

Securing Your Own Internet of Things

Best Practices To Protect Your Organization & Your Data

Justin Hall
Director, Security Services



/usr/bin/whoami

Twelve years with CBTS as security consultant to shops small (5 person) and large (Fortune 5)

GIAC Certified Penetration Tester, Incident Handler,
Forensic Analyst

BSidesCincinnati cofounder

Visit a store to check
out our **NEW**
connected home
devices!*



eero

Home Wi-Fi System
3-Pack Gigabit range extender

\$499.99

+ Free Amazon Echo

---*---

amazon echo

Hands-free voice control speaker

FREE with the purchase
of an eero 3-pack

Limited-time offers, available in-store only. Certain restrictions apply, while supplies last.
Limit 1 free Amazon Echo/eero offer per household. See store for details.

*Note: From our own advertisements!

1. Botnet compromised smart devices on campus network
2. Compromised devices begin to hammer DNS server with bogus lookups
3. College students lose internet connection, weep bitter tears





1. Attackers install malware on connected key management system
2. Attackers demand ransom, threatening to keep all doors locked
3. Hotel pays up, finances additional cybercrime

Internet of...

What things?

At work!

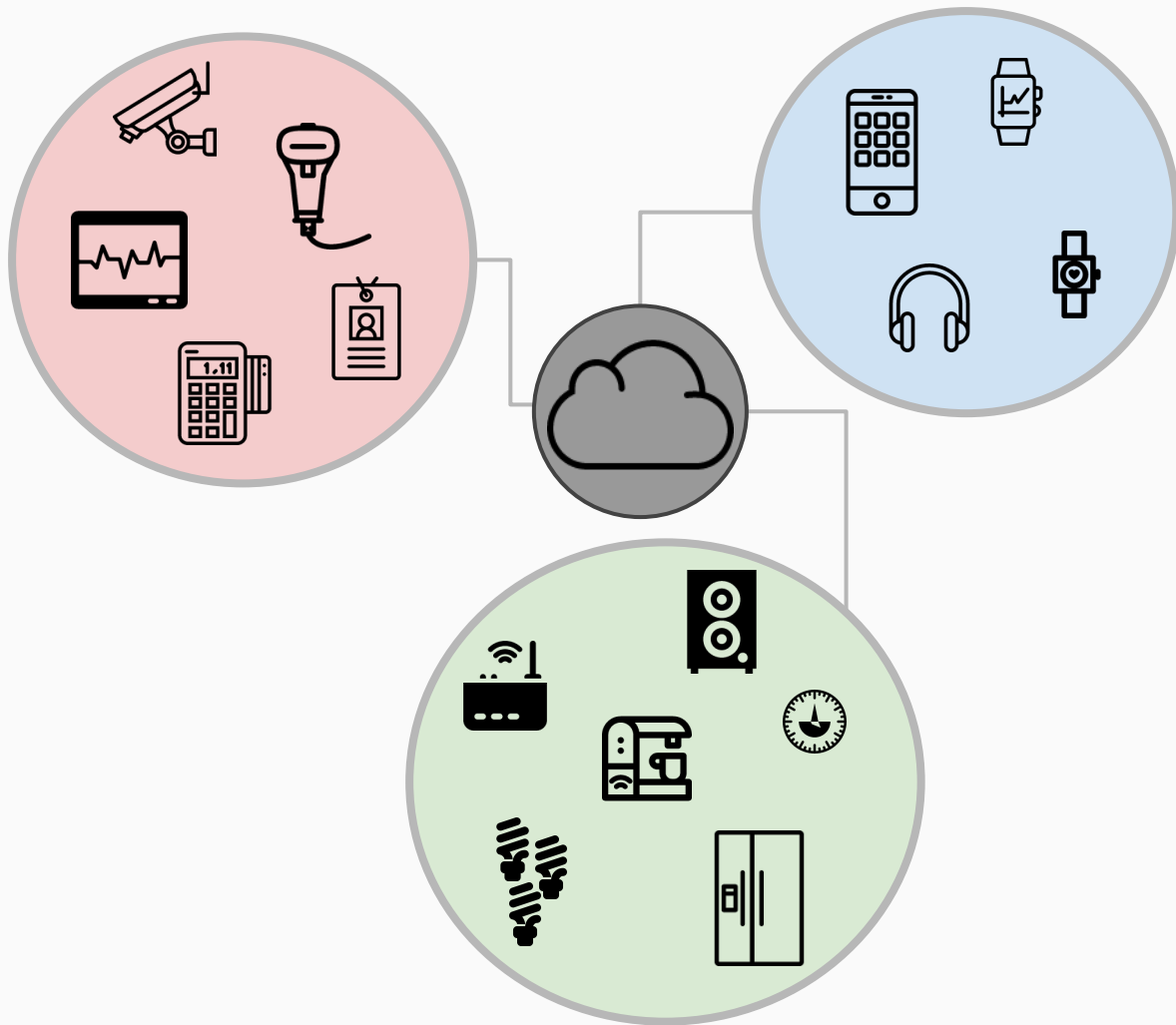
- CCTV cameras
- Barcode scanners
- Medical devices
- Credit card terminals
- Badge readers

At home!

- Appliances
- Light bulbs
- Media devices
- Routers, APs, ISP Modems

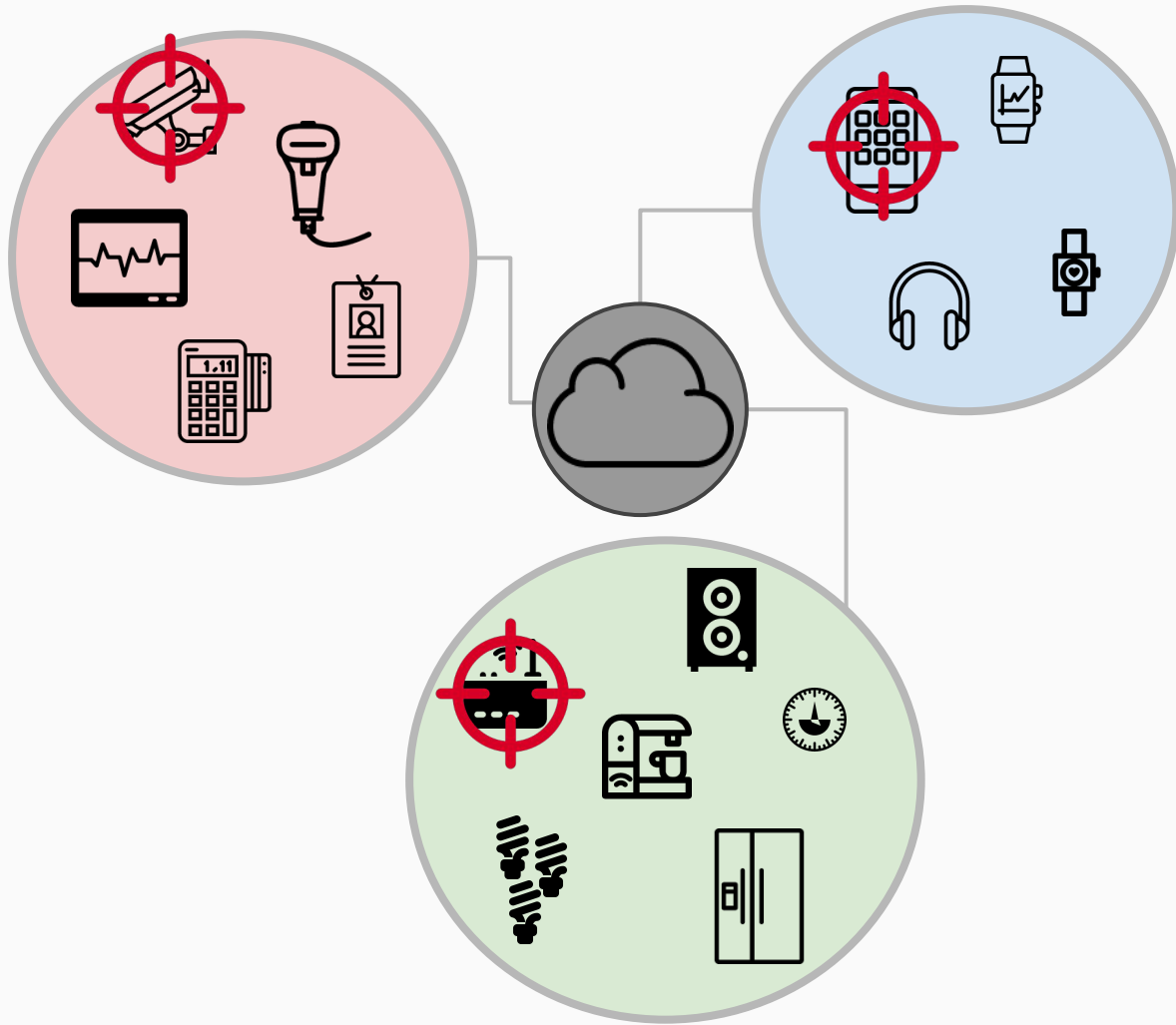
On us!

- Phones
- Smart watches
- Fitness trackers
- Audio devices



Smart Devices Become Targets

- Default vendor-assigned passwords
- Missing patches & out of date firmware
- Open ports & listening management services



What are they after?



Bandwidth



Access



Sensitive Data

1

Know what's in your
environment

1. Know what's in your environment

Complete asset inventory, including servers, workstations, network devices, mobile devices, smart devices

Periodic portscans - what ports should be/are open on assets?

Vulnerability scans - what needs to be patched & fixed?

The screenshot displays the Lansweeper network inventory application. The top navigation bar includes links for Dashboard, Assets, Reports, Licenses, Deployment, Configuration, and Community. The left sidebar lists various actions categorized into Asset options (New asset, Edit asset, Rescan Asset, Wake on Lan, Refresh Warranty, QR Code, Deploy Package), Basic actions (Ping, Pathping, Traceroute, NBTstat, HTTP, HTTPS, SSH (putty), Remote desktop, Open C\$, Open Admin\$, Computer management, Services management, Event viewer, Shared folders, Reboot, Shutdown, Abort shutdown), and Advanced actions (Device tester). The main content area shows details for a specific asset, CHI-DC01, which is a Microsoft Windows Server 2008 R2 Enterprise (x64) SP1. The asset's IP address is 172.16.30.200, and it belongs to the globomantics domain. The interface also displays the asset's scan status (Active), scan server (chi-win81), IP location (Local Sub), and asset location (Undefined). A table of recent eventlog entries is shown at the bottom, indicating no event log information scanned. The bottom status bar shows the time as 2:00.

Lansweeper
network inventory

Trial version **locked as 75 users**, Contact

Dashboard Assets Reports Licenses Deployment Configuration Community

Asset options

- New asset
- Edit asset
- Rescan Asset
- Wake on Lan
- Refresh Warranty
- QR Code
- Deploy Package

Basic actions

- Ping
- Pathping
- Traceroute
- NBTstat
- HTTP
- HTTPS
- SSH (putty)
- Remote desktop
- Open C\$
- Open Admin\$
- Computer management
- Services management
- Event viewer
- Shared folders
- Reboot
- Shutdown
- Abort shutdown

Advanced actions

- Device tester

CHI-DC01 GLOBOMANTICS.local - Microsoft Windows Server 2008 R2 Enterprise (x64) SP1
172.16.30.200 - globomantics

Summary **Config** **Software** **Event log** **Report** **History** **Deployment**

Asset Type: Windows
Last user: Jeff Hicks
OS: Microsoft Windows Server 2008 R2 Enterprise (x64) SP1
Manufacturer: Microsoft Corporation
Model: Virtual Machine
Memory: 1.0 GB
Processor: 1 * Intel Core i7-4500U CPU @ 1.80GHz
Domain: globomantics
OU: OU=Domain Controllers, DC=GLOBOMANTICS, DC=local
C: 0.9 GB free of 14.9 GB

Scan status: Active
Scan server: chi-win81
State: Active
IP Location: Local Sub
Asset location: Undefined
Serial: 8489-963
Uptime: 22 days 4
First seen: 24/03/201
Last seen: 24/03/201
Purchased: unknown
Warranty: unknown

Asset groups

- Default group

Anti-Virus

Name	Status	Virus Signature
No antivirus installed	Warning	

Recent eventlog entries
No event log information scanned

Event summary of
No event log information

Uptime calendar

2:00 4:00 6:00 8:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00

2

Harden authorized
smart devices

2. Harden authorized devices

Patch vulnerabilities

Change default passwords &
SNMP strings

Disable unnecessary services
(file transfer, management, shell,
etc)



3

Remove

unauthorized

devices

3. Remove unauthorized devices

Rogue wireless access points

IP cameras

Appliances

Audio/video streaming systems

Personal tablets, phones, laptops



4 Stay watchful

4. Stay watchful

Monitor your logs and network traffic for suspicious activity

Scan the environment monthly & use passive “scanning”

Have a third party perform a security assessment & penetration test



BSidesCincinnati 2017 - May 20

University of Cincinnati

Listen to excellent talks! Network! Learn! Beer! Food! Swag!

@bsidescincy / bsidescincy.org



Q&A

@justinhall
justin.hall@cbts.net


```
jwhall@albatross:~$ cat readme.nfo
```

A large, abstract, pixelated graphic resembling a barcode or a corrupted image, composed of vertical bars of varying heights and widths, rendered in a dark, textured style. The graphic is composed of many small, dark, rectangular blocks arranged in a way that suggests a digital or corrupted image. The overall effect is one of a heavily distorted or corrupted digital signal.

```

#####
n  Questions? Comments? Email justin.hall@cbts.net!!          n
#####
n  >>>RELEASE NOTES<<<                                       n
n  [Author]: Justin Hall           [Forum]: Central Ohio       n
n  [Release_Date]: 4/20/2017      Infosec Summit              n
#####
n  >>>GREETZ<<<                                               n
n  hamish ° joshv ° n8dogg ° lucky_lindy ° joe_the_kidd      n
n  old_man_tom ° m-ship ° c-wentz ° fortimatt                n
n  ratermaxx ° comp.sys.cbts.connect ° alt.fan.bsides.cincy   n
#####

```