WEAPONIZING (AND DEFENDING) IOT

When Refrigerators Attack!

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

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 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)

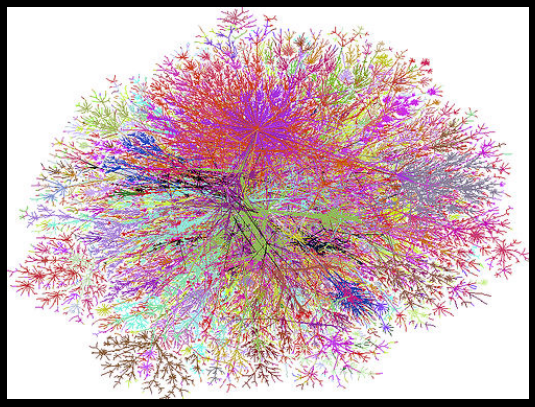
- Device Longevity
  - Updates
- Physical Limitations
  - Crypto limits (key length)
- Data
  - Collecting
  - Personal
- The "How"
  - Built from other stuff
  - Ok, ok, we'll add security

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
  - Govt Building – heating/cooling
  - Blast Furnace
  - Toilet

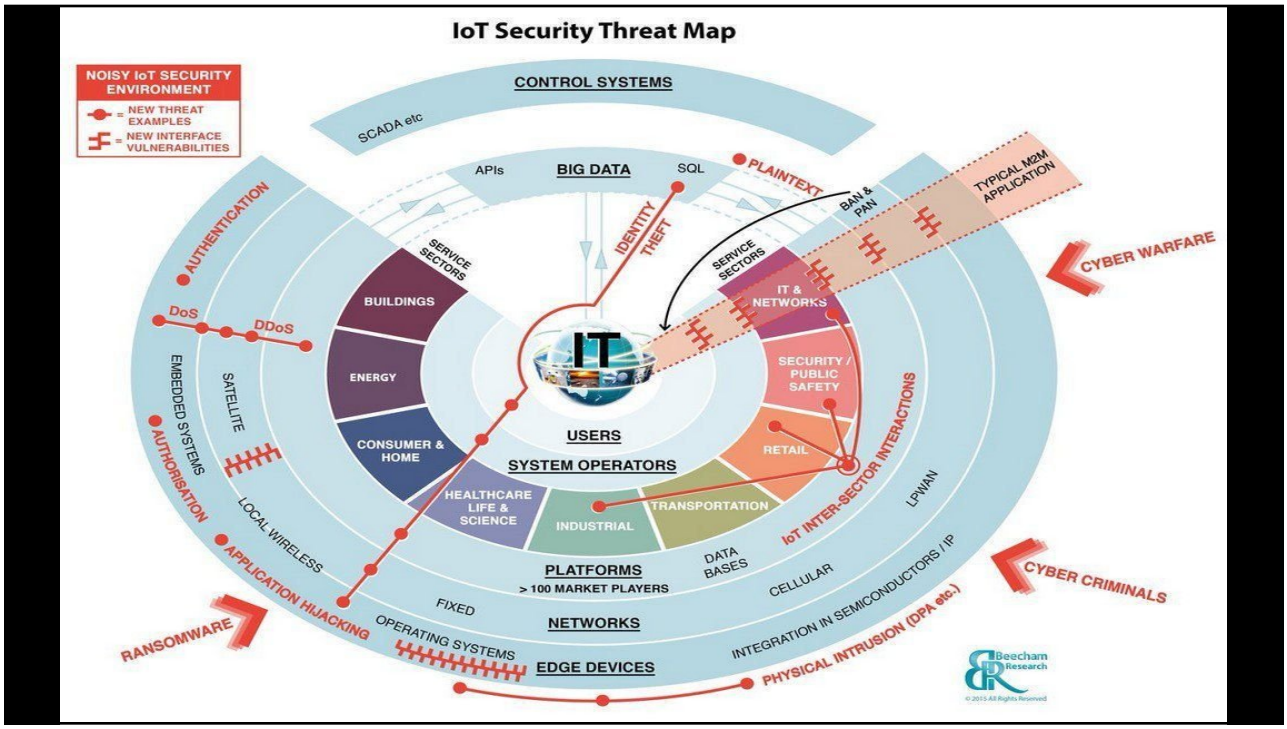
IMPORTANT THINGS

- 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?

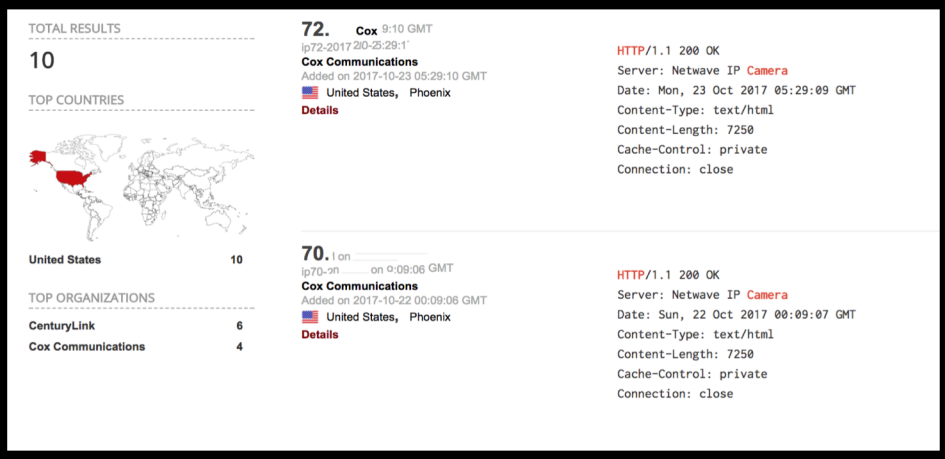
- Autosploit
- Big Data
- BYOD
  - Footprint?
- Patching, Patching, Patching
  - Vulnerability Management
  - Dnsmasq
  - Linux (remember XP?)
  - Android
- Shodan

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"



EXAMPLES (2)

SSID=<redacted>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

.84

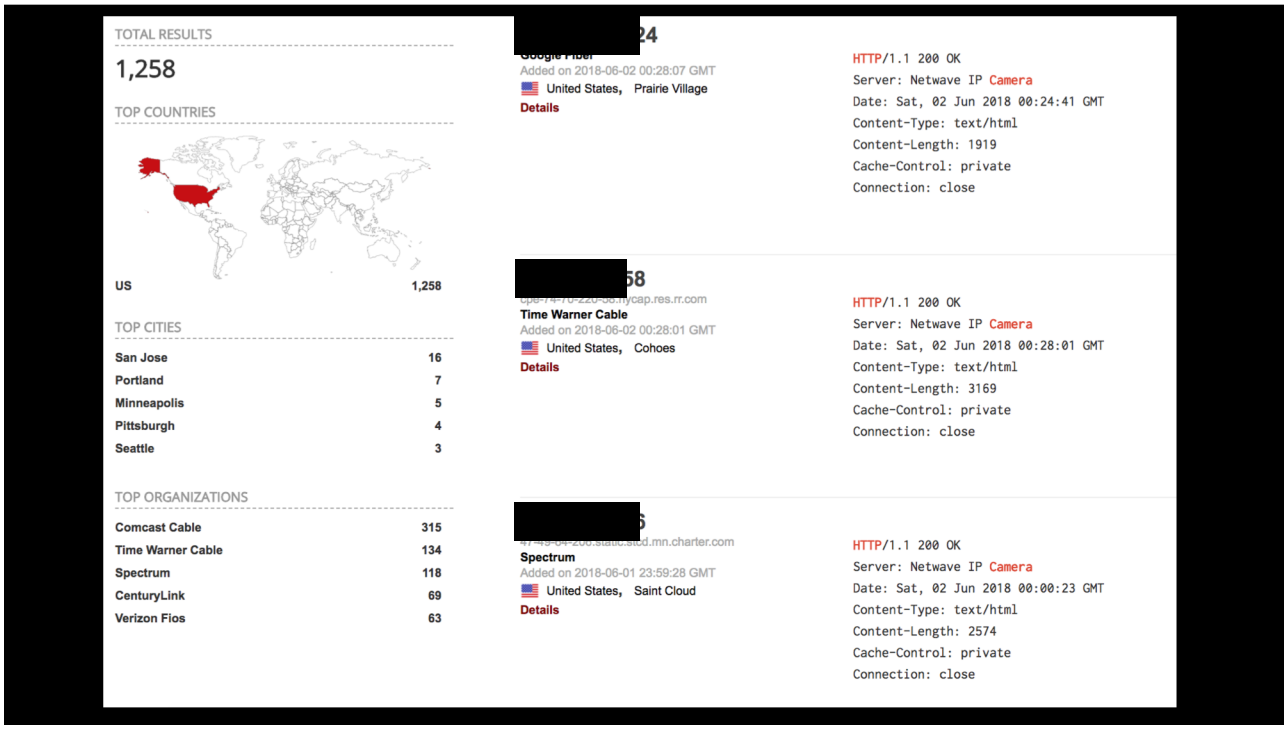
AT&T U-verse

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
```



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	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

SOME THOUGHTS ON DETECTION

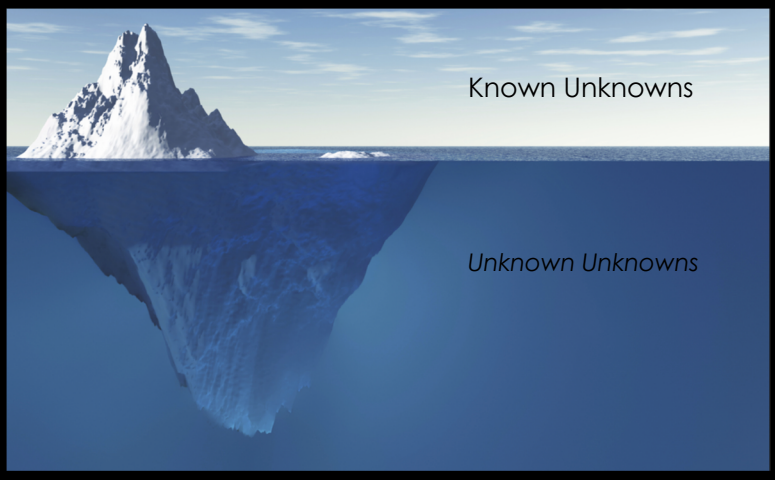
- Honeypots
  - Defense
  - Challenges
    - 1000's of responses
  - 8.38b IoT devices (Gartner)
  - Deployment
    - Stop telling people where they are!
  - Work…

DETECTION (MORE)

- Micros POS
- Geographic

EXAMPLES (4)

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