

Forum:[Hack Forums](#)

Thread: [Antivirus recommendations, malware identification tools, and news sources.](#)

ra1d - March 29, 2017, 8:36 pm

Antivirus recommendations

Antivirus recommendations are always hard to give as it's a very dynamic market. Malware is developing at rapid speed, and so Antivirus software needs to be up-to-date constantly. However, there are Antivirus companies that have a reputation of doing things a bit better than others, which is why it is still important to use an Anti-virus software. I always recommend using non-biased organizations to come to your own conclusions, so I will list some of those sources that I personally trust.

[AV-Comparatives.org](#)

[AV-TEST.org](#)

Malware identification and research tools

Now if you want to do your own research, or want to double check, triple check, etc... then there is a huge list of useful sources for the purpose of malware research.

File Scanners / Analysis:

[Malwr.com](#)

[VirusTotal.com](#)

[ReasonSecurity](#)

[Hybrid Analysis](#)

[ViCheck.ca](#)

Link / Website scanners:

[ZeuS Tracker](#) - Maintained by abuse.ch

[Ransomware Tracker](#) - Maintained by abuse.ch

[VirusTotal.com](#) - Maintained by Google

[hpHosts](#) - Maintained by MalwareBytes

[AbuseIPDB.com](#) - Maintained by Marathon Studios

[Sitecheck Sucuri](#) - Maintained by Sucuri

[MXToolBox Blacklist](#) - Maintained by MXToolBox

[Website Scanner Quttera](#) - Maintained by Quttera

[urlQuery.net](#) - Maintained by urlQuery

[SCUMWARE.ORG](#) - Maintained by SCUMWARE.ORG

[Google Safe Browsing](#) - Maintained by Google

NOTE: Please do not rely on only one source, scan at multiple places.

Other analysis tools or useful websites:

[ThreatMiner.org](#) - Threat search engine

[malc0de.com](#) - Multi-purpose site & has some cool scripts!

[CRDF Labs](#) - Threat search engine

[Norse Attack Map](#) - Overview of live attacks. (Not super useful, but cool to have on a big monitor or projected.)

[CYBERTHREAT REAL-TIME MAP](#) - Overview of live attacks. (Not super useful, but cool to have on a big monitor or projected.)

Security news outlets or persons

[Mikko Hypponen Twitter](#)

[Peter Kruse Twitter](#)

[BleepingComputer.com](#)

[Malware Must Die! \(blog\)](#)

[Malwarebytes Blog](#)

[Microsoft Security Bulletins](#)

[ThehackerNews Twitter](#)

[ThehackerNews Website](#)

[Threatpost](#) - Owned by Kaspersky

[Securelist](#) - Owned by Kaspersky

[Naked Security](#) - Owned by Sophos

FamousHater - March 29, 2017, 8:39 pm

pretty sad u left off one of the best security sites out there in bleepingcomputer.com

Mi2414 - March 29, 2017, 8:41 pm

Some new links for me to read over, Thanks for the great resources. I've heard of Hybrid Analysis before and it works really nicely. I'll have to check out the new ones once I get more sleep.

ra1d - March 29, 2017, 8:41 pm

(Mar 29, 2017 08:39 PM)FamousHater Wrote: [\[CITE\]](#) pretty sad u left off one of the best security sites out there in bleepingcomputer.com

I don't know how that is sad to you.

Added it nonetheless.

Mr. Robot - March 29, 2017, 8:46 pm

Great thread dude. In the future we could collab or do a proper walk through on an analysis of a file.

Eagle 95 - March 29, 2017, 11:52 pm

That's a good list you've got there. Thanks for making it.

ra1d - March 30, 2017, 12:17 am

(Mar 29, 2017 08:46 PM)Mr. Robot Wrote: [\[CITE\]](#) Great thread dude. In the future we could collab or do a proper walk through on an analysis of a file.

That'd be cool. ?

(Mar 29, 2017 11:52 PM)Eagle 95 Wrote: [\[CITE\]](#) That's a good list you've got there. Thanks for making it.

No worries.

Stashyy - March 30, 2017, 12:30 am

I don't use antivirus because i know i dont download
but nice thread you got there man

ra1d - March 30, 2017, 12:36 am

(Mar 30, 2017 12:29 AM)Friedrich Nietzsche Wrote: [\[CITE\]](#) It truly is disappointing how those online sandboxes (Malwr and Hybrid-Analysis) both are extremely easy to detect, despite their attempts to randomizes their VMs and prevents signatures from being created for them. Manual analysis would be much more reliable if you know how to.

This thread is not targeted for malware researchers.

Obviously if you're doing malware research you will need to user way more advanced software such as IDA, OllyDbg, Scylla, OllyDumpExe, etc...

(Mar 30, 2017 12:31 AM)Friedrich Nietzsche Wrote: [\[CITE\]](#) This is a terrible decision. You should look up RIG sometimes, it is a silent infection vector that does not rely on any user actions at all.

Agreed.

Not just RIG, there's plenty of other very useful exploit kits that you need to be vary of.

Might have to make a thread for personal OpSec optimization.

ra1d - March 30, 2017, 3:14 am

(Mar 30, 2017 03:12 AM)Friedrich Nietzsche Wrote: [\[CITE\]](#) I noticed, however my point is that even those services are in NO WAY near reliable. Detecting them takes 2 lines of code.

I can only agree.

You're arguing with your self at this point.

?

Sparkfear - March 30, 2017, 1:10 pm

You forgot <https://www.reverse.it/> even though it's almost the same as hybrid-analysis.

R?gicide - April 1, 2017, 12:01 pm

Nice post, thanks for this.

RepForums - May 10, 2017, 8:12 am

This is great, i can now sub to this and have it at hand when im stuck and need to use something on the list, this is getting added to the collection of handy info, thanks ra1d, good thread! ?