

WEAPONIZING (AND DEFENDING) IOT

When Refrigerators Attack!

Kat Fitzgerald
Principal Security Architect
Zebra Technologies
(Evilkat aka @rnbwkat)

DEF CON
CIRCLE CITY CON 5.0

WHOAMI

\$ whoami

Kat Fitzgerald (@rnbwkat or evilkat@rnbwmail.com)

- First DEFCON was DC 3 (1995) with 16 speakers.
- Over 27(?) years in the Security field, with an emphasis on Security Operations, Incident Response and Purple Teams.
- Based in Chicago and a natural creature of winter, you can typically find me sipping Casa Noble Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos against a barrage of attackers.
- Honeypots & Refrigerators

DISCLAIMER

- The views and opinions expressed in this presentation are my own and do not necessarily reflect the official policy or position of any current or previous employer. Examples of exploitations, coding and vulnerabilities discussed/demonstrated within this presentation are only examples and they should not be utilized in the real-world.

Those of you with an overwhelming fear of the unknown will be happy to learn that there is no intended hidden message revealed by reading this disclaimer backwards.

WHY WE ARE NOT HERE

- I won't solve all your IoT woes
- Neither will the person sitting next to you
- Common Sense went out the window decades ago

WHY ARE WE HERE?

- Defending, not weaponizing (sort of)
- IoT, IoE
 - Five Verticals (Goldman Sachs)
 - Wearables
 - Connected Cars
 - Connected Homes
 - Connected Cities
 - Industrial
 - Older devices
 - How would you know?



WHY ARE WE HERE (2)

- Device Longevity
 - Updates
- Physical Limitations
 - Crypto limits (key length)
- Data
 - Collecting
 - Personal
- The “How”
 - Built from other stuff
 - Ok, ok, we’ll add security

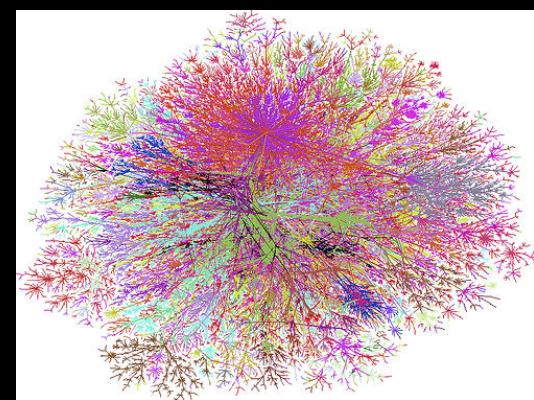


EXAMPLES

- University attacked by its lightbulbs, vending machines and lamp posts
- Cars
 - Students in China hacked a Tesla Model S electric car and made the doors fly open, the wipers wiped and the horn honked
- Industrial
 - Shut down an Oil Rig
 - Govt Building – heating/cooling
 - Blast Furnace
 - Toilet

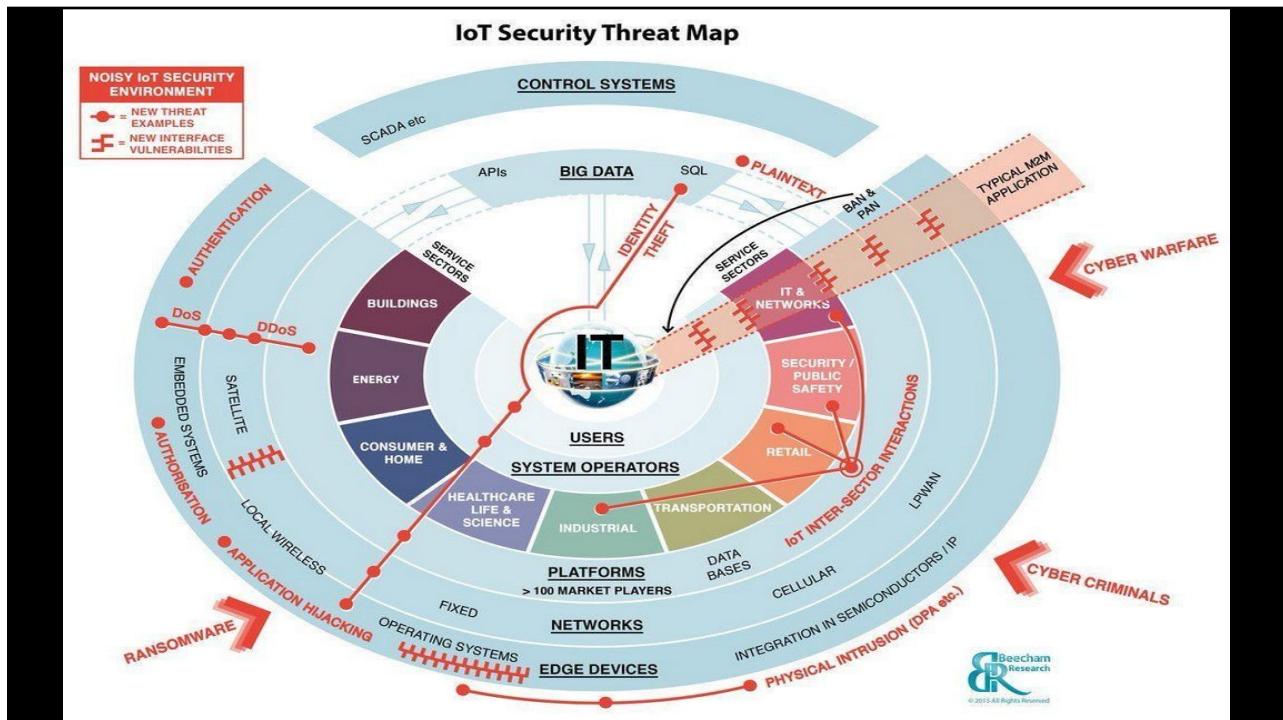
IMPORTANT THINGS

- Devices Collect Data from something
- Devices Send Data to somewhere
- Devices Use Data to control things



BUT... TIMELY(?) UPDATE

- Krack
- IoT_Reaper
 - Based on Mirai
 - Not telnet, but vulns
- ROCA (Return of Coppersmith's Attack)
 - RSA private key recovery
 - Only Public key



GENERAL SECURITY

- Network – Services/ports, firewalls, encryption
- Application – Input Validation, Auth?
- Mobile – APIs, encryption
- Cloud – Same as IoT
- IoT – All of the Above

GENERAL SECURITY (2)

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

DID WE MENTION?

- Autosploit
- Big Data
- BYOD
 - Footprint?
- Patching, Patching, Patching
 - Vulnerability Management
 - Dnsmasq
 - Linux (remember XP?)
 - Android
- Shodan

SHODAN

- HTTP header information
- HTTPS header and certificate information
- System & Service banners
 - NetBIOS server banner
 - SSH header and server key data
 - Telnet banner
 - SMTP banner
 - NTP banner
 - SIP/VoIP banner
- DNS server configuration settings
- C&C

EXPLORING

port:"81" city:"phoenix" product:"Netwave IP camera http config"

TOTAL RESULTS

10

TOP COUNTRIES

United States 10

TOP ORGANIZATIONS

Organization	Count
CenturyLink	6
Cox Communications	4

72. Cox 9:10 GMT
Ip72-2017-26-05:29:1' Cox Communications Added on 2017-10-23 05:29:10 GMT United States, Phoenix [Details](#)

HTTP/1.1 200 OK
Server: Netwave IP Camera Date: Mon, 23 Oct 2017 05:29:09 GMT Content-Type: text/html Content-Length: 7250 Cache-Control: private Connection: close

70. I on 0:09:06 GMT
Ip70-on on 0:09:06 GMT Cox Communications Added on 2017-10-22 00:09:06 GMT United States, Phoenix [Details](#)

HTTP/1.1 200 OK
Server: Netwave IP Camera Date: Sun, 22 Oct 2017 00:09:07 GMT Content-Type: text/html Content-Length: 7250 Cache-Control: private Connection: close

EXAMPLES (2)

```
SSID=<redacted>1
NetworkType=Infra
Channel=0
AuthMode=WPA2PSK
EncrypType=AES
WPAPSK=8<redacted>z
```

```
var sys_ver='4.37.2.38';
var app_ver='4.5.3.45';

var sys_ver='11.37.2.48';
var app_ver='2.0.10.2';
```

Fascinating...

- Comcast
- Comcast Business
- RCN
- AT&T U-Verse
- Network Innovations
- Cox
- CenturyLink

MORE EXPLORING

.84

AT&T U-verse

Added on 2018-05-23 22:14:29 GMT

United States, Indianapolis

[Details](#)

HTTP/1.1 200 OK

Server: Netwave IP Camera

Date: Wed, 23 May 2018 22:14:29 GMT

Content-Type: text/html

Content-Length: 372

Cache-Control: private

Connection: close

TOTAL RESULTS

1,258

TOP COUNTRIES



TOP CITIES

San Jose	16
Portland	7
Minneapolis	5
Pittsburgh	4
Seattle	3

TOP ORGANIZATIONS

Comcast Cable	315
Time Warner Cable	134
Spectrum	118
CenturyLink	69
Verizon Fios	63

24

Google Fiber

Added on 2018-06-02 00:28:07 GMT

United States, Prairie Village

[Details](#)

HTTP/1.1 200 OK

Server: Netwave IP Camera

Date: Sat, 02 Jun 2018 00:24:41 GMT

Content-Type: text/html

Content-Length: 1919

Cache-Control: private

Connection: close

58

Time Warner Cable

Added on 2018-06-02 00:28:01 GMT

United States, Cohoes

[Details](#)

HTTP/1.1 200 OK

Server: Netwave IP Camera

Date: Sat, 02 Jun 2018 00:28:01 GMT

Content-Type: text/html

Content-Length: 3169

Cache-Control: private

Connection: close

5

Spectrum

Added on 2018-06-01 23:59:28 GMT

United States, Saint Cloud

[Details](#)

HTTP/1.1 200 OK

Server: Netwave IP Camera

Date: Sat, 02 Jun 2018 00:00:23 GMT

Content-Type: text/html

Content-Length: 2574

Cache-Control: private

Connection: close

THE POINT?

- What's going on in your neighborhood?
- Local Threat Landscape
- Don't rely on fancy blinky-things

EXAMPLES (3)

USER:	PASS:	USER:	PASS:
root	x3511	admin1	password
root	vizev	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdpC	root	k1v1234
root	default	root	Z0z521
root	jouatch	root	M13518
root	123456	root	jvoid
root	54321	root	anko
support	support	root	zlxz
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	idreambox
user	root	root	realtek
admin	(none)	root	user
root	pass	root	00000000
admin	admin1234	admin	1111111
root	1111	admin	1234
admin	smcadmin	admin	12345
admin	1111	admin	54321
root	666666	admin	123456
root	password	admin	7ujMko0admin
root	1234	admin	1234
root	k1v123	admin	pass
Administrator	admin	admin	meinsm
service	service	admin	tech
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

SOME THOUGHTS ON DETECTION

- Honeypots
 - Defense
 - Challenges
 - 1000's of responses
 - 8.38b IoT devices (Gartner)
 - Deployment
 - Stop telling people where they are!
 - Work...

DETECTION (MORE)

- Micros POS
- Geographic

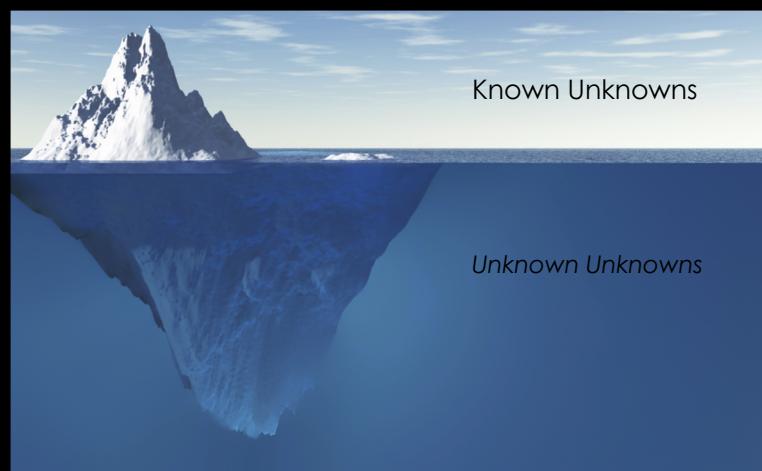


EXAMPLES (4)

```
12345 >/tmp/.ptmx && cd /tmp/
dreambox sh 54321 uClinux
shell admin support
smcadmin antslq 123456
password system 0000 system\x00
enable sh\x00 1001chin xc3511
welc0me 1234
```

```
123456 xc3511
>/dev/.ptmx && cd /dev/
1234 antslq
shell system\x00
system
>/tmp/.ptmx && cd /tmp/ 1111
dreambox admin sh
>/etc/.ptmx && cd /etc/ enable
support
>/.ptmx && cd /
12345 sh\x00
>/dev/shm/.ptmx && cd /dev/shm/
```

CONCLUSIONS



MORE CONCLUSIONS

- You can not *protect* anything without first *identifying* assets and risks faced by each!
- You can not *respond* to events if you have not implemented proper measures to *detect* them!

THANK YOU

Kat Fitzgerald
evilkat@rnbwmail.com
@rnbwkat

