IOT SECURITY

"BE AFRAID. BE VERY AFRAID."

OR "DON'T WORRY, BE HAPPY" – YOUR CHOICE

DUB DUBLIN

CEO, DUBLINVENTION

DUB@INFOWAVE.COM

Presented to: ***TFI Communications Technology & Asset Valuation Conference*** • January 26-27, 2017, Austin, Texas

THE RECENT NEWS ISN'T GOOD…

- Sep 13, 2016 Bruce Schneier blog post: "Someone is learning how to take down the Internet" with probing attacks
- Sep 20, 2016 DDOS attack on KrebsOnSecurity.com
- Oct 21, 2016 Dyn DDOS Attack (.1M of .5M Mirai infected nodes) (Affects Twitter, Paypal, Reddit, Spotify, Netflix, CNN, Amazon, etc.)
- Nov 26, 2016 ~1M (5%) Deutsche Telekom customers knocked off Internet by Mirai botnet (SOAP remote execution on DT routers)
- Nov 30, 2016 Checkpoint Technologies discovers Gooligan, which has rooted 1M Android devices and is adding 13K every day
- Jan 3, 2017 Switcher Trojan: Android phones attack router DNS
- Jan 5, 2017 FTC sues D-Link for insecure routers and webcams

WE’VE KNOWN SECURITY WAS THE BIGGEST CHALLENGE FOR IOT FOR YEARS…

So what did we do about it?

Well, pretty much nothing:

(Ignore it, maybe it’ll go away…)

This actually worked until the device count got big enough to be attractive to the bad guys

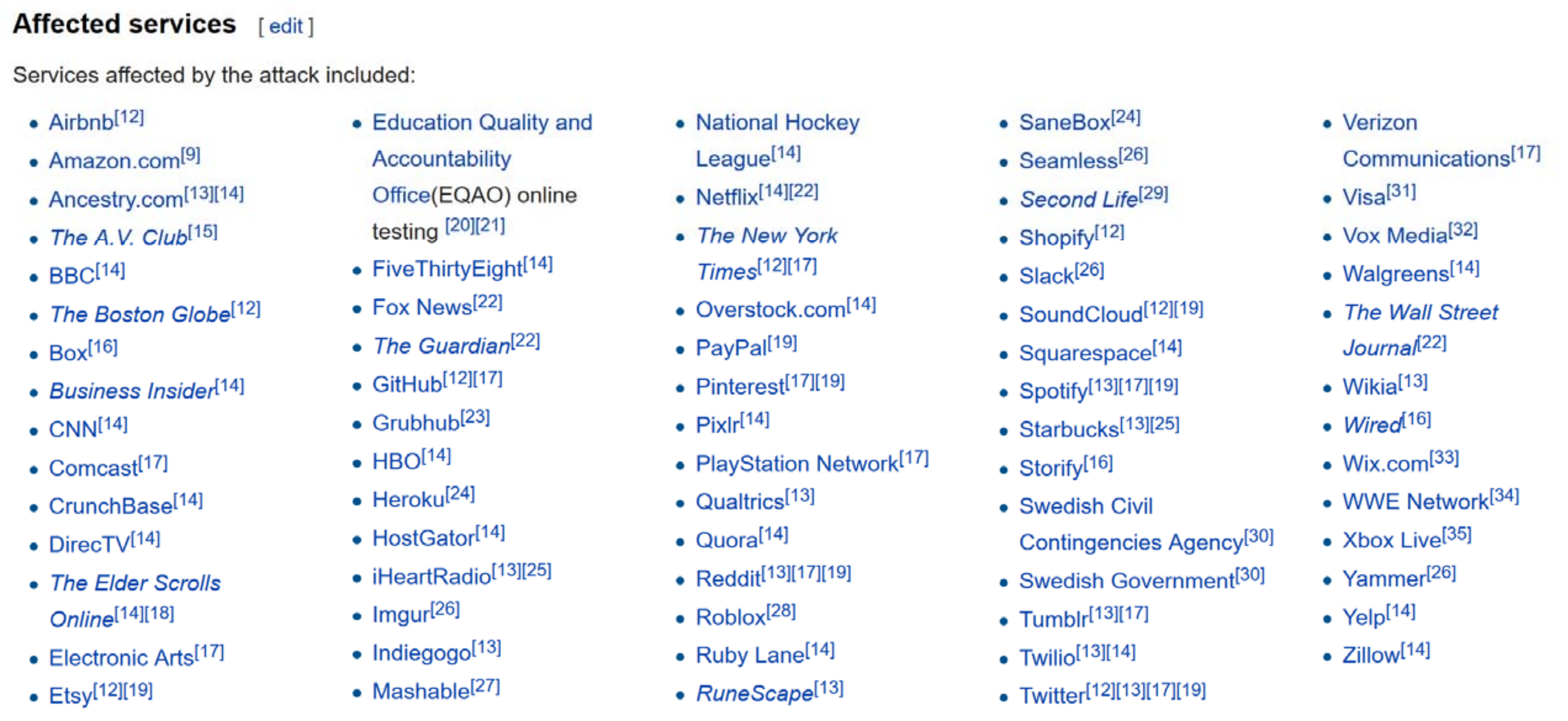
(Note: there **are** bad guys)

HOW BAD WAS THE DYN ATTACK?

- Came from at least 100,000 devices infected by Mirai botnet
- Attack generated compounding recursive DNS retry traffic, further amplifying its impact
- Two attack waves:
  - Started globally, then focused on US-East – 40-50x normal traffic, mostly repelled
  - About 6 hours later, much larger, more distributed attack begins
- **Peak attack traffic estimated at 1.2 Terabits/Second!**

Source: Dyn.com blog

ATTACKS INFRASTRUCTURE HAVE BROAD REACH...



Affected services [edit]

Services affected by the attack included:

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- Education Quality and Accountability Office(EQAO) online testing [20][21]
- FiveThirtyEight[14]
- Fox News[22]
- *The Guardian*[22]
- GitHub[12][17]
- Grubhub[23]
- HBO[14]
- Heroku[24]
- HostGator[14]
- iHeartRadio[13][25]
- Imgur[26]
- Indiegogo[13]
- Mashable[27]
- National Hockey League[14]
- Netflix[14][22]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]
- Qualtrics[13]
- Quora[14]
- Reddit[13][17][19]
- Roblox[28]
- Ruby Lane[14]
- *RuneScape*[13]
- SaneBox[24]
- Seamless[26]
- *Second Life*[29]
- Shopify[12]
- Slack[26]
- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][25]
- Storify[16]
- Swedish Civil Contingencies Agency[30]
- Swedish Government[30]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[31]
- Vox Media[32]
- Walgreens[14]
- *The Wall Street Journal*[22]
- Wikia[13]
- *Wired*[16]
- Wix.com[33]
- WWE Network[34]
- Xbox Live[35]
- Yammer[26]
- Yelp[14]
- Zillow[14]

Source: Wikipedia, 2016 Dyn Cyberattack

THE INTERNET WAS DESIGNED TO **SURVIVE** A NUCLEAR WAR, NOT TO BE FIGHTING IN ONE….

- SECURITY WAS ASSUMED
- ONLY GOOD GUYS WOULD (SHOULD) BE CONNECTED TO THE NETWORK (WHICH WAS FOR SECURE MILITARY USE)
- DARPA WAS JUST TRYING TO GET IT ALL TO WORK, NOT WORRIED ABOUT DEFENDING THE NETWORK ITSELF…

DEVICE ANUFACTURERS ARE RESPONSIBLE FOR THEIR OWN SECURITY, RIGHT?

- “The Internet model” assumes hosts (end devices) are responsible for all policy required to connect safely to the network
- Originally implemented in “Host Requirements” RFCs
- There has never been (and still is not) a security requirement (and that probably is not a good idea anyway…)

MOST IOT DEVICES ARE “EMBEDDED”

Very limited resources

- Hardware
  - Compute Power
  - Memory (RAM)
  - Code Size
  - Storage
  - Updateability
- Software
  - Stacks
  - OS

Often VERY small relatively

SECURITY USUALLY LAST PRIORITY FOR DEVICE MANUFACTURERS

- Ship 1st, then make secure later (*if* someone complains about it)
- Security/Pentesting often not in budget or dev plan
- Only rarely revisited after FCS

RESULT: **BILLIONS** OF INSECURE “ZOMBIE” DEVICES THAT WILL & CAN **NEVER** BE SECURE

WHAT KINDS OF IOT DEVICES ARE VULNERABLE?

- Routers
- NAS Storage
- Thermostats
- DVRs
- Set Top Boxes
- Tablet/Phones
- Home Hubs
- IP Cameras
- Light Bulbs
- Security Sys.
- Sprinklers
- Game Consoles

So really, pretty much anything that talks to the Internet at all…

CASE STUDY: NETGEAR, DECEMBER, 2016…

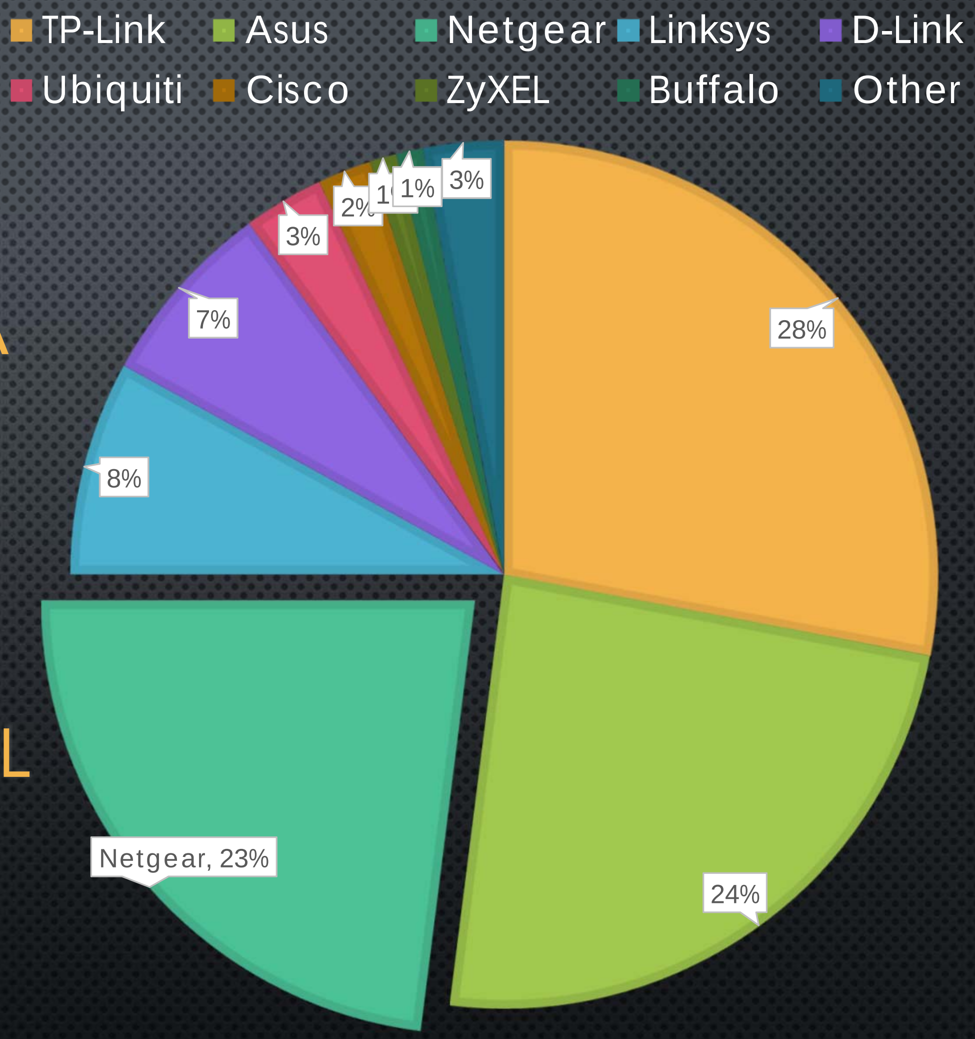
- Aug 25, 2016: Andrew Rollins (Acew0rm) notifies Netgear of trivially exploitable vulnerability
- After waiting more than three months, released details to CERT
- CERT releases advisory, basically saying “unplug these routers”

YEAH, RIGHHHT...

THIS MIGHT BE A BIG DEAL…

NETGEAR IS NEARLY A **QUARTER** OF ALL WIRELESS ROUTER SHIPMENTS.

TOP 3 ARE **75%** OF ALL WIRELESS ROUTERS



Q: HOW BAD IS IT, REALLY?

A: About as bad as it gets…

Most severe AND most easily exploitable class of vulnerability

- Allows Remote, Unauthenticated, attacker to Execute Arbitrary Commands with Root Privileges on the router
- How? Just get ANY user on the network to click a link!

HOW EASY IS IT?

```
http://<router_IP>/cgi-bin/;COMMAND
```

Affects 17 Netgear Routers: R6200, R6250, R6400, R6700, R6900, R7000, R7000P, R7100LG, R7300, R7500, R7800, R7900, R8000, R8500, R9000, D6220, D6400 (~6 added 12/19)

BUG ALLOWS FIXING ITSELF (IF YOU’RE FIRST. AND IF THE POWER DOESN’T GO OUT…)

```
http://<router_IP>/cgi-bin/;killall$IFS'httpd'
```

This uses the bug itself to kill the router’s web server, which is the heart of the vulnerability. Note: This is secure only until the next time router is restarted!

HOW LONG WOULD IT TAKE **YOU** TO REALIZE YOUR ROUTER* IS “PWNED” BY A BOTNET?

IF YOU’RE LIKE MOST PEOPLE, THE ANSWER IS NEARER “FOREVER” THAN ANY FINITE PERIOD OF TIME…

PEOPLE DON’T LOOK AT IOT DEVICES FOR HACKING THE SAME WAY THEY WOULD THEIR PC, OR EVEN PHONE…

*HOW ABOUT YOUR THERMOSTAT? OR YOUR SMART LIGHTBULBS? OR YOUR GARAGE DOOR OPENER, OR SPRINKLER SYSTEM?

FTC SUITS AGAINST ASUS, TRENDNET & D-LINK

- Leaning toward requiring OWASP compliance to avoid negligence
- OWASP.org: Open Web Application Security Project

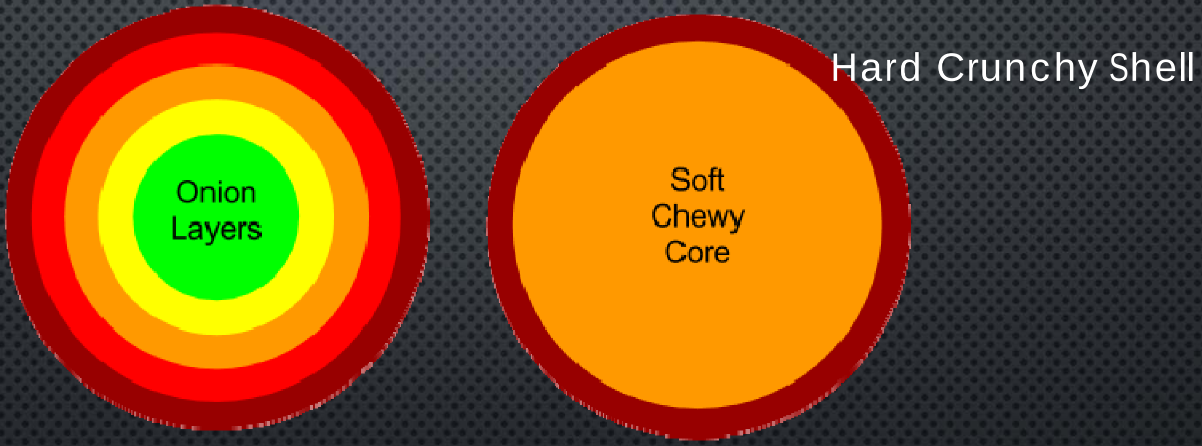
WHY IOT IS DIFFERENT

- Most security aimed at clients, not servers
- IoT devices are almost always inherently servers (web & API, usually)
- How do you configure, secure, authenticate, etc, in loose, undefined environment (about which you know nothing going in)?

HOW MANY COMPROMISED DEVICES DOES IT TAKE TO COMPROMISE YOUR NETWORK?

ONE. JUST ONE.

CONVENTIONAL SECURITY MODELS (DON'T WORK...)



WHY? BECAUSE WITH IOT, THEY'RE ALREADY INSIDE YOUR NETWORK…

SOME RELEVANT QUOTES & TAKEAWAYS

"You have zero privacy, anyway. Get over it."- Scott McNealy, 1999

"You may well have zero security anyway. Get over it."

"With IoT, the barbarians aren't at the gate, they're already inside it."

"Immigration without assimilation is invasion" – Bobby Jindal

"Firewalls won't save you anymore"

USUAL WAYS WON’T SAVE YOU ANYMORE

- A bad IoT botnet invasion is a bit like a Chlorine Triflouride fire:

“It is, of course, extremely toxic, but that’s the least of the problem. It is hypergolic (ignites on contact with) with every known fuel, and so rapidly hypergolic that no ignition delay has ever been measured. It is also hypergolic with such things as cloth, wood, and test engineers, not to mention asbestos, sand, and water - with which it reacts explosively.”

- from “Sand won’t save you this time” (http://bit.ly/2kANzh0)

THE ONLY POSSIBLE WAY OUT

- BUILD SECURITY STRATEGIES THAT (MAY USE, BUT) DO NOT RELY ON FIREWALLS
- ASSUME THE BAD GUYS ARE ALREADY INSIDE YOUR NETWORK
- ADAPTIVE TRAFFIC AND BEHAVIOR ANALYSIS MAY BE THE ONLY GOOD WAY TO CATCH THIS:
  - MONITOR TRAFFIC PATTERNS TO DETECT THREATS AND BAD BEHAVIOR BY ANY NODE OR GROUP OF NODES IN THE NETWORK
  - DEPLOY THESE FILTERS THROUGHOUT YOUR NETWORK (SECURITY MAY BE THE KILLER APP FOR SDN/NFV)

Distributed Behavioral Security Starting to Appear

Norton announced a new device at CES 2017 intended to help this problem

- Smart router monitors traffic and isolates nodes that have been compromised
- Great idea, with a fatal problem: $200 (OK) + $120/yr (no way)

DISTRIBUTED BEHAVIORAL SECURITY STARTING TO APPEAR

McAfee has announced that similar security software will be available not on its own hardware, but to run on Arris SURFboard Home Gateway Routers

(Also has subscription flaw…)

SWEET DREAMS…