Network Forensic Case Studies –

Those Who Don't Learn from the Past are Doomed to Repeat It

Phill “Sherlock” Shade
Merlion’s Keep Consulting & SCOS.NL

phill.shade@gmail.com
Phillip “Sherlock” Shade (Phil)

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

I’m Here to Help… Really
From the Headlines (last 10 Days)

- ‘Creepware’ was used to spy on Miss Teen USA
- More than 1100 people have been arrested in a global takedown of ransomware linked to the BlackBads software, officials say. The malware was used to spy on Celeste Wold, Miss Teen USA. FULL STORY
- Inside FBI’s massive cybercrime battle (Bobby Owen: I was impressed)

EA: Gaming giant hacked and source code stolen

Peloton fixes flaw on bikes that could have let bad actors access tablets

A vulnerability would have allowed hackers to gain control of the bike’s camera and mic, among other things.

Volkswagen says a vendor’s security lapse exposed 3.3 million drivers’ details

Fugitive Anonymous Hacker ‘Commander X’ Arrested, Extradited From Mexico

Over a billion records belonging to CVS Health exposed online

The exposure is another example of misconfiguration that can impact security.

Inside the Market for Cookies That Lets Hackers Pretend to Be You

A representative for the hackers who breached EA said they bought the cookie from a site called Geopolis Market.
Welcome to my World….

Today’s Agenda

1. The Unforeseen Threat - UPNP
2. Buy Your Own Destruction - IoT & Exploits
3. You Expect me to Pay? - Ransomware
4. The Future of Botnets
5. Attacking from the Inside Man-in-the-Middle
6. Application Attacks - Web & Email
Troubleshooting vs. Forensics

Troubleshooting Questions
1. What is the cause of my performance issue?
2. How do I locate and resolve the performance issue?

Forensics Questions
1. What Damage has been Done?
2. Who was the intruder and how did they penetrate the existing security precautions?
3. Did the intruder leave anything such as a new user account, or perhaps some new type of Malware behind?
4. Is there sufficient data to analyze & reproduce the attack and verify the fix will work?
For This to Work - Normal or Abnormal?

### Forensics Analysis Tip:
Be familiar with the expected or Baseline behavior of protocols before trying to identify suspect behavior!
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
- 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
Forensics Case Study #1 – To Get Your Attention

UPNP
(Hiding in Plain Sight)

File: MK - Baseline - UPNP - HTTP Modify & Notify
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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Datagram Protocol</td>
<td>1900 (1900)</td>
<td>1900 (1900)</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol</td>
<td>50993 (50993)</td>
<td>1900 (1900)</td>
</tr>
</tbody>
</table>

**Notify & Search**

#### HTTP/1.1

- **Host**: 239.255.255.250:1900
- **NT**: urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
- **NTS**: ssdp:alive
- **Location**: http://192.168.29.129:2869/upnphost/udhisapi.dll?content=uuid:72d0d11-9361-46aa-8f42-bd4a5c94840d
- **USN**: uuid:72d0d11-9361-46aa-8f42-bd4a5c94840d:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
- **Cache-Control**: max-age=900
- **Server**: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
- **OPT**: "http://schemas.upnp.org/upnp/1/0/"; ns=0
- **01-NLS**: e2732ce167a1bfc60898911c8761771

---

**M-SEARCH**

- **HOST**: 239.255.255.250:1900
- **MAN**: "ssdp:discover"
- **MX**: 5
- **ST**: urn:schemas-upnp-org:device:MediaServer:1

[Full request URI: http://239.255.255.250:1900]

[HTTP request 8/8]

[Prev request in frame: 1541]
Buy Your Own Destruction – IoT Technologies & Exploits

File: Philips Hue Idle v2
How Many of You Have at Least one of These?
Small Office / Home Office (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)
It’s Getting Worse…

There are A LOT of Vulnerabilities

Monthly volume of published CVEs from 1999 through 2019

120,000+
Published vulns

Source: Kenna / Cyentia

#sf21veu • 16 -18 June 2021
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

• **Wireless Personal Area Networks (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
  • 3 variable power settings
    • 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
Bluetooth Pcap

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>153082 controller</td>
<td>host</td>
<td>HCI_EVT</td>
<td>Rcvd Number of Completed</td>
</tr>
<tr>
<td>153083</td>
<td>host</td>
<td>USB</td>
<td>URB_INTERRUPT in</td>
</tr>
<tr>
<td>153085</td>
<td>host</td>
<td>USB</td>
<td>URB_BULK in</td>
</tr>
<tr>
<td>153086 NokiaDan_15:a2:c7</td>
<td>Integrat_55:90:80 (Nagasaki)</td>
<td>RFCOMM</td>
<td>Rcvd SABM Channel=0</td>
</tr>
<tr>
<td>153087</td>
<td>host</td>
<td>USB</td>
<td>URB_BULK out</td>
</tr>
<tr>
<td>153088 Integrat_55:90:80</td>
<td>NokiaDan_15:a2:c7 (GenkiDesu)</td>
<td>RFCOMM</td>
<td>Sent UIH Channel=0</td>
</tr>
<tr>
<td>153089</td>
<td>6.5.2</td>
<td>USB</td>
<td></td>
</tr>
<tr>
<td>153090</td>
<td>controller</td>
<td>HCI_EVT</td>
<td>Rcvd Number of Completed Pack</td>
</tr>
<tr>
<td>153091</td>
<td>host</td>
<td>USB</td>
<td>URB_INTERRUPT in</td>
</tr>
<tr>
<td>153092 NokiaDan_15:a2:c7</td>
<td>Integrat_55:90:80 (Nagasaki)</td>
<td>RFCOMM</td>
<td>Rcvd UIH Channel=0 -&gt; 9 MPX</td>
</tr>
<tr>
<td>153093</td>
<td>host</td>
<td>USB</td>
<td>URB_BULK in</td>
</tr>
<tr>
<td>153094 Integrat_55:90:80</td>
<td>NokiaDan_15:a2:c7 (GenkiDesu)</td>
<td>RFCOMM</td>
<td>Sent UIH Channel=0 -&gt; 9 MPX</td>
</tr>
<tr>
<td>153095</td>
<td>6.5.2</td>
<td>USB</td>
<td>URB_BULK out</td>
</tr>
<tr>
<td>153096 controller</td>
<td>host</td>
<td>HCI_EVT</td>
<td>Rcvd Number of Completed Pack</td>
</tr>
</tbody>
</table>
Withing's 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
Bluetooth Exploit – Tesla’s
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
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</manufacturerURL>
<modelDescription>Philips hue Personal Wireless Lighting</modelDescription>
<modelName>Philips hue bridge 2012</modelName>
<modelNumber>929000226503</modelNumber>
<modelURL>http://www.meethue.com/modelURL</modelURL>
<serialNumber>0017881892ca</serialNumber>
<UDN>uuid:2f402f80-da50-11e1-9b23-0017881892ca</UDN>
<serviceList>
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…

#sf21veu • 16 -18 June 2021
WiFi Connected Printer Exploit
Forensics Case Study #3 - You Expect me to Pay? - Ransomware

Not How You Want to Start Your Day...

**File hijacker - 192.168.112.30**

**MIGHTYMUSE**

**ATTENTION!**

Warning! Please take your time to read the following text for your own best. Your computer has basically been hijacked, and your private files stored on your computer has now been encrypted, which means that they are impossible to access, and can only be decrypted/restored by us.

Now, it's your decision to choose whether to ignore this, or follow the easy instructions:

Please settle X USD

IBAN: XX27 0040 0168 0000 0178 2101 XXXX
SWIFT: XX XX XXXXXXXX
Account: IBAN506010000000226-1000
Name: Somename Surname
City: Somocity

Reference: Blackshades (Note, this key may be included as a message or reference for future steps orรางted.

**Help:**
- Read the help section if this is your first time using the application.
- Background color: White

**Settings:**
- Encryption key: Blackshades_key
- Display duration: 3000 sec
- Target path: [Path]

[Image of a computer screen with a warning message and a character with a laptop and code]

#sf21veu • 16 - 18 June 2021
Sample Web-Based Exploit

Malicious Code Decoded:

```javascript
<script src="javascript:alert('Malware!');"></script>
```

Malicious Code Encoded:

```
//Encoded malicious code
```

---

**One:** Our league is an organization against www.google.com treating large-scale net friends and the heads of station unfair. The purpose of our league is to collect the unfair proof and supervise google company to go to fair.

**Two:** The league is organized by net friends spontaneously, our league isn’t controlled and assisted by any organizations or companies at home and in abroad.

**Three:** Users want to join in our league must obey our country law, illegal, etoticism, virus and so on are prohibited in our league.
They got Me – What do I Do?

Forensics Case Study #4 - The Future of Botnets

File: Mirai - Command & Control
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
### Sample Mirai Command / Control

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

Mac address: 08:00:27 Vendor: PcsCompu PCS Computer Systems GmbH
Authors Personal Experience with Mirai

ResMed S9 Wireless Module
## Mirai TCP SYN Attack (I)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>2997 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>2 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>2999 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>3 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3000 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>4 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3002 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>5 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3004 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>6 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3006 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>7 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3008 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>8 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3010 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>9 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3012 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
<tr>
<td>10 10.8.0.184</td>
<td>10.8.0.131</td>
<td>TCP</td>
<td>3013 &gt; [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
</tbody>
</table>

---

## Source 1: 152.157.116.14

<table>
<thead>
<tr>
<th>Source 1</th>
<th>Destination 1</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 152.157.116.14</td>
<td>152.157.116.14</td>
<td>ICMP</td>
<td>echo (ping) request</td>
</tr>
<tr>
<td>2 152.157.116.14</td>
<td>152.157.116.14</td>
<td>ICMP</td>
<td>echo (ping) reply</td>
</tr>
<tr>
<td>5 152.157.116.14</td>
<td>152.157.116.14</td>
<td>TCP</td>
<td>3302 &gt; 3 [SYN] Seq=0 Len=0 MSS=1460</td>
</tr>
</tbody>
</table>

---

## Source 2: 3305 > echo [SYN] Seq=0 Len=0 MSS=1460
# Mirai TCP SYN Attack (2)

<table>
<thead>
<tr>
<th>Address A</th>
<th>Address B</th>
<th>Port A</th>
<th>Port B</th>
<th>Packets</th>
<th>Bytes</th>
<th>Bytes A-B</th>
<th>Bytes B</th>
<th>Bytes B-A</th>
<th>Red Start</th>
<th>Duration</th>
<th>Bits/s A-B</th>
<th>Bits/s B-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>210</td>
<td>0.14000</td>
<td>1.4140</td>
<td>1765</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>2</td>
<td>2</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.15000</td>
<td>1.4110</td>
<td>1674</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.19200</td>
<td>1.4660</td>
<td>1702</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.22000</td>
<td>1.4340</td>
<td>1740</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>5</td>
<td>5</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.24000</td>
<td>1.5100</td>
<td>1652</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.28100</td>
<td>1.4750</td>
<td>1687</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.30600</td>
<td>1.4530</td>
<td>1713</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.33100</td>
<td>1.4270</td>
<td>1749</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>9</td>
<td>9</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.36100</td>
<td>1.5010</td>
<td>1662</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.38700</td>
<td>1.4760</td>
<td>1691</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>11</td>
<td>11</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.41200</td>
<td>1.4520</td>
<td>1719</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>12</td>
<td>12</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.43600</td>
<td>1.4250</td>
<td>1751</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>13</td>
<td>13</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.47100</td>
<td>1.4940</td>
<td>1670</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>14</td>
<td>14</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.51200</td>
<td>1.4540</td>
<td>1716</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>15</td>
<td>15</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.52000</td>
<td>1.4460</td>
<td>1726</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>16</td>
<td>16</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.54700</td>
<td>1.5200</td>
<td>1642</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>17</td>
<td>17</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.58100</td>
<td>1.4880</td>
<td>1679</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>18</td>
<td>18</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.60700</td>
<td>1.4610</td>
<td>1708</td>
</tr>
<tr>
<td>152.157.116.14</td>
<td>152.157.116.44</td>
<td>19</td>
<td>19</td>
<td>8</td>
<td>552</td>
<td>4</td>
<td>312</td>
<td>4</td>
<td>240</td>
<td>0.62200</td>
<td>1.4370</td>
<td>1736</td>
</tr>
</tbody>
</table>
The Result...

Sorry NO
INTERNET Today
Unfortunately…

Mirai Still Reigns Supreme, but…

- Mirai variants in the wild increased significantly at the start of the COVID-19 pandemic (right).
- Attackers are still leveraging the same username and password combos with Mirai and many of the same exploits (below).
## Mirai was Only the First

<table>
<thead>
<tr>
<th>Name</th>
<th>Dates</th>
<th>Size / Nodes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirai (The Future)</td>
<td>October 2016</td>
<td>10.5 – 14 Million</td>
<td>IoT-based</td>
</tr>
<tr>
<td>Star Wars</td>
<td>January 2018</td>
<td>350,000 +</td>
<td>Twitter-based</td>
</tr>
<tr>
<td>Hajime (Beginning)</td>
<td>October 2016 – April 2017</td>
<td>300,000 +</td>
<td>IoT-based / Anti-Mirai features</td>
</tr>
<tr>
<td>WireX</td>
<td>August 2017 - ??</td>
<td>Unknown (Large)</td>
<td>Android-based</td>
</tr>
<tr>
<td>Reaper</td>
<td>September 2017</td>
<td>100,000 +</td>
<td>IoT-based / IP Cameras</td>
</tr>
<tr>
<td>Satori (Awakening)</td>
<td>December 2017</td>
<td>280,000 +</td>
<td>IoT-based</td>
</tr>
<tr>
<td>Torii</td>
<td>September 2018</td>
<td>3,000,000 +</td>
<td>IoT – Telnet Based / FTP / SSL</td>
</tr>
</tbody>
</table>
Forensics Case Study #5 -

**Attacking from Within – Man-in-the-Middle**

*File:MK - Attack - Man in The Middle (Pri)*
Man-in-the-Middle Attack

Setting the Stage...

1. A major software vendor had been working on a key project for two years.
2. One week prior to product launch, a competitor trademarked the primary and secondary names for the product.
3. Company was forced to research, develop, and produce an entirely new marketing campaign, literature, and product documentation.
4. A forensics investigation aided by the company's data recorders revealed that the software company had been "Man-in-the-Middle" victimized.
5. Cost to company was in excess of $2,000,000 USD.
Anatomy of a Man-in-the-Middle Attack

• Attacker “insert” itself into a key location within the network
  • Originated within the early Ethernet community, returned with the advent of wide-spread Wi-Fi networking
    • Favorite of industrial espionage and banking attackers
  • It will then launch a diversionary attack such as the classic “ARP-poison” to trick the targeted systems into accepting it as the “true” Server / Gateway / Router / Client / etc..
• The targeted devices will now send their traffic to the intruder
  • Intruder can copy / reinsert / manipulate the traffic
MiTM Hardware Tools

WiFi Pineapple
2.4/5 GHz a/b/g/n
Power over USB Ethernet Port
Power over USB Serial Port

PwnPlug

WiFi Robber
$150.00
Scene of the Crime...
Forensic Reconstruction of the Crime...
ARP Poison in Progress

The device IntelCor_ac:b1:5e is attempting to trick the Projector (CiscoInc_cd-fe-do) into thinking it is the client while making the client (IntelCor_ac:b1:3e) think it is the Projector.
Results of the Investigation...

The results of the internal Forensic Investigation revealed several findings:

1. The original Wired Projector in the executive conference room had been replaced with an unauthorized WiFi model (that did not support any type of NAC or encryption)
2. Encryption was switched off on the presenters laptop to enable connecting to the WiFi projector
3. Rogue Access point was located outside conference room in a tree!
Forensics Case Study #6 - Application Attacks
Web & Email

FILE: MK - Virus - W32.SillyFDC (names.exe)
FILE: MK - Bot - Zeus-Sample-2 (OpenPacket)
**Compare and Contrast**

**Phishing** is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic Communication…. (Wikipedia)

**Spear-Phishing** is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. (WhatIs.com)
Office 365 and Google G Suite

- Cyber criminals are targeting organizations who use Microsoft Office 365 and Google G Suite to conduct Business E-mail Compromise scams.
  - Scams initiated through custom phishing kits mimicking cloud-based e-mail services.
  - Phishing kits deployed in large batches of e-mails to US organizations can identify the e-mail service associated with each set of compromised credentials.
  - Once accounts compromised, accounts analyzed to identify financial transactions.
  - Actors configure mailboxes to delete key messages or enable automatic forwarding to an outside e-mail account.

SolarWinds

- Malicious actors are exploiting SolarWinds Orion products containing SUNBURST malware to gain access to network traffic management systems.
- These actors pursued several objectives, including achieving full privileged persistent access through trusted legitimate credentials, accounts, and applications.
- These credentials are often leveraged from victim-dedicated IPs in the victim’s own country to avoid detection.
Is it Legitimate?
Sample Email Malware

```
HELO aim.com
MAIL FROM: <eslee_my@yahoo.com>
RCPT TO: <phillwood@philwoodgardens.com>
DATA
Received: from Haxx([218.22.178.116]) by aim.com (AIMC 2.9.5.6)
    with SMTP id jm3aas906177; Thu, 17 Apr 2003 09:24:41 +0800
From: au confirm <au.confirm@yoh.com>
To: phillwood@philwoodgardens.com
Subject: Let's be friends
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary=59D3767223343D3155151551
X-AIMC-AUTH: (null)
X-AIMC-MAILFROM: eslee_my@yahoo.com
Message-ID: <1k665829679555.907645@yoh>

--59D3767223343D3155151551
Content-Type: text/html;
    Content-Transfer-Encoding: quoted-printable

<HTML><HEAD></HEAD><BODY>
<iframe src="303c1605903194520fom height=300 width=300"></iframe>
</iframe>
</BODY></HTML>

--59D3767223343D3155151551
Content-Type: audio/x-midi;
    name=names.exe
Content-Transfer-Encoding: Base64
Content-ID: <8088831942af0fa3>
```

TvIGQAA==AAAgADAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
China Gmail Hack

- Google executives received an Email containing a PDF with an embedded link saying "Corporate Information – Google Management"
  - Clicking the link took them to a web page in Chinese – http://www.google.com/corporate/execs.html
  - Site purports to list Google's executives, including Eric Schmidt, Sergey Brin and Larry Page

- The site executed a “Drive-by” exploit that installed Trojan spyware on the victims computers
  - Compromised information included Identities of numerous Human-Rights activists using Gmail to evade Chinese security agencies

- Cost – not publically released, but numerous dissidents have reportedly “disappeared”
What They Saw…

Eric Schmidt

Larry Page

Sergey Brin
Example – Fake Login Screen

Fake Gmail login page
(ServiceLoginAuth.htm)

Sign in with your
Google Account

Username: 
Password:
Stay signed in
Sign in

Wrong password alert
(Alert pop up)

2. Victim ID is hardcoded in HTML

Wrong password alert
(red text)

Real Gmail login page
(ServiceLoginAuth.htm)

A Google approach to email.
Gmail is built on the idea that email can be more intuitive, efficient, and useful.

Login screen

Keep unstered messages out of your inbox with Gmail's innovative technology.

Mobile access

Get Gmail on your mobile phone by pointing your phone's web browser to
m.google.com.

Lots of space

Over 700 MB of storege (and counting) of free storage.

2010 and text

Icons & text

Some links are en_KR (Google in English for Korea)

Blue ribbon

Icons & text

2011 and text

All links are for Google USA

- 16 -18 June 2021
Web-Based Hijack Exploit: I
Web-Based Hijack Exploit: 2

Malicious Code Encoded:

```html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>

<script type="text/javascript" src="js/lib/jquery.js"></script>
<script type="text/javascript" src="js/lib/date.js"></script>
<script type="text/javascript" src="js/lib/fn.js"></script>
<script type="text/javascript" src="js/lib/flash/flashcontent.js"></script>

<!-- This script is needed for Flash -->
<script type="text/javascript">
var IE8_BugContent = 0;
</script>

<script type="text/javascript" src="js/main.js"></script>
</head>
<body>

How it Works:

1. Client visits the landing site
2. Redirect to get the exploit
3. Redirect to get the exploit
4. Download the malware executable

Kaspersky Lab

#sf21veu • 16 - 18 June 2021
Real World Event – Zeus Bot Network

- Zeus is a do-it-yourself kit that allows the creation of custom malware with a point and click interface

- In October 2010, a Zeus-bot network owned by “Kristina Svechinskaya” struck numerous major financial institutions principally in the U.S. and UK
  - Compromised accounts experienced a transaction “fee” of $0.99 (USD) during a 30-minute period
  - Cost is estimated to be in excess of $12.5 million (USD)
    - $3 million dollars from American banks and $9.5 million from UK banks
Sample Malware Download

This example contains a copy of the “Ribbon Worm” designed to install a remote back-door access point into the client machine.
“Kits” For Sale....

Hi everyone,

I am selling Zeus 1.3.0.0.

TRUSTED MEMBERS ONLY

[Version 1.3.0.0, 20.11.2009]

[*] Interception WinApi by splicing.

[*] Be fully operational in Windows Vista / 7.

[*] Temporarily disable hidden files, etc.

[*] Removed IM-grabber.

[-] Fixed duplicate records in nspad.dll.

[*] Grabbed certificates are now written with the name grabbed_dd_mm_yy.pfx, and password in UTF-8.

[*] Team gotten, obtained certificates only from My-store, and not from all. Since obtaining certificates from all hranish not make sense.

[*] Changed behavior grabber certificates.

[*] Rewrote FTP/POP3 sniffer, hashcash detection logins, mode support for IPv6-addresses.

[*] Rewrote the interception of keywords, fixed method of working with international characters to.

[-] Corrected a bug in HTTP-fake, which could lead to deadlock.

Price: $700 USD

Payment Methods:

[Credit Card (3-5 day wait]

Liberty Reserve (2 day wait)

Western Union (no wait)
No One is Safe…

HOHOHO, ihr stubenhockenden Computer-Kids!

OK, versuch mal Username “santa” und Passwort “hohoho” auf den üblichen Plattformen …
A Final Example…

Does this look infected?

Stuxnet
Pay Attention or You’re Just Wasting Time
Questions ?

#sf21veu • 16 -18 June 2021
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
Where do I go From Here? - Continuing Your Wireshark Education

Wireshark Core Curriculum Network Troubleshooting and Analysis Classes
- Wireshark 0 – TCP/IP Networking Fundamentals Using Wireshark
- Wireshark 1 - TCP/IP Troubleshooting & Network Optimization with Wireshark
- Wireshark 2 – Masterclass - Advanced Network & Security Analysis

Wireshark Advanced Curriculum and Specialty Analysis Classes
- Wireshark 3 – Network Forensics Analysis
- Wireshark 4 – Mobile Device Forensics Analysis
- Wireshark 5 - Cloud & Internet of Things (IoT) Network Analysis
- Wireshark 6 - VoIP Advanced Network Analysis
- Wireshark 7 - WiFi Advanced Network Analysis
- Wireshark 8 – SCADA & ICS Network Analysis
- Wireshark 9 – Wireshark Command Line Tools
- Wireshark WCNA Bootcamp