TeamViewer

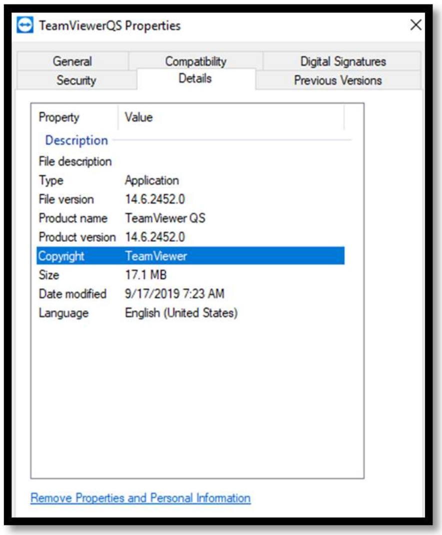
September 18th, 2019.

This is a review of TeamViewer. This software is used by organizations to allow remote interaction among users. The JA3 is used to provide TLS/SSL fingerprinting that when used for security reasons results in the ability to identify, log, alert and or block specific traffic in an encrypted network traffic.

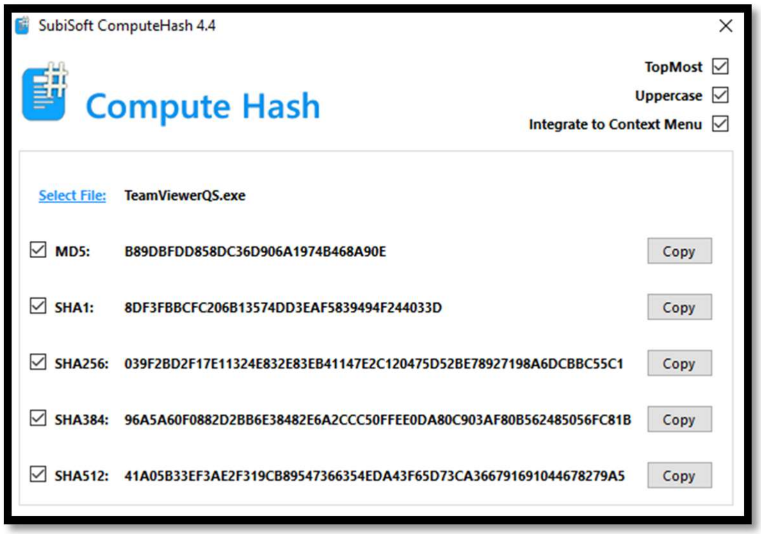
The software has a possible integrity vulnerability. While examining the software it was identified a similar JA3 hash signature (“4d7a28d6f2263ed61de88ca66eb011e3”) associated with malware samples that could be using encryption to hide themselves in the noise.

A possible explanation for this finding may be due to the inappropriate use of JA3 during the development or recent updates of the software.

1. File Identification (e.g. SHA256)



Property	Value
Description	
File description	
Type	Application
File version	14.6.2452.0
Product name	TeamViewer QS
Product version	14.6.2452.0
Copyright	TeamViewer
Size	17.1 MB
Date modified	9/17/2019 7:23 AM
Language	English (United States)



Select File: TeamViewerQS.exe

☑ MD5: B89DBFDD858DC36D906A1974B468A90E

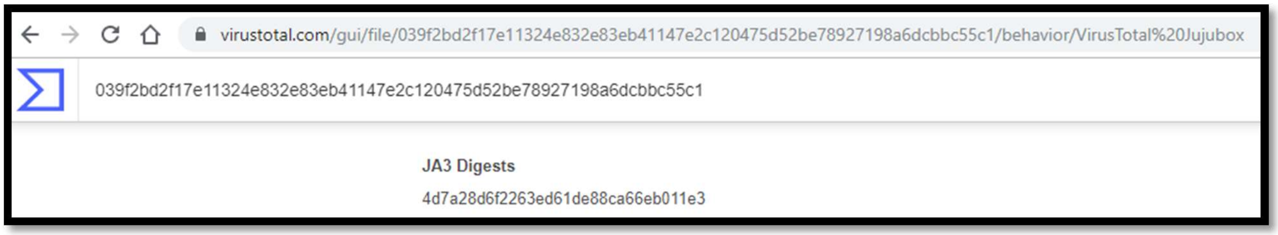
☑ SHA1: 8DF3FBBCFC206B13574DD3EAF5839494F244033D

☑ SHA256: 039F2BD2F17E11324E832E83EB41147E2C120475D52BE78927198A6DCBBC55C1

☑ SHA384: 96A5A60F0882D2BB6E38482E6A2CCC50FFEE0DA80C903AF80B562485056FC81B

☑ SHA512: 41A05B33EF3AE2F319CB89547366354EDA43F65D73CA366791691044678279A5

2. JA3 Hash identified:

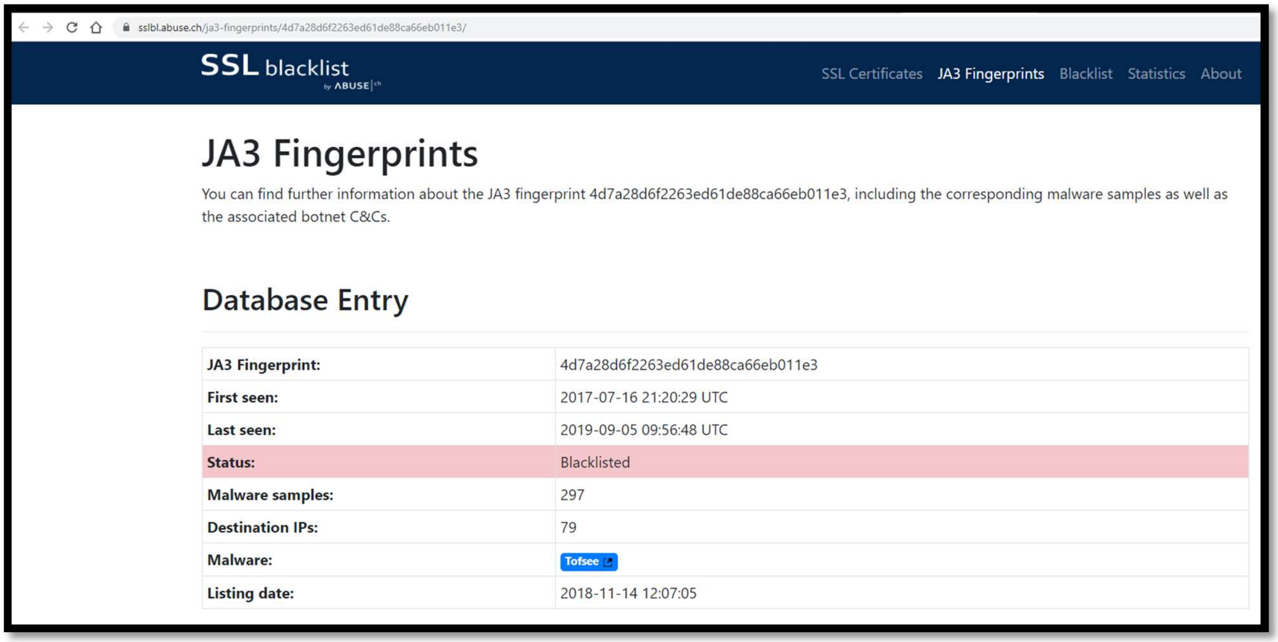

virustotal.com/gui/file/039f2bd2f17e11324e832e83eb41147e2c120475d52be78927198a6dcbbc55c1/behavior/VirusTotal%20Jujubox

039f2bd2f17e11324e832e83eb41147e2c120475d52be78927198a6dcbbc55c1

JA3 Digests

4d7a28d6f2263ed61de88ca66eb011e3

3. The hash can be found referring to malwares like:

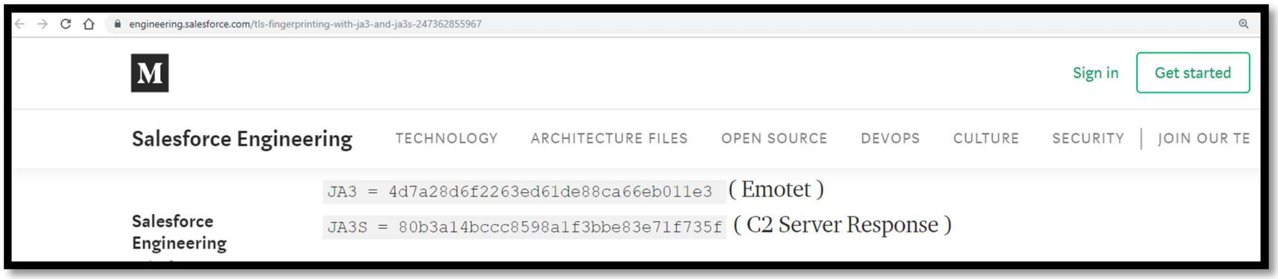

sslbl.abuse.ch/ja3-fingerprints/4d7a28d6f2263ed61de88ca66eb011e3/

JA3 Fingerprints

You can find further information about the JA3 fingerprint 4d7a28d6f2263ed61de88ca66eb011e3, including the corresponding malware samples as well as the associated botnet C&Cs.

Database Entry

JA3 Fingerprint:	4d7a28d6f2263ed61de88ca66eb011e3
First seen:	2017-07-16 21:20:29 UTC
Last seen:	2019-09-05 09:56:48 UTC
Status:	Blacklisted
Malware samples:	297
Destination IPs:	79
Malware:	Tofsee
Listing date:	2018-11-14 12:07:05

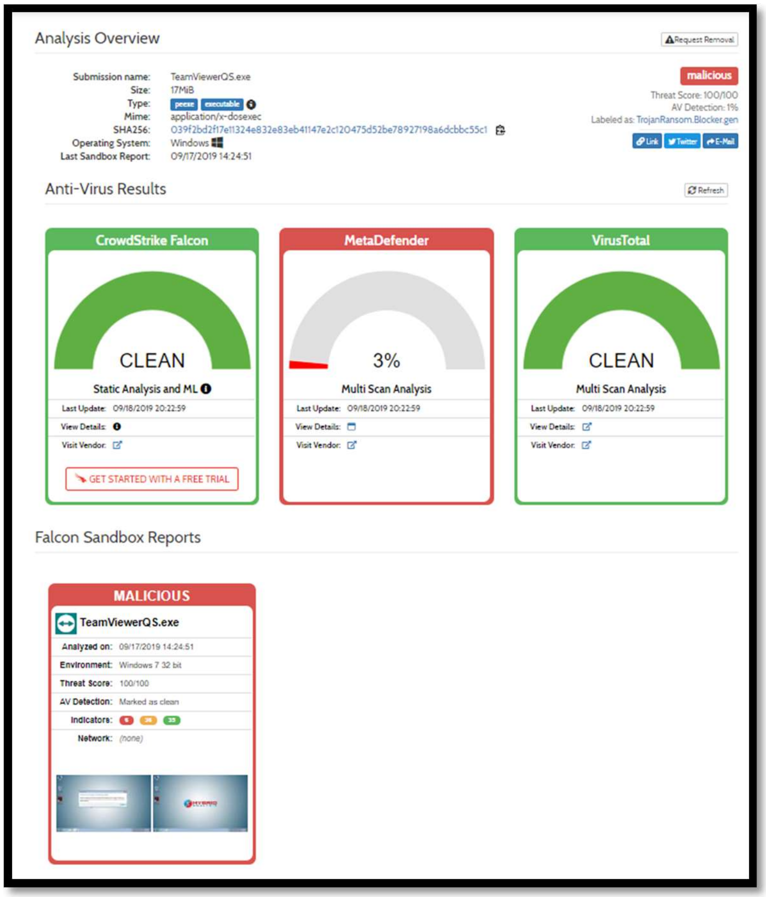

engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967

JA3 = 4d7a28d6f2263ed61de88ca66eb011e3 (Emotet)

JA3S = 80b3a14bccc8598a1f3bbe83e71f735f (C2 Server Response)

For instance, the Emotet mentioned above could support stealing sensitive and private information.

4. This type of event is difficult to be detected by antivirus tools:



Analysis Overview

Submission name: TeamViewerQS.exe
Size: 17MiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: 039f2bd2f17e11324e832e83eb41147e2c120475d52be78927198a6dcbbc55c1
Operating System: Windows
Last Sandbox Report: 09/17/2019 14:24:51

malicious
Threat Score: 100/100
AV Detection: 1%
Labeled as: TrojanRansom.Blocker.gen

Anti-Virus Results

CrowdStrike Falcon
CLEAN
Static Analysis and ML
Last Update: 09/18/2019 20:22:59
View Details:
Visit Vendor:

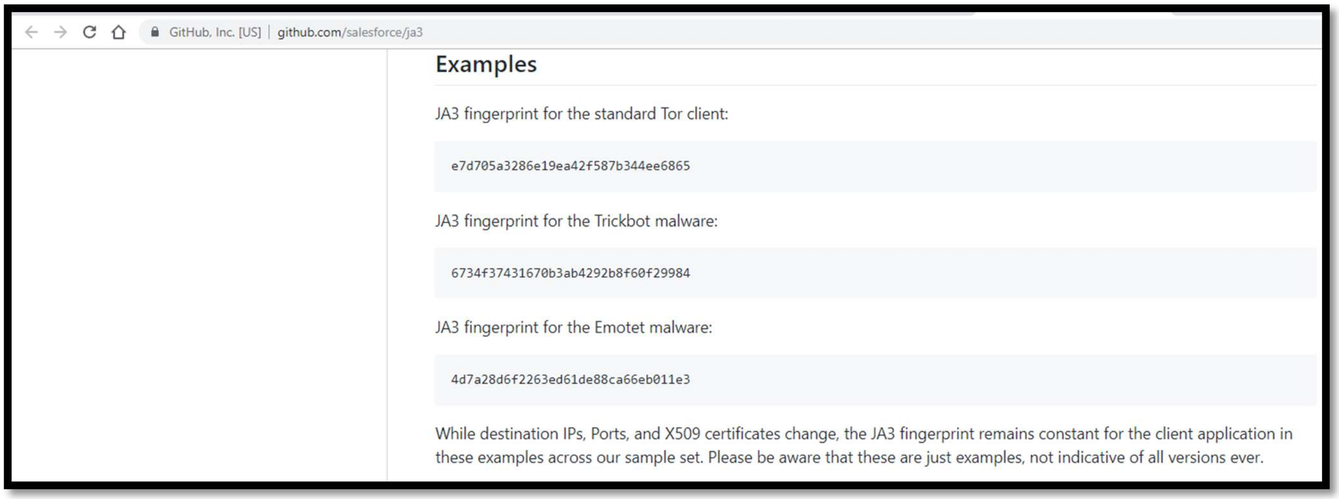
MetaDefender
3%
Multi Scan Analysis
Last Update: 09/18/2019 20:22:59
View Details:
Visit Vendor:

VirusTotal
CLEAN
Multi Scan Analysis
Last Update: 09/18/2019 20:22:59
View Details:
Visit Vendor:

Falcon Sandbox Reports

MALICIOUS
TeamViewerQS.exe
Analyzed on: 09/17/2019 14:24:51
Environment: Windows 7 32 bit
Threat Score: 100/100
AV Detection: Marked as clean
Indicators: 6 38 33
Network: (none)

5. A possible explanation for the results obtained may be due to the inappropriate use of the JA3 in the development or recent updates of the software.



Examples

JA3 fingerprint for the standard Tor client:

```
e7d705a3286e19ea42f587b344ee6865
```

JA3 fingerprint for the Trickbot malware:

```
6734f37431670b3ab4292b8f60f29984
```

JA3 fingerprint for the Emotet malware:

```
4d7a28d6f2263ed61de88ca66eb011e3
```

While destination IPs, Ports, and X509 certificates change, the JA3 fingerprint remains constant for the client application in these examples across our sample set. Please be aware that these are just examples, not indicative of all versions ever.

References

- https://www.virustotal.com/gui/file/039f2bd2f17e11324e832e83eb41147e2c120475d52be78927198a6dcbbc55c1/behavior/VirusTotal%20Jujubox
- https://www.hybrid-analysis.com/sample/039f2bd2f17e11324e832e83eb41147e2c120475d52be78927198a6dcbbc55c1
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/inspecting-encrypted-network-traffic-with-ja3/
- https://www.malwarebytes.com/emotet/
- https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967
- https://sslbl.abuse.ch/ja3-fingerprints/4d7a28d6f2263ed61de88ca66eb011e3/
- https://github.com/salesforce/ja3