

Forum:[Hack Forums](#)

Thread: [Can Someone check and see if this product is infected or not?](#)

Root - November 23, 2015, 1:58 am

Can someone please check this product for Viruses?

<https://hackforums.net/showthread.php?tid=5068025>

Download link: <https://www.dropbox.com/s/66decy276jc9h1t/DarkTrack.rar?dl=0>

Virus Scan:

<https://www.virustotal.com/fi/file/2d4f34d5d7a551d3091e0ba2298cad44882287b3c831f5341c243b583db39749/analysis/1448225441/>

Ik you guys don't like blackhats specially RAT users?

Who Soup - November 23, 2015, 2:05 am

I didn't download it but judging by the virus total link you provided it was a not widely used virus scanner (qihoo-360) that detected malware. I'd say the odds of it NOT being a virus are pretty high. Also it detected it as HEUR/QVM13.0.Malware.Gen which isn't a type of back door; it's simply saying it could be malware.

That's just my 2 cents ?

spyglass - November 23, 2015, 12:58 pm

The virus scans do not ring the right bells here.

First look at the virustotal scan in OP thread.

<https://www.virustotal.com/fi/file/2d4f34d5d7a551d3091e0ba2298cad44882287b3c831f5341c243b583db39749/analysis/1448225441/>

Under relationships and what do we get.

<https://www.virustotal.com/fi/file/bde16d1d4d503398fef2e3e809f6bf0ffc19b7b8d366ecd6d5a8bcb924f8ae42/analysis/>

SHA256: bde16d1d4d503398fef2e3e809f6bf0ffc19b7b8d366ecd6d5a8bcb924f8ae42

File name: DarkTrack.rar

Here a user states avast detects it.

<https://hackforums.net/showthread.php?tid=5068025&pid=48675221#pid48675221>

There is a very strong reason to think there is a virus binded to the downloaded rar and also the main client.exe inside.

Here you can see the real vt scan.

Download from the official site.

<https://www.virustotal.com/fi/file/498b3fed80c8376eb5676e89e564f05343096b9a602172f4f0fd7316a>

[4ea42c2/analysis/1448311773/](https://www.virustotal.com/fi/file/4ea42c2/analysis/1448311773/)

This is from the official site

<http://www.darktrack.comlu.com>

5chn4pp - November 23, 2015, 1:21 pm

(Nov 23, 2015 01:58 PM)spyglass Wrote: [\[CITE\]](#) The virus scans do not ring the right bells here. First look at the virustotal scan in OP thread.

<https://www.virustotal.com/fi/file/2d4f34d5d7a551d3091e0ba2298cad44882287b3c831f5341c243b583db39749/analysis/1448225441/>

Under relationships and what do we get.

<https://www.virustotal.com/fi/file/bde16d1d4d503398fef2e3e809f6bf0ffc19b7b8d366ecd6d5a8bcb924f8ae42/analysis/>

SHA256: bde16d1d4d503398fef2e3e809f6bf0ffc19b7b8d366ecd6d5a8bcb924f8ae42

File name: DarkTrack.rar

Here a user states avast detects it.

<https://hackforums.net/showthread.php?tid=5068025&pid=48675221#pid48675221>

There is a very strong reason to think there is a virus binded to the downloaded rar and also the main client.exe inside.

Here you can see the real vt scan.

Download from the official site.

<https://www.virustotal.com/fi/file/498b3fed80c8376eb5676e89e564f05343096b9a602172f4f0fd7316a4ea42c2/analysis/1448311773/>

This is from the official site

<http://www.darktrack.comlu.com>

No nigga

the reason for 14 detections is because you also scan the stub

Niko - November 23, 2015, 1:28 pm

(Nov 23, 2015 02:21 PM)Polymorphic Plague Wrote: [\[CITE\]](#) No nigga

the reason for 14 detections is because you also scan the stub

^ This.

Stub = Virus

Its suppose to be like that.

spyglass - December 2, 2015, 12:30 pm

Thank you both for the wise words and advice.

I understand the stub would bring them detections but silly me never noticed the official site download was pass protected.

And why the second scan came back fud.

After testing fully I can confirm that the file uploaded is the same as the ones from the official site.

You can see here.

Spoiler [\(Click to View\)](#) <http://www.digdeeperglobal.org/cleanDT1.bmp>

Spoiler [\(Click to View\)](#) <http://www.digdeeperglobal.org/cleanDT2stub.bmp>

I tested this on a few virtual machines and it is infact quite stable.

