

Forum:[Hack Forums](#)

Thread: [Can anyone tell me if this .exe is infected? \(backdoor check\)](#)

abadguy87 - August 3, 2017, 1:56 pm

Hi guys, so I'd like to know if this version of SQLI dumper 9.2 is 100% clean. My eset nod32 says it is, and after uploading it to virustotal it seems ok. However I'd like someone to check for backdoors by reverse engineering it. Is anybody capable of doing so? Thank you in advance.

link edited.

Sparkfear - August 3, 2017, 2:08 pm

I'll take a look, will update if I find anything.

Didn't find anything suspicious, I recommend taking down that link though.
Those downloads are not allowed on HF.

We recommend you take the time to read the [HF Help Documents](#) section. The answer to your questions should be contained in there.

H4K453 - August 3, 2017, 2:17 pm

it's html file not executable but will look into all possible danger in it

notice 1: it adds itself to autorun

notice 2: it drops suspicious looking file

has shit ton of js code for tracking,twitter,google,facebook

I would say one of tracker installs itself to system to track you as none harmful js found on webpage

abadguy87 - August 3, 2017, 2:41 pm

(Aug 3, 2017 02:08 PM)Sparkfear Wrote: [\[CITE\]](#) I'll take a look, will update if I find anything.

Didn't find anything suspicious, I recommend taking down that link though.
Those downloads are not allowed on HF.

We recommend you take the time to read the [HF Help Documents](#) section. The answer to your questions should be contained in there.

Thank you for taking the time. I didn't know it was forbidden to post this kind of stuff, I'll take it down, I just want to have more confirmations.

(Aug 3, 2017 02:17 PM)H4K453 Wrote: [\[CITE\]](#) it's html file not executable but will look into all possible danger in it

notice 1: it adds itself to autorun

notice 2: it drops suspicious looking file

has shit ton of js code for tracking,twitter,google,facebook

I would say one of tracker installs itself to system to track you as none harmful js found on webpage

uhm ? I'm running the exe inside sandboxie and I don't see anything dropped, also what html file are you talking about? there is just "SQLi Dumper 9.2.1 Cracked by CN\$quad NextGenZ & Bleach.exe" inside the rar I uploaded, not sure which html file you are referring to.

H4K453 - August 3, 2017, 2:56 pm

(Aug 3, 2017 02:41 PM)abadguy87 Wrote: [\[CITE\]](#) uhm ? I'm running the exe inside sandboxie and I don't see anything dropped, also what html file are you talking about? there is just "SQLi Dumper 9.2.1 Cracked by CN\$quad NextGenZ & Bleach.exe" inside the rar I uploaded, not sure which html file you are referring to.

fun thing because I got dropped to html page from your rar

edit: naming had special Unicode that fucked up my malware debugger will do testing with exe rn tho

abadguy87 - August 3, 2017, 3:03 pm

(Aug 3, 2017 02:56 PM)H4K453 Wrote: [\[CITE\]](#) fun thing because I got dropped to html page from your rar

edit: naming had special Unicode that fucked up my malware debugger will do testing with exe rn tho

I tried opening the RAR inside sandboxie this time...still no html..I think it may be just on your side.

H4K453 - August 3, 2017, 3:05 pm

(Aug 3, 2017 03:03 PM)abadguy87 Wrote: [\[CITE\]](#) I tried opening the RAR inside sandboxie this time...still no html..I think it may be just on your side.

as I said my malware debugger couldn't do auto extract because fucked up Unicode in name so I am doing this manually soon with results

results are in:

nothing really suspicious but one thing I noticed it created 2 files with random names

abadguy87 - August 3, 2017, 3:39 pm

(Aug 3, 2017 03:05 PM)H4K453 Wrote: [\[CITE\]](#) as I said my malware debugger couldn't do auto extract because fucked up Unicode in name so I am doing this manually soon with results

results are in:

nothing really suspicious but one thing I noticed it created 2 files with random names

ok thank you man ?