

Forum:[Hack Forums](#)

Thread: [Bought a NON-Malicious Program here, Computer says it's a virus](#)

Ooze - July 9, 2017, 5:08 pm

Hello White Hats of HF

I recently bought

<https://hackforums.net/showthread.php?tid=5661413>

Which is not a malicious program like some Rats or Keyloggers sold here

Which is why I was surprised to me my computer pre-emptively delete the file believing it was a virus

Any chance one of you could look at the program and see if it is doing something it should not be doing.

wit - July 9, 2017, 5:08 pm

Send me a link and i will check for malicious intent.

Reyyzan - July 9, 2017, 5:08 pm

Could you send me a download link so i'll take a look at it

Ooze - July 9, 2017, 5:10 pm

Only going to send the link to one known member

I don't want to get in trouble with the owner

Reyyzan - July 9, 2017, 5:10 pm

(Jul 9, 2017 05:10 PM)Ooze Wrote: [\[CITE\]](#) Only going to send the link to one known member

I don't want to get in trouble with the owner

See the details on my profile such as time spent and posts.

But no problem I understand, hope you'll resolve this and also hope this is just some false positives

wit - July 9, 2017, 5:13 pm

(Jul 9, 2017 05:10 PM)Ooze Wrote: [\[CITE\]](#) Only going to send the link to one known member

I don't want to get in trouble with the owner

The service is licensed based - sharing the program for decompilation won't affect anything.

gringo - July 9, 2017, 5:13 pm

Run it through hybrid analysis and paste the results here if you don't want to give out the bin to people. Surely a "traffic bot" can't be doing anything suspicious unless it's the way it's packed.

<https://www.hybrid-analysis.com>

Wafflemonger - July 9, 2017, 5:14 pm

(Jul 9, 2017 05:13 PM)Coder1 Wrote: [\[CITE\]](#) The service is licensed based - sharing the program for decompilation won't affect anything.

I would personally still verify with the program owner that he authorizes the decompilation of the program. Still ... it is a bot ... usually they're picked up as riskware or PUPs. Sometimes trojans depending on the bot functionality. It has automated processes that access URLs - it'll be picked up

by anti-malware.

Ooze - July 9, 2017, 5:15 pm

(Jul 9, 2017 05:13 PM)gringo Wrote: [\[CITE\]](#) Run it through hybrid analysis and paste the results here if you don't want to give out the bin to people. Surely a "traffic bot" can't be doing anything suspicious unless it's the way it's packed.

<https://www.hybrid-analysis.com>

The zip includes

3 .dll files

1 .xml files

1 .exe.config file

2 .exe files

What all do you want scanned

(Jul 9, 2017 05:14 PM)Wafflemonger Wrote: [\[CITE\]](#) I would personally still verify with the program owner that he authorizes the decompilation of the program. Still ... it is a bot ... usually they're picked up as riskware or PUPs. Sometimes trojans depending on the bot functionality. It has automated processes that access URLs - it'll be picked up by anti-malware.

This was my concern, the only 2 TOS rules Im worried about are

1. You may not leak this program

2. You may not crack my program

SO if i only share once, and they only check for a virus, then neither of those would be broken

Reyyzan - July 9, 2017, 5:31 pm

(Jul 9, 2017 05:15 PM)Ooze Wrote: [\[CITE\]](#) The zip includes

3 .dll files

1 .xml files

1 .exe.config file

2 .exe files

What all do you want scanned

This was my concern, the only 2 TOS rules Im worried about are

1. You may not leak this program

2. You may not crack my program

SO if i only share once, and they only check for a virus, then neither of those would be broken

I won't crack/unpack it and since it's license based how would I leak it ?

But you're right for looking at ToS, maybe you may ask the dev

Ooze - July 9, 2017, 6:04 pm

Hmmm ran fine in my vmbox

But would not run in a sandbox

PvPPPrincipal - July 9, 2017, 10:10 pm

(Jul 9, 2017 06:04 PM)Ooze Wrote: [\[CITE\]](#) Hmmm ran fine in my vmbox

But would not run in a sandbox

could be anti-sandboxie

5chn4pp - July 10, 2017, 12:35 am

I can check this file for you, I'm probably the only one here who knows malware best.

The program has anti-debugging features that detects the following: burp, wireshark, ettercap, dsniff, ethereal, tcpdump, ettercap, sandboxie.

Dispite that, I'm 98% sure that this program is clean, I've seen multiple HF users use the same program and none of then had malicious FRST entries.

The program is also packed with upx so the detections can be explained.

For now, you can consider the file as clean, I will continue doing a bit more debugging on it to fully make sure.

EDIT: program is officially clean.