

Forum:[Hack Forums](#)

Thread: [AVCheck, antiscan and these kind of sites \[GIVE YOUR OPINION\]](#)

justalemon - July 9, 2022, 7:14 pm

Hi there!

These past days had a few issues where I checked a file which wasn't previously detected by WD on Avcheck, and afterwards when I try to copy the file again into the VM with WD, it gets detected. I was wondering myself if AVCheck distributes the file checked. What about antiscan.me? Same happened to me with checkzilla.io.

What do you think about this? Did this happened to you in the past? Do you think they distribute the files against what they confirm at their sites?

Thanks in advance for your time and opinions.
Cheers ?

NotKover - July 9, 2022, 7:45 pm

The issue with most of those scanners is the operators dont keep all the scanners up to date

justalemon - July 9, 2022, 8:33 pm

(Jul 9, 2022 07:45 PM)NotKover Wrote: [\[CITE\]](#) The issue with most of those scanners is the operators dont keep all the scanners up to date

Yeah, but anyhow, it shouldn't get your file detected because of that right? I mean, why would WD detect it after scanning it there? It's crazy XD

Athr - July 9, 2022, 8:43 pm

(Jul 9, 2022 08:33 PM)justalemon Wrote: [\[CITE\]](#) Yeah, but anyhow, it shouldn't get your file detected because of that right? I mean, why would WD detect it after scanning it there? It's crazy XD

Can you try disabling internet on the VM and rescan it?

I have read on the forums that WD has cloud detection.

Jack Herrer - July 9, 2022, 8:51 pm

The Best Way is Don't Scan Anywhere for a week or month, and check again.

(Jul 9, 2022 08:33 PM)justalemon Wrote: [\[CITE\]](#) Yeah, but anyhow, it shouldn't get your file detected because of that right? I mean, why would WD detect it after scanning it there? It's crazy XD

Sometimes it's detecting Clean File with No Code Inside, WD Is Broken, Microsoft is not good on this work.

Frost Crypt - July 10, 2022, 12:32 am

i can confirm avcheck is sometimes slow of updating wd database, tested in my vm and it was showing detection while it was clean on avcheck, no it wasn't cloud detection.

also when i refuted my stub for avast and forgot to release the update that day and released it the next day, avast was seeing the stub again while nobody ever used that stub so what can i say...is hard to live with these websites but harder to live without.

NotKover - July 10, 2022, 6:34 am

(Jul 9, 2022 08:33 PM)justalemon Wrote: [\[CITE\]](#) Yeah, but anyhow, it shouldn't get your file detected because of that right? I mean, why would WD detect it after scanning it there? It's crazy XD

because the scanner is out dated

nulluser123 - July 13, 2022, 12:59 pm

Looking for a dynamic scanner similar to dyncheck - I know checkzilla exists but that stuff sucks, doesn't show detections the same dyncheck once did. Price doesnt matter. Does anyone know of any?

Ph4n70M Phr34K - July 13, 2022, 1:02 pm

My opinion is that scanning websites such as avcheck, antiscan, checkzilla are never accurate and it is always better to just do manual check in virtual environment, it takes time but at least you have full control and you can be sure that your file will not be distributed.

nulluser123 - July 14, 2022, 4:25 am

(Jul 13, 2022 06:36 PM)Dyne Wrote: [\[CITE\]](#) Yes.

Adding a bit to this;

There is a common misconception in what people need, or truly need really. Especially when it comes to a crypter.

You test against what you're up against. Simple. There are ESET, Kaspersky, Avast etc licenses for dirt cheap, [AmazingLicense](#) is one to name, in which they can be installed on virtual machines for security research and manual scanning. Remember to roll your snapshot back in your VM, and make sure sharing of samples is OFF.

The big 5, ESET, Kaspersky, Avast, AVG and WD should handle the majority portion of home targets.

For corporate/commercial (depending on spearfishing target by threat actor), WebRoot Enterprise, Comodo, HP Wolf ENTERPRISE(not to be confused with HP Wolf freeware with modern workstations) etc. class which are, imo, the best in the business require specialty tools to avoid dynamic and tripwire detections as well as SOCKS hollowing functionality for internal corporate VPNs.

The problem is that when you're pushing out, say, 10-100 stubs, polymorphically generated, and want to test the % of FUD of the stubs, you don't have the time to load up VMs and scan every binary manually. An automated service that provides API interface is very useful to have. Dyncheck used to work great, now its gone. Any alternatives?

SIM-4982069 - August 19, 2022, 6:46 am

(Jul 14, 2022 04:25 AM)nulluser123 Wrote: [\[CITE\]](#) The problem is that when you're pushing out, say, 10-100 stubs, polymorphically generated, and want to test the % of FUD of the stubs, you don't have the time to load up VMs and scan every binary manually. An automated service that provides API interface is very useful to have. Dyncheck used to work great, now its gone. Any alternatives?
Try kleenscan

justalemon - August 20, 2022, 2:44 am

(Aug 19, 2022 06:46 AM)leviackerman_ Wrote: [\[CITE\]](#) Try kleenscan
Yeah, I have tested it already, but results aren't very accurate always either. I preffer antiscan for the moment, but I appreciate very much the suggestion. Thanks!

nulluser123 - August 21, 2022, 11:36 am

(Aug 20, 2022 02:44 AM)justalemon Wrote: [\[CITE\]](#) Yeah, I have tested it already, but results aren't very accurate always either. I preffer antiscan for the moment, but I appreciate very much the suggestion. Thanks!
Antiscan is just reselling avcheck!

Capos666 - August 30, 2022, 6:26 am

(Jul 13, 2022 12:59 PM)nulluser123 Wrote: [\[CITE\]](#) Looking for a dynamic scanner similar to dyncheck - I know checkzilla exists but that stuff sucks, doesn't show detections the same dyncheck once did. Price doesnt matter. Does anyone know of any?

Agree With You, i was Crypting some Files, Full FUD in AVCheck, as soon as i download the Files in My RDP Windows Defender Prompt a new Virus scan and delete the payload, i think is test and error, Crypt Your file, change Stub, Icon, Assembly, Execution Delay and SO, install Mos common AV in RDP, uncheck all the "Send Sample" From AV and WD and just download your freshly Crypted payload, If some AV prompts a virus, Then Refud everything, is a pain in the ass, Buy 100% Accurate, since You can Update the AV and WD Database and scan With Up to date software. AVCheck is not good enough, 100% Clean and WD immediately detects.

Frost Crypt - August 30, 2022, 10:48 am

(Aug 30, 2022 06:26 AM)Capos666 Wrote: [\[CITE\]](#) Agree With You, i was Crypting some Files, Full FUD in AVCheck, as soon as i download the Files in My RDP Windows Defender Prompt a new Virus scan and delete the payload, i think is test and error, Crypt Your file, change Stub, Icon, Assembly, Execution Delay and SO, install Mos common AV in RDP, uncheck all the "Send Sample" From AV and WD and just download your freshly Crypted payload, If some AV prompts a virus, Then Refud everything, is a pain in the ass, Buy 100% Accurate, since You can Update the AV and WD Database and scan With Up to date software. AVCheck is not good enough, 100% Clean and WD immediately detects.

checkzilla has internet off and your defender detection is cloud detection and requires internet so is not a bug, more like a limitation