

Forum:[Hack Forums](#)

Thread: [Check a source for backdoor](#)

Josh? - February 9, 2016, 10:29 am

Hi all,

Could anyone check the source of something for a backdoor for me please? It is obfuscated and in Java 8. PM me for the download (don't want to publicly link something potentially backdoored)

Thanks to anyone who can.

hintss - February 10, 2016, 3:24 am

How big is this thing that you want checked?

Swish - February 10, 2016, 4:31 am

Wondering the same as the above question.

Josh? - February 11, 2016, 1:42 am

(Feb 10, 2016 04:24 AM)hintss Wrote: [\[CITE\]](#) How big is this thing that you want checked?

(Feb 10, 2016 05:31 AM)Swish Wrote: [\[CITE\]](#) Wondering the same as the above question.

It's just over 7MB

Key Punch - February 11, 2016, 1:46 am

(Feb 11, 2016 02:42 AM)Josh? Wrote: [\[CITE\]](#) It's just over 7MB

I can do 2 things for you..

1. Run it through my local cuckoo sandbox on a one of the headless vm's which will support .jar.

2. Manually look through the java for anything..

I can do either one or 1 and 2..

PM me if you still are in need of said check.

Sogomn - February 11, 2016, 3:37 am

Just use a decompiler and look for classes that might be suspicious.

Josh? - February 11, 2016, 3:46 am

(Feb 11, 2016 04:37 AM)Sogomn Wrote: [\[CITE\]](#) Just use a decompiler and look for classes that might be suspicious.

That would require me to have more than a basic understanding of Java. It's heavily obfuscated which makes it even harder for me

Sogomn - February 11, 2016, 4:01 am

(Feb 11, 2016 04:46 AM)Josh? Wrote: [\[CITE\]](#) That would require me to have more than a basic understanding of Java. It's heavily obfuscated which makes it even harder for me

Copy to Eclipse -> Control + Shift + F -> Formatted.

Folks - February 11, 2016, 12:48 pm

(Feb 11, 2016 05:01 AM)Sogomn Wrote: [\[CITE\]](#) Copy to Eclipse -> Control + Shift + F -> Formatted.

Obfuscation doesn't just rearrange the code so formatting it correctly won't help, also he said he doesn't have more than a basic understand of java.

CodeLeaks™ - February 11, 2016, 1:19 pm

(Feb 11, 2016 04:37 AM)Sogomn Wrote: [\[CITE\]](#) Just use a decompiler and look for classes that might be suspicious.

On 7mb of code? Yeah, good luck and have fun with that.

Surely I don't have a better answer because I'd suggest the same thing, but it's still going to suck. And since it's obfuscated, it's going to be even worse.