

DNSMon

# 一些网站https证书出现问题的情况分析



Zhang Zaifeng

Mar 27, 2020 • 6 min read

[20200328 17:00 更新] 更新数据到20200328 16:00.

20200326下午，有[消息说](#)[1]github的TLS证书出现了错误告警。证书的结构很奇怪，在其签发者信息中有一个奇怪的email地址：346608453@qq.com。明显是一个伪造的证书。

为了弄清楚其中的情况，我们对这一事件进行了分析。

## DNS劫持？

出现证书和域名不匹配的最常见的一种情况是DNS劫持，即所访问域名的IP地址和真实建立连接的IP并不相同。

以被劫持的域名go-acme.github.io为例，我们的passiveDNS库中该域名的IP地址主要使用如下四个托管在fastly上的IP地址，可以看到其数据非常干净。

2019-03-12 10:28:06	2020-03-23 12:52:01	622	go-acme.github.io	A	185.199.109.153
2019-03-12 10:28:06	2020-03-23 12:52:01	622	go-acme.github.io	A	185.199.108.153
2019-03-12 10:28:06	2020-03-23 12:52:01	622	go-acme.github.io	A	185.199.111.153
2019-03-12 10:28:06	2020-03-23 12:52:01	622	go-acme.github.io	A	185.199.110.153

对该域名直接进行连接测试，可以看到，TCP连接的目的地址正是185.199.111.153，但其返回的证书却是错误的证书。因此github证书错误的问题并不是在DNS层面出现问题。

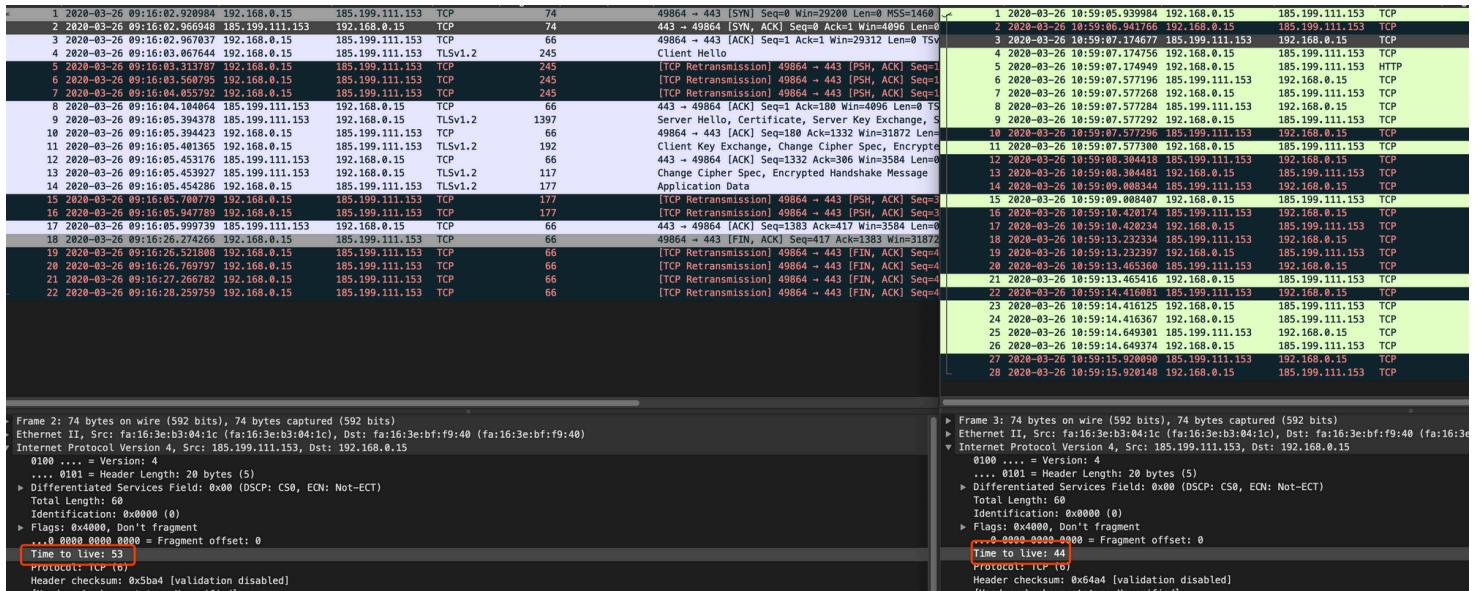
```

curl -vvv https://go-acme.github.io/ -k -I
* About to connect() to go-acme.github.io port 443 (#0)
* Trying 185.199.111.153...
* Connected to go-acme.github.io (185.199.111.153) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*       subject: E=346608453@qq.com,CN=SERVER,OU=NSP,O=COM,L=SZ,ST=GD,C=CN
*       start date: Sep 26 09:33:13 2019 GMT
*       expire date: Sep 23 09:33:13 2029 GMT
*       common name: SERVER
*       issuer: E=346608453@qq.com,CN=CA,OU=NSP,O=COM,L=SZ,ST=GD,C=CN
> HEAD / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: go-acme.github.io
> Accept: */*

```

## 劫持如何发生的？

为了搞清楚这个问题，可以通过抓取链路上的数据包来进行分析。为了有较好的对比性，我们先后抓取了443端口和80端口的数据。如下图



左边的数据包为https连接，右边的数据包为http连接。可以看到https的服务器应答TTL为53，http的则为44。一般来说，在时间接近的情况下，连接相同的目标IP，数据包在链路上的路径是近似的。https的TTL显著大于http的TTL，看起来很有可能是在链路上存在劫持。

有意思的是在https后续的连接中其TTL值并不稳定，比如在响应证书的数据包中，其TTL变成了47，介于44和53之间，更接近于http链路的情况。作为对比，http的后续数据包的TTL值则一直稳定在44。

[20200327 23:00 更新] 在数据包内容方面，另一个值得关注的点是：被劫持的会话数据包(https)全部回包的IPID都是0. 正常数据包(http)首次回包IPID是0，之后的回包就不是了。

这是两个有意思的现象。

1	2020-03-26 09:16:02.920984	192.168.0.15	185.199.111.153	TCP	74	49864 → 443 [SYN] Seq=0 Win=29200 Len=0
2	2020-03-26 09:16:02.966948	185.199.111.153	192.168.0.15	TCP	74	443 → 49864 [SYN, ACK] Seq=0 Ack=1 Win=293
3	2020-03-26 09:16:02.967037	192.168.0.15	185.199.111.153	TCP	66	49864 → 443 [ACK] Seq=1 Ack=1 Win=293
4	2020-03-26 09:16:03.067644	192.168.0.15	185.199.111.153	TLSv1.2	245	Client Hello
5	2020-03-26 09:16:03.313787	192.168.0.15	185.199.111.153	TCP	245	[TCP Retransmission] 49864 → 443 [PSH]
6	2020-03-26 09:16:03.560795	192.168.0.15	185.199.111.153	TCP	245	[TCP Retransmission] 49864 → 443 [PSH]
7	2020-03-26 09:16:04.055792	192.168.0.15	185.199.111.153	TCP	245	[TCP Retransmission] 49864 → 443 [PSH]
8	2020-03-26 09:16:04.104064	185.199.111.153	192.168.0.15	TCP	66	443 → 49864 [ACK] Seq=1 Ack=180 Win=4
9	2020-03-26 09:16:05.394378	185.199.111.153	192.168.0.15	TLSv1.2	1397	Server Hello, Certificate, Server Key
10	2020-03-26 09:16:05.394423	192.168.0.15	185.199.111.153	TCP	66	49864 → 443 [ACK] Seq=180 Ack=1332 Win=4
11	2020-03-26 09:16:05.401365	192.168.0.15	185.199.111.153	TLSv1.2	192	Client Key Exchange, Change Cipher Spec
12	2020-03-26 09:16:05.453176	185.199.111.153	192.168.0.15	TCP	66	443 → 49864 [ACK] Seq=1332 Ack=306 Win=4
13	2020-03-26 09:16:05.453927	185.199.111.153	192.168.0.15	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake
14	2020-03-26 09:16:05.454286	192.168.0.15	185.199.111.153	TLSv1.2	177	Application Data
15	2020-03-26 09:16:05.700779	192.168.0.15	185.199.111.153	TCP	177	[TCP Retransmission] 49864 → 443 [PSH]
16	2020-03-26 09:16:05.947789	192.168.0.15	185.199.111.153	TCP	177	[TCP Retransmission] 49864 → 443 [PSH]
17	2020-03-26 09:16:05.999739	185.199.111.153	192.168.0.15	TCP	66	443 → 49864 [ACK] Seq=1383 Ack=417 Win=4
18	2020-03-26 09:16:26.274266	192.168.0.15	185.199.111.153	TCP	66	49864 → 443 [FIN, ACK] Seq=417 Ack=1383
19	2020-03-26 09:16:26.521808	192.168.0.15	185.199.111.153	TCP	66	[TCP Retransmission] 49864 → 443 [FIN]
20	2020-03-26 09:16:26.769797	192.168.0.15	185.199.111.153	TCP	66	[TCP Retransmission] 49864 → 443 [FIN]
21	2020-03-26 09:16:27.266782	192.168.0.15	185.199.111.153	TCP	66	[TCP Retransmission] 49864 → 443 [FIN]
22	2020-03-26 09:16:28.259759	192.168.0.15	185.199.111.153	TCP	66	[TCP Retransmission] 49864 → 443 [FIN]

Frame 9: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits)  
Ethernet II, Src: fa:16:3e:b3:04:1c (fa:16:3e:b3:04:1c), Dst: fa:16:3e:bf:f9:40 (fa:16:3e:bf:f9:40)  
Internet Protocol Version 4, Src: 185.199.111.153, Dst: 192.168.0.15  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 1383  
Identification: 0x0000 (0)  
► Flags: 0x4000, Don't fragment  
.... 0000 0000 0000 = Fragment offset: 0  
Time to live: 47  
Protocol: TCP (6)  
Header checksum: 0x5c79 [validation disabled]  
[Header checksum status: Unverified]  
Source: 185.199.111.153  
Destination: 192.168.0.15  
Transmission Control Protocol, Src Port: 443, Dst Port: 49864, Seq: 1, Ack: 180, Len: 1331

被劫持会话后续返回的TTL值

因此，结合https会话过程中TTL值和IPID的异常，我们猜测是在链路上发生了劫持。

证书是怎么回事？

事实上，从我们DNSMon系统的证书信息来看，这个证书  
(9e0d4d8b078d7dfoda18efc23517911447b5ee8c) 的入库时间在20200323早上六点。考虑到数据分析的时延，其开始在大网上使用最晚可以追溯到20200322。

同时可以看到，这个证书在证书链上的父证书

(03346f4c61e7b5120e5db4a7bbbf1a3558358562) 是一个自签名的证书，并且两者使用相同的签发者信息。

相关证书信息

## 受影响的域名及时间

从上图中可以看到，该证书的影响不仅仅在github，实际上范围非常大。通过DNSMon系统，我们提取出了受影响的域名共 **15462**个。

通过DNSMon系统查看这些域名的流行度，在TOP1000的域名中，有40个域名受影响，列表如下：

- 1 www.jd.com
- 5 www.baidu.com
- 10 www.google.com
- 37 www.sina.com
- 44 www.163.com
- 51 www.douyu.com
- 62 www.suning.com
- 86 www.pconline.com.cn
- 91 sp1.baidu.com
- 126 twitter.com
- 137 www.eastmoney.com
- 143 mini.eastday.com
- 158 spo.baidu.com
- 174 www.jianshu.com
- 177 www.mgtv.com
- 185 www.zhihu.com

232 www.toutiao.com  
241 price.pcauto.com.cn  
271 www.google.com.hk  
272 video.sina.com.cn  
299 www.youtube.com  
302 www.acfun.cn  
365 www.vip.com  
421 news.ifeng.com  
451 car.autohome.com.cn  
472 www.facebook.com  
538 www.gamersky.com  
550 www.xiaohongshu.com  
552 www.zaobao.com  
580 www.xxsy.net  
621 www.huya.com  
640 mp.toutiao.com  
643 www.ifeng.com  
689 www.ip138.com  
741 dl.pconline.com.cn  
742 v.ifeng.com  
784 www.yicai.com  
957 passport2.chaoxing.com  
963 3g.163.com  
989 www.doyo.cn

对这些域名发生证书劫持时的DNS解析情况分析发现，这些域名的解析IP均在境外，属于这些域名在境外的CDN服务。值得一提的是尽管这些域名都是排名靠前的大站，但是因为国内访问的时候，CDN解析会将其映射为国内的IP地址，因此国内感知到这些大站被劫持的情况比较小。

## 受影响二级域排名

在二级域方面，github.io 是受影响最大的二级域，也是此次劫持事件的关注焦点。

1297 github.io

35 app2.xin

25 github.com  
18 aliyuncs.com  
17 app2.cn  
14 nnqp.vip  
10 jov.cn  
8 pragmaticplay.net  
7 tpdz1o.monster  
7 suning.com

从时间维度来看，这些域名的首次被劫持时间分布如下：

从图中可以看出域名首次受影响的数量有日常作息规律，并且在3月26号数量有了较大幅度的增加。

## 结论

- 1) 劫持涉及域名较多，共计15462个，其中TOP1000的网站有40个；
- 2) 劫持主要发生在国内用户访问上述域名的海外CDN节点的链路上。国内用户访问国内节点的情况下未见影响；
- 3) 所有这些劫持均使用了以 [346608453@qq.com](#) 名义签名的证书，但我们没有找到编号 346608453 的QQ用户与本次劫持事件相连的直接证据，也不认为该QQ用户与本次事件有直接关联；
- 4) 所有这些劫持最早出现在 20200321 23时附近并且在20200326处于高峰。
- 5) 在20200327 11时之后，此劫持现象已经消失。前后共约131小时。

## 参考链接

1. <https://v2ex.com/t/656367?p=2>



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name



Share

Best Newest Oldest

Be the first to comment.

[Subscribe](#)[Privacy](#)[Do Not Sell My Data](#)

— 360 Netlab Blog - Network Security Research Lab at 360 —

## DNSMon



俄乌危机中的数字证书：吊销、影响、缓解

商业数字证书签发和使用情况简介(删减版)

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

0-day

## DrayTek Vigor企业级路由器和交换机设备在野0-day 漏洞分析报告

本文作者：马延龙，叶根深，刘宏达 背景介绍 从2019年12月4开始，360Netlab未知威胁检测系统持续监测到两个攻击团伙使用DrayTek Vigor企业级路由器和交换机设备0-day漏洞，窃听设备网络流量，开启SSH服务并创建系统后门账号，创建Web Session后门等恶意行为。2019年12月25号，我们在Twitter[1][2]上披露了DrayTek Vigor在野0-day漏洞攻击IoC...

Icnanker

## Icnanker, a Linux Trojan-Downloader Protected by SHC

Background On August 15, 2019, 360Netlab Threat Detecting System flagged an unknown ELF sample (5790dedae465994d179c63782e51bac1) which generated Elknot Botnet related network traffic. We manually took a look and noticed that it is a Trojan-Downloader which utilizes "SHC (Shell script compiler)" technique and...

See all 28 posts →



• Mar 27, 2020 • 6 min read



• Mar 23, 2020 • 8 min read