

Forum:[Hack Forums](#)

Thread: [\[solved\]Ran this file in sandboxie, help determining if file is a virus or not?](#)

Mr. Anderson - June 5, 2015, 10:06 pm

Hey there,

I was wondering if any of you guys could do me quick favor and analyze a file for me? I am noob when it comes to this stuff, so if you could help it could be appreciated:

There is an EXE file in this zip file:

http://gamedata.box.sk/_cht5/Life.Is.Strange.+3.Trainer-ALI213.zip

I was wondering if you could take a look at the EXE file inside that zip file for me and tell me if its a virus or not. I ran it in sandboxie(stupid I know), and for some reason skype opened up :c. I just dont want all my contacts to get lost, so I changed my password. Any help is appreciated. I just dont want to worry about this all the time. I thought sandboxie was enough and I scanned this file and it looked like a typical cheat engine script, but imagine my suprise when skype opened up!

So far my system appears to be fine, but as we all know, appearances can be deceiving. I have a dynamic firewall which catches everything and it has not notified me of any new programs. I use kaspersky.

Any help is really appreciated, thanks. If anyone could give me peace of mind, that would be great.

XionHacks - June 5, 2015, 11:06 pm

It seems a little odd, I was unable to run it because of my anti malware responding to it as a "HackTool.CheatEngine" I would presume safe but do not take that as a 100% im still analyzing so please do not run it yet.

edit: Theres nothing I can find in it, it doesnt run anything on startup at all nor does it do anything malicious it is all detected and as far as I can see as a CheatEngine, Most likely safe for use. Although I would recommend waiting for someone more, well trained than me I am just a user attempting to help.

Mr. Anderson - June 5, 2015, 11:14 pm

Yes supposedly it is a cheatengine file, and you shouldn't run this without a VM!

XionHacks - June 5, 2015, 11:47 pm

(Jun 5, 2015 11:14 PM)Mr. Anderson Wrote: [\[CITE\]](#) Yes supposedly it is a cheatengine file, and you shouldn't run this without a VM!

I had it ran through VirusTotal Malwr and Anubis

?Lax - June 6, 2015, 12:51 am

If you are running it through a VM you are fine, but other than that if looks safe to me.

Mr. Anderson - June 6, 2015, 10:56 am

(Jun 6, 2015 12:51 AM)?Lax Wrote: [\[CITE\]](#) If you are running it through a VM you are fine, but other than that if looks safe to me.

So it didn't launch skype like it did for me?

XionHacks - June 6, 2015, 11:03 am

(Jun 6, 2015 10:56 AM)Mr. Anderson Wrote: [\[CITE\]](#) So it didn't launch skype like it did for me? Nope, I even ran it on my computer after analyzing with my VM nothing happened I use ApateDNS to see if theres any DNS callouts there was nothing

Mr. Anderson - June 6, 2015, 12:43 pm

(Jun 6, 2015 11:03 AM)XionHacks Wrote: [\[CITE\]](#) Nope, I even ran it on my computer after analyzing with my VM nothing happened I use ApateDNS to see if theres any DNS callouts there was nothing Did the program even launch then at all? Or did it just shut down?

Sennheiser - June 6, 2015, 12:48 pm

(Jun 6, 2015 12:43 PM)Mr. Anderson Wrote: [\[CITE\]](#) Did the program even launch then at all? Or did it just shut down?

the program does launch, i ran it on my test machine and it doesn't do anything except, well what its intended lol

Mr. Anderson - June 6, 2015, 1:16 pm

(Jun 6, 2015 12:48 PM)Sennheiser Wrote: [\[CITE\]](#) the program does launch, i ran it on my test machine and it doesn't do anything except, well what its intended lol

Thank you mate, closing this then.