypto?

» Blockchain?
## Payloads

<table>
<thead>
<tr>
<th>#</th>
<th>Downloaded Malware</th>
<th>% of Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Backdoor.Linux.Mirai.c</td>
<td>15.97%</td>
</tr>
<tr>
<td>2</td>
<td>Trojan-Downloader.Linux.Hajime.a</td>
<td>5.89%</td>
</tr>
<tr>
<td>3</td>
<td>Trojan-Downloader.Linux.NyaDrop.b</td>
<td>3.34%</td>
</tr>
<tr>
<td>4</td>
<td>Backdoor.Linux.Mirai.b</td>
<td>2.72%</td>
</tr>
<tr>
<td>5</td>
<td>Backdoor.Linux.Mirai.ba</td>
<td>1.94%</td>
</tr>
<tr>
<td>6</td>
<td>Trojan-Downloader.Shell.Agent.p</td>
<td>0.38%</td>
</tr>
<tr>
<td>7</td>
<td>Trojan-Downloader.Shell.Agent.as</td>
<td>0.27%</td>
</tr>
<tr>
<td>8</td>
<td>Backdoor.Linux.Mirai.n</td>
<td>0.27%</td>
</tr>
<tr>
<td>9</td>
<td>Backdoor.Linux.Gafgyt.ba</td>
<td>0.24%</td>
</tr>
<tr>
<td>10</td>
<td>Backdoor.Linux.Gafgyt.af</td>
<td>0.20%</td>
</tr>
</tbody>
</table>

Top 10 malware downloaded onto infected IoT device following a successful Telnet password crack.
SECURING THE MIST, OR FOG, OR WHATEVER
OK BUT REALLY

» The Edge

» The Fog

» The Mist

» The Cloud
COMPONENTS

» Networking

» Messaging

» Ecosystems

» Data
NETWORKING

» Which part?
  » User -> Stand Alone Device?
  » User -> Cloud Connected Device?
  » User -> Hub?
  » Device -> Hub?
  » Hub -> Cloud?
  » User -> Cloud?
  » Device -> Device?
  » Device -> Cloud?
DNS REBINDING

» Same Origin Policy

» bad.js

» CVEs? You bet
DNS REBINDING

» Vulns Everywhere!

- 87% of switches, routers, and access points
  - Aruba
  - Avaya
  - Cisco
  - Dell
  - Extreme
  - Netgear
  - 14 million

- 78% of streaming media players/speakers
  - Apple
  - Google
  - Roku
  - Sonos
  - 5.1 million

- 77% of IP phones
  - Avaya
  - Cisco
  - NEC
  - Polycom
  - 124 million

- 75% of IP cameras
  - Axis Communications
  - GoPro
  - Sony
  - Vivotek
  - 160 million

- 66% of printers
  - Hewlett Packard
  - Epson
  - Konica
  - Lexmark
  - Xerox
  - 165 million

- 57% of smart TVs
  - Roku-integrated
  - Samsung
  - Vizio
  - 28.1 million
SECURE NETWORKING?

» Heavy Use of HTTPS

» Authentication?

» FIDO Alliance
QUEUES

- RabbitMQ
  - Complex setup
  - Basic security

- nats.io
  - Auth
  - TLS

```python
authorization {
    users = [
        {user: alice, password: foo}
        {user: bob, password: bar}
    ]
}
```
MQTT

Publisher -> MQTT Broker -> Subscriber

Virtual channel

Topic
MQTT

» Anything interesting on a public broker?

» SHODAN

» C2 through MQTT
SECURING MQTT

» Enterprise Solution (HiveMQ)

» 3rd party broker
NODERED
NODERED

» Security?

» Anything live?

» API!
SECURING NODERED

» Authentication

» Secure Comms

⚠️ There have been a few cases of “unsecured” Node-RED instances having a crypto-mining flow deployed by someone scanning for port 1880.

Don’t exposing Node-RED on the internet without proper security applied.

🔐 Secure your Node-RED now!

nodered.org/docs/security
WEB INTERFACES

» Basic Vulnerabilities

» Custom HTTP servers ... but why?
Databases

» Mongo

» Postgres

```
# TYPE   DATABASE   USER   ADDRESS               METHOD
# "local" is for Unix domain socket connections only
local all all all trust
# IPv4 local connections:
host all all 127.0.0.1/32 trust
# IPv6 local connections:
host all all ::1/128 trust
# Allow replication connections from localhost, by a user with the
# replication privilege.
local replication all all trust
host replication all 127.0.0.1/32 trust
host replication all ::1/128 trust
host all all all all trust
```

pg_hba.conf
INDICES

» ElasticSearch
05 | SECURING THE DATA
SECURING THE DATA

» Make No Mistake ... I mean PRIVACY

» Is perimeter security dead?
SECURING THE DATA

» Cameras

United States
Japan
Italy
France
UK

0  1500  3000  4500  6000
SECURING THE DATA

» Cars and Cities?

General Motors Watches You Listen To The Radio

Alphabet’s ‘smart city’ idea sparks concerns over data use, sharing of profits
SECURING THE DATA

» Wearable Medical Devices

“Frankly, I don’t give a damn if someone wants to change their heart rate data.”
We’re still working on getting you more information about the Smart Ball on adidas.com so come back soon. In the meantime, here’s the product article number G83963 for your reference, it’s categorized as: Training and Soccer Balls

adidas miCoach Smart Soccer Ball
by adidas miCoach

Note: This item is only available from third-party sellers (see all offers).

Available from these sellers.

Color: White
Size: 5

- Training tool for placing kicks
- Integrated sensor package records strike point, speed, spin and trajectory when you kick the ball
- Compatible with Bluetooth Smart capable devices using iOS (vers. 7 or later), Android (4.3 or later) or Windows 10.
- Size 5 regulation weight, highest quality thermal bonded 32-panel ball; Requires inflation
- Battery life: approx. 2,000 kicks/one week; Charging time: approx. 1hr;
  Package includes charging base and AC power plug

New (7) from $238.63 + $9.95 shipping

Report incorrect product information.

Order tracking, upgraded.
Alexa can tell you when a package is at your door. Learn more
QUESTIONS?

THANK YOU.