2019

sec-getsplendid.pcapng HTTP Malicious Redirection Analysis

sec-getsplendid.pcapng

LAURA CHAPPELL – CHAPPELL-UNIVERSITY.COM

General File Information

Name:	D:\00000-Master Trace Files\sec-getsplendid.pcapng
Length:	67 MB
Hash (SHA256):	38cefa46dc4aa59c6f15dc45bc9b25f6b2b7703137e9c45cfa0d577122a47218
Hash (RIPEMD160):	816a6901ca3c9ad327a76b01716568669cf60d87
Hash (SHA1):	5b914b8f066382e8711321ce36c5b039f17af1d0
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time Information

First packet:	2019-04-23 14:23:27
Last packet:	2019-04-23 15:06:37
Elapsed:	00:43:10

Capture Information

Hardware:	Intel(R) Core(TM) i7-3930K CPU @ 3.20GHz (with SSE4.2)
OS:	64-bit Windows 10 (1803), build 17134
Application:	Dumpcap (Wireshark) 3.0.1 (v3.0.1-0-gea351cd8)

Interface Information

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Ethernet	194 (0.3 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	76143	8 (0.0%)	—
Time span, s	2590.272	165.850	—
Average pps	29.4	0.0	—
Average packet size, B	855	708	—
Bytes	65070236	5664 (0.0%)	0
Average bytes/s	25 k	34	—
Average bits/s	200 k	273	—

File Comment

(info@chappellu.com) Sign up for our newsletter at www.chappell-university.com to get the latest news on analysis, Wireshark, forensics and more.

In hopes of demonstrating a DNS name error response, I typed www.asdfasdfasdfasdfasdf.com into my browser. Watch as I was redirected around to malicious sites.

Packet Comments

Frame 1: Here's the first DNS query generated by my client system.

Frame 2: Whoa - I didn't expect that to resolve!

Frame 3: Not the best behavior by my client, on which I was capturing. Why send out another query when we received an answer. Note this is another separate query, not a retransmission - look at the DNS Transaction ID field.

Frame 5: There are quite a few DNS retransmissions in this trace file. Try the filter dns.retransmission == 1 to see how many.

Frame 7: I recommend you add a column for the tcp.stream field. My host will be bounced around through a bunch of TCP connections.

Frame 12: Add a column for the HTTP Host field now.

Frame 15: And here the redirections start. Add a column for the HTTP Location field now.

Frame 18: Here my host begins resolving btpnative.com.

Frame 29: Well this IP address looks a bit familiar! Compare to the IP address of the asdfasdfasdfasdfasdf.com host.

Frame 46: Whoa... Normally when you ask for the favicon.ico (the little icon that goes on your browser tab), you don't send a cookie up to the server... suspicious!

Frame 48: Yup - my host is running McAfee Web Advisor. Not helping in this case.

Frame 54: Another connection to btpnative.com...

Frame 64: Favicon.ico errors don't show up on your browser screen.

Frame 68: Look in the Packet Bytes pane of TLS Client Hello packets - many times the target server name is easy to read there. This is my connection to a McAfee server.

Frame 79: Ah... sending something up to the btpnative server. Now is a good time to add a "Referer" column.

Frame 121: This is the response to the POST in Frame 79. I'm being redirected again - to forwrdnow.com.

Frame 123: Resolving forwrdnow.com's address.

Frame 130: These failed DNS AAAA (IPv6) queries are interesting. We can find the SOA information - dnsmadeeasy.com on this one.

Frame 133: Connecting to forwrdnow.com. This is a good time to consider turning on name resolution in Wireshark. We aren't finished bouncing around.

Frame 144: But wait! There's more! The site forwrdnow.com is sending us over to 7lyonline.com.

Frame 145: Resolving the address for 7lyonline.com.

Frame 158: Actually... forwrdnow.com referred us to 7lyonline.com.

Frame 162: Now I'm being told to go to givemeofferlnk.com.

If you turned on name resolution and the Source column indicates 7proof.com, look down at 1045 to see the start of that address resolution.

Both 7lyonline.com and 7proof.com resolve to the same address. The 7proof.com is the later one, so that is displayed by Wireshark's name resolution feature.

By the way, when I set name resolution I only used resolution information available within the trace file (not an external resolver).

Frame 172: Connecting to givemeofferlnk.com.

Frame 175: Another interesting "Referer" field value.

Frame 182: This is a good time to compare right click Follow | TCP Stream vs. Follow | HTTP Stream since the content is gzipped (compressed). That's when you want to use Follow | HTTP Stream.

Frame 193: Encrypted connection to givemeofferlnk.com.

Frame 194: Another encrypted connection to givemeofferlnk.com.

Frame 237: Without decrypting the communications to getmeofferlnk.com, we must just assume that last set of traffic pointed us to getsplendidapps.com because we are suddenly resolving the name.

Frame 246: And now we connect to getsplendidapps.com.

Frame 249: The getsplendidapps.com page started to appear on my host after this download.

Frame 255: If you have the length column visible, you'll notice data is flowing towards my client system from getsplendidapps.com. The data sizes are kind of funky.

Frame 345: Hmmm. gstatic.com, eh? Do a bit of research into gstatic virus.

Frame 425: Oh yes... more getsplendid stuff... now getsplendidresult.com resolution begins.

Frame 771: If you do a lookup of the source IP address, you'll notice we're going to a Cloudflare server to get data.

Frame 980: Now we're resolving getawesome6.com... this is not a good day.

Frame 1015: If you haven't done so already, add a column for the tls.handshake.extensions_server_name field.

Alternately, you can typically get the name of the target server in TLS connections by looking in the packet bytes pane of the Client Hello.

This connection is being estabilshed to trf.getawesome6.com.

Frame 1028: Yes - my service provider is AT&T.

Frame 1054: If you wonder why we have repeated DNS requests, look at the DNS response Time to live value. The field value denotes the seconds for which you can cache the information.

Frame 1070: Hmmm... www.cherami-cloud.com is a questionable site... at least to some malware detection systems.

Frame 1094: Ok... now spend a little time looking through the remaining traffic to see if you can identify any other suspicious traffic. Check the DNS traffic and your TLS Name column contents. Enjoy! -Laura