Your Lightbulb Is Not Hacking You – Observation from a Honeypot Backed by Real Devices

Max Goncharov, Philippe Lin

2015/8/28-29

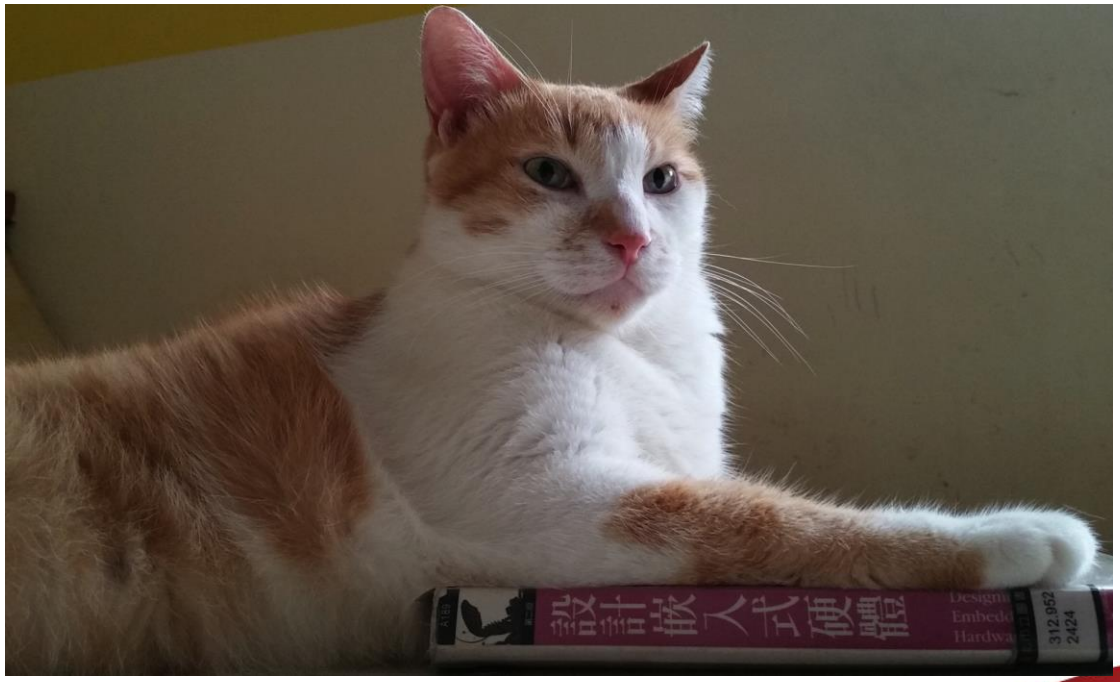
TREND MICRO™

Securing Your Journey to the Cloud

Hit-Point
“ねこあつめ”

$ whoami

- Philippe Lin
- Staff engineer, Trend Micro
- (x) Maker
  (o) Cat Feeder



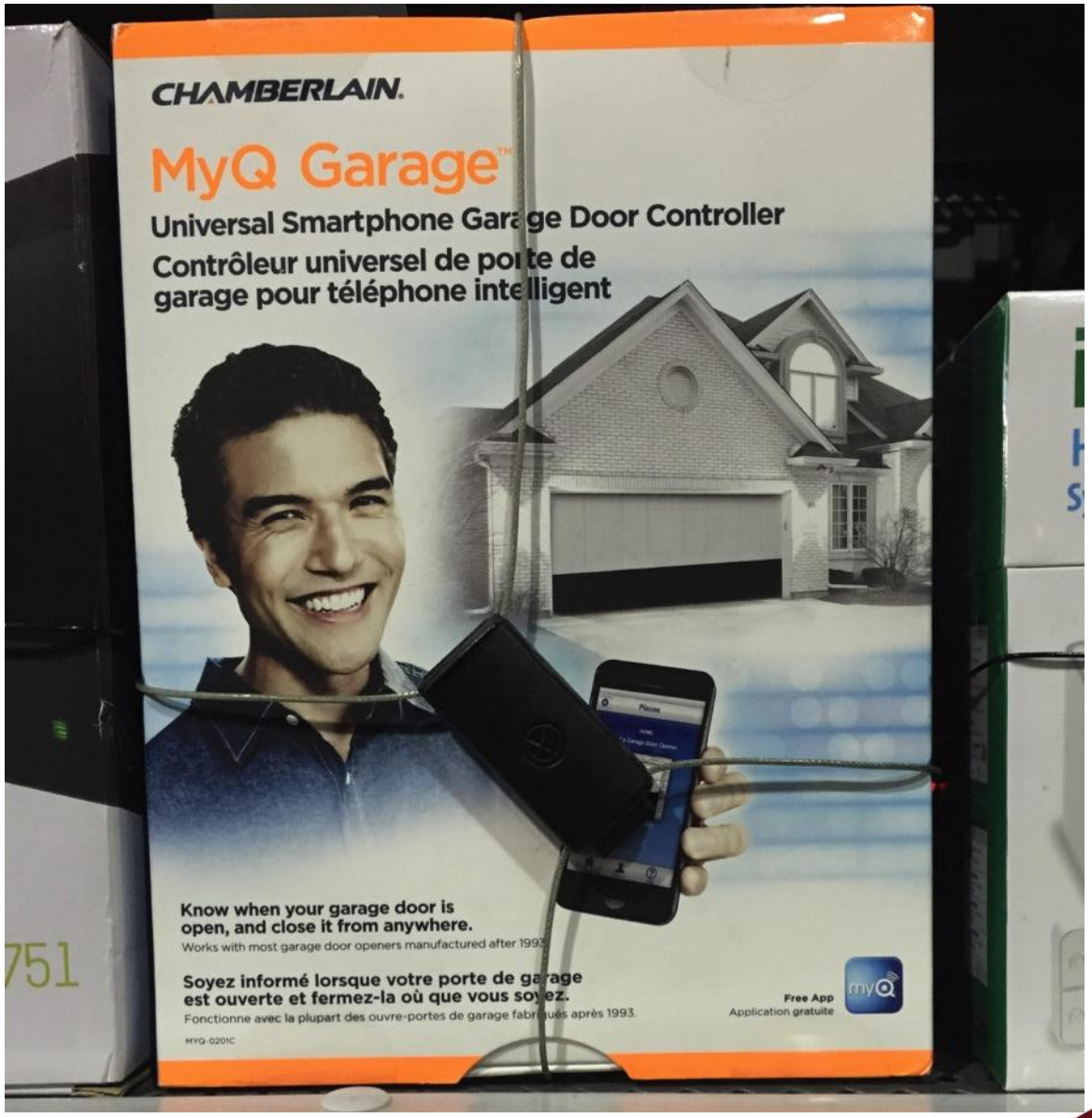
$ whoami

- Max Goncharov
- Senior Threat Researcher, Trend Micro
- (x) Evil Russian Hacker
  (o) Ethnical Russian Hacker

IoT Devices – Surveillance System

IoT Devices – Smart Alarm

IoT Devices – Garage Door Controller



IoT Devices – Philips hue / WeMo Switch

IoT Devices – Door Lock

IoT Devices – Thermostat

IoT Devices – Wireless HiFi & SmartTV

IoT Devices – Game Console

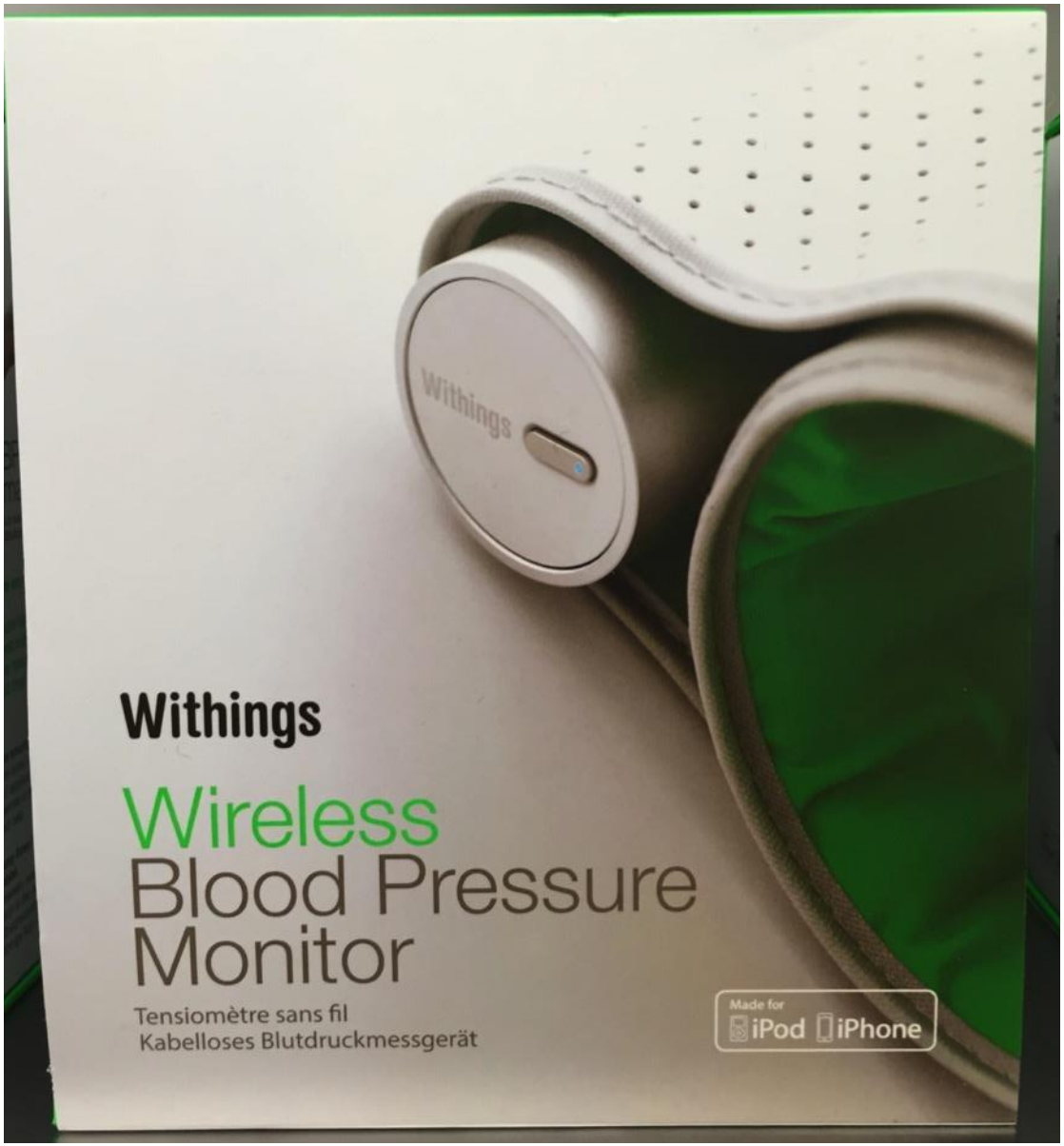
IoT Devices – Wireless HDD

IoT Devices – Blu-ray Player

IoT Devices – IPCam

IoT Devices – Kitchenware

IoT Devices – Personal Health Devices



Yes, IoT is hot and omnipresent …

developerWorks 日本語版 > テクニカル・トピックス > ビジネス・アナリティクス > 技術文書一覧 >

IBM IoT Foundation と IBM Bluemix を使用して独自のウェアラブル端末を作成する

Bluetooth 対応のウェアラブル端末キットをモバイル・アプリに接続して、センサー・データを IBM IoT Foundation クラウドに送信する

Credit: IBM, iThome and SmartThings.

How to Use Your Cat to Hack Your Neighbor's Wi-Fi

BY ANDY GREENBERG 08.08.14 | 6:30 AM | PERMALINK

Share 29.0k Tweet 3,480 +1 2,067 Share Pin it 98

teh collar. Gene Bransfield

Credit:
Apple Daily,
Weird,
net-core

19

TREND MICRO

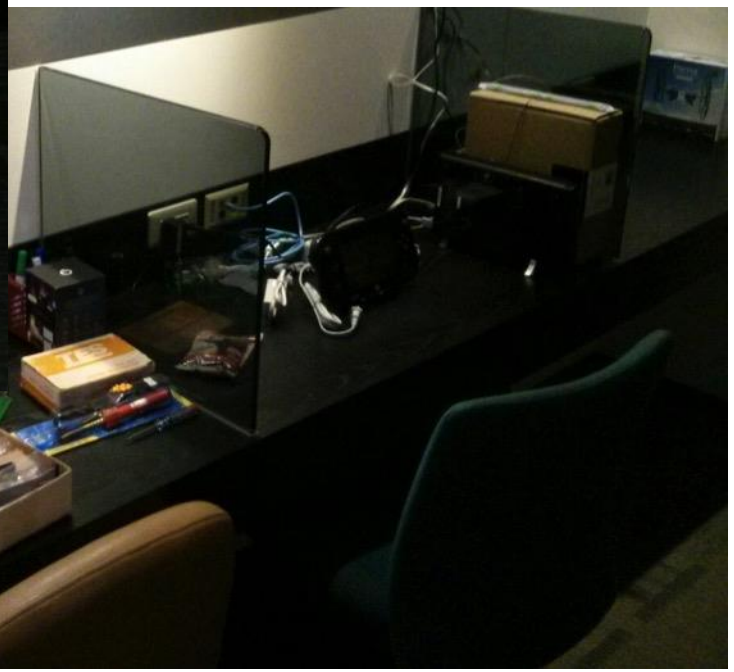
Credit: Tom Sachs (2009)

Methodology

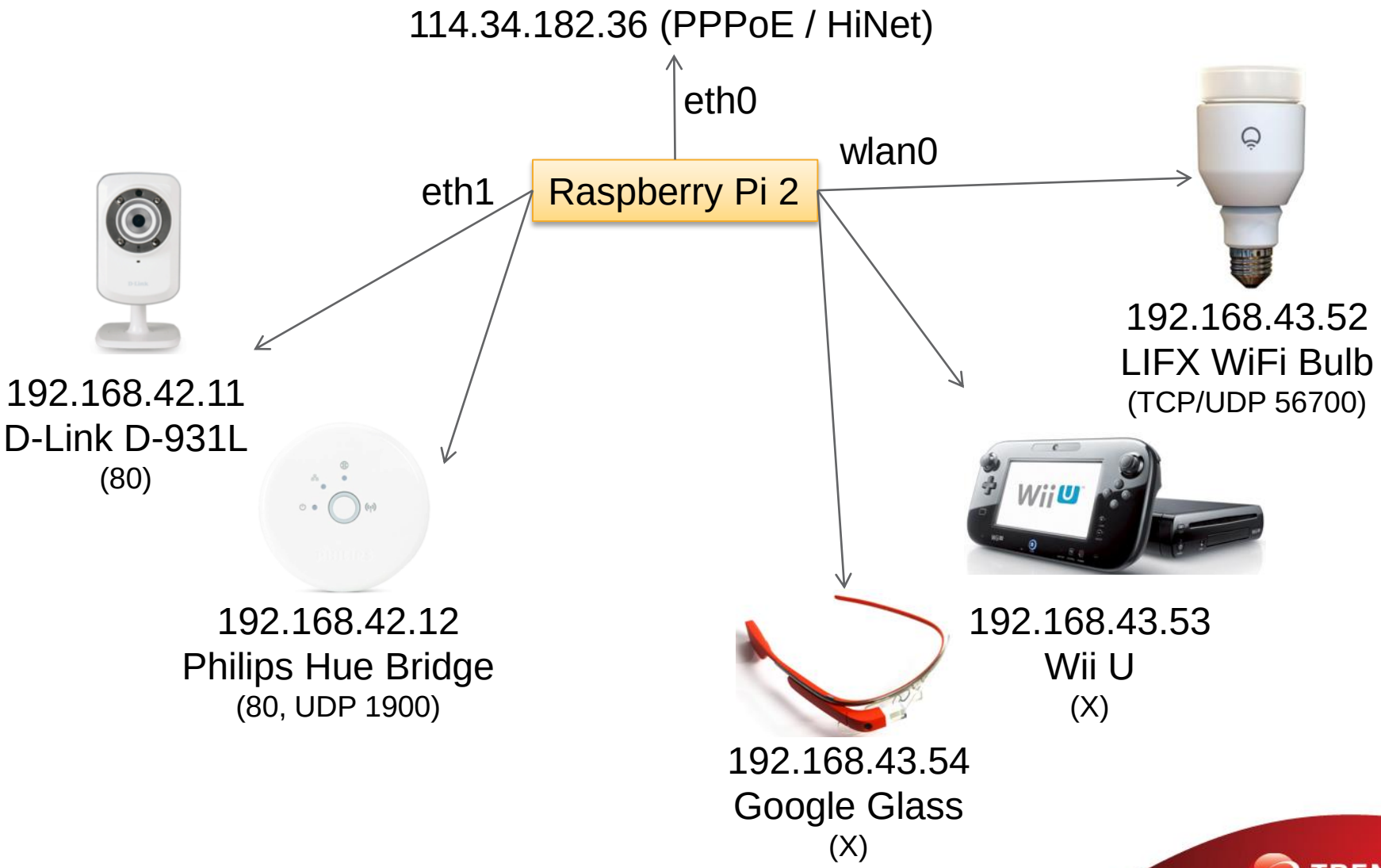
- Taipei from March 23 - July 23, 2015
- Munich from April 22 - June 22

- URL / credential randomly pushed on Shodan and Pastebin
- Faked identity, Avatar
  - Facebook
  - Dyndns
  - Skype
  - private documents in WDCloud

Taipei Lab

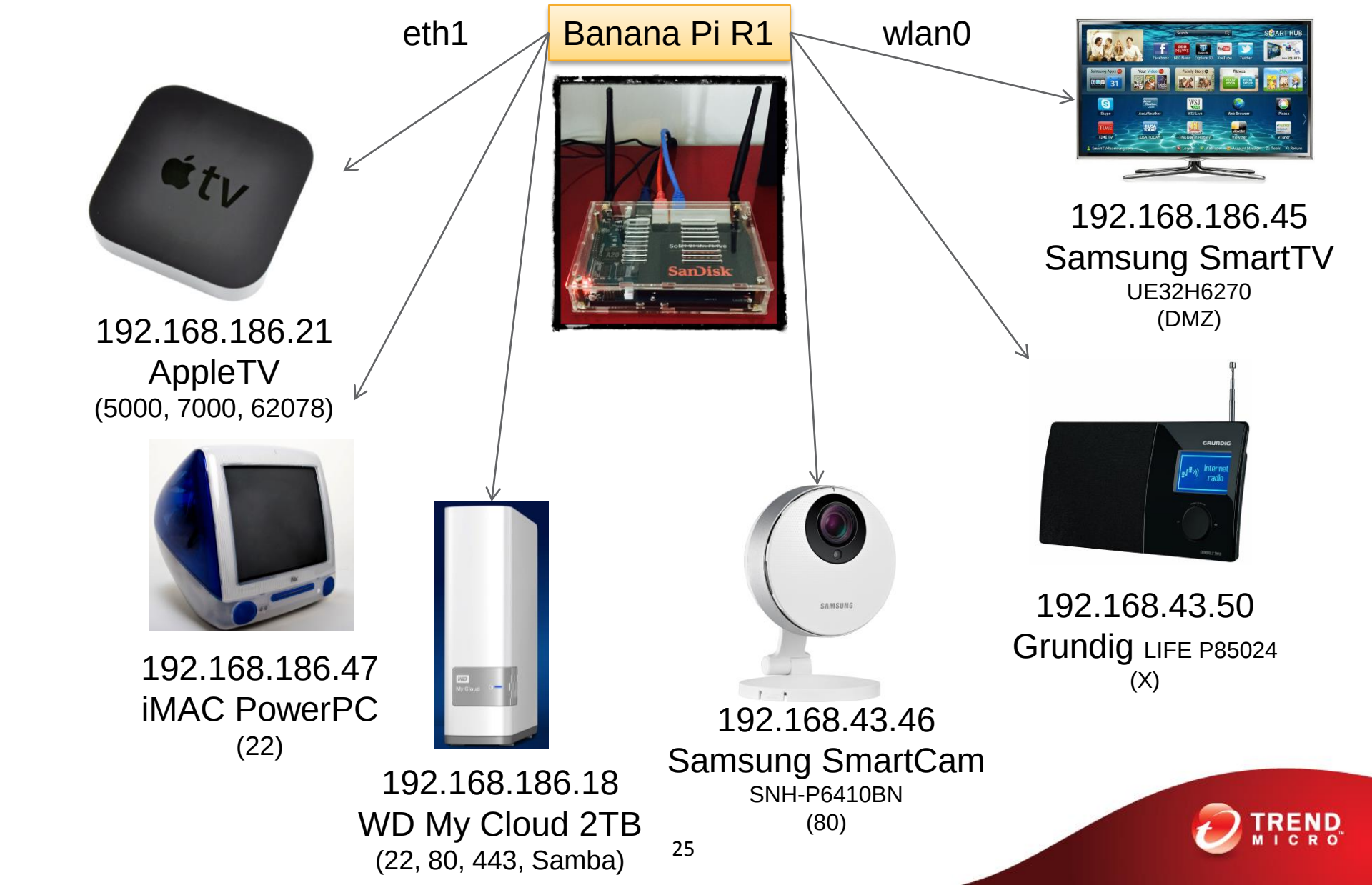


Block Diagram – Taipei Lab



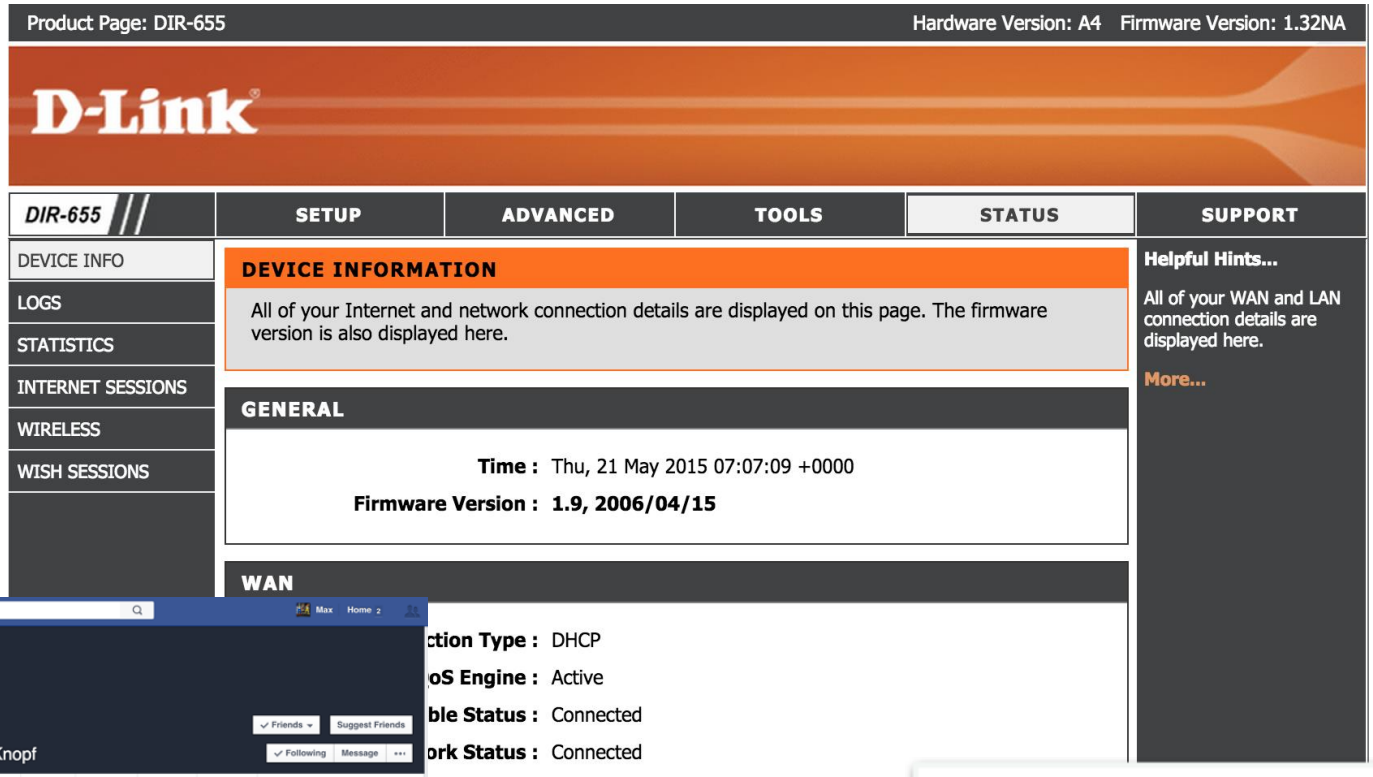
Munich Lab

Block Diagram – Munich Lab



Munich Lab: Fake D-Link DIR-655

http://tomknopf.homeip.net/



Why Backed by Real Devices?

- Shodan knows
- and so do hackers

114.34.182.36 114-34-182-36.HINET-IP.hinet.net

Country	Taiwan
Organization	CHTD, Chunghwa Telecom Co., Ltd.
ISP	CHTD, Chunghwa Telecom Co., Ltd.
Last Update	2015-06-14T09:56:42.442918
Hostnames	114-34-182-36.HINET-IP.hinet.net
ASN	AS3462

Ports

80 8080

Services

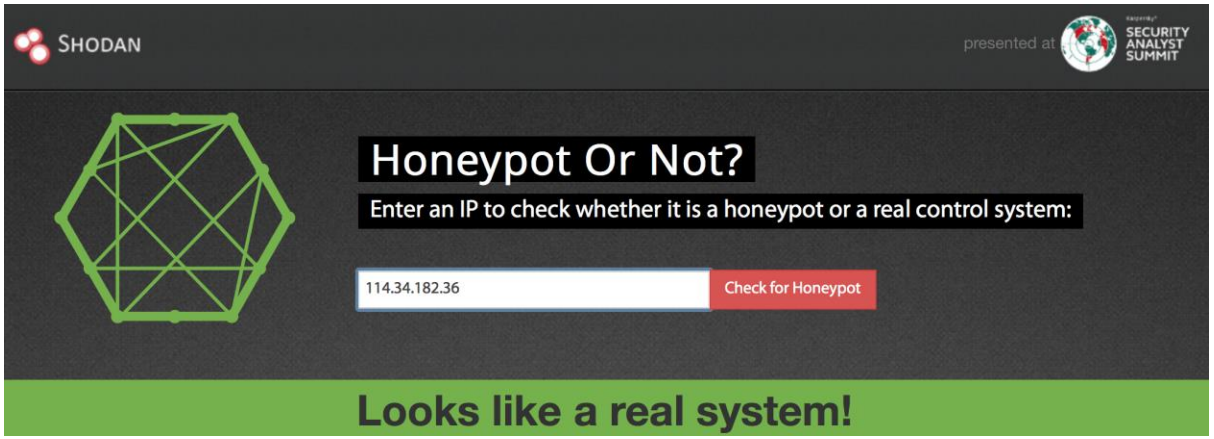
80 HTTP

```
HTTP/1.1 200 OK
Content-type: text/html
```

8080 HTTP (8080)

D-Link DCS-931L webcam http interface

```
HTTP/1.0 401 Authorization Required
Server: alphapd
Date: Mon Jun  8 23:11:41 2015
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html
WWW-Authenticate: Basic realm="DCS-931L"
```



Now, the lousy part ...

D-Link DCS-931L IPCAM

- No more “blank” password. Set to 123456.
- My D-Link cloud service
  - I failed to enable it. ☹
- Firmware 1.02 vulnerabilities
  - CVE 2015-2048 CSRF to hijack authentication
  - CVE 2015-2049 Unrestricted file upload to execute
- /video.cgi + admin:123456
- “Peeped” for Only two times. They went to port 8080 directly, without trying port 80.
- Maybe they used Shodan in advance.

D-Link DCS-931L IPCAM (2)

142.218.137.94.in-addr.arpa. 3600 IN PTR 94-137-218-142.pppoe.irknet.ru. With a browser

110.199.137.94.in-addr.arpa. 3600 IN PTR 94-137-199-110.pppoe.irknet.ru.

Jun 2, 2015 22:29:28.754491000 CST	94.137.218.142	8457	192.168.42.11	80	HTTP/1.1	GET	/aview.htm
Jun 2, 2015 22:29:32.464749000 CST	94.137.218.142	8458	192.168.42.11	80	HTTP/1.1	GET	/aview.htm
Jun 2, 2015 22:29:33.393077000 CST	94.137.218.142	8464	192.168.42.11	80	HTTP/1.1	GET	/dlink.css?cidx=1.022013-07-15
Jun 2, 2015 22:29:33.399200000 CST	94.137.218.142	8467	192.168.42.11	80	HTTP/1.1	GET	/security.gif
Jun 2, 2015 22:29:33.403489000 CST	94.137.218.142	8465	192.168.42.11	80	HTTP/1.1	GET	/devmodel.jpg?cidx=DCS-931L
Jun 2, 2015 22:29:33.410560000 CST	94.137.218.142	8463	192.168.42.11	80	HTTP/1.1	GET	/function.js?cidx=1.022013-07-15
Jun 2, 2015 22:29:33.411512000 CST	94.137.218.142	8466	192.168.42.11	80	HTTP/1.1	GET	/title.gif
Jun 2, 2015 22:29:35.241203000 CST	94.137.218.142	8471	192.168.42.11	80	HTTP/1.1	GET	/favicon.ico
Jun 2, 2015 22:29:35.474530000 CST	94.137.218.142	8474	192.168.42.11	80	HTTP/1.0	GET	/dgh264.raw
Jun 2, 2015 22:29:35.495830000 CST	94.137.218.142	8473	192.168.42.11	80	HTTP/1.0	GET	/dgaudio.cgi
Jun 2, 2015 22:29:36.470095000 CST	94.137.218.142	8475	192.168.42.11	80	HTTP/1.0	GET	/dgh264.raw
Jun 2, 2015 22:29:36.516931000 CST	94.137.218.142	8476	192.168.42.11	80	HTTP/1.0	GET	/dgaudio.cgi

Jun 7, 2015 21:23:43.888173000 CST 94.137.199.110 40454 192.168.42.11 80 HTTP/1.1 GET /video.cgi

```
GET     /cgi-bin/mft/wireless_mft?ap=testname;cat%20/var/www/secret.passwd
GET     /maker/snwrite.cgi?mac=1234;echo%20thisisatest
GET     /cgi_test.cgi?write_tan&;ls&ls%20-la
```

Got attack for TP-Link, but sorry it's a D-Link ...
(TP-Link Multiple Vuln, CVE-2013-2572, 2573)

Philips Hue

- Hacking Lightbulbs Hue (Dhanjani, 2013)
- MeetHue: Getting Started
- Port 30000 malicious takeover

Hourly traffic

- HTTP/1.0 POST /DcpRequestHandler/index.ashx Per bulb per hour
- HTTP/1.0 POST /DevicePortalICPRequestHandler/RequestHandler.ashx
- HTTP/1.1 POST /queue/getmessage?duration=180000&…

OTA Firmware update

- HTTP/1.0 GET /firmware/BSB001/1023599/firmware_rel_cc2530_encrypted_stm32_encrypted_01023599_0012.fw

Philips Hue (2)

- ZigBee
- Broadcast using UDP port 1900, SSDP

NOTIFY * HTTP/1.1

HOST: 239.255.255.250:1900

CACHE-CONTROL: max-age=100

LOCATION: http://192.168.42.12:80/description.xml

SERVER: FreeRTOS/6.0.5, UPnP/1.0, IpBridge/0.1

NTS: ssdp:alive

NT: upnp:rootdevice

USN: uuid:2f402f80-da50-11e1-9b23-0017881778fd::upnp:rootdevice

- API

curl -X PUT -d '{"on": true}'
http://114.34.182.36:80/api/newdeveloper/groups/0/action

Philips Hue (3)

- API user as in official tutorial
  curl -X PUT -d '{"on": true}'
  http://114.34.182.36:80/api/newdeveloper/groups/0/action
- No one has tried Philips Hue API, even we leaked API of newdeveloper on Pastebin.
- Three people visited its homepage, and no further actions.
- We forgot to forward port 30000 until June 18.
- For broadcasted UDP port 1900, we have set an iptables rule, but not sure if it's the right way.

LIFX

- Discovery protocol in UDP port 56700
- Controlling stream in TCP port 56700
- Official cloud API: http://developer.lifx.com/
- Current API: 2.0
  - Official cloud API: http://developer.lifx.com/
  - Official API 2.0 Doc: https://github.com/LIFX/lifx-protocol-docs
- Maintains a keep-alive connection to LIFX cloud API.
- Once get “turn on” from TCP, it broadcasts the message via UDP to local bulbs.

LIFX (2)

$ curl -k -u "ca8430430f954e1198daa6057a1f9f810d2fffeaa5d12acbcc21825e859ae5a6:" "https://api.lifx.com/v1beta1/lights/all”


```
{
   "id": "d073d5028d8e",
   "uuid": "026da25d-dbd7-4290-8437-09f61f1960cd",
   "label": "LIFX Bulb 028d8e",
   "connected": true,
   "power": "on",
   "color": {
     "hue": 159.45799954222935,
     "saturation": 0.0,
     "kelvin": 3000
   },
```

LIFX (3)

Turn on

```
2407 16:40:42.36… 146.148.44.137  192.168.43.52     TCP   123 0x364c (13… 56700→10740 [PSH, ACK] Seq=3571393060 Ack=830038859 Win=20368 …
2408 16:40:42.39… 192.168.43.52   192.168.43.255    UDP    80 0x0030 (48)  Source port: 56700  Destination port: 56700
2409 16:40:42.44… 192.168.43.52   146.148.44.137    TCP   123 0x0031 (49)  10740→56700 [PSH, ACK] Seq=830038859 Ack=3571393129 Win=1460 L…
2410 16:40:42.61… 146.148.44.137  192.168.43.52     TCP    54 0x364d (13… 56700→10740 [ACK] Seq=3571393129 Ack=830038928 Win=20368 Len=0
```

```
0000  ff ff ff ff ff ff d0 73  d5 02 8d 8e 08 00 45 00   .......s ......E.
0010  00 42 00 30 40 00 ff 11  a2 f6 c0 a8 2b 34 c0 a8   .B.0@... ....+4..
0020  2b ff dd 7c dd 7c 00 2e  8f ce 26 00 00 54 ee 58   +..|.|.. ..&..T.X
0030  bf 4e d0 73 d5 02 8d 8e  00 00 4c 49 46 58 56 32   .N.s.... ..LIFXV2
0040  00 01 84 a6 c8 89 41 2b  e8 13 76 00 00 00 00 00   ......A+ ..v.....
```

Turn off

```
2427 16:42:42.51… 146.148.44.137  192.168.43.52     TCP   123 0x3650 (13… 56700→10740 [PSH, ACK] Seq=3571393129 Ack=830039066
2428 16:42:42.54… 192.168.43.52   192.168.43.255    UDP    80 0x0038 (56)  Source port: 56700  Destination port: 56700
2429 16:42:42.59… 192.168.43.52   146.148.44.137    TCP   123 0x0039 (57)  10740→56700 [PSH, ACK] Seq=830039066 Ack=3571393198
2430 16:42:42.76… 146.148.44.137  192.168.43.52     TCP    54 0x3651 (13… 56700→10740 [ACK] Seq=3571393198 Ack=830039135 Win=2
```

```
0000  ff ff ff ff ff ff d0 73  d5 02 8d 8e 08 00 45 00   .......s ......E.
0010  00 42 00 38 40 00 ff 11  a2 ee c0 a8 2b 34 c0 a8   .B.8@... ....+4..
0020  2b ff dd 7c dd 7c 00 2e  ed 65 26 00 00 54 89 6c   +..|.|.. .e&..T.l
0030  c3 bf d0 73 d5 02 8d 8e  00 00 4c 49 46 58 56 32   ...s.... ..LIFXV2
0040  00 01 84 91 af 82 5d 2b  e8 13 76 00 00 00 ff ff   ......]+ ..v.....
```

LIFX (3)

2407 2139.812670 146.148.44.137 -> 192.168.43.52

TCP 123 56700 > 10740 [PSH, ACK] Seq=2419 Ack=2119 Win=20368 Len=69

2408 2139.846425 192.168.43.52 -> 192.168.43.255

UDP 80 Source port: 56700 Destination port: 56700

2409 2139.893891 192.168.43.52 -> 146.148.44.137

TCP 123 10740 > 56700 [PSH, ACK] Seq=2119 Ack=2488 Win=1460 Len=69

2410 2140.061866 146.148.44.137 -> 192.168.43.52

TCP 54 56700 > 10740 [ACK] Seq=2488 Ack=2188 Win=20368 Len=0

- No one has ever tried it.

Nintendo Wii U

- Quite safe
- No open port while standing by and playing
- Regular phone-home for OTA

HTTP/1.1 GET /pushmore/r/8298800e4375f7108b2bf823addaf70d

- So we decided to remove it from research
  - Euh, not really.
    We removed the device in July.

Google Broken (?) Glass

- A noisy source, but mostly /generate_204
- # nmap -sU 192.168.43.54 and it's disconnected from WiFi.
- A lot of opened ports: TCP 8873, TCP 44014, etc.
- Removed from research. Maybe next time.

WDCloud 2TB

- Lots of traffic, including ARP broadcasting, SSDP M-SEARCH, SSDP NOTIFY
- Mostly from embedded Twonky Media Server that pings iRadio, IPCam in LAN
- SSH, SMB, HTTP
- Beyond what you can expect from a NAS (?)

```
GET /api/1.0/rest/port_test?format=xml HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.6.0_18
Host: 82.135.81.156
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.1 200 OK
Date: Thu, 23 Apr 2015 09:51:36 GMT
Server: Apache
Vary: Accept-Encoding
X-Orion-Version: 2.5
Content-Length: 94
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/xml; charset=utf-8
Content-Language: en

<?xml version="1.0" encoding="utf-8"?>
<port_test>
  <deviceid>2208751</deviceid>
</port_test>
```

```
GET /api/1.0/rest/remote_access_status/2208751 HTTP/1.1
Host: 129.253.8.107
Accept: */*

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked
Date: Tue, 19 May 2015 07:42:06 GMT
Set-Cookie: BIGipServerorion_web_http_pool=2316569098.20480.0000; path=/

8b
<?xml version="1.0" encoding="utf-8"?>
<remote_access_status>
  <action>proceed</action>
  <wait_time></wait_time>
</remote_access_status>

0
```

WDCloud 2TB (2)

- Phones home

24 0.936172 192.168.186.18 -> 54.186.91.233 HTTP

GET /rest/nexus/onlineStatus?tsin=WD01 HTTP/1.1

341 12.629990 192.168.186.18 -> 54.186.91.233 HTTP

GET /rest/nexus/registerDevice?ip_internal=192.168.186.18 ...

5337 3302.850595 192.168.186.18 -> 54.68.185.97 HTTP

GET /rest/nexus/ipCheck HTTP/1.1

18195 780.084983 192.168.186.18 -> 129.253.55.203 HTTP

GET /nas/list.asp?devtype=sq&devfw=04.01.03-421&devlang=eng&devsn=&auto=1 HTTP/1.1

164167 1770.338099 192.168.186.18 -> 129.253.8.107 HTTP

GET /api/1.0/rest/remote_access_status/2208751 HTTP/1.1

WDCloud 2TB (3)

- Noisy Twonky Media Server

2584 32.926206 192.168.186.18 -> 192.168.186.46 HTTP
GET /rootDesc.xml HTTP/1.1

332562 3489.183064 192.168.186.18 -> 192.168.186.46 HTTP/XML
POST / HTTP/1.1

- IPCam returns 500 Internal Server Error when asked to DeletePortMapping, so WD bothers it every hour
- To iRadio (subscribed once)

38907 529.893728 192.168.186.18 -> 192.168.186.50 HTTP
GET /dd.xml HTTP/1.1

38924 529.978422 192.168.186.18 -> 192.168.186.50 HTTP
GET /AVTransport/scpd.xml HTTP/1.1

38956 530.107191 192.168.186.18 -> 192.168.186.50 HTTP
GET /ConnectionManager/scpd.xml HTTP/1.1

38970 530.187170 192.168.186.18 -> 192.168.186.50 HTTP
GET /RenderingControl/scpd.xml HTTP/1.1

WDCloud 2TB (4)

- Of course there are kiddie scans...

1176 373.536912 83.197.91.35 -> 192.168.186.18 HTTP
GET /cgi-bin/authLogin.cgi HTTP/1.0

1186 373.698023 83.197.91.35 -> 192.168.186.18 HTTP
GET /cgi-bin/index.cgi HTTP/1.0

- And SMB scans (why don't they list dirs first?)

8036 3452.474672 41.71.142.112 -> 192.168.186.18 SMB
Trans2 Request, GET_DFS_REFERRAL, File: \88.217.9.124\Video

8123 3477.168920 41.71.142.112 -> 192.168.186.18 SMB
Trans2 Request, GET_DFS_REFERRAL, File: \88.217.9.124\TimeMachineBackup

8174 3483.358429 41.71.142.112 -> 192.168.186.18 SMB
Trans2 Request, GET_DFS_REFERRAL, File: \88.217.9.124\SmartWare

8186 3485.339545 41.71.142.112 -> 192.168.186.18 SMB
Trans2 Request, GET_DFS_REFERRAL, File: \88.217.9.124\Public

WDCloud 2TB (5)

- Directly from WDC.Com (port_test and returns deviceID)

129317 3094.970315 129.253.8.24 -> 192.168.186.18 HTTP
GET /api/1.0/rest/port_test?format=xml HTTP/1.1

- Phones home (in HTTPS and we didn't MITM)

11159 123.071890 192.168.186.18 -> 129.253.8.107 TCP
57021→443 [ACK] Seq=1302534518 Ack=2477249199 Win=17424 Len=0

- Tons of people trying to guess SSH password

3307 1300.264326 205.185.102.90 -> 192.168.186.18 SSHv2
Client: Key Exchange Init

AppleTV

- Port 7000 from Mac
- iphone-sync port 62078
  "In a nutshell, a service named lockdownd sits and listens on the iPhone on port 62078. By connecting to this port and speaking the correct protocol, it's possible to spawn a number of different services on an iPhone or iPad." (http://www.zdziarski.com/blog/?p=2345)
- 360, Shodan, and unknown source from many countries scanned port 5000 (not open), 7000, 62078
- No other incoming connections
- Phone home (https://support.apple.com/ja-jp/HT202944)

17.130.254.28 TCP 54 0x9a8d (39565) 49416→443

17.130.254.23 TCP 54 0x9a8d (39565) 49416→5223 iCloud DAV service

AppleTV (2)

- 360 (from port 60000, are you China network scanner?)

5216 2529.232297 61.240.144.65 -> 192.168.186.21 TCP
60000→5000 [SYN] Seq=65854669 Win=1024 Len=0

- From Denmark, Netherland, Colocrossing (all from port 7678)

2444 1821.852847 91.224.160.18 -> 192.168.186.21 TCP
7678→5000 [SYN] Seq=1298173523 Win=8192 Len=0 MSS=1452 WS=256 SACK_PERM=1

8816 2941.786677 80.82.78.2 -> 192.168.186.21 TCP
7678→5000 [SYN] Seq=762579296 Win=16384 Len=0

10688 3272.477803 198.23.176.130 -> 192.168.186.21 TCP
7678→5000 [SYN] Seq=2114495098 Win=8192 Len=0 MSS=1452 WS=256 SACK_PERM=1

Samsung SmartTV

- Noisy outbound connection
- Shodan and others probe port 22, 80, 443
  - https://securityledger.com/2012/12/security-hole-in-samsung-smart-tvs-could-allow-remote-spying/
  - http://thehackernews.com/2015/02/smart-tv-spying.html
- Many incoming connections to port 34363, but the content is encrypted
  - Talk
  - Naver
  - AuthSMG
  - NRDP32
  - …

```
HTTP/1.1 200 OK
x-amz-id-2: XxpRRX3K1NHKNO+WpWd/ln8cfIqViOKpwg3J2zrSKJK/bu9njTCYDNFfHbpuqodc
x-amz-request-id: 4601D99BE6756CDD
Date: Tue, 21 Apr 2015 09:33:02 GMT
Last-Modified: Tue, 07 Apr 2015 04:20:38 GMT
ETag: "1439f6cb2fee234ef1b0adba8386ea78"
Accept-Ranges: bytes
Content-Type: text/xml
Content-Length: 5541
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<emplist>
<file id="empWLibPlugin" version="2.001" name="X12_2.000_empWLibPlugin_VER_2.001.zip" url="http://
oempprd.samsungcloudsolution.net/emp/emp/X12_2.000_empWLibPlugin_VER_2.001.zip" size="986650"
type="zip" protocol="https" boot="yes"><signature /></file>
<file id="empTalk" version="2.424" name="X12_2.000_empTalk_VER_2.424.zip" url="http://
oempprd.samsungcloudsolution.net/emp/emp/X12_2.000_empTalk_VER_2.424.zip" size="866272" type="zip"
protocol="https" boot="yes"><signature /></file>
<file id="empNaver" version="1.008" name="X12_2.000_empNaver_VER_1.008.zip" url="http://
oempprd.samsungcloudsolution.net/emp/emp/X12_2.000_empNaver_VER_1.008.zip" size="48236" type="zip"
protocol="https" boot="yes"><signature /></file>
<file id="empAuthSMG" version="0.300" name="X12_2.000_empAuthSMG_VER_0.300.zip" url="http://
oempprd.samsungcloudsolution.net/emp/emp/X12_2.000_empAuthSMG_VER_0.300.zip" size="766073" type="zip"
protocol="https" boot="yes"><signature /></file>
<file id="empNRDP32" version="1.031" name="X12_2.000_empNRDP32_VER_1.031.zip" url="http://
oempprd.samsungcloudsolution.net/emp/emp/X12_2.000_empNRDP32_VER_1.031.zip" size="3364291" type="zip"
protocol="https" boot="yes"><signature /></file>
<file id="empSignature" version="1.300" name="X12_2.000_empSignature_VER_1.300.zip" url="http://
oempprd.samsungcloudsolution.net/emp/emp/X12_2.000_empSignature_VER_1.300.zip" size="405886"
type="zip" protocol="https" boot="yes"><signature /></file>
```

Samsung SmartTV (2)

- Normal outbound

2787 174.504888 192.168.186.45 -> 23.57.87.46 HTTP
GET /global/products/tv/infolink/us.xml HTTP/1.1

2827 174.670619 192.168.186.45 -> 137.116.197.29 HTTP
GET /openapi/timesync?client=TimeAgent/1.0 HTTP/1.1

4693 2578.933492 192.168.186.45 -> 137.116.197.29 HTTP
GET
/openapi/zipcode/timezoneoffset?cc=DE&zip=85399&client=TimeAgent/1.0
HTTP/1.1

- https://infolink.pavv.co.kr/
- https://rmfix.samsungcloudsolution.net/
- http://noticeprd.trafficmanager.net/notice/config?svc_id=HOME&country_code=DE&lang=en
- rd.mch.us1.samsungadhub.com

Samsung SmartTV (3)

28440 1149.846158 213.61.179.34 -> 192.168.186.45 HTTP GET / HTTP/1.1

3375 1090.844205 80.68.93.65 -> 192.168.186.45 HTTP GET / HTTP/1.1

6374 2108.239633 188.138.89.16 -> 192.168.186.45 HTTP GET / HTTP/1.1

- netclue.de scans

27331 1000.731556 31.15.66.15 -> 192.168.186.45 TCP 46277→7676 [SYN]

27335 1000.807136 31.15.66.15 -> 192.168.186.45 TCP 36978→4443 [SYN]

27362 1002.788254 31.15.66.15 -> 192.168.186.45 TCP 33607→443 [SYN]

27366 1003.109546 31.15.66.15 -> 192.168.186.45 TCP 55482→6000 [SYN]

27370 1003.135391 31.15.66.15 -> 192.168.186.45 TCP 51068→80 [SYN]

Samsung SmartTV (4)

- Weird incoming TCP 34363

18074 469.608644 99.237.147.66 -> 192.168.186.45 50778→34363 [SYN]
Seq=2262400578 Win=8192 Len=0 MSS=1452 WS=256 SACK_PERM=1

```
0000032D  8f 4d ed 42 c5 b7 df 7d  22 22 94 e9 e9 1b 3b 6a .M.B...} ""....;j
0000033D  79 32 6f cc 81 79 10 2a  50 d7 52 3d 71 4b a1 05 y2o..y.* P.R=qK..
0000034D  f5 61 d2 91 29 0a 01 d2  d9 e2 5c f9 6c 54 5e f1 .a..)... ..\.lT^.
0000035D  cf 98 ef 03 a6 cf ac 20  5c 5f 9e ca c5 9d 57 48 ....... \_....WH
    00000360  85 77 02 20 f7 c4 4d 15  fc da 57 f0 05 23 be a8 .w. ..M. ..W..#..
    00000370  34                                            4
0000036D  3f d4 02 e4 1f 69 a8 d7  f2 11 e7 4e 80 ec 91 d9 ?....i.. ...N....
0000037D  82 7d 2c ff 47 14 24 ed  7c c7 56 5b bf 19 90 22 .},.G.$. |.V[..."
0000038D  9f ac 3e 80 18 12 bb c9  10 e4                  ..>..... ..
    00000371  85 d9 02 b9 e6 6e 08 03  71 fc fc f8 a6 33 63 8a .....n.. q....3c.
    00000381  c9 94 c3 07 49                                  ....I
00000397  40 1d 02 8b f3 d8 21 16  ce 95 b3 91 d9 22 83 06 @.....!. ....."..
000003A7  a7 f3 5a 6e 65 df 80 58  23 ef bd 62 8d 02 1b 20 ..Zne..X #..b...
000003B7  71 91 ff 1e d1 95 c4 f2  bb 48 f6 ac 9e 11 80 cd q....... .H......
000003C7  53 3a 5a ed 40 d6 de 42  e6 02 5a b0 d9 00 16 0c S:Z.@..B ..Z.....
000003D7  3c f3 ab 3e 0f 1e 22 05  f1 0b f9 7d 1f 56 df 93 <..>.". ...}.V..
000003E7  91 be 25 c1 20 92 5b fa  58 31 19 bb 05 53 b6 09 ..%. .[. X1...S..
000003F7  fd 65 9c 5a 1b db ad fe  8c c2 bf cc 2b 27 28 0f .e.Z.... ....+'(.
00000407  94 f0 6b 1a 4e 0b e2 d2  b6 36 31 3f ad c2 8f 4e ..k.N... .61?...N
00000417  89 70 7f df c2 86 8a 4e  69 63 e1 04 1e c0 16 c7 .p.....N ic......
00000427  89 12 e4 99 68 3b 2f 56  ea 2c 17 d5 33 e3 68 05 ....h;/V .,..3.h.
00000437  39 cd cc 8f 4b f7 91 63  1f ed 80 4f 14 e2 30 5d 9...K..c ...O..0]
00000447  d4 db 7c 70 10 ce 55 15  28 77 ff 34 3f bf f5 77 ..|p..U. (w.4?..w
```

TREND MICRO

Samsung SmartCam

- 2013-3964 URI XSS Vulnerability
- Samsung Electronics default password
  root/root
  admin/4321
- Only script kiddies, no one even tried root/root

Samsung SmartCam (2)

- Brainless scanning like

9103 2881.778773 183.60.48.25 -> 192.168.186.46 HTTP
GET http://www.baidu.com/ HTTP/1.1

2086 1310.725002 50.16.184.158 -> 192.168.186.46 HTTP
GET /languages/flags/ptt_bbrr.gif HTTP/1.1

4792 1376.142669 88.217.137.70 -> 192.168.186.46 HTTP
GET /jmx-console HTTP/1.1

- Named probes

1442 925.665117 212.34.129.217 -> 192.168.186.46 HTTP
GET /w00tw00t.at.ISC.SANS.DFind:) HTTP/1.1

iMac

- Open ports: SSH
- Several fake documents with personal identities
- Traffic to Apple: upgrades, Apple store
- Port 22 is probed nearly everyday …
  - April 24, port 22 probed by 222.184.24.6 (CN)
  - April 25, port 22 probed by 80.138.250.177 (DE)
  - April 28, 222.186.42.171 (Jiangsu, CN) tried to login, played around for 11.5 mins
  - April 29, probed by Shodan :)
  - May 16, 45.34.102.240 tried to brute force SSH.
  - May 20, 223.94.94.117 tried to brute force SSH.

iMac (2)

```
Host: www.apple.com

HTTP/1.1 200 OK
Last-Modified: Thu, 18 May 2006 21:51:56 GMT
nnCoection: close
ntCoent-Length: 4
Content-Type: text/plain; charset=UTF-8
Cache-Control: max-age=99
Expires: Tue, 21 Apr 2015 19:19:23 GMT
Date: Tue, 21 Apr 2015 19:17:44 GMT
Content-Length: 4
Connection: close
Server: Apache
```

```
b3DQEHAaCAJIAEOi
TnY9yhcFfWh/
iG9w0BAQUFADBgMQswCQYDVQQGEwJVUzEdMBsGA1UEChMUQXBwb
GA1UEAxMVRGFzaGJvYXJkIEFkdmlzb3J5IENBMB4XDTA2MDUxNz
BgNVBAoTFEFwcGxlIENvbXB1dGVyLCBJbmMuMRIwEAYDVQQLEwl
SIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANJkOc7PdgTr
ju+Ckq0/p
KjtKvYEs2NSf8+LK
+S8tOTO0ng8jfPmcTDpiTVFh3rmukoypZJ722iBXJS5MOjXwGeMd8eib3mbPrHi4kFhQzuG48d7f7LrPdQ
+mIfMk69yAymGtyQf7Uubi8wXGgKxUBXkS3EE8l8Pd6mybz5Yz/42RPfEG2FrinaggJE/TaW4Kb9Di5S4jt/j8csA+6YYMR7GxGuC/hoo
+gHimG+kD1UCAwEAAaN6MHgwDgYDVR0PAQH/BAQDAgeAMA8GA1UdEwEB/
wQFMAMCAQAwFQYDVR0lBA4wDAYKKoZIhvdjZAQBBDAdBgNVHQ4EFgQUlxwKOog1HQ1DbOELsmm3KEMOVuYwHwYDVR0jBBgwFoAUSr8UjJ
UmkWRrNzinPFKtr9B5FN4wDQYJKoZIhvcNAQEFBQADggEBAHOofvRSyOEIXgYsaWZDIBFdV61hZ3CTkdTD9rq6DnECW/gwhTcLZHuAG/
MfWJeake+jKUGPTNnVIcRczCqOXoqlLgoKwAzzg+DOqsa5UpEqvL3lrhELbBcj+c0cg1Pbng4w+VIpQgE0t29umqV4TXH/
jkBygQrl0IsQoDKsW1HxAAMjrm1xF7Z6RYXpIi5QNw26768puZu+BUWj12vE89Z5GqXigvnet
+M83jgiRvBYMQrlDnuITZ3ZPtlKowIqGvqYMJ4gUXJR//1Pd/oMKJv0GHQZtm6E4KXxpbpqZytNV2S1xxYvzjvsd
+Txe04GzSZPMDvZ8JtcZPuG6pmyaLYxggGMMIIBiAIBATBlMGAxCzAJBgNVBAYTAlVTMR0wGwYDVQQKExRBcHBsZSBDb21wdXRlciwgSW
5jLjESMBAGA1UECxMJRGFzaGJvYXJkMR4wHAYDVQQDExVEYXNoYm9hcmQgQWR2aXNvcnkgQ0ECAQIwCQYFKw4DAhoFADANBgkqhkiG9w0
BAQEFAASCAQCwtBTzu2nqG44g13ihSNGgyYVhDdIknwGCkJeGR1brO8X/TQskasXeqLsUFjtMtZyDKcFiMPq7BCfaM/
SkwCi8lCmCrYxQVccBIQt19sHpQFj/+u2C0KI7603jgbOCN8rgvojmvCPVYkc13/
bM5vwl7Oxtu5fgnmCqwSk5lkZJl4AJT0Ju9kBXY7dnRGgb5mCkCJCdU5CW5FQ4wlguARLmir6wR3f8n6xRTyYru2OlJJZwEr0ayqrEKBH
gXY3+BYcpN+P3MPmpCoS83vNcYzItHbNmh9v6Ln7uUR3H2l5lFshqK2p3pgqXBYBTmv03uAp2L2pF0J6MdBirohWiqq31AAAAAAAA
----- END SIGNATURE -----
BEGIN;
INSERT OR REPLACE INTO meta VALUES ('serial-number', 1);
COMMIT;
```

iRadio

- No open ports, so just a decoration
- Gets token from Grundig
- Listens to MPG streaming audio
- Pinged by WDCloud Twonky for UPnP AV DCP
  https://technet.microsoft.com/zh-tw/ms890335
- Many zero-lengthed packet to rfe2b-r1.alldigital.net on April 30.
- Otherwise it's very quiet.

19227 179.258446 192.168.186.50 -> 162.249.57.151 TCP
50044→8000 [RST, ACK] Seq=7037960 Ack=2828210800
Win=16384 Len=0

Attacks?

- Mostly script kiddies
- Not hacked (so far)
- Only one guy peeped D-Link IPCam, once in 4 months

Attacks – Script Kiddies (list)

1. vtigercrm attack (target: Vtiger)
2. Finding Proxy (mostly from China)
3. Linksys (E Series) Router Vulnerability
4. Tomcat manager exploit (CVE-2009-3843)
5. Morpheus Scans
6. Apache Struts (?)
7. Shellshock (?)
8. OpenCart
9. PHPMyAdmin
10. Interesting Romanian Anti-sec ☺
11. Muieblackcat
12. Redhat Jboss
13. FastHTTPAuthScanner200test From Wuhan, Hubei Province, China

Attacks – Script Kiddies (1)

vtigercrm attack (target: Vtiger)

- Mar 12, 2015 15:06:32.614481000 CST 217.160.180.27 51048 HTTP/1.1 GET /vtigercrm/test/upload/vtigercrm.txt
- Mar 12, 2015 19:28:40.635673000 CST 177.69.137.97 36571 HTTP/1.1 GET //vtigercrm/matrix.php?act=f&f=sip_additional.conf&d=%2Fetc%2Fasterisk

Attacks – Script Kiddies (2)

Finding Proxy (mostly from China)

- Mar 12, 2015 17:25:11.681911000
  CST 222.186.128.52 3125 HTTP/1.1 GET http://www.baidu.com/
- Mar 13, 2015 00:00:01.669619000
  CST 61.157.96.80 43134 HTTP/1.1 GET http://www.so.com/?rands=_6
  820349128203886981513 6

Attacks – Script Kiddies (3)

Linksys Router Vulnerability

For E Series Router

- Mar 13, 2015 08:59:41.790785000
  CST 149.129.49.120 35675 HTTP/1.1 GET /tmUnblock.cgi

For older Linksys

- Mar 18, 2015 23:02:11.820423000
  CST 114.216.84.142 1998 HTTP/1.1 GET /HNAP1/
- Mar 19, 2015 00:43:37.161583000
  CST 62.24.91.163 49246 HTTP/1.1 GET /HNAP1/

Attacks – Script Kiddies (4)

Tomcat manager exploit (CVE-2009-3843)

- Mar 14, 2015 12:28:48.344370000
  CST 119.167.227.55 4308 HTTP/1.1 GET /manager/html
- Mar 21, 2015 05:57:23.279693000
  CST 61.160.211.56 2948 HTTP/1.1 GET /manager/html

Attacks – Script Kiddies (5)

Morpheus Scans

- Mar 15, 2015 04:08:36.934818000
  CST 118.98.104.21 59420 HTTP/1.1 GET /user/soapCaller.bs

Attacks – Script Kiddies (6)

Apache Struts (?)

- Mar 22, 2015 19:10:24.120794000 CST 115.230.127.188 3657 HTTP/1.1 POST /login.action

Attacks – Script Kiddies (7)

Shellshock (?)

- Mar 22, 2015 21:45:15.510522000
  CST 218.91.204.30 1466 HTTP/1.1 POST /cgi-bin/wlogin.cgi

Attacks – Script Kiddies (8)

OpenCart

- Mar 27, 2015 00:32:11.438060000 CST 209.236.125.108 38783 HTTP/1.1 GET /admin/config.php

Attacks – Script Kiddies (9)

PHPMyAdmin

- Mar 29, 2015 11:08:15.980407000
  CST 115.193.234.32 64256 HTTP/1.1 GET /pma/scripts/setup.php

Attacks – Script Kiddies (10)

Interesting Romanian Anti-sec ☺

- Mar 18, 2015 01:35:15.161683000 CST 188.214.58.140 42259 HTTP/1.1 GET /w00tw00t.at.blackhats.romanian.anti-sec:)
- Mar 18, 2015 01:35:16.030473000 CST 188.214.58.140 42324 HTTP/1.1 GET /phpMyAdmin/scripts/setup.php
- Mar 18, 2015 01:35:16.751057000 CST 188.214.58.140 42381 HTTP/1.1 GET /phpmyadmin/scripts/setup.php
- Mar 18, 2015 01:35:17.617702000 CST 188.214.58.140 42433 HTTP/1.1 GET /pma/scripts/setup.php
- Mar 18, 2015 01:35:18.325491000 CST 188.214.58.140 42495 HTTP/1.1 GET /myadmin/scripts/setup.php
- Mar 18, 2015 01:35:19.152408000 CST 188.214.58.140 42546 HTTP/1.1 GET /MyAdmin/scripts/setup.php

Attacks – Script Kiddies (11)

Muieblackcat

- Mar 27, 2015 07:03:33.244268000 CST 69.197.148.87 44151 HTTP/1.1 GET /muieblackcat
- Mar 27, 2015 07:03:33.595012000 CST 69.197.148.87 44311 HTTP/1.1 GET //phpMyAdmin/scripts/setup.php
- Mar 27, 2015 07:03:33.948931000 CST 69.197.148.87 44477 HTTP/1.1 GET //phpmyadmin/scripts/setup.php
- Mar 27, 2015 07:03:34.308116000 CST 69.197.148.87 44646 HTTP/1.1 GET //pma/scripts/setup.php
- Mar 27, 2015 07:03:34.709562000 CST 69.197.148.87 44812 HTTP/1.1 GET //myadmin/scripts/setup.php
- Mar 27, 2015 07:03:35.072852000 CST 69.197.148.87 44994 HTTP/1.1 GET //MyAdmin/scripts/setup.php

Attacks – Script Kiddies (12)

Redhat Jboss

- Apr 2, 2015 20:15:17.478626000 CST 23.21.156.5 48188 HTTP/1.0 GET /jmx-console/

Attacks – Script Kiddies (13-1)

FastHTTPAuthScanner200test From Wuhan, China

- Apr 5, 2015 20:38:54.958254000 CST 121.60.104.246 36360 HTTP/1.1 GET /operator/basic.shtml AXIS Video Server and IP Cam
- Apr 5, 2015 20:38:55.066767000 CST 121.60.104.246 36364 HTTP/1.1 GET /setup
- Apr 5, 2015 20:38:55.181412000 CST 121.60.104.246 36369 HTTP/1.1 GET /secure/ltx_conf.htm Lantronix Xport
- Apr 5, 2015 20:38:55.300158000 CST 121.60.104.246 36372 HTTP/1.1 GET /syslog.htm
- Apr 5, 2015 20:38:55.422017000 CST 121.60.104.246 36374 HTTP/1.1 GET /cgi-bin/webif/info.sh OpenWRT?
- Apr 5, 2015 20:38:55.530658000 CST 121.60.104.246 36379 HTTP/1.1 GET /control/index_ctrl.html
- Apr 5, 2015 20:38:55.634389000 CST 121.60.104.246 36384 HTTP/1.1 GET /cgi-bin/camera

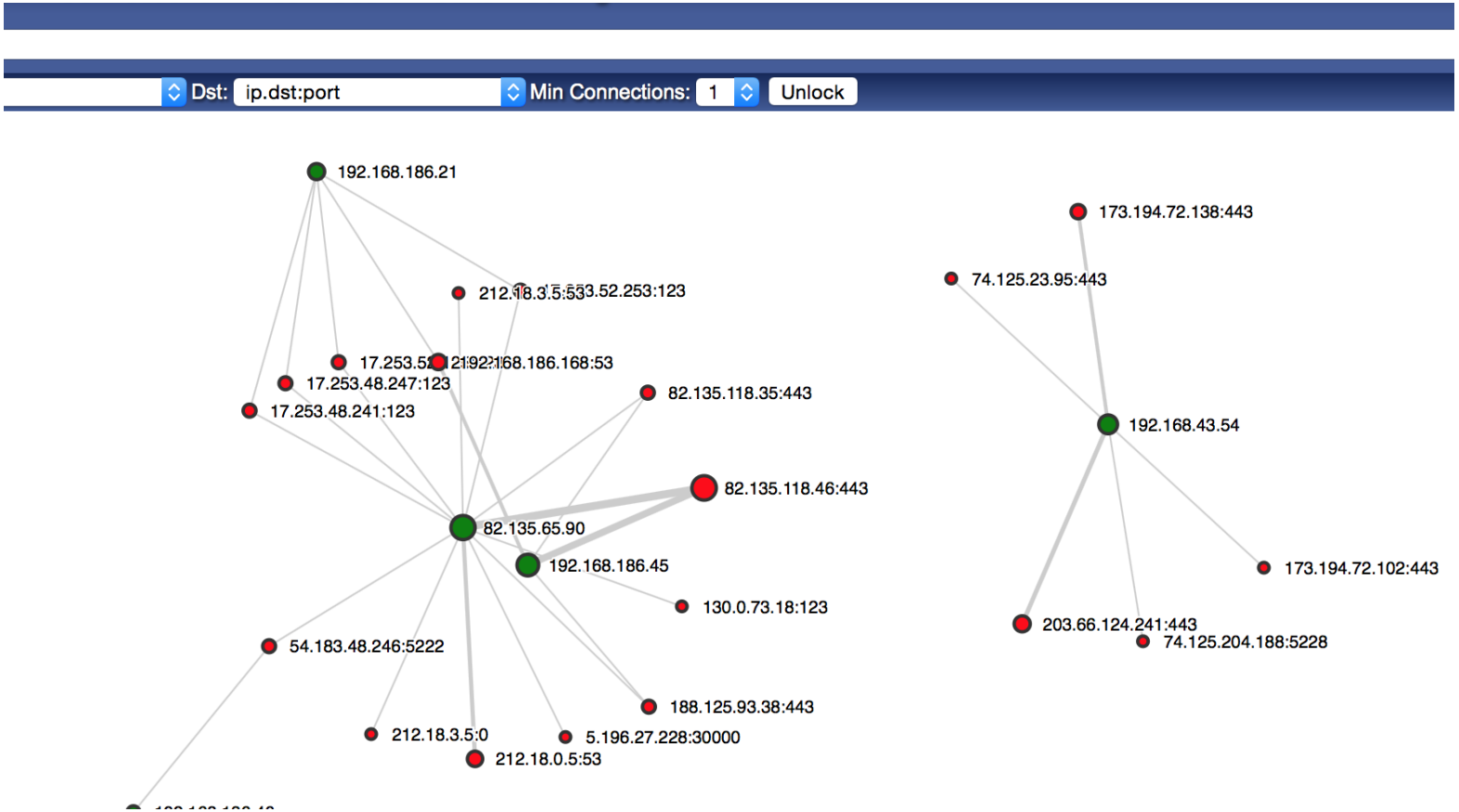
Attacks – Script Kiddies (13-2)

FastHTTPAuthScanner200test From Wuhan, China

- Apr 5, 2015 20:38:55.948539000 CST 121.60.104.246 36395 HTTP/1.1 GET http://www.fbi.gov/
- Apr 5, 2015 20:38:56.059004000 CST 121.60.104.246 36398 HTTP/1.0 CONNECT www.fbi.gov:80
- Apr 5, 2015 20:38:56.165412000 CST 121.60.104.246 36401 HTTP/1.1 GET /FastHTTPAuthScanner200test/
- Apr 5, 2015 20:38:57.882063000 CST 121.60.104.246 36470 HTTP/1.1 GET /%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/etc/passwd
- Apr 5, 2015 20:38:58.003634000 CST 121.60.104.246 36475 HTTP/1.1 GET /%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/boot.ini
- Apr 5, 2015 20:38:58.118258000 CST 121.60.104.246 36478 HTTP/1.1 GET /../../../../../../../../etc/passwd
- Apr 5, 2015 20:38:58.355473000 CST 121.60.104.246 36488 HTTP/1.1 GET /portal/page/portal/TOPLEVE

Moloch

Green: src Red: dst
Easy to identify frequent destinations (and ignore them to find anomalies)



Tshark still helps

/Ringing.at.your.doorbell!

```
May 14, 2015 05:26:04.420680000 CST     84.232.234.207  2076    HTTP/1.0        GET     /Ringing.at.your.dorbell!
May 14, 2015 05:26:05.130222000 CST     84.232.234.207  2085    HTTP/1.0        GET     /
May 14, 2015 05:26:05.823285000 CST     84.232.234.207  2095    HTTP/1.1        GET     /
May 14, 2015 05:26:06.556744000 CST     84.232.234.207  2111    HTTP/1.0        GET     /Diagnostics.asp
May 14, 2015 05:26:07.247503000 CST     84.232.234.207  2123    HTTP/1.0        GET     /
May 14, 2015 05:26:07.976700000 CST     84.232.234.207  2137    HTTP/1.0        GET     /
May 14, 2015 05:26:08.701755000 CST     84.232.234.207  2152    HTTP/1.0        GET     /
```

Recap

- Mostly script kiddies
  - OK, only 1 peeping. Thanks him/her. ☺
- No serious IoT hackers
  - Scripts for popular IPCam, yes.
  - Targeted on low hanging fruits.
- Very hard to meet those who want to play

Backed by Real Devices?

- Pros
  - Shodan thinks it's not a honeypot
  - Correct response, correct action
  - Hackers know how to identify a CONPOT
- Cons
  - Scalability
- Future works
  - Route many IP to one lab
  - Rewrite at layer 7 to change serial number, footprints

Questions?

Philips Hue Port 30000 Takeover

Telnet to port 30000 of the bridge and type:

[Link,Touchlink]

The light should blink a few times to acknowledge the hostile takeover.

Ref:

https://nohats.ca/wordpress/blog/2013/05/26/philips-hue-alternative-for-lamp-stealer/

WD Twonky pings iRadio

```
POST /AVTransport/control HTTP/1.1
Accept: */*
User-Agent: Twonky-NMC/7.2.9 (Linux 3.2.26; armv7l) DLNADOC/1.50
Host: 192.168.186.50:80
SOAPACTION: "urn:schemas-upnp-org:service:AVTransport:1#GetCurrentTransportActions"
Content-Type: text/xml; charset="utf-8"
Content-Length: 332

<?xml version="1.0" encoding="utf-8"?><s:Envelope s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/" xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><u:GetCurrentTransportActions
xmlns:u="urn:schemas-upnp-org:service:AVTransport:1"><InstanceID>0</InstanceID></
u:GetCurrentTransportActions></s:Body></s:Envelope>HTTP/1.1 200 OK
Transfer-Encoding: chunked
EXT:
CONTENT-TYPE: text/xml; charset="utf-8"
SERVER: POSIX, UPnP/1.0, Intel MicroStack/1.0.2777

157
<?xml version="1.0" encoding="utf-8"?>
<s:Envelope s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:s="http://
schemas.xmlsoap.org/soap/envelope/"><s:Body><u:GetCurrentTransportActionsResponse xmlns:u="urn:schemas-
upnp-org:service:AVTransport:1"><Actions></Actions></u:GetCurrentTransportActionsResponse></s:Body></
s:Envelope>
0
```

WDCloud → Samsung IPCam

```
GET /rootDesc.xml HTTP/1.1
Host: 192.168.186.46:49152
Connection: Close
User-Agent: Darwin/11.4.0, UPnP/1.0, MiniUPnPc/1.8

HTTP/1.1 200 OK
Content-Type: text/xml; charset="utf-8"
Connection: close
Content-Length: 1023
Server: Ubuntu/precise UPnP/1.1 MiniUPnPd/1.7

<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0"><specVersion><major>1</major><minor>0</minor></
specVersion><device><deviceType>urn:schemas-upnp-org:device:Basic:1</deviceType><friendlyName>SAMSUNG-SNH-
P6410BN-00166C8EA032</friendlyName><manufacturer>SAMSUNG</manufacturer><manufacturerURL>http://
www.samsungtechwin.com/</manufacturerURL><modelDescription>SNH-P6410BN Network Camera</
modelDescription><modelName>SNH-P6410BN</modelName><modelNumber>SNH-P6410BN</modelNumber><modelURL>http://
www.samsungtechwin.com/</modelURL><serialNumber>KHNQ6V2FB00073R</serialNumber><UDN>uuid:Upnp-
BasicDevice-1_0-00166C8EA032</
UDN><serviceList><service><serviceType>urn:SamsungTechwin:service:BasicService:1</
serviceType><serviceId>urn:SamsungTechwin:BasicServiceId</serviceId><controlURL>/upnp/control/
BasicServiceId</controlURL><eventSubURL>/upnp/event/BasicServiceId</eventSubURL><SCPDURL>/scpd_basic.xml</
SCPDURL></service></serviceList><presentationURL>http://192.168.186.46:80/</presentationURL></device></
root>[1064315425 bytes missing in capture file]POST / HTTP/1.1
Host: 192.168.186.46:49152
User-Agent: Darwin/11.4.0, UPnP/1.0, MiniUPnPc/1.8
Content-Length: 330
Content-Type: text/xml
SOAPAction: "#DeletePortMapping"
Connection: Close
Cache-Control: no-cache
Pragma: no-cache
```