SharkFest '18 Europe

Phill "Sherlock" Shade

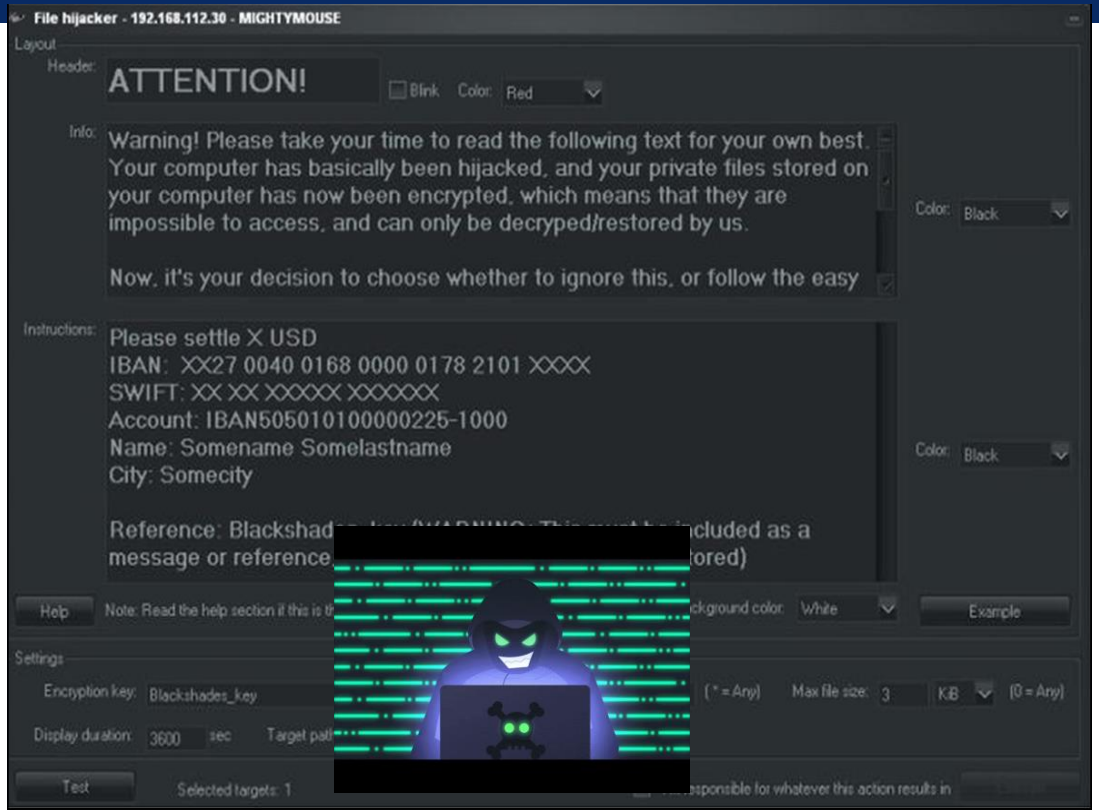
Merlion's Keep Consulting
& SCOS.NL

Phillip “Sherlock” Shade (Phill)

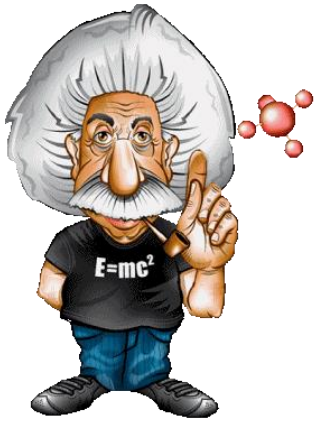
phill.shade@gmail.com

- Certified instructor and internationally recognized network security and forensics expert with more than 30 years of experience
- Retired US Navy and the founder of Merlion’s Keep Consulting, a professional services company specializing in network and forensics analysis
- A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, and the IEEE and volunteer at Cyber Warfare Forum Initiative
- Holds numerous certifications, including Certified Network Expert (CNX)-Ethernet, CCNA, Certified Wireless Network Administrator (CWNA), and WildPackets Certified Network Forensics Analysis Expert (WNAX)
- Certified Wireshark University, Sniffer University and Planet 3 Wireless instructor

Thank You for Joining Us Today



Welcome to my World….
Today's Agenda

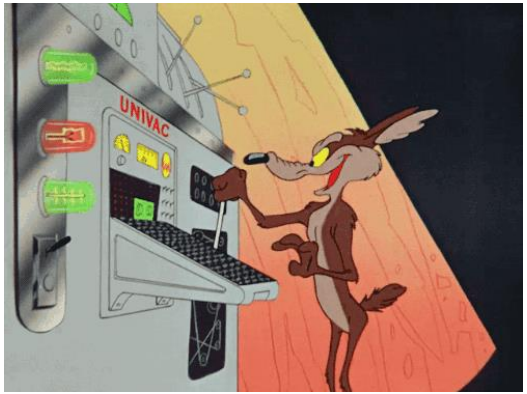


1. UPNP – The Unforeseen Threat?
2. Bluetooth and Exploits
3. ZigBee
4. WeMo
5. IoT Bot & Botnets – Mirai and Others

28 march just nest setup 2 long capture (#54).pcapng

Case Studies

1. MK - Baseline - UPNP - HTTP Modify & Notify
2. Bluetooth - HCI & OBEX Transaction over USB
3. 802.15.4 - ZigBee-join-authenticate
4. Philips_hue_trace (KLPD 03Oct16)
5. Philips Hue Idle v2
6. 28 march just nest setup 2 long capture (#54)
7. irdademo (Pcap = Infared)
8. Mirai – Command & Control



For This to Work - Normal or Abnormal?

Source	Destination	Protocol	Length	Src Port	Dst Port	Info
Micro-St_70:13:b7	IPv6mcast_00:00:00:	SSDP	208	51760	1900	M-SEARCH * HTTP/1.1
Micro-St_70:13:b7	IPv6mcast_00:00:00:	SSDP	208	51760	1900	M-SEARCH * HTTP/1.1
Micro-St_70:13:b7	Netgear_52:9e:a0	DNS	71	58501	53	Standard query A www.cnn.com
Netgear_52:9e:a0	Micro-St_70:13:b7	DNS	288	53	58501	Standard query response A 157.166.255.19
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	66	65045	80	65045 > 80 [SYN] Seq=419029810 Win=8192 L
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	66	80	65045	80 > 65045 [SYN, ACK] Seq=1914813027 Ack=
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	54	65045	80	65045 > 80 [ACK] Seq=419029811 Ack=191481
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	1448	65045	80	[TCP segment of a reassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	1448	65045	80	[TCP segment of a reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Micro-St_70:13:b7	Netgear_52:9e:a0	HTTP	1194	65045	80	GET / HTTP/1.1
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	1448	80	65045	[TCP segment of a reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e					q=419033739 Ack=191481
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e					q=419033739 Ack=191481
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]
Netgear_52:9e:a0	Micro-St_70:1					eassembled PDU]

Forensics Analysis Tip: Be familiar with the expected or Baseline behavior of protocols before trying to identify suspect behavior!

The Key – Reference / Baseline Files

- How can you recognize suspicious behavior unless you understand the expected behavior of a protocol?
- This is where the use of known-good reference or baseline files becomes important!
  - Reference files of standard network activities
  - Samples of network device behavior
  - Many devices, Scanning tools, Exploits, Hackers have specific signatures or patterns that can be used to identify a specific behavior

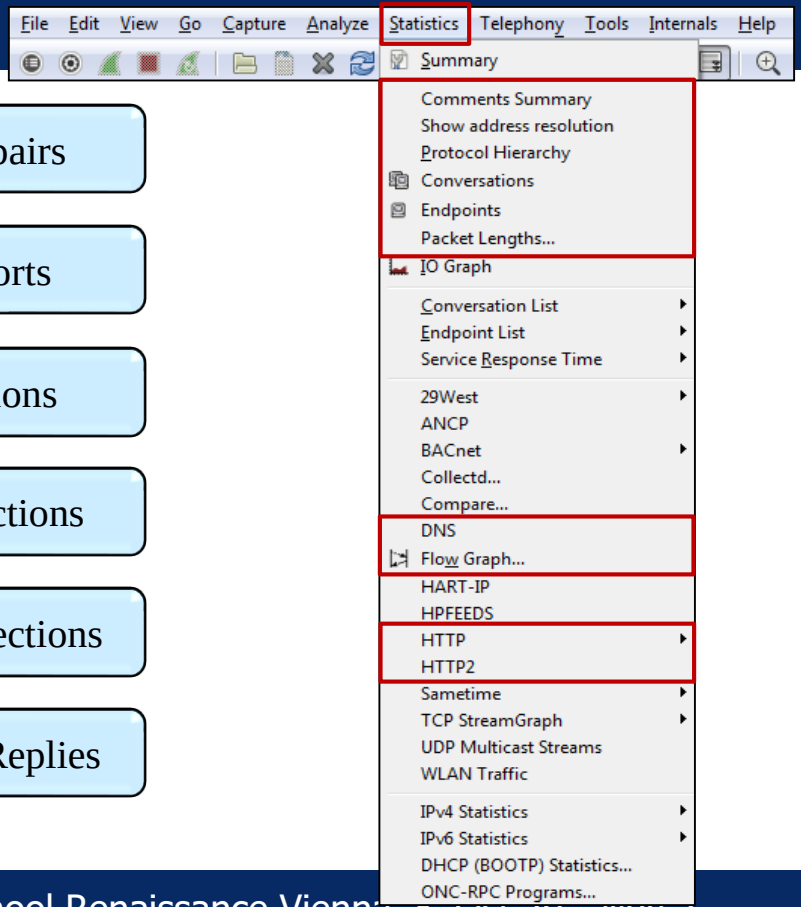
So… Where do I Get Samples?

- https://wiki.wireshark.org/SampleCaptures
- http://packetlife.net/captures/
- http://www.pcapr.net
- http://www.netresec.com/?page=PcapFiles
- http://ambitwire.com/useful-links/public-pcap-repositories/link/public-pcap-repositories-ambitwires-ultimate-collection
- http://contagiodump.blogspot.nl/2013/04/collection-of-pcap-files-from-malware.html
- https://www.evilfingers.com/repository/pcaps.php
- https://www.bro.org/community/traces.html
- http://www.secrepo.com/

Forensics Analysis Tip: For specific requests, email me! *phill.shade@gmail.com*

What Should I Look For?

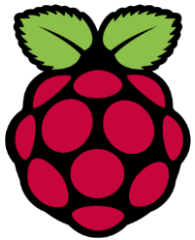
- Unusual communication pairs
- Unusual protocols and ports
- Excessive failed connections
- Suspicious inbound connections
- Suspicious Outbound Connections
- Suspicious DNS Queries / Replies



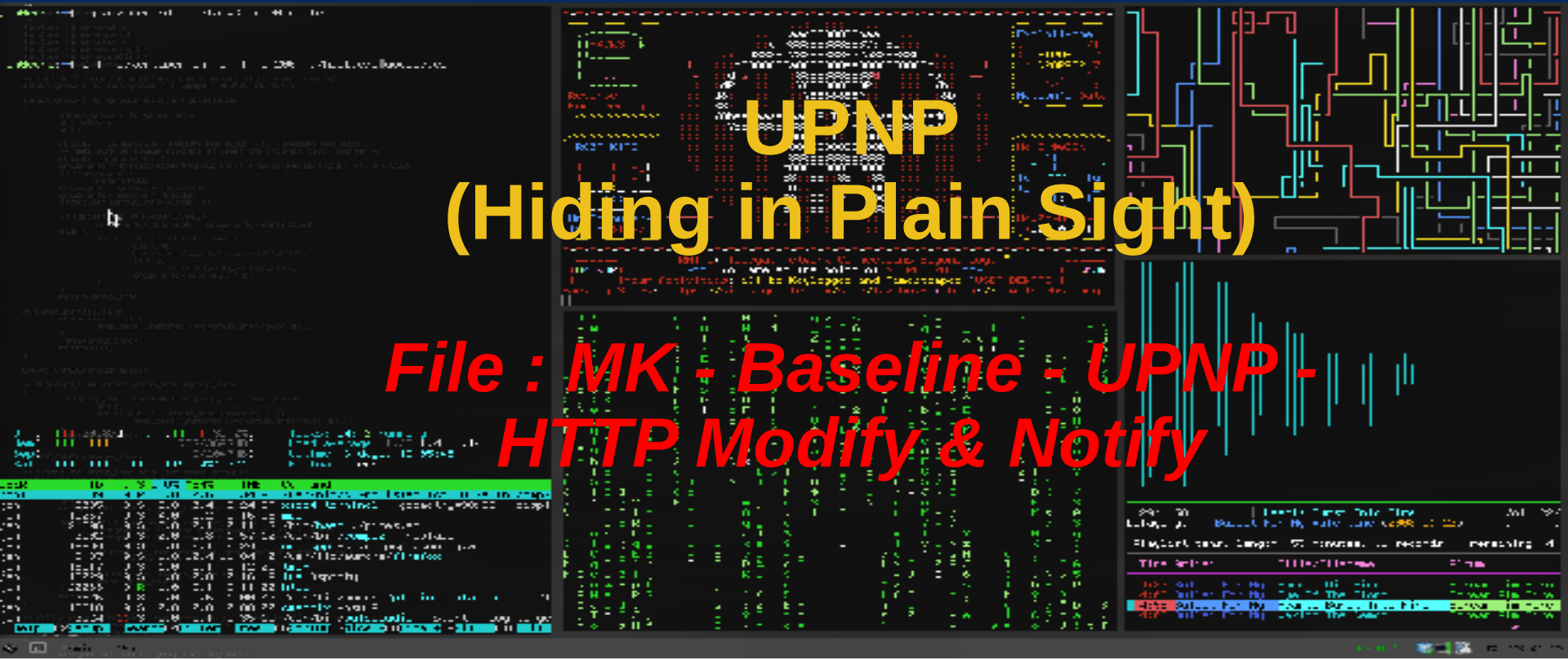
How Many of You Have at Least one of These?

SoHo / IoT WiFi Technologies

- **S**mall **O**ffice / **H**ome **O**ffice (SoHo) / IoT (Internet of Things) technologies comprise a specialized area of WiFi technology
  - Based upon existing IEEE 802.xx WiFi specifications
    - Modified to use low power, small form factor devices
    - Primarily use the 2.4Ghz ISM bands (some exceptions)
    - Intended to provide short range – PAN networking (<30m)



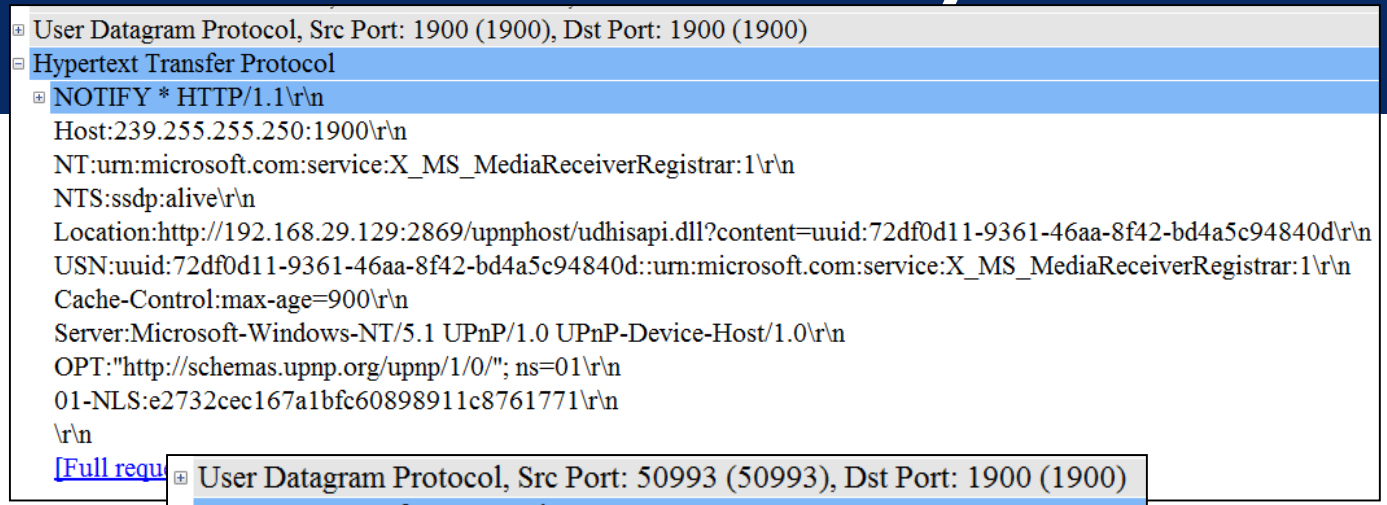
IoT Case Study #1 – To Get Your Attention



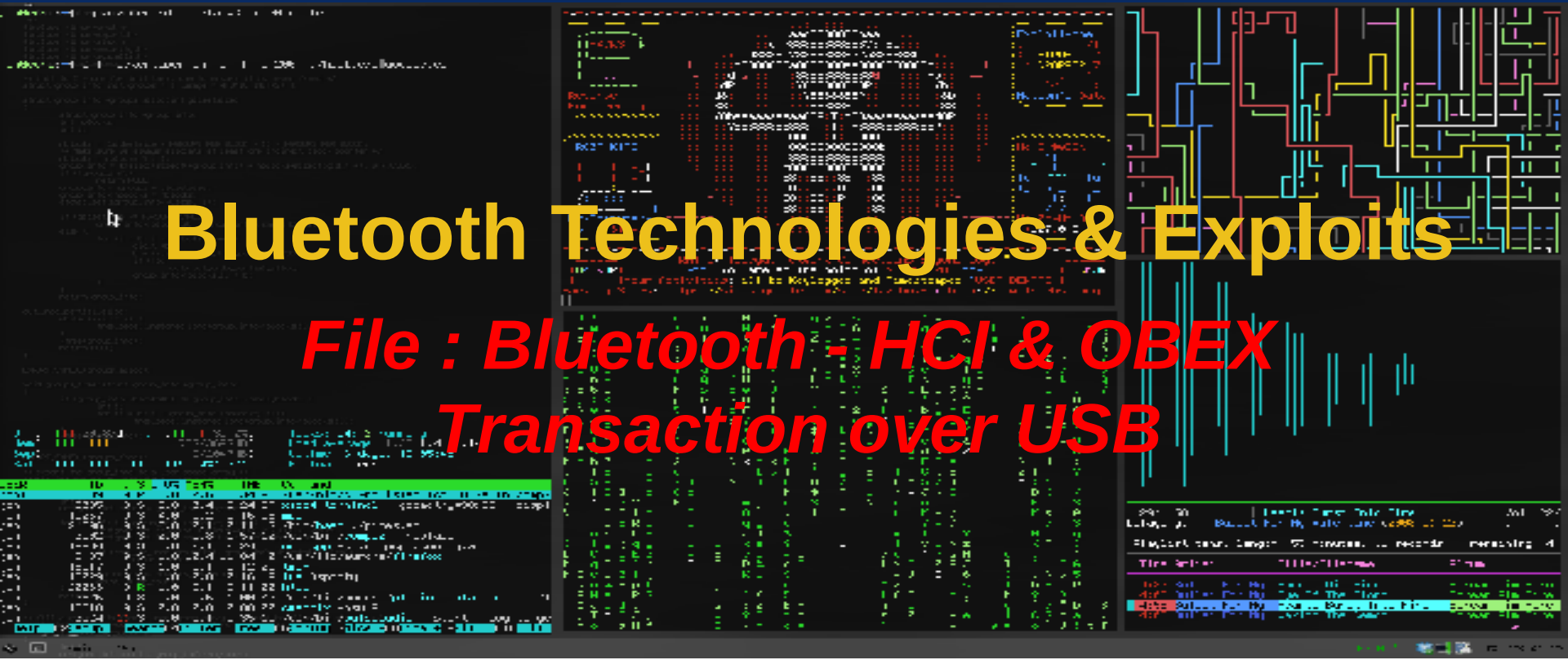
UPnP - Unforeseen HTTP Threat

- Universal Plug-and-Play
- ISO/IEC 29341, in December, 2008
  - Enable connectivity to stand-alone devices and computers from multiple vendors
    - Intended to provide zero configuration networking for residential, SOHO wireless networks and networked home appliances
    - Managed by the Open Connectivity Foundation (OCF)
      - www.upnp.org
- HTTP / SSDP Multicast over UDP Port 1900
  - HTTP Notify
  - HTTP M-Search

UPnP Details - Notify & Search



IoT Forensics Case Study #2 -



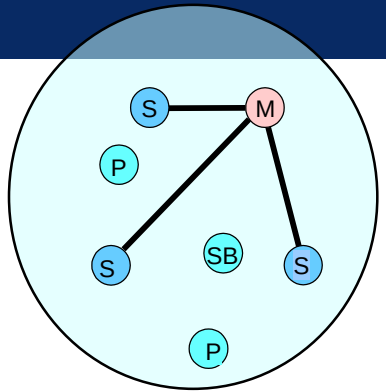
Bluetooth Technologies & Exploits

File : Bluetooth - HCI & OBEX Transaction over USB

Bluetooth Overview

- FHSS based technology that operates in the same 2.4Ghz band as IEEE 802.11b (1Mb/s data rate)
  - Signals hop from one channel to another in a pseudo-random fashion, determined by the master station
- **W**ireless **P**ersonal **A**rea **N**etworks (WPAN)
  - Short-range, Low Power, Low Cost, Small form factor
  - Small networks, No configuration, common user experience
  - Communication of devices within a Personal Operating Space
- Defined in IEEE 802.15 as a WPAN technology
  - Class 3 radios – have a range of up to 1 meter or 3 feet
  - Class 2 radios – mobile devices – have a range of 10 meters
  - Class 1 radios – used primarily in industrial use cases – have a range of 100 meters
  - 3 variable power settings

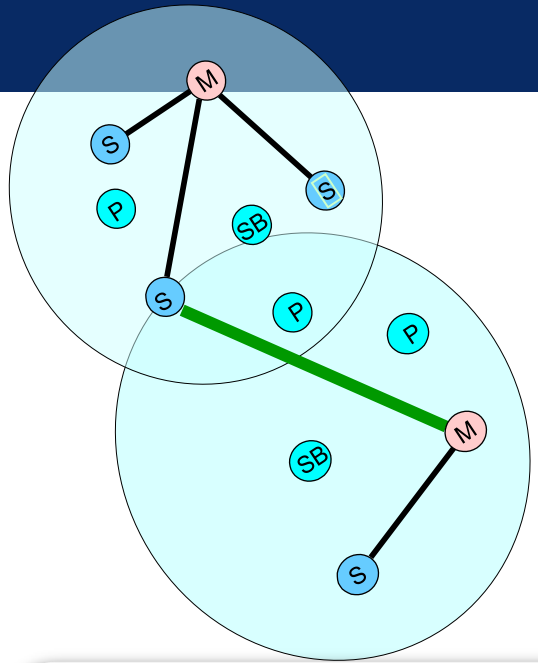
Bluetooth Piconet vs. Scatternet



M = Master P = Parked

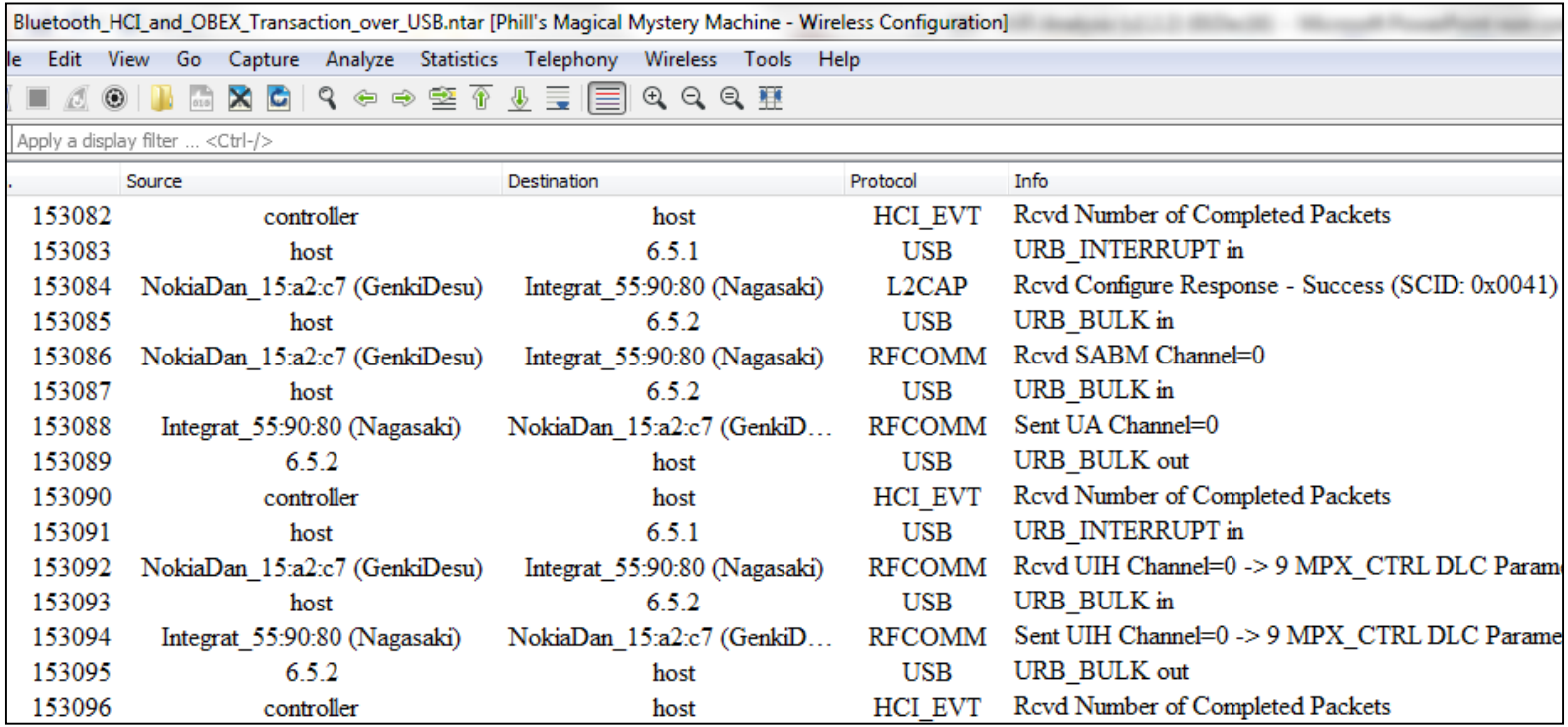
S = Slave SB = Standby

- Pcionet: Ad hoc connectivity
- Master sets the clock, unique hopping pattern & ID
- Master can connect to 7 simultaneous or 200+ inactive (parked) slave stations



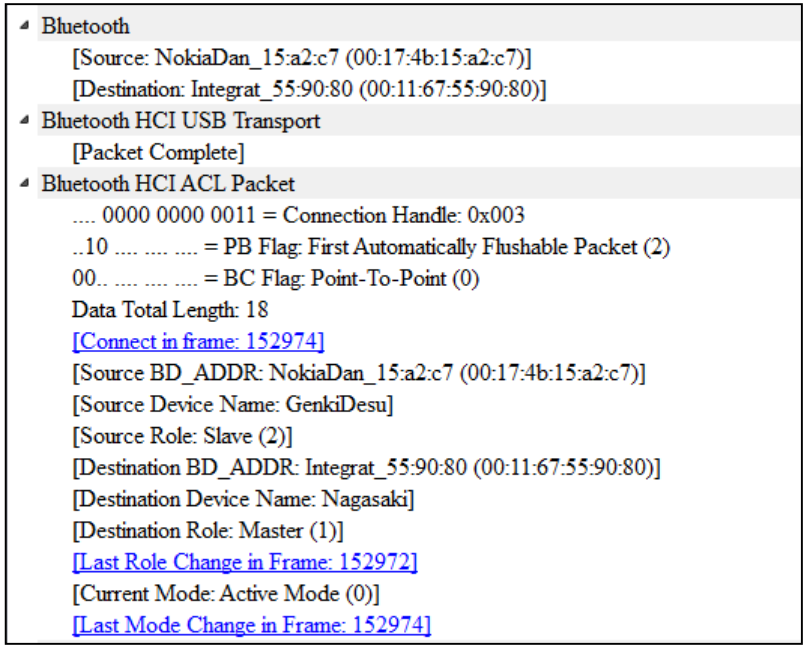
- Scatternet
- Piconets linked through a shared Master or Slave
- A device can be both a Master and a Slave at the same time with a maximum capacity: 720 Kbps

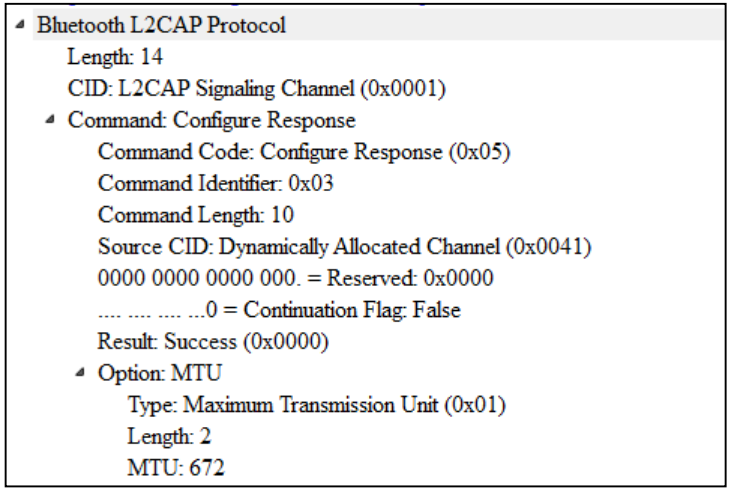
Bluetooth Pcap



	Source	Destination	Protocol	Info
153082	controller	host	HCI_EVT	Rcvd Number of Completed Packets
153083	host	6.5.1	USB	URB_INTERRUPT in
153084	NokiaDan_15:a2:c7 (GenkiDesu)	Integrat_55:90:80 (Nagasaki)	L2CAP	Rcvd Configure Response - Success (SCID: 0x0041)
153085	host	6.5.2	USB	URB_BULK in
153086	NokiaDan_15:a2:c7 (GenkiDesu)	Integrat_55:90:80 (Nagasaki)	RFCOMM	Rcvd SABM Channel=0
153087	host	6.5.2	USB	URB_BULK in
153088	Integrat_55:90:80 (Nagasaki)	NokiaDan_15:a2:c7 (GenkiD…	RFCOMM	Sent UA Channel=0
153089	6.5.2	host	USB	URB_BULK out
153090	controller	host	HCI_EVT	Rcvd Number of Completed Packets
153091	host	6.5.1	USB	URB_INTERRUPT in
153092	NokiaDan_15:a2:c7 (GenkiDesu)	Integrat_55:90:80 (Nagasaki)	RFCOMM	Rcvd UIH Channel=0 -> 9 MPX_CTRL DLC Param
153093	host	6.5.2	USB	URB_BULK in
153094	Integrat_55:90:80 (Nagasaki)	NokiaDan_15:a2:c7 (GenkiD…	RFCOMM	Sent UIH Channel=0 -> 9 MPX_CTRL DLC Parame
153095	6.5.2	host	USB	URB_BULK out
153096	controller	host	HCI_EVT	Rcvd Number of Completed Packets

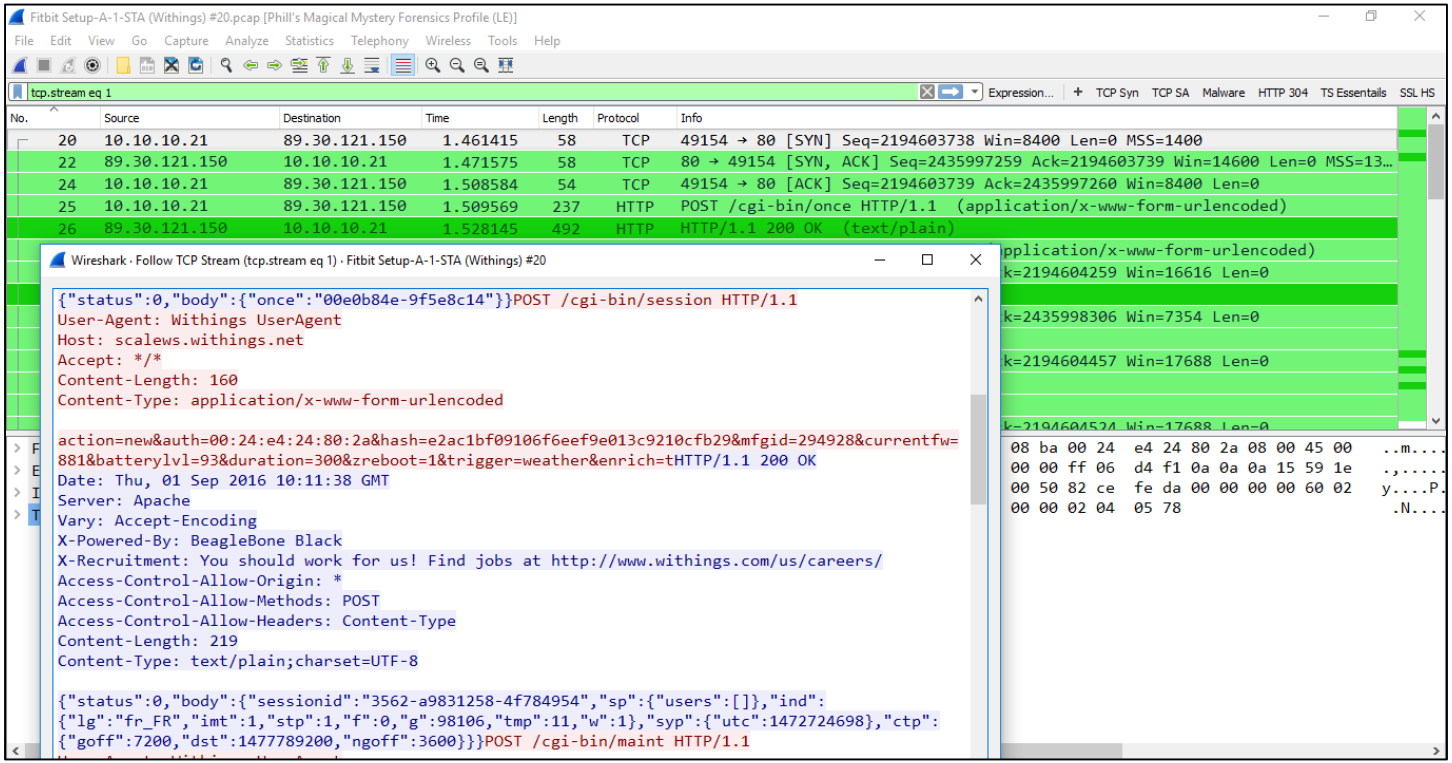
Sample Bluetooth Decode





Nokia Withings…

Withings Details



Security Issue - Bluebug

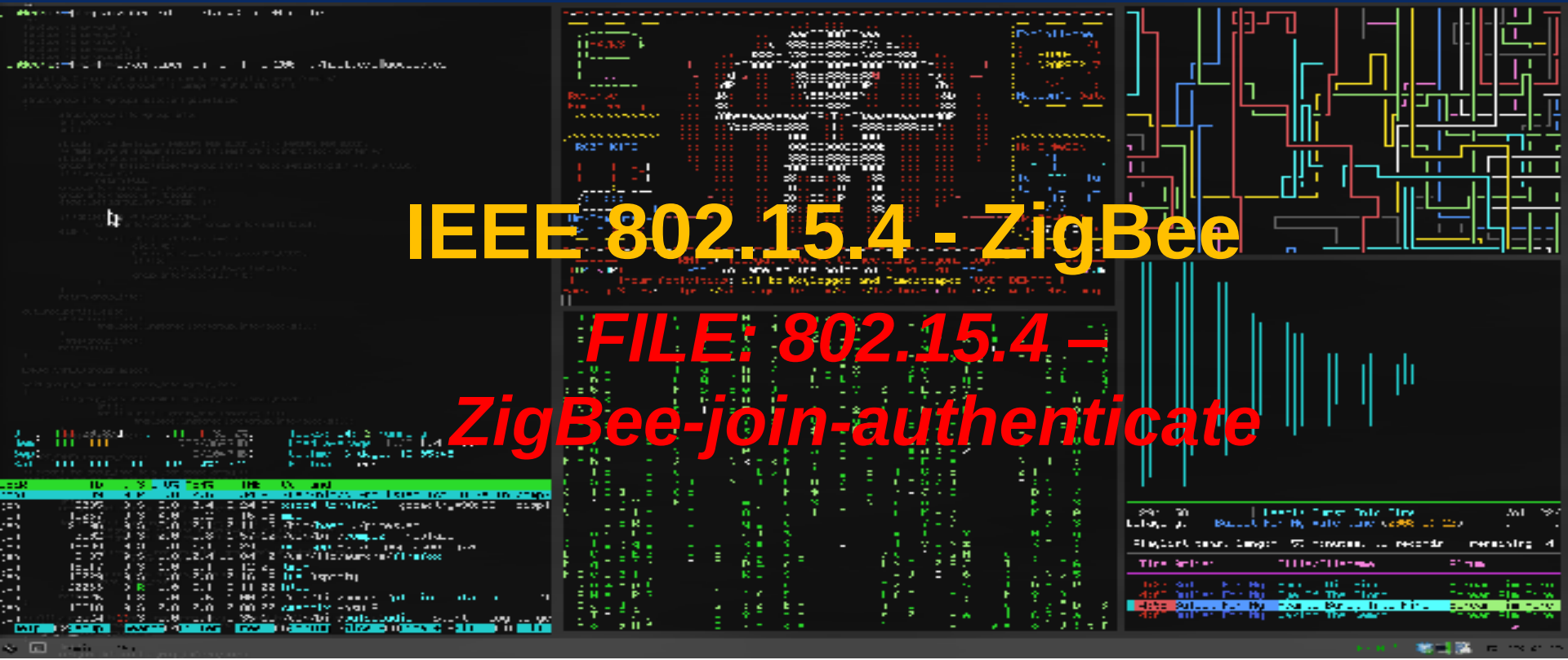
- Exploit developed by a German researcher (Martin Herfurt in 2004
- Allows the attacker to use the phone to initiate calls to premium rate numbers, send SMS messages, read SMS messages, connect to data services such as the Internet, and eavesdrop on conversations in the vicinity
  - Allows the listening post to be anywhere in the world.
    - Bluetooth access is only required for a few seconds in order to set up the call
- Creates a serial profile connection to the device, giving full access to the AT command set, which is then exploited using standard off the shelf tools
  - PPP for networking or gnokii for messaging

Security Issue – BlueSnarfing

- BlueSnarfing is the unauthorized accessing of features on Bluetooth-enabled devices
  - Phones / PDA's / WiFi network devices
- Typically employed in long-range attacks
  - Favorite industrial espionage attack

"…BlueSniper rifle, a yagi-antenna and scope affixed to a gun-like stock that this week broke a distance record for BlueSnarfing… by slurping data from a Nokia 6310i from 1.1 away (2 Km) away…"
Wired News Aug2004

IoT Forensics Case Study #3 -



IEEE 802.15.4 - ZigBee

FILE: 802.15.4 – ZigBee-join-authenticate

ZigBee Overview

- Uses OFDM in the following 3 bands:
  - 16 channels in the 2.4GHz ISM band / 10 channels in the 915MHz ISM band / 1 channel in the European 868MHz band
- Defined in IEEE 802.15.4
  - CSMA / CA data rates:
    - 250kb/s @ 2.4Ghz Band
    - 40 kb/s @ 915 MHz ISM Band
    - 20 kb/s @ 868 MHz Band

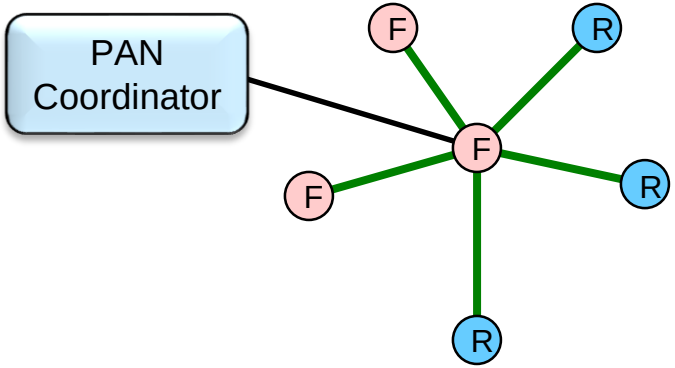
- Designed for use with small form factor, low power, low latency devices
  - Maximum power is 1mW
  - Used in small or PAN type networks
    - Connected in P2P or Star configuration

IEEE 802.15.4 ZigBee Node Types

- Full function device (**FFD**)
  - Any topology
  - Network coordinator capable
  - Talks to any other device

- Reduced function device (**RFD**)
  - Limited to star topology
  - Cannot become a network coordinator

802.15.4 ZigBee Star Network



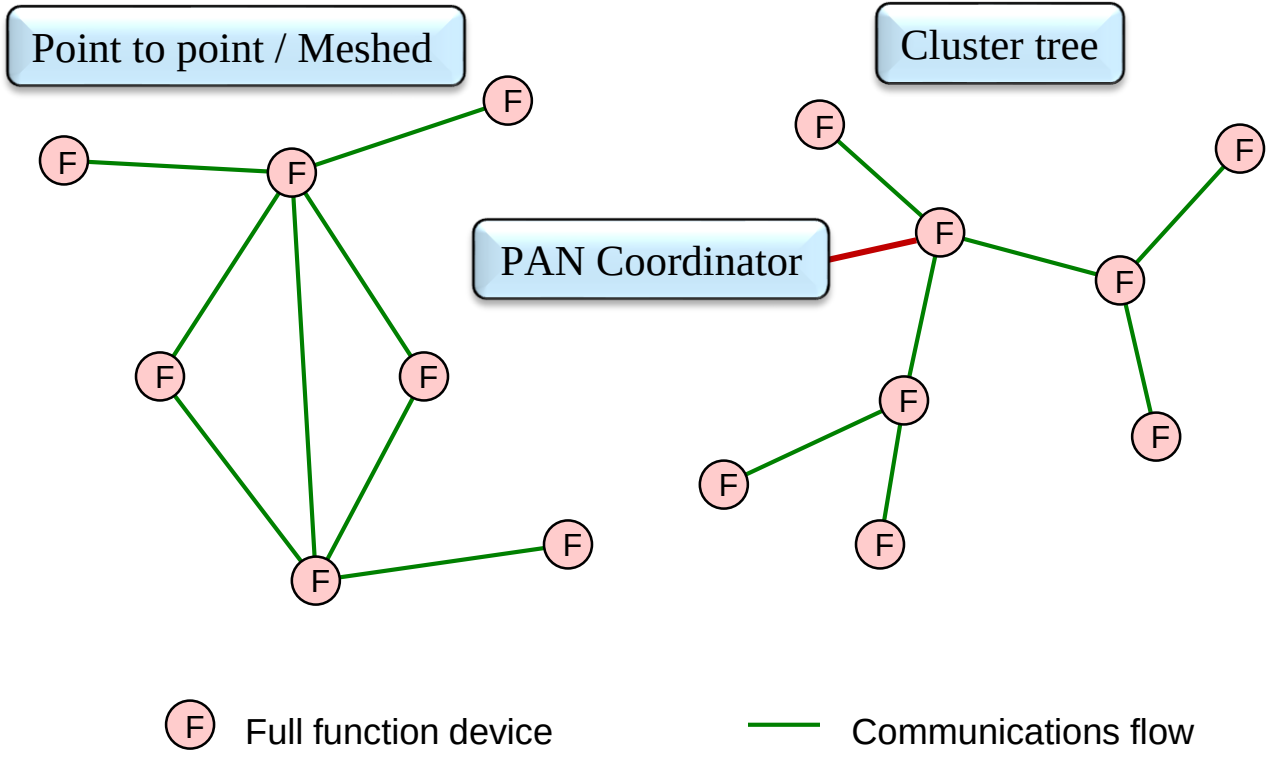
Master/slave

F Full function device

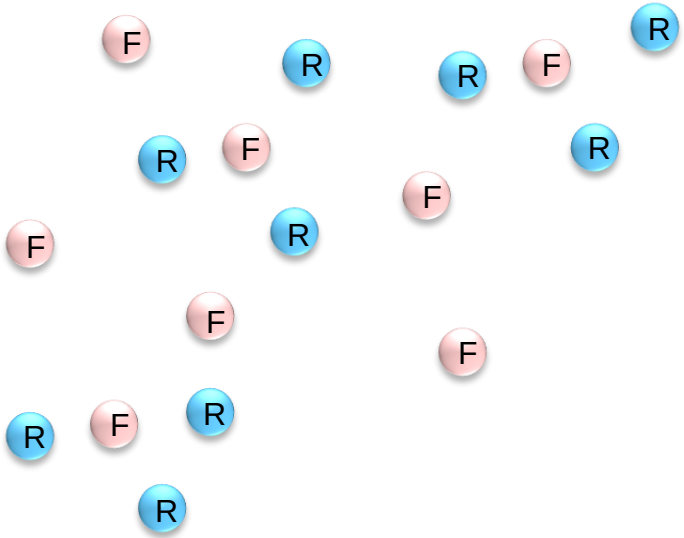
R Reduced function device

Communications flow

802.15.4 ZigBee P2P Network



802.15.4 ZigBee Combination / Mixed Network



Clustered stars Example: between Rooms of a hotel and each room has a star network for control.

F Full function device

R Reduced function device

Communications flow

Sample ZigBee Capture

802.16 - zigbee-join-authenticate.pcap [Phill's Magical Mystery Machine - Wireless Configuration]

le Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

	Source	Destination	Protocol	Info
28	0x2c4d	Broadcast	ZigBee	Command, Dst: Broadcast, Src: 0x2c4d
29	0x0000	0x2c4d	ZigBee	Command, Dst: 0x2c4d, Src: 0x0000
30			IEEE 802.15.4	Ack
31	0x2c4d	0x0000	ZigBee	Data, Dst: 0x0000, Src: 0x2c4d
32			IEEE 802.15.4	Ack
33	0x0000	0x2c4d	ZigBee	Data, Dst: 0x2c4d, Src: 0x0000
34			IEEE 802.15.4	Ack
35	0x2c4d	0xdb18	ZigBee	APS: Command
36	0xdb18	Broadcast	ZigBee	Data, Dst: Broadcast, Src: 0xdb18
37	0xdb18	Broadcast	ZigBee	Data, Dst: Broadcast, Src: 0xdb18
38	0x0000	0x2c4d	ZigBee	Command, Dst: 0x2c4d, Src: 0x0000
39			IEEE 802.15.4	Ack
40	0x0000	0x2c4d	ZigBee	Command, Dst: 0x2c4d, Src: 0x0000
41			IEEE 802.15.4	Ack
42	0x2c4d	Broadcast	ZigBee	Command, Dst: Broadcast, Src: 0x2c4d
43	0x0000	Broadcast	ZigBee	Command, Dst: Broadcast, Src: 0x0000

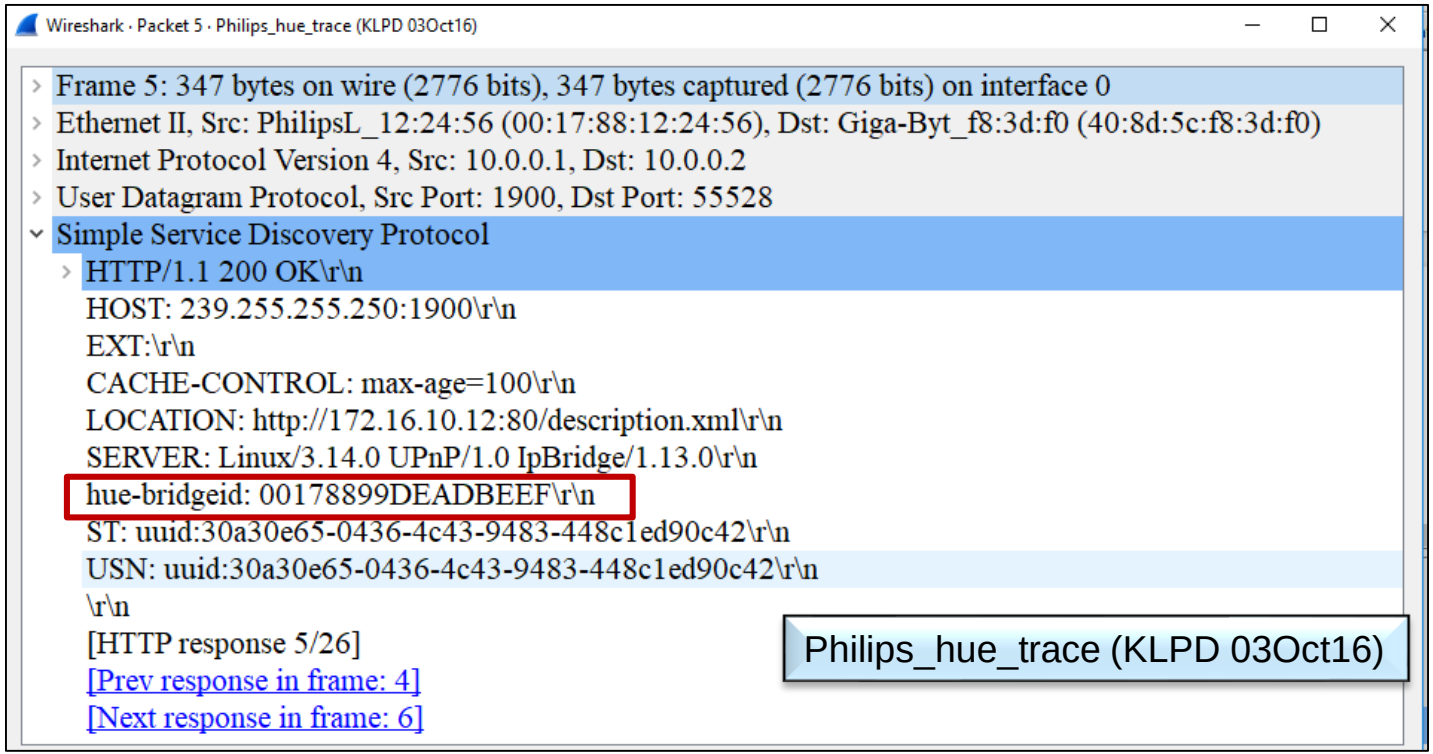
Sample ZigBee Decode

IEEE 802.15.4 Data, Dst: 0xdb18, Src: 0x2c4d
- Frame Control Field: 0x8861, Frame Type: Data, Acknowledge Request, PAN ID
  - .... .001 = Frame Type: Data (0x1)
  - .... 0... = Security Enabled: False
  - ....0 .... = Frame Pending: False
  - ....1. .... = Acknowledge Request: True
  - .... .1.. .... = PAN ID Compression: True
  - ....0 .... = Sequence Number Suppression: False
  - .... ..0. .... = Information Elements Present: False
  - .... 10.. .... = Destination Addressing Mode: Short/16-bit (0x2)
  - ..00 .... = Frame Version: IEEE Std 802.15.4-2003 (0)
  - 10.. .... = Source Addressing Mode: Short/16-bit (0x2)
- Sequence Number: 19
- Destination PAN: 0x01ff
- Destination: 0xdb18
- Source: 0x2c4d
- [Extended Source: ExeginTe_ffff:00:20:07 (00:1c:daffff:00:20:07)]
- [Origin: 19]

ZigBee Network Layer Data, Dst: 0xdb18, Src: 0x2c4d
- Frame Control Field: 0x0008, Frame Type: Data, Discover Route: Suppress Data
- Destination: 0xdb18
- Source: 0x2c4d
- Radius: 1
- Sequence Number: 127
- [Extended Source: ExeginTe_ffff:00:20:07 (00:1c:daffff:00:20:07)]
- [Origin: 23]

ZigBee Application Support Layer Command
- Frame Control Field: Command (0x21)
  - .... ..01 = Frame Type: Command (0x1)
  - .... 00.. = Delivery Mode: Unicast (0x0)
  - ..1. .... = Security: True
  - .0.. .... = Acknowledgement Request: False
  - 0... .... = Extended Header: False
- Counter: 2
- ZigBee Security Header
  - Security Control Field: 0x30, Key Id: Key-Transport Key, Extended Nonce
    - ...1 0... = Key Id: Key-Transport Key (0x2)
    - ..1. .... = Extended Nonce: True
  - Frame Counter: 1
  - Extended Source: EmberCor_00:00:0d:c5:58 (00:0d:6f:00:00:0d:c5:58)
  - Message Integrity Code: a4 2f 8d 59
  - [Expert Info (Warning/Undecoded): Encrypted Payload]
- Data (35 bytes)
  - Data: 38 e1 3f f0 7e 31 53 76 53 4c b3 bd cb d3 e2 e5 ...
  - [Length: 35]

Philips Hue Lightbulb (v1) Details



Philips Hue Lightbulb (v2) Details

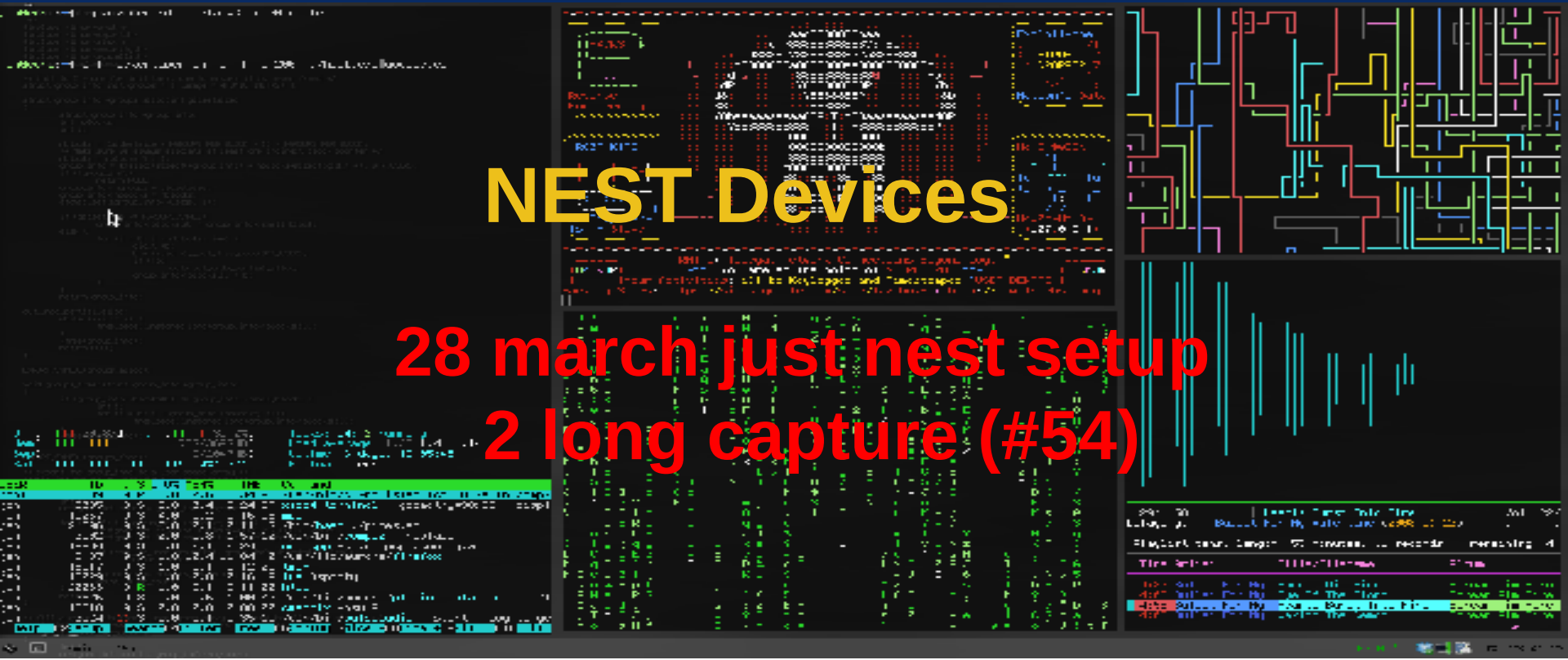
```
GET /description.xml HTTP/1.1
HOST: 129.94.5.95:80
DATE: Mon, 21 Apr 2014 13:50:38 GMT
CONNECTION: close
USER-AGENT: Unspecified, UPnP/1.0, Unspecified

HTTP/1.1 200 OK
Content-type: text/xml
Connection: Keep-Alive

<?xml version="1.0" encoding="UTF-8" ?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
<specVersion>
<major>1</major>
<minor>0</minor>
</specVersion>
<URLBase>http://129.94.5.95:80/</URLBase>
<device>
<deviceType>urn:schemas-upnp-org:device:Basic:1</deviceType>
<friendlyName>Philips hue (129.94.5.95)</friendlyName>
<manufacturer>Royal Philips Electronics</manufacturer>
<manufacturerURL>http://www.philips.com</manufacturerURL>
<modelDescription>Philips hue Personal Wireless Lighting</modelDescription>
<modelName>Philips hue bridge 2012</modelName>
<modelNumber>929000226503</modelNumber>
<modelURL>http://www.meethue.com</modelURL>
<serialNumber>0017881892ca</serialNumber>
<UDN>uuid:2f402f80-da50-11e1-9b23-0017881892ca</UDN>
<serviceList>
```

Philips Hue Idle v2

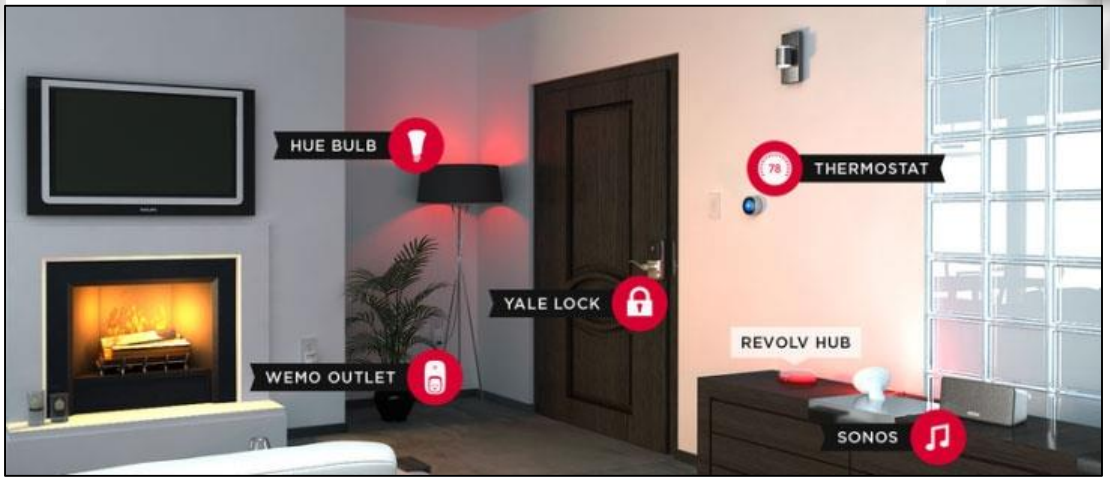
Phillips Hue Light Bulbs Hacked

This exploit was the handiwork of researchers Eyal Ronen, Adi Shamir, and Achi-Or Weingarten of the Weizmann Institute of Science, Israel, along with Colin O'Flynn of Dalhousie University, Canada. They flew a drone along this street in Paris while executing the exploit from a kilometer away…

IoT Forensics Case Study #4 -

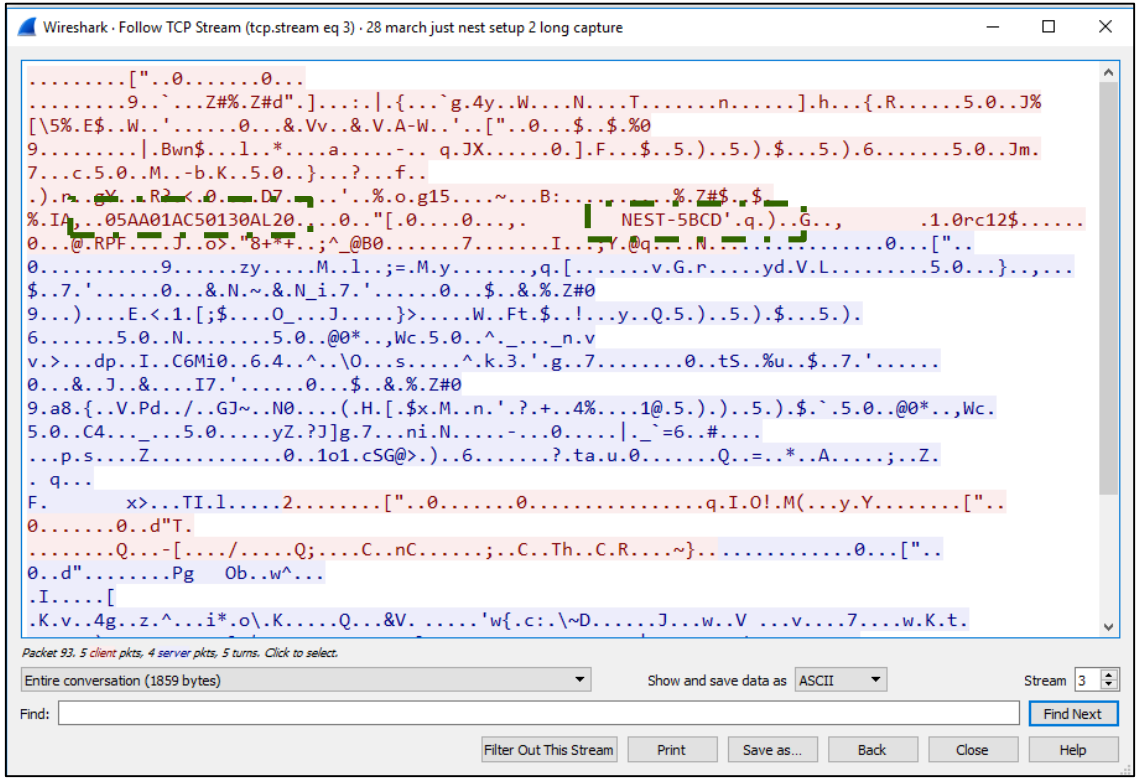


NEST Devices



How About Any of These?

NEST Decode Details...



NEST Exploits…

- https://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264

- https://www.exploitee.rs/index.php/Exploiting_Nest_Thermostats

WEMO Plug

belkin SHOP LEARN SUPPORT

home > products > mobile accessories > app-enabled accessories

Wemo® Switch Smart Plug

F7C027fc

3.5 (128)

Write a review Ask a question

$39.99

BUY NOW

Add to wish list

Wemo Mini Smart Plug, WiFi Enabled, Works with Alexa, Google Assistant & Apple HomeKit

by WeMo

11,049 customer reviews | 1000+ answered questions

#1 Best Seller in Electrical Light Switches

List Price: ~~$34.99~~

Price: $27.99 prime | FREE Same-Day

You Save: $7.00 (20%)

Get a $125 Amazon.com Gift Card upon approval for the Amazon Business Prime Card. Terms apply.

Style: **Mini Smart Plug**

Dimmer Light Switch
$64.99
prime

Insight Smart Plug
$34.99
prime

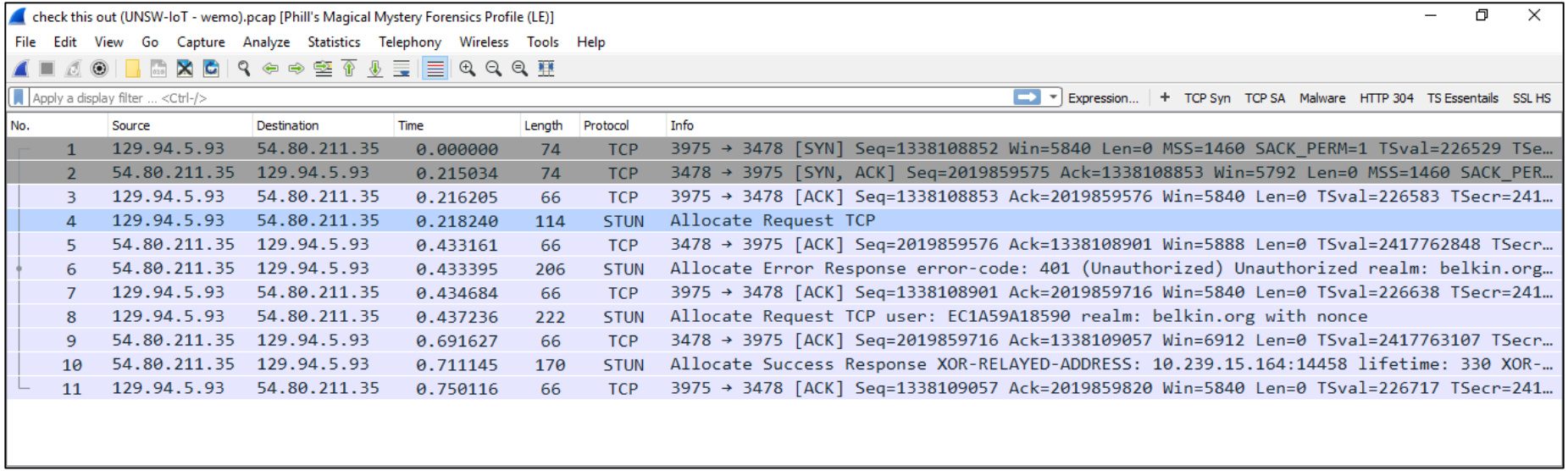
Light Switch
$39.99
prime

WeMo Technology

- Series of products from Belkin that enable users to control home electronics remotely. The product suite includes electrical plugs, motion sensors, light switches, cameras, light bulbs, and a mobile app
  - Can also be controlled by voice through the Amazon Echo

- Essentially Unencrypted = multiple vulnerabilities
  - https://hackaday.com/2013/01/31/turning-the-belkin-wemo-into-a-deathtrap/
  - https://www.kb.cert.org/vuls/id/656302

WeMo PCAP



No.	Source	Destination	Time	Length	Protocol	Info
1	129.94.5.93	54.80.211.35	0.000000	74	TCP	3975 → 3478 [SYN] Seq=1338108852 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=226529 TSe…
2	54.80.211.35	129.94.5.93	0.215034	74	TCP	3478 → 3975 [SYN, ACK] Seq=2019859575 Ack=1338108853 Win=5792 Len=0 MSS=1460 SACK_PER…
3	129.94.5.93	54.80.211.35	0.216205	66	TCP	3975 → 3478 [ACK] Seq=1338108853 Ack=2019859576 Win=5840 Len=0 TSval=226583 TSecr=241…
4	129.94.5.93	54.80.211.35	0.218240	114	STUN	Allocate Request TCP
5	54.80.211.35	129.94.5.93	0.433161	66	TCP	3478 → 3975 [ACK] Seq=2019859576 Ack=1338108901 Win=5888 Len=0 TSval=2417762848 TSecr…
6	54.80.211.35	129.94.5.93	0.433395	206	STUN	Allocate Error Response error-code: 401 (Unauthorized) Unauthorized realm: belkin.org…
7	129.94.5.93	54.80.211.35	0.434684	66	TCP	3975 → 3478 [ACK] Seq=1338108901 Ack=2019859716 Win=5840 Len=0 TSval=226638 TSecr=241…
8	129.94.5.93	54.80.211.35	0.437236	222	STUN	Allocate Request TCP user: EC1A59A18590 realm: belkin.org with nonce
9	54.80.211.35	129.94.5.93	0.691627	66	TCP	3478 → 3975 [ACK] Seq=2019859716 Ack=1338109057 Win=6912 Len=0 TSval=2417763107 TSecr…
10	54.80.211.35	129.94.5.93	0.711145	170	STUN	Allocate Success Response XOR-RELAYED-ADDRESS: 10.239.15.164:14458 lifetime: 330 XOR-…
11	129.94.5.93	54.80.211.35	0.750116	66	TCP	3975 → 3478 [ACK] Seq=1338109057 Ack=2019859820 Win=5840 Len=0 TSval=226717 TSecr=241…

Amazon Key…

- Theory – Deliveryman uses a private “key” to open the door to deliver package and the event is recorded to the cloud
  - **Amazon Key uses a smart lock from Yale or Kwikset**, plus an Amazon Cloud Cam security camera. Couriers can enter the property after scanning a barcode, which is checked against Amazon's own records in the cloud to make sure that they're in the right place at the right time. The camera also records the delivery
- Exploits –
  - https://www.theinquirer.net/inquirer/news/3021294/amazon-key-flaw-could-let-rogue-couriers-enter-your-home

Amazon Key Exploit - Deauthentication Flood

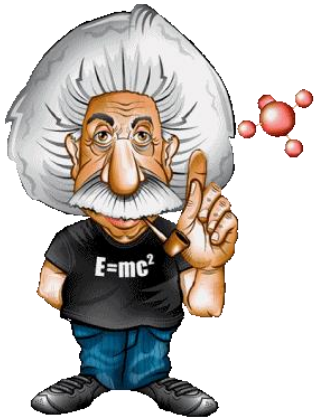
Attack - DeAuthentication Attack (WideOpen) 1.apc [Phill's Magical Mystery Machine - Wireless Configuration]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + 802.11 Be

No.	Source	Destination	Size	Protocol	Channel	Info
10	Proxim_4f:39:07	Broadcast	30	802.11	6	Deauthentication, SN=2622, FN=0, Flags=....
11	Proxim_4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=2079, FN=0, Flags=....
12	MitronCo_6e:19:45	Broadcast	30	802.11	6	Deauthentication, SN=870, FN=4, Flags=.....
13	Proxim_4f:39:07	Broadcast	30	802.11	6	Deauthentication, SN=577, FN=0, Flags=.....
14	DaystarD_4b:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=612, FN=0, Flags=.....
15	Proxim_4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=579, FN=0, Flags=.....
16	MitronCo_6e:19:45	Broadcast	30	802.11	6	Deauthentication, SN=1128, FN=1, Flags=....
17	Proxim_4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=581, FN=0, Flags=.....
18	Proxim_4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=2630, FN=0, Flags=....
19	22:21:a6:6d:1a:06	Broadcast	30	802.11	6	Deauthentication, SN=2217, FN=9, Flags=....
20	Proxim_4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=584, FN=0, Flags=.....
21	Proxim_4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=585, FN=0, Flags=.....
22	80:68:a6:4f:1b:06	Broadcast	30	802.11	6	Deauthentication, SN=586, FN=0, Flags=.....

Case Study: From the Real World*



A Minnesota hacker prosecutors described as a "depraved criminal" was handed an 18-year prison term Tuesday for unleashing a vendetta of cyber terror that turned his neighbors' lives into a living nightmare.

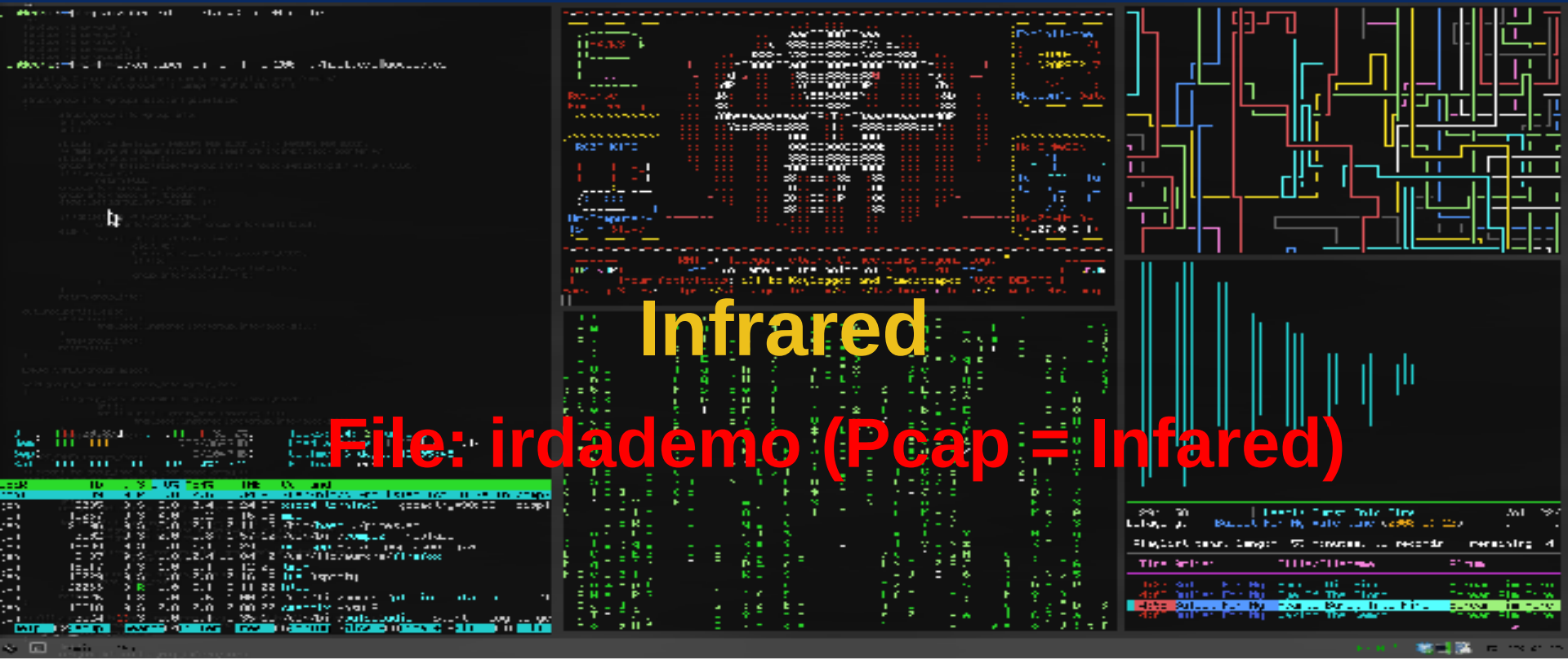
Barry Ardolf, 46, repeatedly hacked into his next-door neighbors' Wi-Fi network in 2009, and used it to try and frame them for child pornography, sexual harassment, various kinds of professional misconduct and to send threatening e-mail to politicians, including Vice President Joe Biden.

His motive was to get back at his new neighbors after they told the police he'd kissed their 4-year-old son on the lips. "Barry Ardolf has demonstrated by his conduct that he is a dangerous man.

When he became angry at his neighbors, he vented his anger in a bizarre and calculated campaign of terror against them," prosecutor Timothy Rank said in a court filing. "And he did not wage this campaign in the light of day, but rather used his computer hacking skills to strike at his victims while hiding in the shadows.

*SecNews 27Jul11

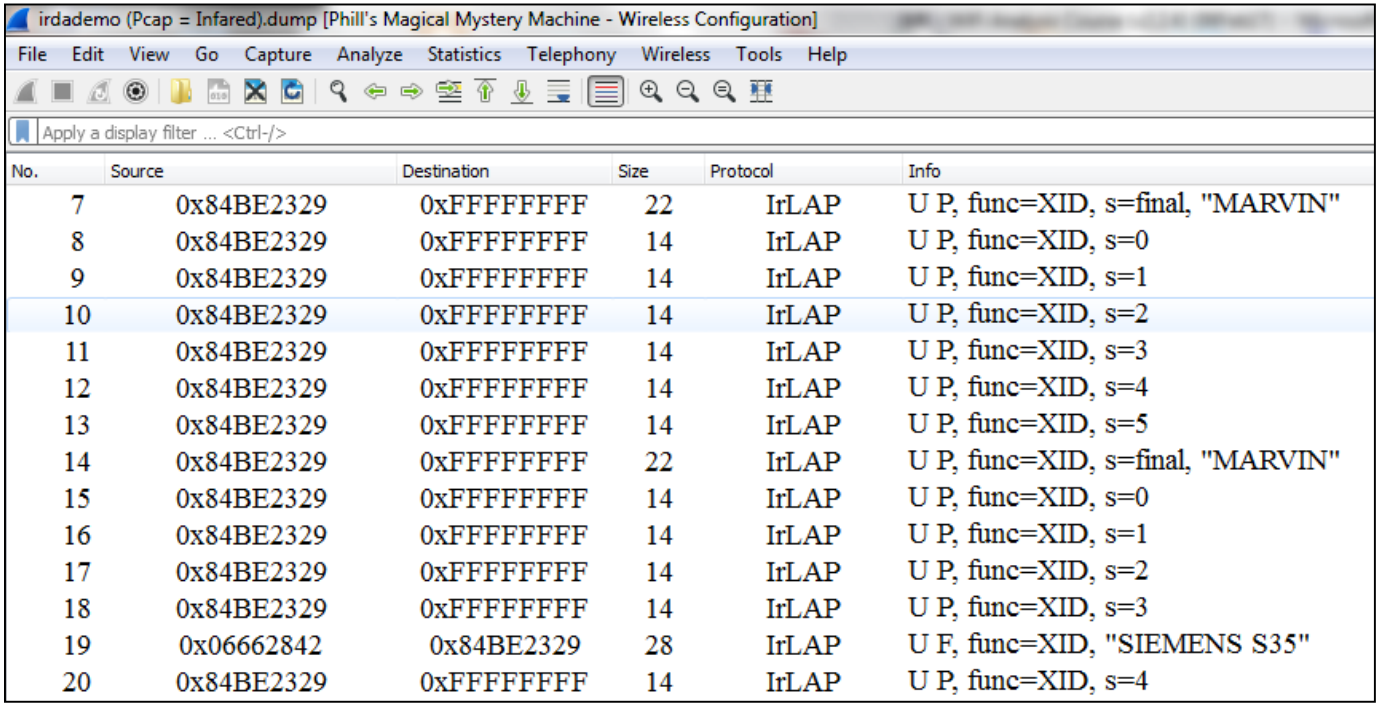
IoT Forensics Case Study #5 -



Infrared Overview

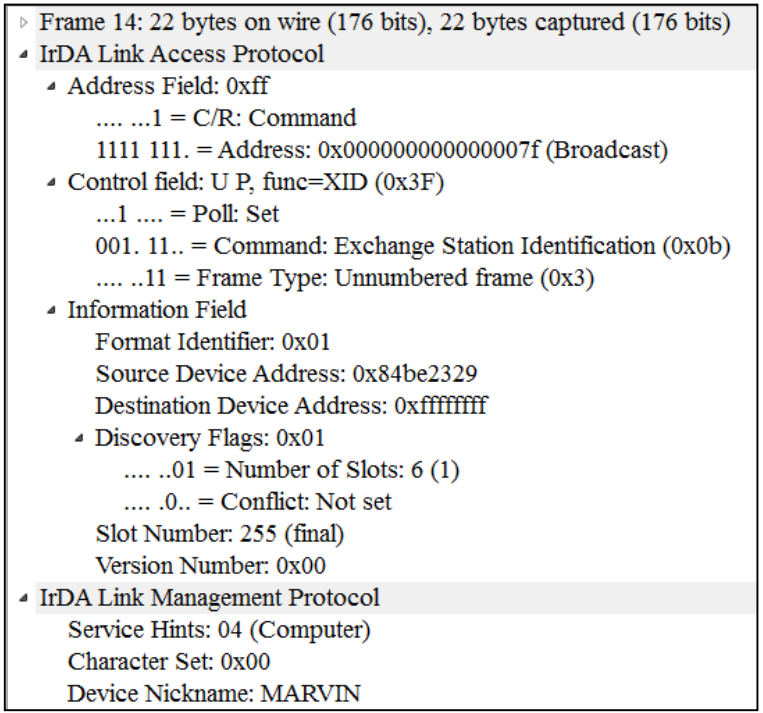
- **I**nfra **R**ed – **L**ocal **A**rea **N**etwork (IR-LAN)
  - Developed by the **I**nfra**r**ed **D**ata **A**ssociation (IrDA)
- Defined in IEEE 802.11
  - CSMA / CA data rate: 115 kb/s – 4 Mb/s (Transmit power limited to 2mw)
- Designed for use with small form factor, low power, low latency devices
  - Used in small or PAN type networks
    - Connected in P2P

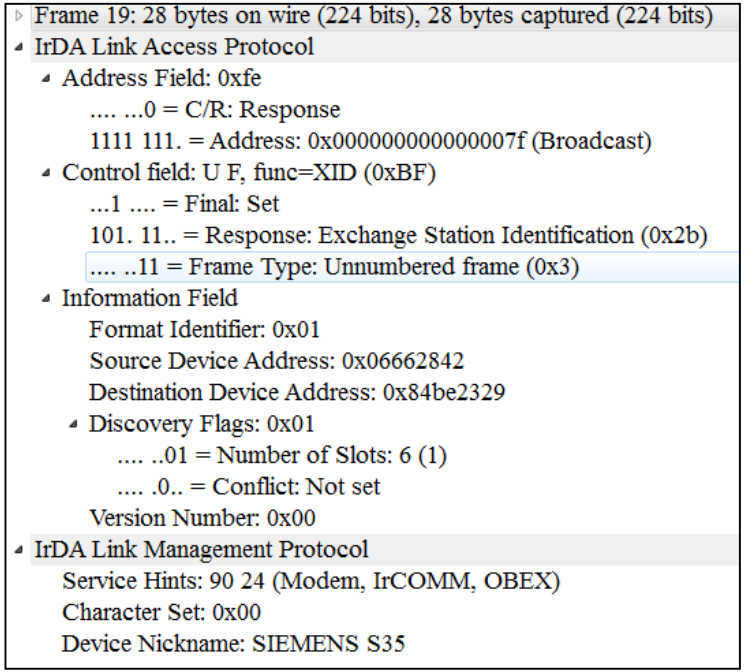
Sample Infrared Capture



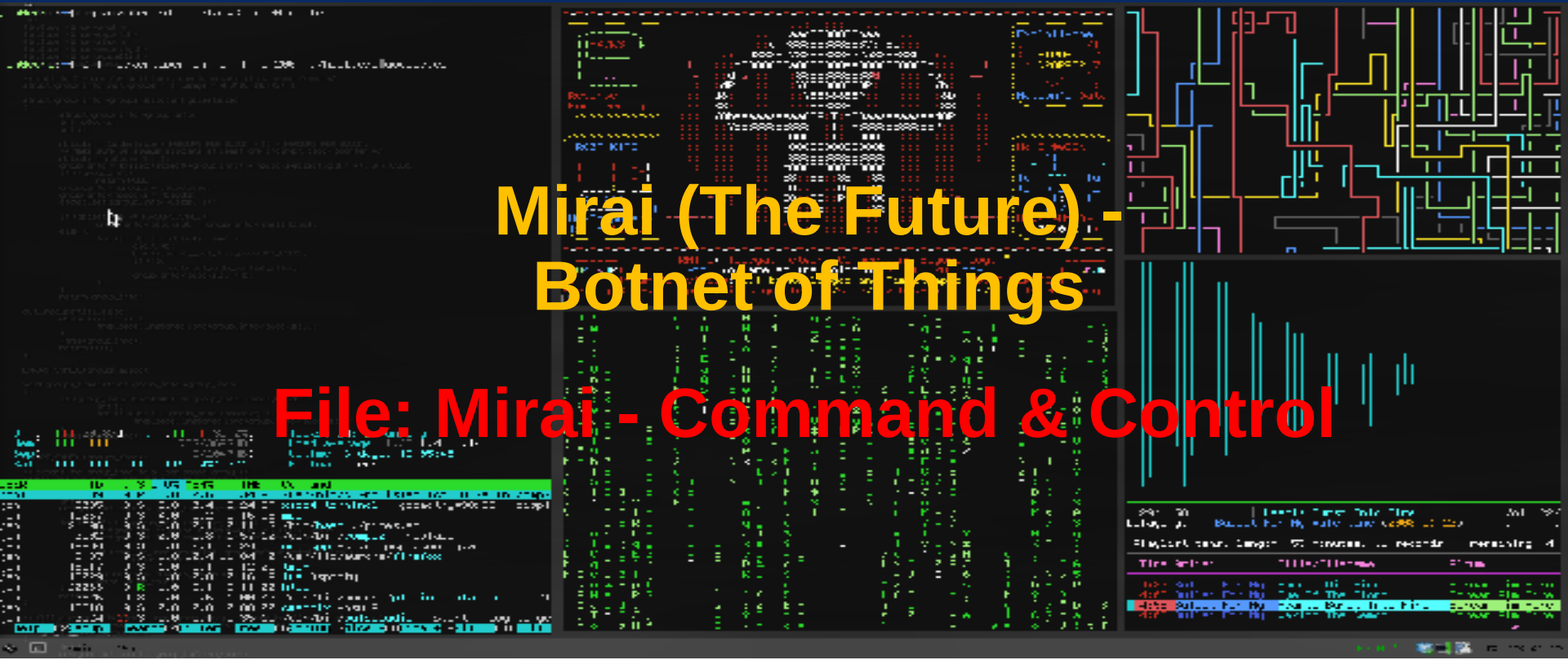
No.	Source	Destination	Size	Protocol	Info
7	0x84BE2329	0xFFFFFFFF	22	IrLAP	U P, func=XID, s=final, "MARVIN"
8	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=0
9	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=1
10	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=2
11	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=3
12	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=4
13	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=5
14	0x84BE2329	0xFFFFFFFF	22	IrLAP	U P, func=XID, s=final, "MARVIN"
15	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=0
16	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=1
17	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=2
18	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=3
19	0x06662842	0x84BE2329	28	IrLAP	U F, func=XID, "SIEMENS S35"
20	0x84BE2329	0xFFFFFFFF	14	IrLAP	U P, func=XID, s=4

Infrared Capture Details





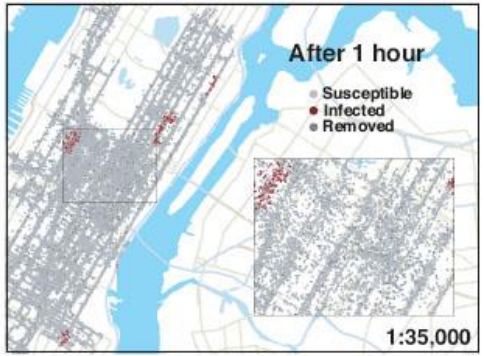
IoT Forensics Case Study #6 -



Mirai (The Future) - Botnet of Things

File: Mirai - Command & Control

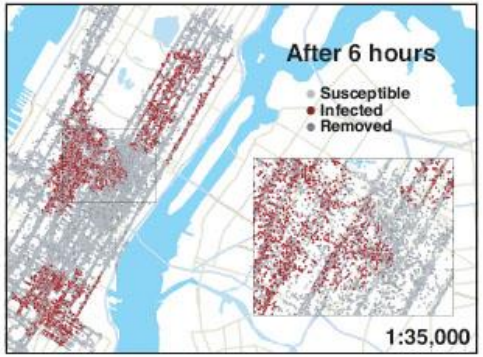
Bots & Botnets – How Fast Do They Spread?

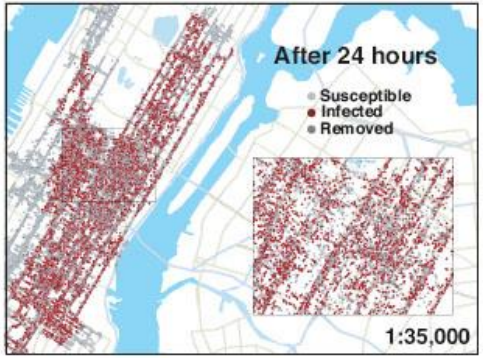


WiFi Networks and Malware Epidemiology

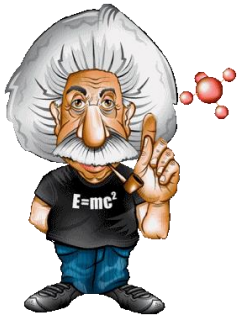
Hao Hua, Steven Myers, Vittoria Colizzac, and Alessandro Vespignani

Illustration of the spread of a worm through Manhattan in several time slices.





Mirai Bot Network Details



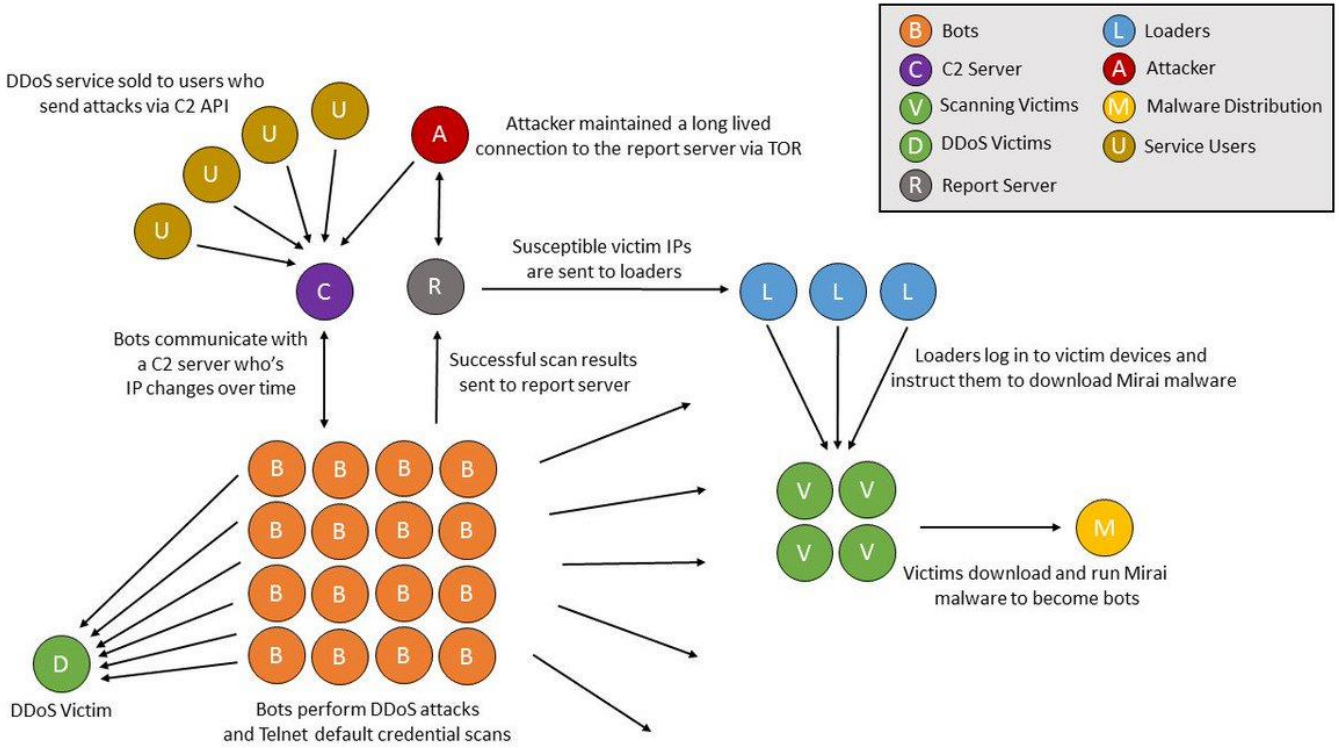
Mirai botnet seeks out poorly secured Internet of Things (IoT) devices

Primarily targets online consumer devices such as IP cameras, home routers and medical equipment

In October 2016, a massive DDoS attack target portions of the DNS architecture in the United States; in particular DYN

10.5 million Mirai-powered TCP SYN floods, peaking at 280 Gbps / 130 Mpps

Mirai Mechanism Mechanic's



Compromise Mechanism – Brute Force

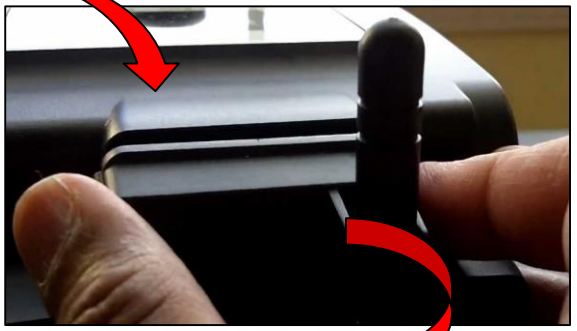
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Sample Mirai Command / Control

No.	Source	Destination	Length	Protocol	Info
1	10.16.0.5	10.16.0.100	74	TCP	54650 → 23 [SYN] Seq=2031964219 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=136171 TSecr
2	10.16.0.100	10.16.0.5	74	TCP	23 → 54650 [SYN, ACK] Seq=3643247368 Ack=2031964220 Win=28960 Len=0 MSS=1460 SACK_PERM
3	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964220 Ack=3643247369 Win=29312 Len=0 TSval=136171 TSecr=998715
4	10.16.0.5	10.16.0.100	70	TELNET	Telnet Data ...
5	10.16.0.100	10.16.0.5	66	TCP	23 → 54650 [ACK] Seq=3643247369 Ack=2031964224 Win=28992 Len=0 TSval=998715 TSecr=136171
6	10.16.0.5	10.16.0.100	67	TELNET	Telnet Data ...
7	10.16.0.100	10.16.0.5	66	TCP	23 → 54650 [ACK] Seq=3643247369 Ack=2031964225 Win=28992 Len=0 TSval=998715 TSecr=136171
8	10.16.0.5	10.16.0.100	68	TELNET	Telnet Data ...
9	10.16.0.100	10.16.0.5	66	TCP	23 → 54650 [ACK] Seq=3643247369 Ack=2031964227 Win=28992 Len=0 TSval=1001217 TSecr=138674
10	10.16.0.100	10.16.0.5	68	TELNET	Telnet Data ...
11	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964227 Ack=3643247371 Win=29312 Len=0 TSval=138674 TSecr=1001217
12	10.16.0.5	10.16.0.100	68	TELNET	Telnet Data ...
13	10.16.0.100	10.16.0.5	68	TELNET	Telnet Data ...
14	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964229 Ack=3643247373 Win=29312 Len=0 TSval=153690 TSecr=1016233
15	10.16.0.5	10.16.0.100	68	TELNET	Telnet Data ...
16	10.16.0.100	10.16.0.5	68	TELNET	Telnet Data ...
17	10.16.0.5	10.16.0.100	66	TCP	54650 → 23 [ACK] Seq=2031964231 Ack=3643247375 Win=29312 Len=0 TSval=168704 TSecr=1031248

Mac address: 08:00:27 Vendor: PcsCompu PCS Computer Systems GmbH

Here was the Device…



ResMed S9 Wireless Module

Mirai TCP SYN Attack (1)

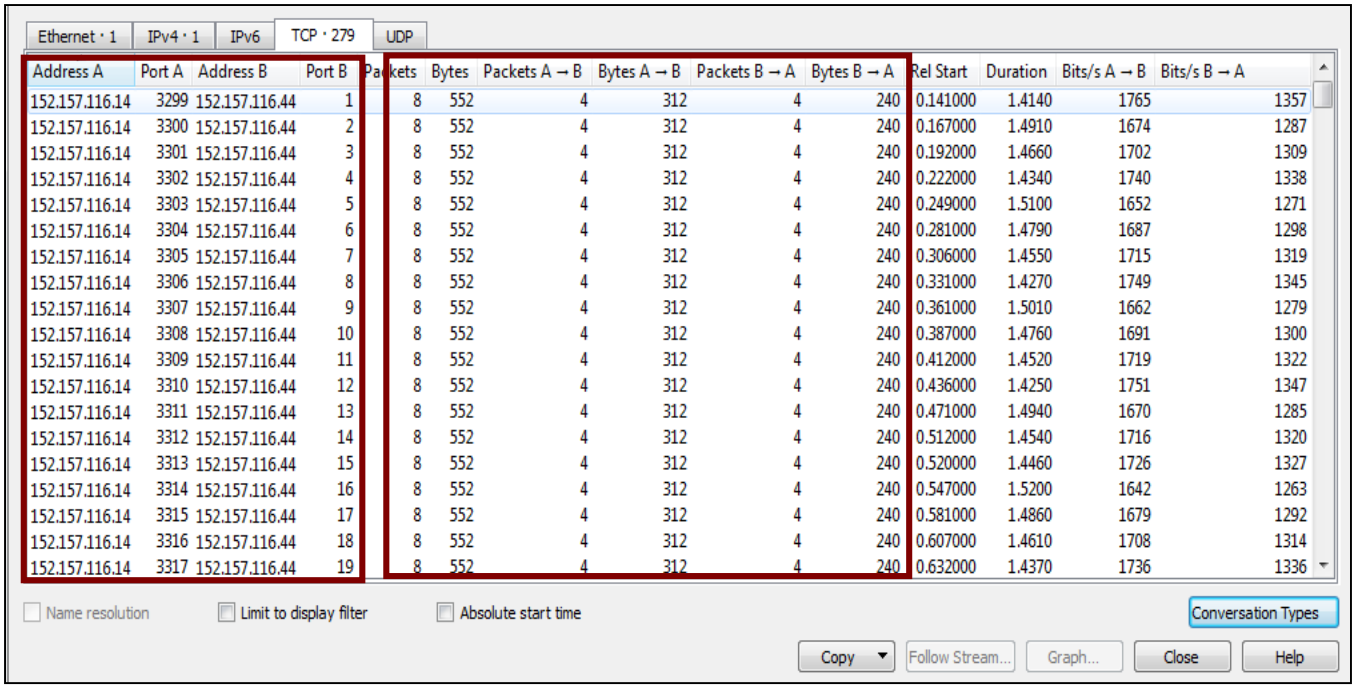
#1

	Source	Destination	Protocol	Info
1	10.8.0.184	10.8.0.131	TCP	2997 > http [SYN] Seq=0 Len=0 MSS=1460
2	10.8.0.184	10.8.0.131	TCP	2998 > http [SYN] Seq=0 Len=0 MSS=1460
3	10.8.0.184	10.8.0.131	TCP	2999 > http [SYN] Seq=0 Len=0 MSS=1460
4	10.8.0.184	10.8.0.131	TCP	3000 > http [SYN] Seq=0 Len=0 MSS=1460
5	10.8.0.184	10.8.0.131	TCP	3001 > http [SYN] Seq=0 Len=0 MSS=1460
6	10.8.0.184	10.8.0.131	TCP	3002 > http [SYN] Seq=0 Len=0 MSS=1460
7	10.8.0.184	10.8.0.131	TCP	3003 > http [SYN] Seq=0 Len=0 MSS=1460
8	10.8.0.184	10.8.0.131	TCP	3004 > http [SYN] Seq=0 Len=0 MSS=1460
9	10.8.0.184	10.8.0.131	TCP	3005 > http [SYN] Seq=0 Len=0 MSS=1460
10	10.8.0.184	10.8.0.131	TCP	3006 > http [SYN] Seq=0 Len=0 MSS=1460
11	10.8.0.184	10.8.0.131	TCP	3007 > http [SYN] Seq=0 Len=0 MSS=1460
12	10.8.0.184	10.8.0.131	TCP	3008 > http [SYN] Seq=0 Len=0 MSS=1460
13	10.8.0.184	10.8.0.131	TCP	3009 > http [SYN] Seq=0 Len=0 MSS=1460
14	10.8.0.184	10.8.0.131	TCP	3010 > http [SYN] Seq=0 Len=0 MSS=1460
15	10.8.0.184	10.8.0.131	TCP	3011 > http [SYN] Seq=0 Len=0 MSS=1460
16	10.8.0.184	10.8.0.131	TCP	3012 > http [SYN] Seq=0 Len=0 MSS=1460
17	10.8.0.184	10.8.0.131	TCP	3013 > http [SYN] Seq=0 Len=0 MSS=1460
18	10.8.0.184	10.8.0.131	TCP	3014 > http [SYN] Seq=0 Len=0 MSS=1460

#2

	Source	Destination	Protocol	Info
1	152.157.116.14	152.157.116.44	ICMP	Echo (ping) request
2	152.157.116.44	152.157.116.14	ICMP	Echo (ping) reply
3	152.157.116.14	152.157.116.44	TCP	3299 > 1 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
4	152.157.116.44	152.157.116.14	TCP	1 > 3299 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
5	152.157.116.14	152.157.116.44	TCP	3300 > 2 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
6	152.157.116.44	152.157.116.14	TCP	2 > 3300 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
7	152.157.116.14	152.157.116.44	TCP	3301 > 3 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
8	152.157.116.44	152.157.116.14	TCP	3 > 3301 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
9	152.157.116.14	152.157.116.44	TCP	3302 > 4 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
10	152.157.116.44	152.157.116.14	TCP	4 > 3302 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
11	152.157.116.14	152.157.116.44	TCP	3303 > 5 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
12	152.157.116.44	152.157.116.14	TCP	5 > 3303 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
13	152.157.116.14	152.157.116.44	TCP	3304 > 6 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
14	152.157.116.44	152.157.116.14	TCP	6 > 3304 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
15	152.157.116.14	152.157.116.44	TCP	3305 > echo [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
16	152.157.116.44	152.157.116.14	TCP	echo > 3305 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
17	152.157.116.14	152.157.116.44	TCP	3306 > 8 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
18	152.157.116.44	152.157.116.14	TCP	8 > 3306 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0

Mirai TCP SYN Attack (2)



Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 279 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
152.157.116.14	3299	152.157.116.44	1	8	552	4	312	4	240	0.141000	1.4140	1765	1357
152.157.116.14	3300	152.157.116.44	2	8	552	4	312	4	240	0.167000	1.4910	1674	1287
152.157.116.14	3301	152.157.116.44	3	8	552	4	312	4	240	0.192000	1.4660	1702	1309
152.157.116.14	3302	152.157.116.44	4	8	552	4	312	4	240	0.222000	1.4340	1740	1338
152.157.116.14	3303	152.157.116.44	5	8	552	4	312	4	240	0.249000	1.5100	1652	1271
152.157.116.14	3304	152.157.116.44	6	8	552	4	312	4	240	0.281000	1.4790	1687	1298
152.157.116.14	3305	152.157.116.44	7	8	552	4	312	4	240	0.306000	1.4550	1715	1319
152.157.116.14	3306	152.157.116.44	8	8	552	4	312	4	240	0.331000	1.4270	1749	1345
152.157.116.14	3307	152.157.116.44	9	8	552	4	312	4	240	0.361000	1.5010	1662	1279
152.157.116.14	3308	152.157.116.44	10	8	552	4	312	4	240	0.387000	1.4760	1691	1300
152.157.116.14	3309	152.157.116.44	11	8	552	4	312	4	240	0.412000	1.4520	1719	1322
152.157.116.14	3310	152.157.116.44	12	8	552	4	312	4	240	0.436000	1.4250	1751	1347
152.157.116.14	3311	152.157.116.44	13	8	552	4	312	4	240	0.471000	1.4940	1670	1285
152.157.116.14	3312	152.157.116.44	14	8	552	4	312	4	240	0.512000	1.4540	1716	1320
152.157.116.14	3313	152.157.116.44	15	8	552	4	312	4	240	0.520000	1.4460	1726	1327
152.157.116.14	3314	152.157.116.44	16	8	552	4	312	4	240	0.547000	1.5200	1642	1263
152.157.116.14	3315	152.157.116.44	17	8	552	4	312	4	240	0.581000	1.4860	1679	1292
152.157.116.14	3316	152.157.116.44	18	8	552	4	312	4	240	0.607000	1.4610	1708	1314
152.157.116.14	3317	152.157.116.44	19	8	552	4	312	4	240	0.632000	1.4370	1736	1336

Name resolution | Limit to display filter | Absolute start time | Conversation Types

Copy | Follow Stream... | Graph... | Close | Help

The Result…

Unfortunately…

Mirai was Only the First

Name	Dates	Size / Nodes	Notes
Mirai (The Future)	October 2016	10.5 – 14 Million	IoT-based
Star Wars	January 2018	350,000 +	Twitter-based
Hajime (Beginning)	October 2016 – April 2017	300,000 +	IoT-based / Anti-Mirai features
WireX	August 2017 - ???	Unknown (Large)	Android-based
Reaper	September 2017	100,000 +	IoT-based / IP Cameras
Satori (Awakening)	December 2017	280,000 +	IoT-based
Torii	September 2018	3,000,000 +	IoT – Telnet Based / FTP / SSL

One Last Thought…

A Final Example…

Questions & Answers
Discussion

Instructor Contact Information

Phill Shade: phill.shade@gmail.com

LinkedIn: Phill “Sherlock” Shade

Merlion’s Keep Consulting: merlions.keep@gmail.com

International: info@cybersecurityinstitute.eu

Merlion’s Keep Consulting & Training

Packets Never Lie


LOUNGE BAR
Thank You!