Analysis of Chinese MITM on Google

Thursday, 04 September 2014 23:55:00 (UTC/GMT)

The Chinese are running a MITM attack on SSL encrypted traffic between Chinese universities and Google. We've performed technical analysis of the attack, on request from GreatFire.org, and can confirm that it is a real SSL MITM against www.google.com and that it is being performed from within China.

We were contacted by GreatFire.org yesterday (September 3) with a request to analyze two packet captures from suspected MITM-attacks before they finalized their blog post. The conclusions from our analysis is now published as part of GreatFire.org's great blog post titled "Authorities launch man-in-the-middle attack on Google".

In their blog post GreatFire.org write:

> From August 28, 2014 reports appeared on Weibo and Google Plus that users in China trying to access google.com and google.com.hk via CERNET, the country's education network, were receiving warning messages about invalid SSL certificates. The evidence, which we include later in this post, indicates that this was caused by a man-in-the-middle attack.
>
> While the authorities have been blocking access to most things Google since June 4th, they have kept their hands off of CERNET, China's nationwide education and research network. However, in the lead up to the new school year, the Chinese authorities launched a man-in-the-middle (MITM) attack against Google.

Our network forensic analysis was performed by investigating the following to packet capture files:

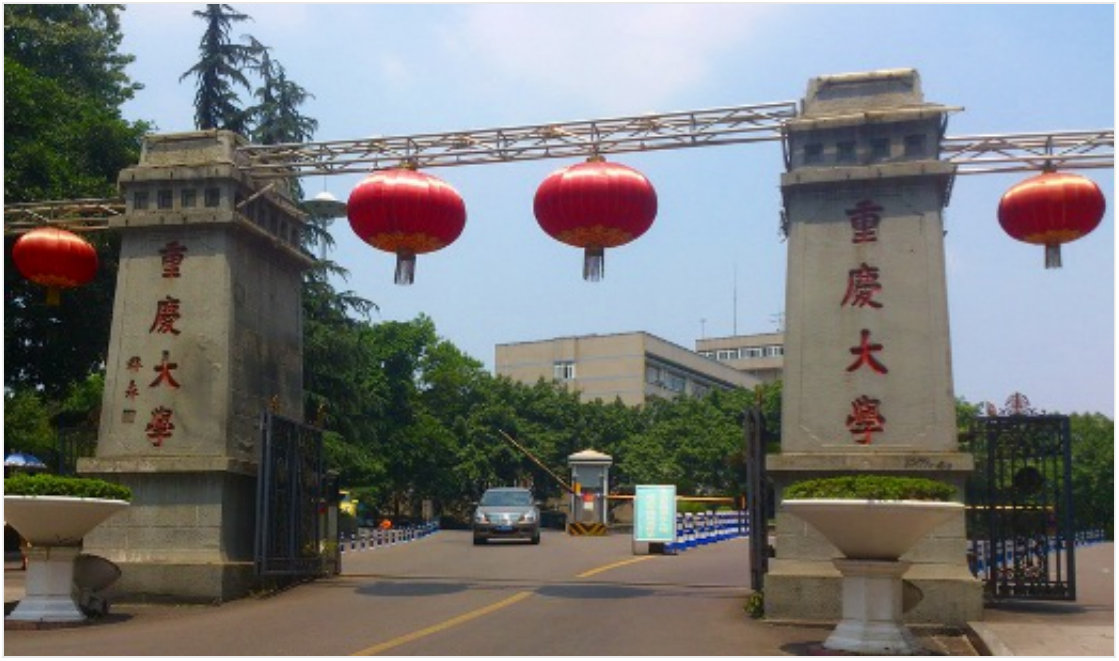
Capture Location	Client Netname	Capture Date	Filename	MD5
Peking University	PKU6-CERNET2	Aug 30, 2014	google.com.pcap	aba4b35cb85ed218 7a8a7656cd670a93
Chongqing University	CQU6-CERNET2	Sep 1, 2014	google_fake.pcapng	3bf943ea453f9afa 5c06b9c126d79557

Client and Server IP adresses

The analyzed capture files contain pure IPv6 traffic (CERNET is a IPv6 network) which made the analysis a bit different then usual. We do not disclose the client IP addresses for privacy reasons, but they both seem legit; one from Peking University (netname PKU6-CERNET2) and the other from Chongqing

University (CQU6-CERNET2). Both IP addresses belong to AS23910, named "China Next Generation Internet CERNET2".

Peking University entrance, by galaygobi (Creative Commons Attribution 2.0)



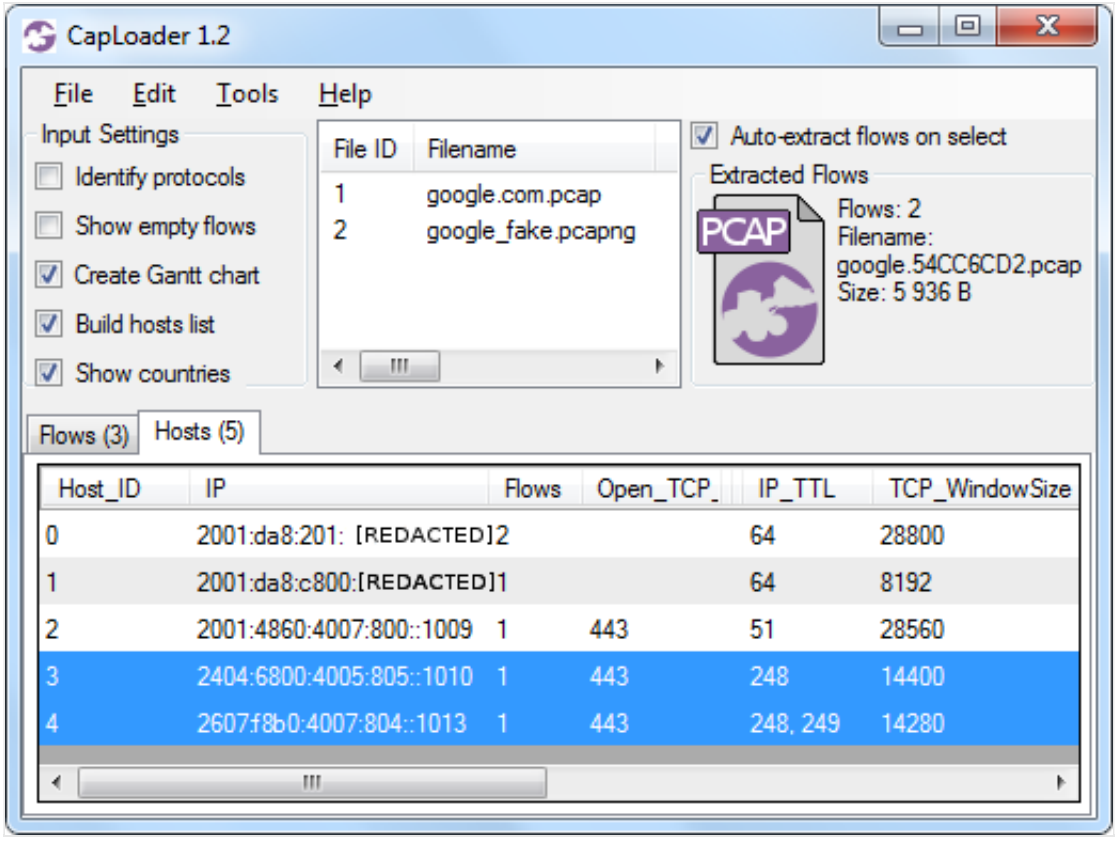
Chongqing University gate, by Brooktse (Creative Commons Attribution-Share Alike 3.0)

The IP addresses received for www.google.com were in both cases also legit, so the MITM wasn't carried out through DNS spoofing. The Peking University client connected to 2607:f8b0:4007:804::1013

(GOOGLE-IPV6 in United States) and the connection from Chongqing University went to 2404:6800:4005:805::1010 (GOOGLE_IPV6_AP-20080930 in Australia).

Time-To-Live (TTL) Analysis

The Time-To-Live (TTL) values received in the IP packets from www.google.com were in both cases 248 or 249 *(note: TTL is actually called "Hop Limit" in IPv6 nomenclature, but we prefer to use the well established term "TTL" anyway)*. The highest possible TTL value is 255, this means that the received packets haven't made more than 6 or 7 router hops before ending up at the client. However, the expected number of router hops between a server on GOOGLE-IPV6 and the client at Peking University is around 14. The low number of router hops is is a clear indication of an IP MITM taking place.



CapLoader with both capture files loaded, showing TTL values

Here is an IPv6 traceroute from AS25795 in Los Angeles towards the IP address at Peking University (generated with ARP Networks' 4or6.com tool):

```
#traceroute -6 2001:da8:[REDACTED]
 1  2607:f2f8:1600::1 (2607:f2f8:1600::1) 1.636 ms 1.573 ms 1.557 ms
 2  2001:504:13::1a (2001:504:13::1a) 40.381 ms 40.481 ms 40.565 ms
 3  * * *
 4  2001:252:0:302::1 (2001:252:0:302::1) 148.409 ms 148.501 ms 148.595 ms
```

```
 5  * * *
 6  2001:252:0:1::1 (2001:252:0:1::1) 148.273 ms 147.620 ms 147.596 ms
 7  pku-bj-v6.cernet2.net (2001:da8:1:1b::2) 147.574 ms 147.619 ms 147.420 ms
 8  2001:da8:1:50d::2 (2001:da8:1:50d::2) 148.582 ms 148.670 ms 148.979 ms
 9  cernet2.net (2001:da8:ac:ffff::2) 147.963 ms 147.956 ms 147.988 ms
10  2001:da8:[REDACTED] 147.964 ms 148.035 ms 147.895 ms
11  2001:da8:[REDACTED] 147.832 ms 147.881 ms 147.836 ms
12  2001:da8:[REDACTED] 147.809 ms 147.707 ms 147.899 ms
```

As can be seen in the traceroute above, seven hops before the client we find the 2001:252::/32 network, which is called “CNGI International Gateway Network (CNGIIGN)”. This network is actually part of CERNET, but on AS23911, which is the network that connects CERNET with its external peers. A reasonable assumption is therefore that the MITM is carried out on the 2001:252::/32 network, or where AS23910 (2001:da8:1::2) connects to AS23911 (2001:252:0:1::1). This means that the MITM attack is being conducted from within China.

Response Time Analysis

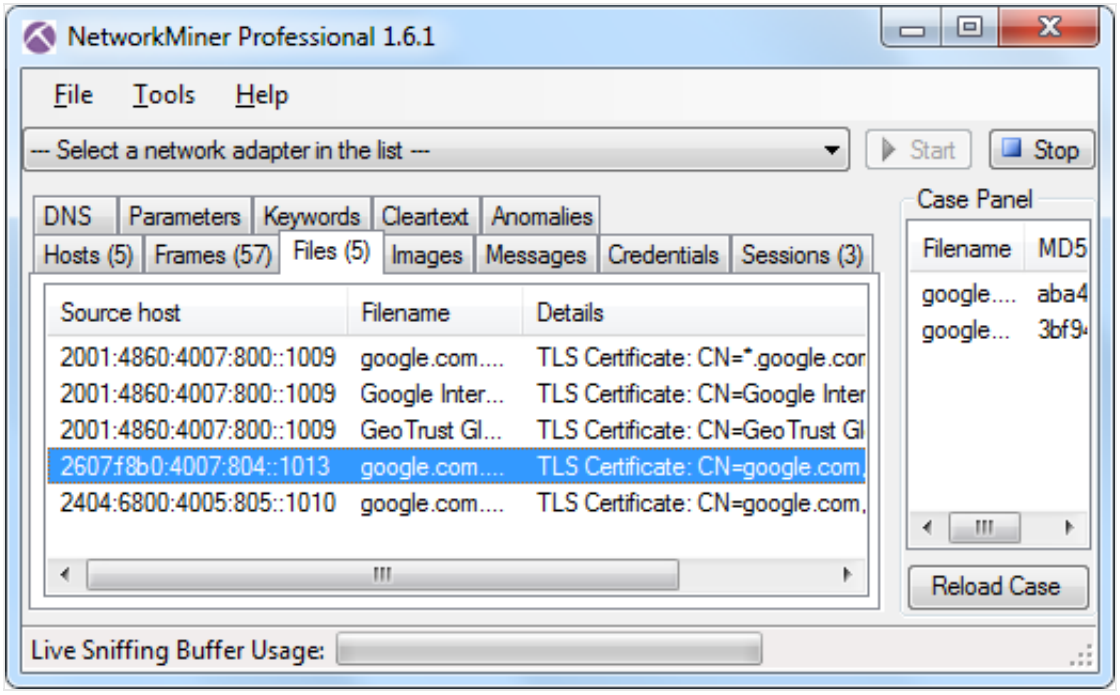
The round-trip time between the client and server can be estimated by measuring the time from when the client sends it initial TCP SYN packet to when it receives a TCP SYN+ACK from the server. The expected round-trip time for connecting from CERNET to a Google server overseas would be around 150ms or more. However, in the captures we've analyzed the TCP SYN+ACK package was received in just 8ms (Peking) and 52ms (Chongqing) respectively. Again, this is a clear indication of an IP MITM taking place, since Google cannot possibly send a response from the US to CERNET within 8ms regardless of how fast they are. The fast response times also indicate that the machine performing the MITM is located fairly close to the network at Peking University.

Even though the machine performing the MITM was very quick at performing the TCP tree-way handshake we noticed that the application layer communication was terribly slow. The specification for the TLS handshake (RFC 2246) defines that a ClientHello message should be responded to with a ServerHello. Google typically send their ServerHello response almost instantly, i.e. the response is received after one round-trip time (150ms in this case). However, in the analyzed captures we noticed ServerHello response times of around 500ms.

X.509 Certificate analysis

We extracted the X.509 certificates from the two capture files to .cer files using NetworkMiner. We noticed that both users received identical certificates, which were both self signed for “google.com”. The

fact that the MITM used a self signed certificate makes the attack easily detectable even for the non-technical user, since the web browser will typically display a warning about the site not being trusted. Additionally the X.509 certificate was created for ”google.com” rather than ”*.google.com”. This is an obvious miss from the MITM'ers side since they were attempting to MITM traffic to ”www.google.com” but not to ”google.com”.



NetworkMiner showing list of X.509 certificates extracted from the two PCAP files

> Certificate SHA1 fingerprint: f6beadb9bc02e0a152d71c318739cdecfc1c085d
> Certificate MD5 fingerprint: 66:D5:D5:6A:E9:28:51:7C:03:53:C5:E1:33:14:A8:3B

A copy of the fake certificate is available on Google drive thanks to GreatFire.org.

Conclusions

All evidence indicates that a MITM attack is being conducted against traffic between China’s nationwide education and research network CERNET and www.google.com. It looks as if the MITM is carried out on a network belonging to AS23911, which is the outer part of CERNET that peers with all external networks. This network is located in China, so we can conclude that the MITM was being done within the country.

It's difficult to say exactly how the MITM attack was carried out, but we can dismiss DNS spoofing as the used method. The evidence we've observed instead indicate that the MITM attack is performed either by performing IP hijacking or by simply reconfiguring a router to forward the HTTPS traffic to a transparent SSL proxy. An alternative to changing the router config would also be to add an in-line device that redirects the desired traffic to the SSL proxy. However, regardless of how they did it the attacker would be

able to decrypt and inspect the traffic going to Google.

We can also conclude that the method used to perform the MITM attack was similar to the Chinese MITM on GitHub, but not identical.

Share | Short URL: http://netresec.com/?b=14955CB

Posted by Erik Hjelmvik on Thursday, 04 September 2014 23:55:00 (UTC/GMT)