

1

\$ whoami

- CEO @BSidesChicago,
2019 COO @dianainitiative,
CFP Chair @BSidesPGH, DefCon 3!
- Many years in Security, with an emphasis on
Blue Teams, (former Purple), DevSecOps, IR.
- Based in ~~Pittsburgh~~ Kirkland, WA and a natural
creature of winter, you can typically find me
sipping Casa Noblé Añejo whilst simultaneously
defending my systems using OSS, magic spells
and Dancing Flamingos.
- Honeypots, Refrigerators and IoT (Internet of
Threats) are a few of my favorite things!

2

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.

3

WHY ARE WE NOT HERE

- This is not a demo of 5000 different honeypots
- I'm not showing you all my honeypots (duh)
- Honeypots are only PART of your Security Posture



4

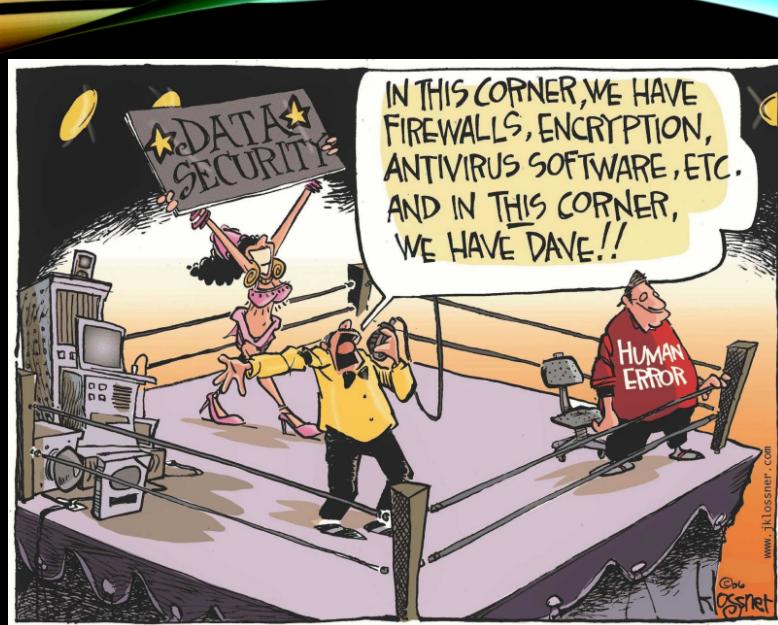
WHY ARE WE HERE?

- Spending exceeded \$114 billion - 2018
- Attacks and breaches are commonplace
- Security “stuff” is vulnerable
- Lateral Movement – (*this will become more important*)
- But what about –
 - Your Security Architecture is not unique
 - What is your “typical day”

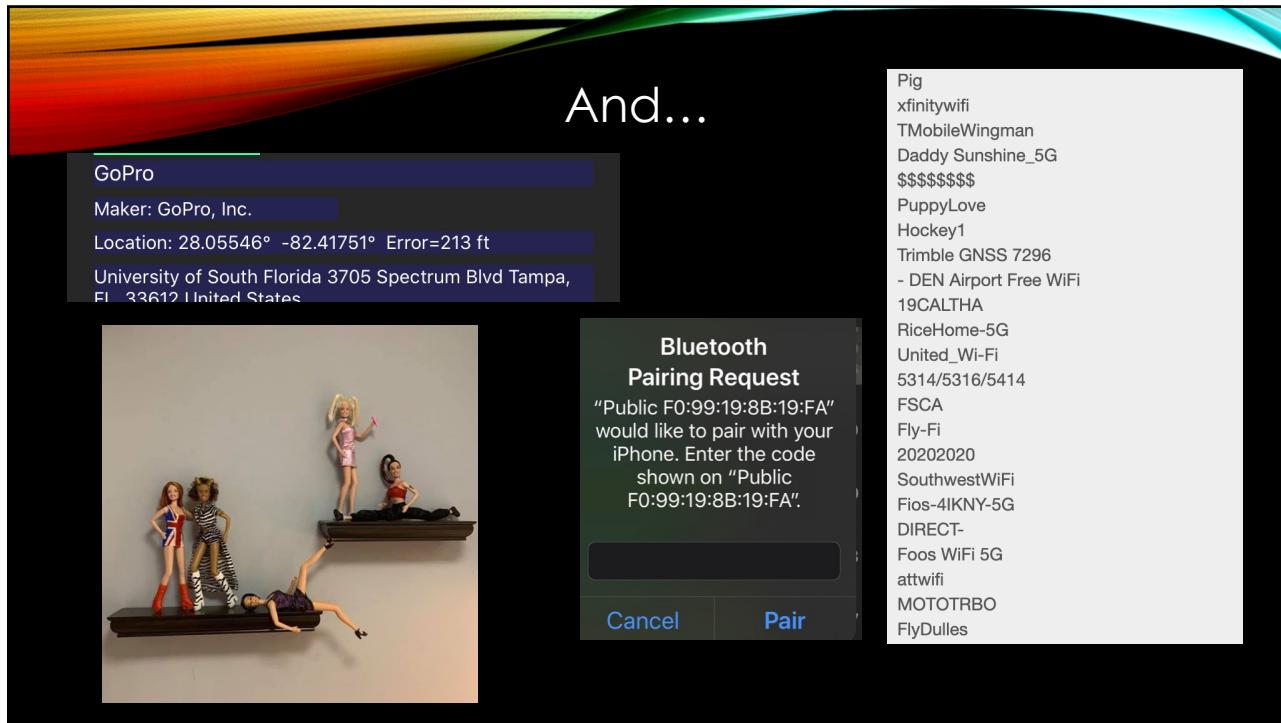


Instead of Brilliance, we have standardized mediocrity.
– John Strand, Offensive Countermeasures

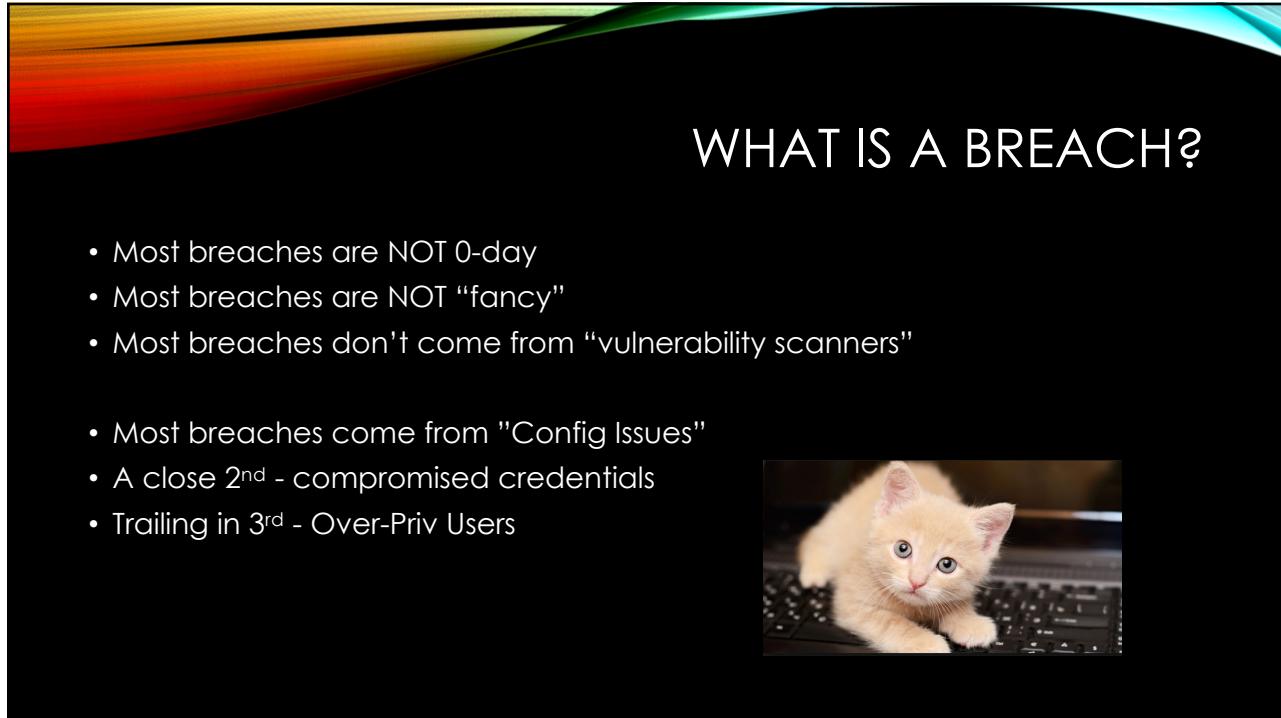
5



6



7



8

EXAMPLES

- University attacked by its lightbulbs, vending machines and lamp posts
- Industrial
 - Shut down an Oil Rig
 - Blast Furnace
 - Toilet

9

HONEYPOTS

- Honeypots vs Deception
 - A resource with no value(?)
 - Value = Use of Resource
 - Does Not Hack Back
- Important Points
 - Deployment
 - Customization = Planning! (more on this)
 - 100's of "types"



10

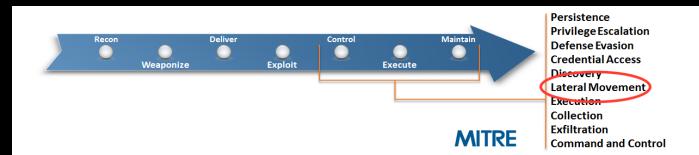
PICK ONE

- Adhd – <https://www.activecountermeasures.com/free-tools/adhd/>
- Honey Badger -- <https://github.com/adhdproject/honeybadger> (GEO!)
- Community Honey Network -- <https://communityhoneynetwork.readthedocs.io/en/stable/>
- Canarytokens -- <https://canarytokens.org/generate>
- OpenCanary -- <https://opencanary.readthedocs.io/en/latest/>
- WebThings -- <https://iot.mozilla.org/docs/gateway-getting-started-guide.html>
- T-pot -- <https://github.com/dtag-dev-sec/tpotce>
- Twisted-honeypot -- <https://github.com/lanjelot/twisted-honeypots>
- Lots more -- <https://github.com/paralax/awesome-honeypots>
- What about the “Real Thing”? Hmmmm..

11

LATERAL MOVEMENT

- Enables an adversary to access and control remote systems on a network.
- *(See, I told you it would become important later)*



https://attack.mitre.org/wiki/Lateral_Movement

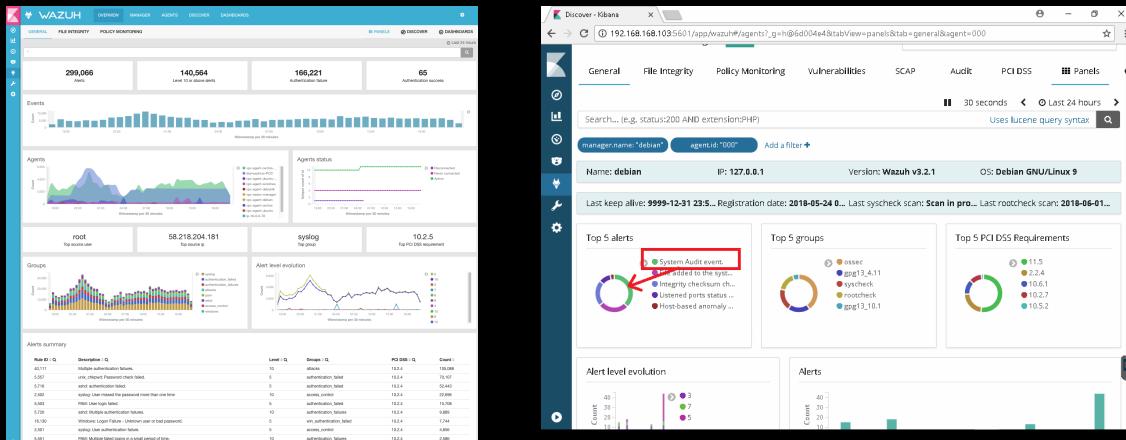
12

OODA VS CCAD

- OODA
 - Observe
 - Orient
 - Decide
 - Act
- CCAD
 - Confuse
 - Confound
 - Annoy
 - Delay

13

MONITORING - WAZUH.COM



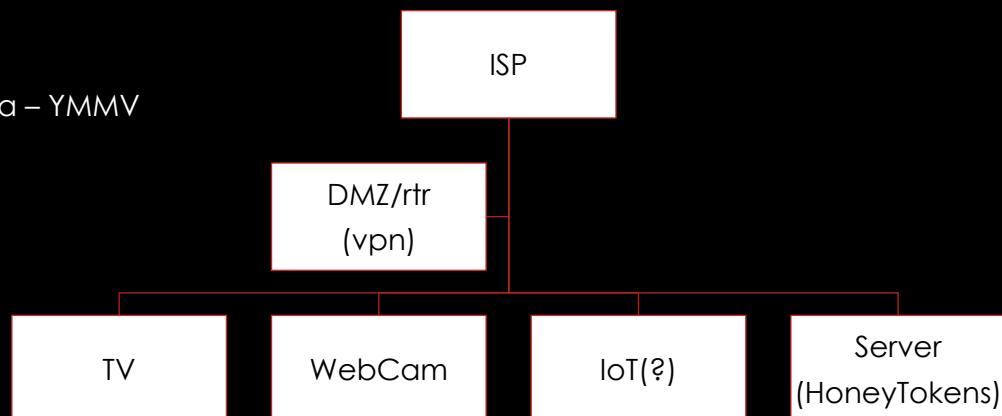
14

DEPLOYMENT

- Plan, Plan, Plan!
 - Low, Medium, **High**
 - Honeypots, Honeyports, Honeytokens, Honeycreds
 - Customization ← *Ding ding ding!*
 - Real vs Self-Signed Certs
 - Actual Applications
 - HIDS / OSSEC / Wazuh / SIEM
 - Rules! Tuning
- Where?
 - Server Farms
 - Cloud Storage
 - IoT (Shodan is your friend!!)
 - <https://shodan.io>
 - DMZ (Guest WiFi)
 - MX, DNS
 - PoS
 - WP, Rpi, VMs, VPS

15

- An Idea – YMMV



16

CUSTOMIZATION

- Start with your (friends? Neighbors?) devices
- Shodan
 - Banners
 - Versions!
 - HTML
- Certificates
- HoneyTokens
- Storage
- Real Servers and Apps
 - Staging?

17

WHAT IS IT?

```
# uname -a
Linux RT-AC5300 2.6.36.4brcmarm #1 SMP PREEMPT Fri Oct 18 16:13:51 CST 2019 armv7l ASUSWRT
# df
Filesystem      1K-blocks   Used Available Use% Mounted on
rootfs          40960     40960        0 100% /
/dev/root       40960     40960        0 100% /
devtmpfs        257456        0  257456  0% /dev
tmpfs           257600     944  256656  0% /tmp
/dev/mtdblock4    65536    2064   63472  3% /jffs
```

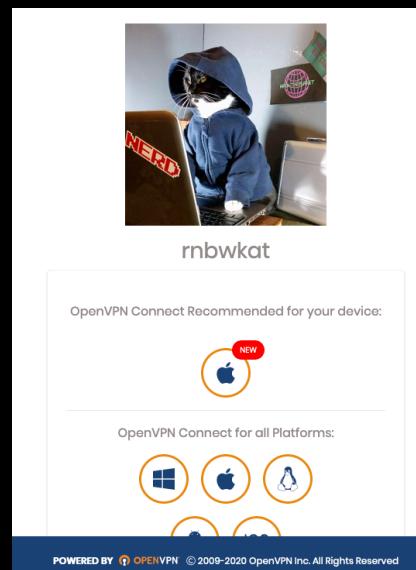
18

COWRIE

```
# ls -al /etc
srwxrwxrwx 1 admin root 0 May 5 2018 amas_lib_socket
-rw-rw-rw- 1 admin root 1017 May 5 2018 cert.pem
drwxrwxrwx 2 admin root 100 May 5 2018 cfg_mnt
srwxrwxrwx 1 admin root 0 May 5 2018 cfgmnt_ipc_socket
-rw-rw-rw- 1 admin root 380 May 5 2018 dnsmasq.conf
drwx----- 2 admin root 100 Feb 27 13:24 dropbear
lrwxrwxrwx 1 admin root 20 Dec 31 1969 e2fsck.conf -> /rom/etc/e2fsck.conf
drwxrwxrwx 2 admin root 60 May 5 2018 email
lrwxrwxrwx 1 admin root 19 Dec 31 1969 ethertypes -> /rom/etc/ethertypes
-rw-r--r-- 1 admin root 0 Dec 31 1969 fstab
-rw-r--r-- 1 admin root 52 May 5 2018 group
-rw-rw-rw- 1 admin root 0 May 5 2018 group.custom
-rw-r--r-- 1 admin root 52 May 5 2018 gshadow
-rw-r--r-- 1 admin root 176 May 5 2018 hosts
lrwxrwxrwx 1 admin root 23 Dec 31 1969 hotplug2.rules -> /rom/etc/hotplug2.rules
-rw-r--r-- 1 admin root 365 May 5 2018 ipsec.conf
drwxr-xr-x 10 admin root 200 May 5 2018 ipsec.d
-rw-rw-rw- 1 admin root 1675 May 5 2018 key.pem
```

19

WHAT IS IT?



20

PORTSPOOF (1)

```
nmap -p200-300 gonzo

PORT      STATE SERVICE
200/tcp    open  src
201/tcp    open  at-rtmp
202/tcp    open  at-nbp
203/tcp    open  at-3
204/tcp    open  at-echo
205/tcp    open  at-5
206/tcp    open  at-zis
207/tcp    open  at-7
208/tcp    open  at-8
209/tcp    open  tam
210/tcp    open  z39.50
211/tcp    open  914c-g
212/tcp    open  anet
213/tcp    open  ipx
214/tcp    open  vmpwscs
215/tcp    open  softpc
216/tcp    open  atl5
217/tcp    open  dbase
218/tcp    open  mpp
219/tcp    open  uarps
220/tcp    open  imap3
221/tcp    open  fln-spx
222/tcp    open  rsh-spx
223/tcp    open  cdc
224/tcp    open  masqdialer
```

21

PORTSPOOF (2)

```
nmap -A gonzo
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-27 09:52 EST
Stats: 0:04:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 75.58% done; ETC: 09:58 (0:01:31 remaining)
Stats: 0:04:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 77.22% done; ETC: 09:58 (0:01:26 remaining)
Stats: 0:07:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```

22

HIDING IN PLAIN SIGHT

84%

of organizations breached had evidence of the breach in their log files...

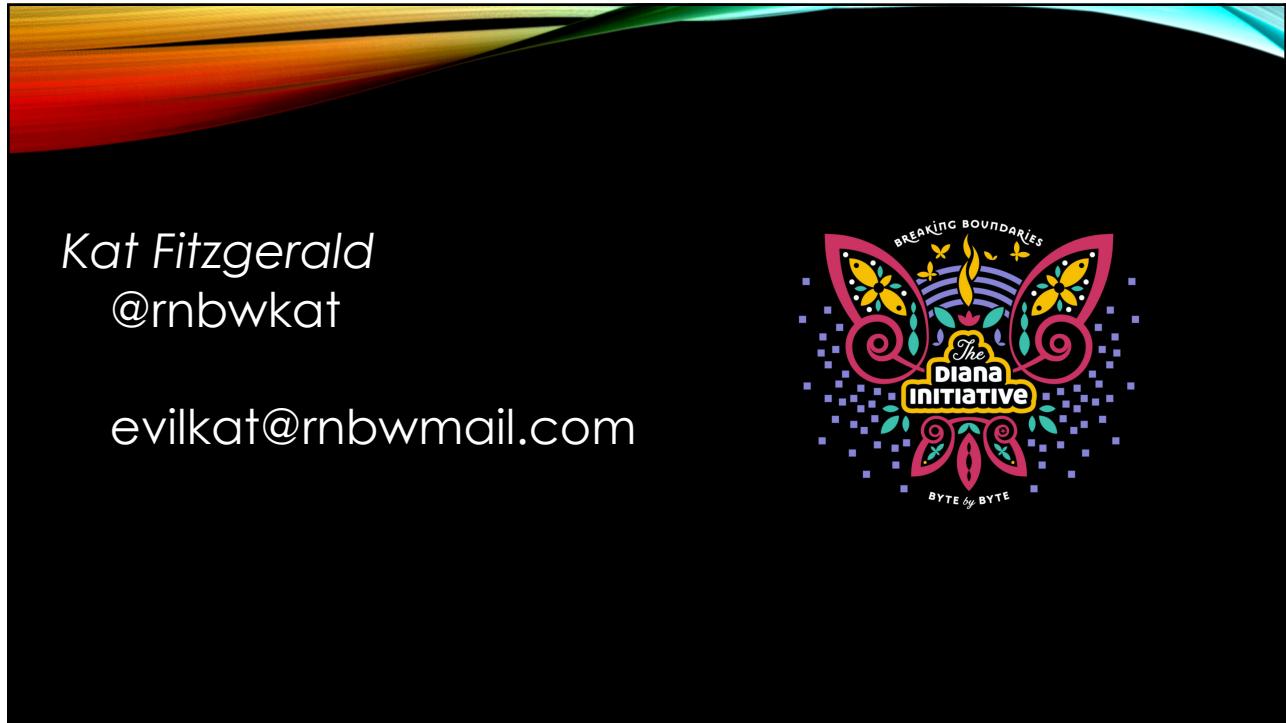
Source: Verizon Data Breach Report, 2014

23

TAKEAWAYS

- CCAD
- Low False Positives
 - Defend & Detect
- Lateral Movement
- Cost Effective
- Forensics
- REAL Threat Intelligence
 - It's About Thinking Differently, not "watching everything"
- <https://github.com/ElevenPaths/HomePWN>

24



25