

Forum:[Hack Forums](#)

Thread: [Scan/Analyze files for malware?](#)

ailo - February 14, 2022, 3:15 am

What's the best way to analyze/scan files beside using virustotal, as most malware can bypass it. Is there any tutorials or way to figure out if the code is malicious, what's the best way to reverse engineer files?

SentByGod - February 14, 2022, 2:29 pm

I came across this website [analyze.intezer.com](#) seems like after you upload a file it gets analyze I don't know much but maybe this can help someone.

SIM-5033784 - February 14, 2022, 5:32 pm

(Feb 14, 2022 04:15 AM)ailo Wrote: [\[CITE\]](#) What's the best way to analyze/scan files beside using virustotal, as most malware can bypass it.

Is there any tutorials or way to figure out if the code is malicious, what's the best way to reverse engineer files?

This is a rather broad question but to address a few things:

> beside using virustotal, as most malware can bypass it

Well yes and no. Obfuscators can evade anti-malware processes but it's a cat and mouse game. Most obfuscator vendors will ask you to not upload samples to virustotal because the output files get shared as part of VirusTotal's security intelligence data feed where anyone who is paying can pull samples from the feed which the AV companies have people paid to do that all day long. I've found that <https://www.hybrid-analysis.com/> is useful for this kind of things.

> Is there any tutorials or way to figure out if the code is malicious

There are tutorials, I don't know any good ones as I don't do security research as my job. I would start with learning what Software Reverse Engineering is (<https://www.geeksforgeeks.org/software-engineering-reverse-engineering/>) and go down the rabbit hole.

> what's the best way to reverse engineer files

It depends on what you're trying to accomplish. The NSA released a tool called Ghidra (<https://ghidra-sre.org/>) which allows you to open executables and read the disassembly. It will even try to convert it back to C for you. Other tools like BinaryNinja and IDA Pro are also good at this. But they all assume you have an understanding of reverse engineering and know how to read C + Assembly. Often malware is more simple and written in C#/VisualBasic or AutoIt where specialized tools for those languages are better suited. You'll have to learn the right tool for the job.

ailo - February 15, 2022, 1:34 pm

(Feb 15, 2022 02:31 PM)Incog Wrote: [\[CITE\]](#) btw on the other end, the common malware analysis detection tricks youll see are

- Checking disk space (under 50 gigs = vm)
- Checking device username (some analysers have hardcoded usernames)

- Checking IP (there are api's that can check if the ip of the machine it is running on is part of a datacenter)
- Checking system info (disk names, certain cpu models, since they can be indicators of a VM)
- Checking if the program is being emulated (normally very simple to bypass in an analysis sense, but make sure to watch out for sleep calls)
- Checking if certain processes are running (dnspy, taskmgr, ghidra, etc)
- Checking if sandboxie ddl's are loaded

Those obviously aren't all, but some things malware may do
seems like malware is pretty sophisticated, i'm just tryna download some pirated files.

K1. - February 15, 2022, 2:11 pm

[ailo](#) if it's your malware then you don't want to use VT atall because they report the data back to AV companies

If it's just a file you have and you want to check if it's safe or not then in my opinion VT should be fine, if it's gonna bypass that then chances are it'll bypass the AV you have running on your machine anyway

ailo - February 16, 2022, 3:22 am

(Feb 15, 2022 02:35 PM)Incog Wrote: [CITE](#) it's a cat and mouse game between AV and malware, so it will keep getting more advanced, but if you wanna download pirated stuff, just do what others have said and your risk to being infected is reduced ?

Not zero tho, so do be careful ailo.

What about apk files and lets say the setup files for the adobe products, do i check it the same way?

Stetsed - February 18, 2022, 8:21 am

For scanning I would agree with Incog Hybrid Analysis is a good one. If you want to observe behavior I would generally recommend a virtual machine, with wireshark running on the host to avoid detection.(And spoofing alot of the common VM detection methods like smbios)

\$hady - February 22, 2022, 8:07 pm

Can use Floss in command prompt to reverse engineer the file statically. If the results are gibberish you know the malware is encrypted.

Can also download process dump to dynamically analyze the malware (pd64.exe). Let's you dump the malware directly from the memory so you have a chance of seeing what it's actually doing. Import the dump in something like IDA and get a more fruitful view. I'd do this in a virtual machine for obvious reasons.