

Forum:[Hack Forums](#)

Thread: [I believe I am infected can't confirm](#)

y389525 - March 16, 2019, 5:19 am

FRST.txt: <https://hastebin.com/penavupive.md>

Addition.txt: <https://hastebin.com/ewayadebal.makefile>

mbam.txt: <https://hastebin.com/oxicifupej.sql>

Rkill.txt: <https://hastebin.com/defihesibi.cs>

Please help.

5chn4pp - March 16, 2019, 5:42 am

(Mar 16, 2019 05:19 AM)y389525 Wrote: [\[CITE\]](#) FRST.txt: <https://hastebin.com/penavupive.md>

Addition.txt: <https://hastebin.com/ewayadebal.makefile>

mbam.txt: <https://hastebin.com/oxicifupej.sql>

Rkill.txt: <https://hastebin.com/defihesibi.cs>

Please help.

All logs are clean, your computer is not infected. However this does not mean that the file is legit, it might be taking passwords while running for example. Again its impossible to know.

y389525 - March 16, 2019, 5:46 am

(Mar 16, 2019 05:42 AM)5chn4pp Wrote: [\[CITE\]](#) All logs are clean, your computer is not infected. However this does not mean that the file is legit, it might be taking passwords while running for example. Again its impossible to know.

Not sure if its just me but HF seems to be running pretty slow for me today, also I downloaded but never executed the file so I can't tell if it is clean. I scanned the program with mbam also at first and it came back like this. I quarantined it but when I restored it to scan it again it came back clean. I have already deleted the program.

First scan: <https://hastebin.com/ugowuroren.sql>

Restored from quarantine: <https://hastebin.com/sukepegopo.sql>

5chn4pp - March 16, 2019, 6:52 am

(Mar 16, 2019 05:46 AM)y389525 Wrote: [\[CITE\]](#) Not sure if its just me but HF seems to be running pretty slow for me today, also I downloaded but never executed the file so I can't tell if it is clean. I scanned the program with mbam also at first and it came back like this. I quarantined it but when I restored it to scan it again it came back clean. I have already deleted the program.

First scan: <https://hastebin.com/ugowuroren.sql>

Restored from quarantine: <https://hastebin.com/sukepegopo.sql>

That's one of the files that it drops, also noted in the hybrid analysis.

For a faster internet, consider using a fast dns resolver, it might help:

Code <https://1.1.1.1/> (HF) doesn't like this link apparently.

y389525 - March 16, 2019, 6:53 am

(Mar 16, 2019 06:52 AM)5chn4pp Wrote: [\[CITE\]](#) That's one of the files that it drops, also noted in the

hybrid analysis.

For a faster internet, consider using a fast dns resolver, it might help:

[qoute]https://1.1.1.1/[/qoute] (HF) doesn't like this link apparently.

What do I do with or where do I place it? Also does this mean I am clean for now?

1.1.1.1/" target="_blank" rel="noopener" class="mycode_url">https:// 1.1.1.1/

5chn4pp - March 16, 2019, 7:22 am

(Mar 16, 2019 06:53 AM)y389525 Wrote: [\[CITE\]](#) What do I do with or where do I place it? Also does this mean I am clean for now?

1.1.1.1/" target="_blank" rel="noopener" class="mycode_url">https:// 1.1.1.1/

Follow this:

<https://support.opendns.com/hc/en-us/articles/228006987-Windows-7-Configuration>

And use 1.1.1.1 and 1.0.0.1

And yes you are clean, but that file is still not safe to use.

y389525 - March 16, 2019, 7:35 am

(Mar 16, 2019 07:22 AM)5chn4pp Wrote: [\[CITE\]](#) Follow this:

<https://support.opendns.com/hc/en-us/articles/228006987-Windows-7-Configuration>

And use 1.1.1.1 and 1.0.0.1

And yes you are clean, but that file is still not safe to use.

Thank you.