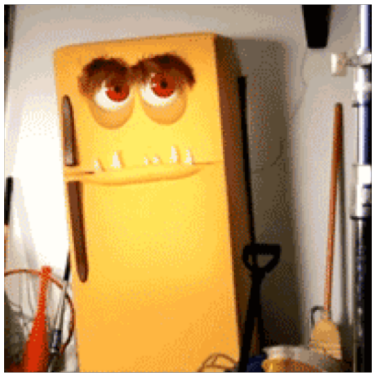
WEAPONIZING (AND DEFENDING) IOT

When Refrigerators Attack!

Kat Fitzgerald
@rnbwkat

Principal Security Architect
Zebra Technologies

BSIDES MELBOURNE 2019



WHOAMI

$ whoami

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

- *@BsidesChicago and @dianainitiative (new COO)*
- *Over (lots) years in Security, with an emphasis on Blue Teams, SecOps, IR and previously Purple Teams.*
- *Based in Chicago and a natural creature of winter, you can typically find me sipping Grand Mayan Extra Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos.*
- *Honeypots & Refrigerators are a few of my favorite things!*

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 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 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

BUT FIRST..

- $66 B! (2018 estimate)
- Attacks and breaches are common place
- Security Appliances and software are vulnerable
- Lateral Movement
- But what about –
  - Your Security Architecture is not unique
  - What is your "typical day"

Instead of Brilliance, we have standardized mediocrity.
– John Strand, Offensive Countermeasures

WHY ARE WE HERE?

- Defending, not weaponzing (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)

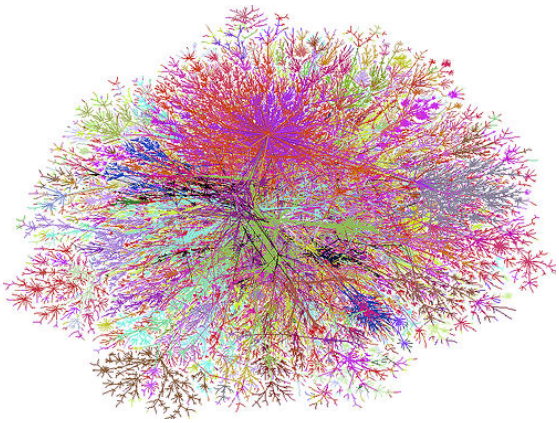
- Device Longevity
  - Updates
- Physical Limitations
  - Crypto limits (key length)
- Data
  - Collecting
  - Personal
- The "How"
  - Built from other stuff
  - Ok, ok, we'll add security

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
  - Blast Furnace
  - Toilet
- PewDiePie

IMPORTANT THINGS

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



PRIVACY CONCERNS

- Growing consumer reliance on IoE (Internet of Everything)
- IoT are easy targets for MITM attacks
- Decryption exists mostly at consumer end where skill-set is weakest and not understood
- Unplanned uses create multiple risks, safety and security threats
  - Children have unexpected results
  - Things that "listen" or monitor
  - Traditional InfoSec threat models fail under IoT
- Lack of network segmentation (especially WiFi)

HELLO GDPR

- InfoSec (encryption, AAA, logging/monitoring, audits, blockchain and InfoSec skills) may not scale well with IoT.
- Complex Network topologies become more complex, creating manageability challenges. Where manageability is weak, security can also be weakened.
- If IoT data is compromised or lost, compliance will be compromised where PII is concerned.
  - But it's not PII! Prove it!

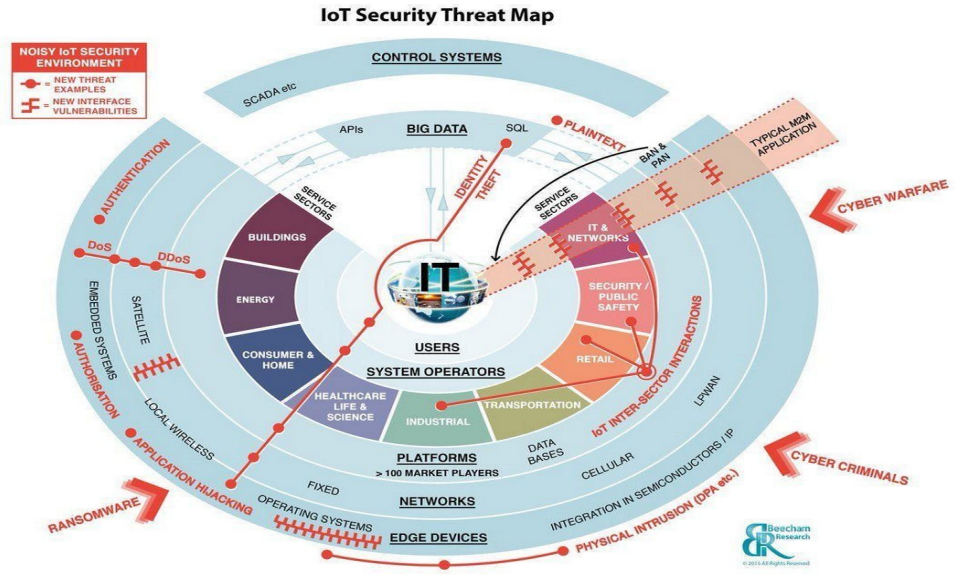
GDPR + IOT = WHAT?

- How to obtain "Consent"
  - Proxy - Healthcare
- What if the device is shared
  - Who is consenting
- What if the space is shared - home or car (rental car)
  - Can one consent and one decline
- Update consent when data collection changes
- Devices have limited power = inexpensive
  - Are they really that smart
- Data enters cloud = combined sources = consent(?)
  - Forensics at scale

SUPPORT

BUT… AN UPDATE

- Iot_Reaper
  - Based on Mirai
  - Not telnet, but vulns
- ROCA (Return of Coppersmith's Attack)
  - RSA private key recovery
  - Only requires Public key
- MicroTek
- *<Insert next exciting attack here>*



GENERAL SECURITY

- Network – Services/ports, firewalls, encryption
- Application – Input Validation, Auth?
- Mobile – APIs, encryption
- Cloud – Same as IoT
- IoT – It hasn't changed

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 I MENTION?

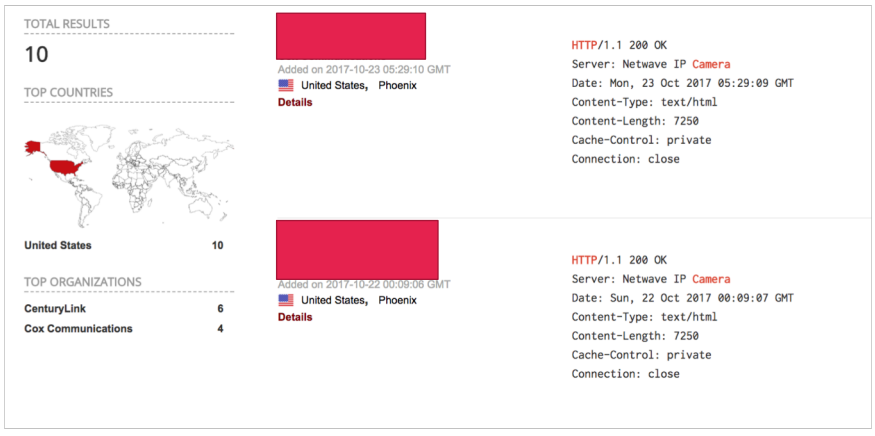
- Autosploit
- Big Data
- BYOD
  - Footprint?
- Patching, Patching, Patching
  - Vulnerability Management
  - Dnsmasq
  - Linux (remember XP?)
  - Android
- Shodan

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"



EXAMPLES (2)

SSID=<redacated>1
NetworkType=Infra
Channel=0
AuthMode=WPA2PSK
EncrypType=AES
WPAPSK=8<*redacted*>zs

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';

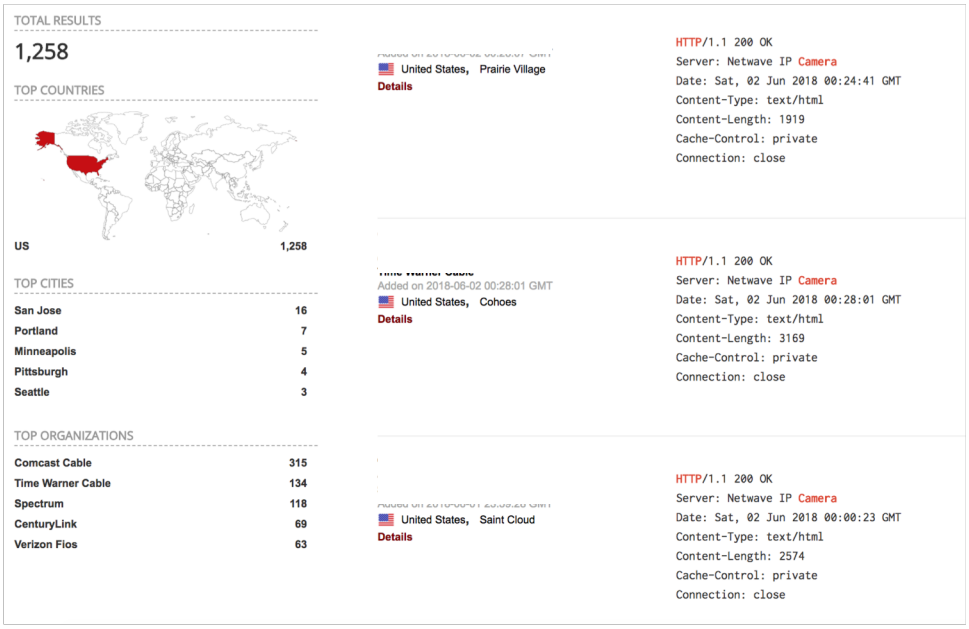
Fascinating…

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

MORE EXPLORING

[redacted]
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

US 1,258

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

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
```

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
```

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
```

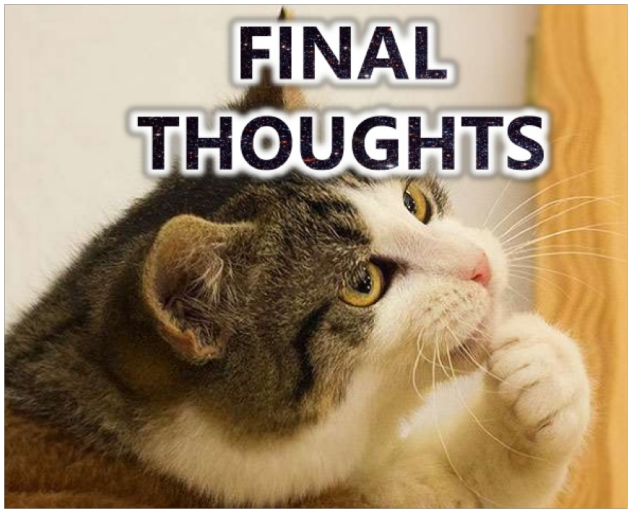
THE POINT?

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

Rely on people!

SOME THOUGHTS ON DETECTION

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



MORE REALLY FINAL THOUGHTS

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

A fun place to start

https://gitlab.com/expliot_framework/expliot

https://cybarrior.com/blog/2019/01/28/expl-iot-internet-of-things-exploitation-framework/

THANK YOU

Kat Fitzgerald
evilkat@rnbwmail.com
@rnbwkat