

A Little Rant About The Use of VirusTotal

Martijn Grooten

Virus Bulletin

@martijn_grooten

A Little Rant About The Use of VirusTotal

Martijn Grooten

Virus Bulletin

@martijn_grooten



SHA256: 28c061018f511dac3ac20cca1b78b57388fd4ecca1e47ec930606d1809e0cab5
File name: 3.js
Detection ratio: 2 / 54
Analysis date: 2016-12-01 11:10:12 UTC (0 minutes ago)



Analysis Additional information Comments Votes

Antivirus	Result	Update
Fortinet	JS/Nemucod.F803!tr.dldr	20161201
Ikarus	Win32.SuspectCrc	20161201
ALYac	✓	20161201
AVG	✓	20161201
AVware	✓	20161201
Ad-Aware	✓	20161201
AegisLab	✓	20161201
AhnLab-V3	✓	20161201
Alibaba	✖	20161201
Antiy-AVL	✓	20161201
Arcabit	✓	20161201
Avast	✓	20161201
Avira (no cloud)	✓	20161201
Baidu	✓	20161201



SHA256: 28c061018f511dac3ac20cca1b78b57388fd4ecca1e47ec930606d1809e0cab5

File name: 3.js

Detection ratio: 2 / 54

Analysis date: 2016-12-01 11:10:12 UTC (0 minutes ago)

Analysis

Additional information

Comments

Votes

AVware	✓	20161201
Ad-Aware	✓	20161201
AegisLab	✓	20161201
AhnLab-V3	✓	20161201
Alibaba	✗	20161201
Antiy-AVL	✓	20161201
Arcabit	✓	20161201
Avast	✓	20161201
Avira (no cloud)	✓	20161201
Baidu	✓	20161201

Conclusion

Bypassing static detection scales quite well.

Bypassing dynamic detection does not.