

Forum: [Hack Forums](#)

Thread: [Dyncheck Suspicious Behavior - Possible Distribution](#)

The Grand Oracle - April 2, 2020, 6:03 pm

I was scanning some test files on Dyncheck and I noticed connections to my server. I don't even have a subscription where I can turn internet on, so naturally I checked that specific scan to see the settings I used. Internet Connection: Block. But clearly not as I'm getting connections. The file I was scanning is private.

Upon testing with known threats like #, Internet Connection: Block, but no connections to my server. Actually blocking the connection this time.

Its possible Dyncheck first scans your file without internet and sees if AVs recognize it as a known threat, and if not, "has a bug", that causes internet to turn on server-side, which we all know causes distributions. Maybe they have some sort of deal on the backend going on with AV companies.

Potential false advertising, be careful. Run your own tests with private + public malware and post your results here.

Ren And Stimpy - April 3, 2020, 2:50 am

(Apr 2, 2020 06:03 PM)The Grand Oracle Wrote: [\[CITE\]](#) I was scanning some test files on Dyncheck and I noticed connections to my server. I don't even have a subscription where I can turn internet on, so naturally I checked that specific scan to see the settings I used. Internet Connection: Block. But clearly not as I'm getting connections. The file I was scanning is private.

Upon testing with known threats like #, Internet Connection: Block, but no connections to my server. Actually blocking the connection this time.

Its possible Dyncheck first scans your file without internet and sees if AVs recognize it as a known threat, and if not, "has a bug", that causes internet to turn on server-side, which we all know causes distributions. Maybe they have some sort of deal on the backend going on with AV companies.

Potential false advertising, be careful. Run your own tests with private + public malware and post your results here.

Always test with internet on for a REAL result, and don't use run time scanners LOL.
Manually test against the popular AVs from your own test machines.

Having internet off, will not give you the TRUE results of a test.

Also when you do "send" your file to your "clients" and they have their AV on, yes its going to be fully on and yes it will distrute, which is why you do the same for a REAL result, and which is why they sell and create crypters....

aude - January 25, 2021, 10:28 am

I read here it was no-distributing : <https://hackforums.net/showthread.php?tid=5571516>

BUT i also check there is no such mention today on their website. (or i missed it)

Also, while they propose to scan on all AV, are the no-distribute option set up in those AV ?

"Manually test against the popular AVs from your own test machines."

Yep, i think there is no best way.. what AV would you prioritize ? (WD and avast for sure, and which ones more ?)