Week 1 Threat Intelligence

Jurjen de Jonge
500731921
Hogeschool van Amsterdam

September 7, 2018

Contents

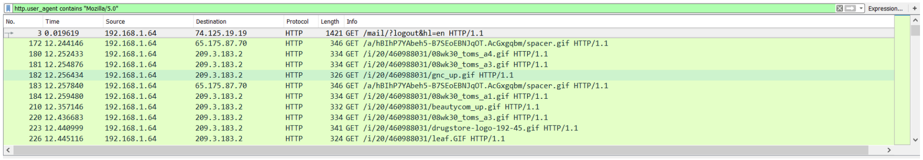
1. *Assignments*

1.1 What is the first HTTP traffic is showing?

The first HTTP traffic is a sign out of a Google account in frame 3

1.2 Identify all traffic generated using Mozilla compatible browsers

The traffic can be found by applying a filter that looks for the ”Mozilla/5.0” in the user agent. That filter will be ”http.user_agent contains ”Mozilla/5.0””



http.user_agent contains "Mozilla/5.0"

No.	Time	Source	Destination	Protocol	Length	Info
3	0.019619	192.168.1.64	74.125.19.19	HTTP	1421	GET /mail/?logout&hl=en HTTP/1.1
172	12.244146	192.168.1.64	65.175.87.70	HTTP	346	GET /a/hBIhP7YAbeh5-B7SEoEBNJqOT.AcGxgqbm/spacer.gif HTTP/1.1
180	12.252433	192.168.1.64	209.3.183.2	HTTP	334	GET /i/20/460988031/08wk30_toms_a4.gif HTTP/1.1
181	12.254876	192.168.1.64	209.3.183.2	HTTP	334	GET /i/20/460988031/08wk30_toms_a3.gif HTTP/1.1
182	12.256434	192.168.1.64	209.3.183.2	HTTP	326	GET /i/20/460988031/gnc_up.gif HTTP/1.1
183	12.257840	192.168.1.64	65.175.87.70	HTTP	346	GET /a/hBIhP7YAbeh5-B7SEoEBNJqOT.AcGxgqbm/spacer.gif HTTP/1.1
184	12.259480	192.168.1.64	209.3.183.2	HTTP	334	GET /i/20/460988031/08wk30_toms_a1.gif HTTP/1.1
210	12.357146	192.168.1.64	209.3.183.2	HTTP	332	GET /i/20/460988031/beautycom_up.gif HTTP/1.1
220	12.436683	192.168.1.64	209.3.183.2	HTTP	334	GET /i/20/460988031/08wk30_toms_a3.gif HTTP/1.1
223	12.440999	192.168.1.64	209.3.183.2	HTTP	341	GET /i/20/460988031/drugstore-logo-192-45.gif HTTP/1.1
226	12.445116	192.168.1.64	209.3.183.2	HTTP	324	GET /i/20/460988031/leaf.GIF HTTP/1.1

1.3 Explain what is happening from frame 9 to frame 41

A DNS lookup is being sent over UDP in frame 9. Requests are made to get the IP addresses of Google servers. After getting the ip addresses a TCP handshake is being initiated and encrypted channel is being opened between the computer and a Google server.

1.4 Explain why frame 42 is out of order?

The handshake [FIN,ACK] has already been sent and is being resend by the server. This might have occurred because the google server might not have received the ACK so it resend it’s [FIN,ACK] tcp packet.

1.5 dentify all HTTP servers which support encrypted communications (i.e. ssl)

The http server will send information about it self including if it supports secure ssl connections. This can be looked for by applying the filter http.server contains ”mod_ssl”. This will filter out all server that do not include mod_ssl being enabled in its configuration.

1.6 Identify Server Software Version running

This information can be found by looking at an HTTP reply for and looking at the Server header. The filter to find traffic coming or originating from an server is ”ip.addr == 66.150.96.119”

1.6.1 69.22.167.239

Apache/1.3.41 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.8a

1.6.2 18.7.22.69

MIT Web Server Apache/1.3.26 Mark/1.5 (Unix) mod_ssl/2.8.9 OpenSSL/0.9.7c

1.6.3 66.150.96.119

Apache/2.0.54 (Debian GNU/Linux) mod_fastcgi/2.4.2 mod_ssl/2.0.54 OpenSSL/0.9.7e

1.7 Find all Google searches recorded in the given network traffic

It’s possible to look for traffic going to a google domain and has the ”search” parameter in the url. This parameter exists in all google searches. The filter that can be used for this is http.request.uri contains ”search” && http.host contains ”google”