

Forum:[Hack Forums](#)

Thread: [Crypter is fud on scan but detected on VM](#)

Aril - April 30, 2024, 3:08 am

i wrote my own crypter and when i scan it on scanner.to (90 seconds, internet enabled) it bypasses WD and almost all important AV's.

But when i download the executable to my VM , WD flags it as a malware. even though the video/scan results produced on scanner.to shows that my runpe is working and not being detected.

Any suggestions ? thanks guys

InspectorGadget - April 30, 2024, 3:15 am

Is that scanner doing runtime detection or just scantime / passive detection?

If it's missing runtime, then yeah there's a huge chance you could have evaded passive scanning but not dynamic analysis.

Aril - April 30, 2024, 3:18 am

(Apr 30, 2024 03:15 AM)InspectorGadget Wrote: [\[CITE\]](#) Is that scanner doing runtime detection or just scantime / passive detection?

If it's missing runtime, then yeah there's a huge chance you could have evaded passive scanning but not dynamic analysis. That scanner is doing both runtime and scantime

Here's the result

<https://scanner.to/result/8EUC8BjYwPVp>

You can even watch the video it produces, FUD on runtime.

Yet being detected when downloaded from the internet to VM...

InspectorGadget - April 30, 2024, 3:21 am

Can you send a screenshot of the exact detection message?

Aril - April 30, 2024, 3:52 am

(Apr 30, 2024 03:21 AM)InspectorGadget Wrote: [\[CITE\]](#) Can you send a screenshot of the exact detection message?

It being detected as soon as i download it, not even clicking on the file.

here is another scantime scan -

<https://i.postimg.cc/3NFxFMNH/Screenshot-2024-04-30-033447.png>

PureCoder - April 30, 2024, 5:59 am

(Apr 30, 2024 03:52 AM)Aril Wrote: [\[CITE\]](#) ~

dropping the file and downloading the file are two different things.

downloading a file from a browser will trigger windows smartscreen.

Aril - April 30, 2024, 6:16 am

(Apr 30, 2024 05:59 AM)PureCoder Wrote: [\[CITE\]](#) dropping the file and downloading the file are two different things.

downloading a file from a browser will trigger windows smartscreen.

I re-obfuscated some strings and added execution delay, seems to solve the problem for now.

But I am not sure how long it will last before being flagged again, I wonder if the execution delay was that important to avoid detection in my case.

ttbr0 - April 30, 2024, 7:05 am

I wonder if the cloud scanners machine resources are low which might disable some features in defender for the performance trade off... the windows 10 defender video has an instance where everything pops in at the same time which makes me think hardware resources might be restricted?

HiDDen12 - April 30, 2024, 8:27 am

can you send the file to check ?

boyah1337 - April 30, 2024, 11:09 am

(Apr 30, 2024 03:08 AM)Aril Wrote: [\[CITE\]](#) -

I am surprised that nobody said this here but it is an obvious case of AI engine detection. It is very strong and it is enough for it to have 2-3 samples of your file in order to flag any of your future files.

With WD the only "correct" test is download from the internet, not "pasting" into VM, scanner.to does it wrong! If you care about technicals go and learn about ZoneID and why it matters.

For those who do not know, WD is region based which means that even if your "file" is undetected in your VM tests (Let's say USA geo), it doesn't mean that it will work the same on China or colombia.

Also, downloading EXE file from web or downloading ZIP with EXE from web is 2 different things..

(Apr 30, 2024 03:52 AM)Aril Wrote: [\[CITE\]](#) -

You leaked your GEO here btw, if you plan on doing illegal shit, at-least don't post stuff like this.

LTC - May 1, 2024, 2:40 pm

It can be that ur scanner uses an outdated version Or only scans Scantime

Sand Ferret - May 1, 2024, 2:51 pm

(Apr 30, 2024 11:09 AM)boyah1337 Wrote: [\[CITE\]](#) I am surprised that nobody said this here but it is an obvious case of AI engine detection. It is very strong and it is enough for it to have 2-3 samples of your file in order to flag any of your future files.

With WD the only "correct" test is download from the internet, not "pasting" into VM, scanner.to does it wrong! If you care about technicals go and learn about ZoneID and why it matters.

For those who do not know, WD is region based which means that even if your "file" is undetected in your VM tests (Let's say USA geo), it doesn't mean that it will work the same on China or colombia.

Also, downloading EXE file from web or downloading ZIP with EXE from web is 2 different things..

Thank god someone said it.

You should be uploading your file to a host, downloading it from a browser like Edge/Chrome and then executing it - just like a victim would.

It blows my mind all the crypter threads that post their fud "proof" by copying and pasting the stub directly into a VM. Not only is it misleading, it's likely a marketing tactic as their product is shit!

AdamEve - May 29, 2024, 11:49 am

couldn't it also depend on the stub?

secret_code - May 30, 2024, 10:06 am

(Apr 30, 2024 06:16 AM)Aril Wrote: [\[CITE\]](#) I re-obfuscated some strings and added execution delay, seems to solve the problem for now.

But i am not sure how long it will last before being flagged again, i wonder if the execution delay was that important to avoid detection in my case.

delays are a good point, but not the best technique, depending on the language you wrote the crypter in, let's say c++ for instance, if your crypter is using low level system calls it will SURELY 100% be detected because AVs will monitor those type of calls very frequently, another reason it might be the encryption algorithm you have used for the crypter, i hope you didn't use xor, that is the most ridiculous way of building crypters, xor is so easy to reverse and so easy to detect, use stronger and safer alternatives like AES for instance. there are better techniques you can use to increase the chance of evasion, one is certificate-signing*, when u sign your executable with a valid certificate, the AV detection system will think it is legit(NOT 100% bulletproof), then you have the *FILE REPUTATION problem, where the AV detects a file type that has not been seen so frequently in the wild, it will flag it as suspicious, then you also have the problem of *FILE SIZE*, large executable files usually will bypass the AV, why? because AV usually have a timeout for large scans, this is because scanning a file requires significant amount of computational resources and time, the AV will skip it instead or partially scan it, fill your source code with useless garbage content to make it bigger, the real code should be placed at the end of the file(after the garbage content), so when the scan occurs, the only thing that will be scanned will be garbage and your actual code will bypass the scan because of the AV scan interruption due to its size, the garbage content should be something normal for the AV to see, otherwise it will be suspicious to the scan. AVs will also detect suspicious network activities(network-fingerprints) in your case that might be a contributor factor...

(Apr 30, 2024 11:09 AM)boyah1337 Wrote: [\[CITE\]](#) I am surprised that nobody said this here but it is an obvious case of AI engine detection. It is very strong and it is enough for it to have 2-3 samples of your file in order to flag any of your future files.

With WD the only "correct" test is download from the internet, not "pasting" into VM, scanner.to does it wrong! If you care about technicals go and learn about ZoneID and why it matters.

For those who do not know, WD is region based which means that even if your "file" is undetected in your VM tests (Let's say USA geo), it doesn't mean that it will work the same on China or colombia.

Also, downloading EXE file from web or downloading ZIP with EXE from web is 2 different things..

You leaked your GEO here btw, if you plan on doing illegal shit, at-least don't post stuff like this. good point