

Forum:[Hack Forums](#)

Thread: [Then how can i know it's not binded or backdoored](#)

reyo47 - July 26, 2012, 11:51 pm

hey HF members

So i hope you all fine

my question is : how do i know if a file isn't binded or backdoored and sandbox can be bypassed by some crypters !!! ?

i thought if sandbox didn't show any suspicious app then it's not infected but it did and i had to remove it with DC remover

So what's the solution ?

Thanks for reading ?

Nordic - July 27, 2012, 12:13 pm

One simple way of checking it is to "Open Archive" with 7zip, then you can see what's inside. When you do that with legit files the message you get is that you can not open it, if the file is binded/backdoored you will see what's inside.

You can also check it with hex editors, I think there are some tutorials on here on how to do it. I know you can get the creator of the virus' email and password if that's what they are using.. But that's another story.

Good luck!

xtraesp - July 27, 2012, 12:18 pm

(Jul 27, 2012 12:13 PM)j0113 Wrote: [\[CITE\]](#) One simple way of checking it is to "Open Archive" with 7zip, then you can see what's inside.

When you do that with legit files the message you get is that you can not open it, if the file is binded/backdoored you will see what's inside.

You can also check it with hex editors, I think there are some tutorials on here on how to do it. I know you can get the creator of the virus' email and password if that's what they are using.. But that's another story.

Good luck!

Right, I just tried the 7-zip thing with a binded file of mine.

Didn't work.

@OP sandboxie should show more than one exe if it is binded.

Check for file drops with sandboxie.

Nordic - July 27, 2012, 12:28 pm

(Jul 27, 2012 12:18 PM)Myers Wrote: [\[CITE\]](#) Right, I just tried the 7-zip thing with a binded file of mine.

Didn't work.

@OP sandboxie should show more than one exe if it is binded.

Check for file drops with sandboxie.

Hmm, well I am sure that I have seen some way to check it with 7-zip.

But my memory from where or how is blurry.

Maybe it depends on how well coded the binder is.

A + - July 28, 2012, 6:09 pm

(Jul 27, 2012 12:18 PM)Myers Wrote: [\[CITE\]](#) Right, I just tried the 7-zip thing with a binded file of mine.

Didn't work.

@OP sandboxie should show more than one exe if it is binded.

Check for file drops with sandboxie.

What he said.

Also, if you learn how to read Anubis scans, you can figure it our from there.

<http://anubis.iseclab.org/>

reyo47 - July 28, 2012, 11:40 pm

(Jul 28, 2012 06:09 PM)TheCause Wrote: [\[CITE\]](#) What he said.

Also, if you learn how to read Anubis scans, you can figure it our from there.

<http://anubis.iseclab.org/>

is there any tut about it ??

or u may explain it to me :)) ??