

Forum:[Hack Forums](#)

Thread: [\[FIXED\] Accidentally Infected myself with own keylogger :s](#)

Shadow™ - December 23, 2014, 12:05 pm

Fixed. Thanks guys ?

Spoiler ([Click to View](#)) I was testing stuff with the new logger I bought. I decided to make a new stub and my dumb self clicked my stub instead of the builder. Now I'm currently logging myself and I want to remove it qq. I've contacted the owner but hes redirecting me to here.

logger link: <https://hackforums.net/showthread.php?tid=4497045>

Greatly appreciated if you can help me remove it. I have already scanned my computer with malwarebytes and it removed the start file in the start folder but its still working. Heard there are 5 startup methods on his thread and I want to remove it.

[spoiler]My friend is laughing because I logged myself qq

Centuries - December 23, 2014, 12:06 pm

Wow.. I am laughing so hard.

It has persistence so when you delete it, it comes back sometimes somewhere else.

If you open up the control panel of your logger... your IP doesn't come up and you can stop logging yourself?

I find it weird if it doesn't, as all my old ones have.

Aura - December 23, 2014, 12:08 pm

Why would he redirect you here? It's his product, he should be the one offering support, that pisses me off so much. Also, you people REALLY need to learn to use a fucking Virtual Machine to test your own fucking stubs. When you start your Keylogger Control Panel like Centuries said, can't you kill the stub?

PHANTOM - December 23, 2014, 12:09 pm

lol you can't remove the stub from the panel? or kill?

Shadow™ - December 23, 2014, 12:11 pm

<https://gyazo.com/32aff4a5364d45c6379cc99fcc2e359c>

Remove log does shit. No kill option

What he said: <https://gyazo.com/e79a087c4ba1844d687384a0af103cdd>

Also I didn't want to test it. I have a RDP for that but I accidentally clicked on my own bloody stub qq

Centuries - December 23, 2014, 12:12 pm

(Dec 23, 2014 01:11 PM)player2190 Wrote: [\[CITE\]](#)

<https://gyazo.com/32aff4a5364d45c6379cc99fcc2e359c>

Remove log does shit. No kill option

That's just the log. Right click your ip and there is no end, kill, or close?

Shadow™ - December 23, 2014, 12:14 pm

(Dec 23, 2014 01:12 PM)Centuries Wrote: [\[CITE\]](#) That's just the log. Right click your ip and there is no end, kill, or close?

Its not installed on my computer, its online if you saw his logger thread

NoodleBot™ - December 23, 2014, 12:14 pm

(Dec 23, 2014 01:08 PM)Aur? Wrote: [\[CITE\]](#) Why would he redirect you here? It's his product, he should be the one offering support, that pisses me off so much. Also, you people REALLY need to learn to use a fucking Virtual Machine to test your own fucking stubs. When you start your Keylogger Control Panel like Centuries said, can't you kill the stub?

Or just not freak out when you need to end a task and startup path...

It's probably not even crypted.

Jon Snow - December 23, 2014, 12:16 pm

(Dec 23, 2014 01:11 PM)player2190 Wrote: [\[CITE\]](#)

<https://gyazo.com/32aff4a5364d45c6379cc99fcc2e359c>

Remove log does shit. No kill option

What he said: <https://gyazo.com/e79a087c4ba1844d687384a0af103cdd>

Also I didn't want to test it. I have a RDP for that but I accidentally clicked on my own bloody stub qq

Well, you should scan the server on VirusTotal and wait for some antivirus to detect it. After detection, use the antivirus to remove it.

Shadow™ - December 23, 2014, 12:16 pm

(Dec 23, 2014 01:14 PM)NoodleBot™ Wrote: [\[CITE\]](#) Or just not freak out when you need to end a task and startup path...

It's probably not even crypted.

I deleted the startup path but it reappears >.>

Aura - December 23, 2014, 12:16 pm

(Dec 23, 2014 01:14 PM)NoodleBot™ Wrote: [\[CITE\]](#) Or just not freak out when you need to end a task and startup path...

It's probably not even crypted.

Still it pisses me the fuck off to see people being that igorant and so careless. About to create a Rant thread, but in the Hacking Programs and Tools section and tell them to be more careful and teach them how to use a VM properly.

NoodleBot™ - December 23, 2014, 12:17 pm

Because the file is probably still running.

Aura - December 23, 2014, 12:17 pm

(Dec 23, 2014 01:16 PM)Jon Snow Wrote: [\[CITE\]](#) Well, you should scan the server on VirusTotal and wait for some antivirus to detect it. After detection, use the antivirus to remove it.

That's not how you remove a stub with persistence.

Centuries - December 23, 2014, 12:18 pm

(Dec 23, 2014 01:17 PM)NoodleBot™ Wrote: [\[CITE\]](#) Because the file is probably still running.

It has persistence, not just because the "file is still running"

OP: Go talk to the owner of his logger again, if you have no kill option that logger is completely horrid in my honest opinion.

NoodleBot™ - December 23, 2014, 12:21 pm

Then do it the lazy way and boot into safe mode and delete it all.

Shadow™ - December 23, 2014, 12:23 pm

(Dec 23, 2014 01:21 PM)NoodleBot™ Wrote: [\[CITE\]](#) Then do it the lazy way and boot into safe mode and delete it all.

And where might the files be located?

Null Byte - December 23, 2014, 12:26 pm

(Dec 23, 2014 01:23 PM)player2190 Wrote: [\[CITE\]](#) And where might the files be located?

Can you upload the stub and PM me a link? I'm going to do an analysis to see how this thing installed itself.

Link to analysis:

<https://www.hybrid-analysis.com/sample/9cb61ca14de347368a46c484e5336bb274e2060beb6e4730ba3fc39b66af9a31>

^ Hybrid analysis not working on this. I'll try a different site.

Link to analysis:

<https://malwr.com/submission/status/ZjdjN2QzZDdlZjFhNDIzMWE1YTAzZWZiNjc4ODImZTM/>

It should be finished in ~10 minutes, then we can figure out how to remove this.

Aura - December 23, 2014, 12:34 pm

(Dec 23, 2014 01:26 PM)Null Byte Wrote: [\[CITE\]](#) Can you upload the stub and PM me a link? I'm going to do an analysis to see how this thing installed itself.

Link to analysis:

<https://www.hybrid-analysis.com/sample/9cb61ca14de347368a46c484e5336bb274e2060beb6e4730ba3fc39b66af9a31>

It should be finished in ~10 minutes, then we can figure out how to remove this.

The analysis crashed. It happened to me a few days ago too.

Shadow™ - December 23, 2014, 12:49 pm

Compiled a new stub with his compiler and uploaded to hybrid-analysis:

<https://www.hybrid-analysis.com/sample/30eff3cb29d4109c183bf24bc1917fed13e50ec14c1aa6845ae3497dda95e249>

Farbar still scanning

Null Byte - December 23, 2014, 12:50 pm

(Dec 23, 2014 01:49 PM)player2190 Wrote: [\[CITE\]](#) Compiled a new stub with his compiler and uploaded to hybrid-analysis:

<https://www.hybrid-analysis.com/sample/30eff3cb29d4109c183bf24bc1917fed13e50ec14c1aa6845ae3497dda95e249>

Farbar still scanning

OK, it seems to have some sort of anti-emulation feature so I don't know if HA will be able to

complete. And just post your logs on pastebin.com when you're done with that.

Shadow™ - December 23, 2014, 12:53 pm

FRST: <http://privatepaste.com/8f51200454>

Addition: <http://privatepaste.com/a6ee040d27>

Shortcut: <http://privatepaste.com/7646a54832>

Analysis of the compiler:

<https://www.hybrid-analysis.com/sample/3f1fbeeee4996dfcd057158f488b254e3a147d8f687cf35e4f50e3198eefd9f2/>

Null Byte - December 23, 2014, 12:59 pm

(Dec 23, 2014 01:53 PM)player2190 Wrote: [\[CITE\]](#) FRST: <http://privatepaste.com/8f51200454>

Addition: <http://privatepaste.com/a6ee040d27>

Shortcut: <http://privatepaste.com/7646a54832>

Analysis of the compiler:

<https://www.hybrid-analysis.com/sample/3f1fbeeee4996dfcd057158f488b254e3a147d8f687cf35e4f50e3198eefd9f2/>

Boot into safe mode, then open up msconfig.exe. Under the Startup tab you should see something called DayZ Hack; disable it. Apply your changes. Open up the an C:\Users\jordan\AppData\Local\Temp\ and delete a file named DayZ Hack.exe. Upload C:\Windows\SysWOW64\PnkBstrA.exe to VirusTotal.com and post the link here. Reboot your computer.

Shadow™ - December 23, 2014, 1:06 pm

(Dec 23, 2014 01:59 PM)Null Byte Wrote: [\[CITE\]](#) Boot into safe mode, then open up msconfig.exe. Under the Startup tab you should see something called DayZ Hack; disable it. Apply your changes. Open up the an C:\Users\jordan\AppData\Local\Temp\ and delete a file named DayZ Hack.exe. Upload C:\Windows\SysWOW64\PnkBstrA.exe to VirusTotal.com and post the link here. Reboot your computer.

Owner of the keylogger told me how to remove it. Thanks for the help tho :).

<http://www.neuber.com/taskmanager/process/pnkbstra.exe.html>

Looks like battlefield or something

Null Byte - December 23, 2014, 1:07 pm

(Dec 23, 2014 02:06 PM)player2190 Wrote: [\[CITE\]](#) Owner of the keylogger told me how to remove it. Thanks for the help tho :).

<http://www.neuber.com/taskmanager/process/pnkbstra.exe.html>

Looks like battlefield or something

Alright, sounds good. Let us know if you need any more help.

Aura - December 23, 2014, 1:11 pm

(Dec 23, 2014 01:59 PM)Null Byte Wrote: [\[CITE\]](#) Boot into safe mode, then open up msconfig.exe. Under the Startup tab you should see something called DayZ Hack; disable it. Apply your changes. Open up the an C:\Users\jordan\AppData\Local\Temp\ and delete a file named DayZ Hack.exe. Upload C:\Windows\SysWOW64\PnkBstrA.exe to VirusTotal.com and post the link here. Reboot your computer.

It's needed to run Battlefield, however it have a spyware-like behavior, nothing you can do.

(Dec 23, 2014 02:06 PM)player2190 Wrote: [\[CITE\]](#) Owner of the keylogger told me how to remove it. Thanks for the help tho :).

<http://www.neuber.com/taskmanager/process/pnkbstra.exe.html>

Looks like battlefield or something
Run my reply above.

Brandenx781 - December 23, 2014, 10:50 pm

Hi,

Just wanted to drop in to say something.

Null Byte Wrote:Upload C:\Windows\SysWOW64\PnkBstrA.exe to VirusTotal.com and post the link here.

PnkBstrA.exe is a legitimate file. It is part of an anti-cheat program thingymabob. ?

Null Byte Wrote:Open up the an C:\Users\jordan\AppData\Local\Temp\ and delete a file named DayZ Hack.exe

Whattttt, is that it?!?! I'm seeing tons of malicious stuff in his temp folder! ?

But anyways, since the issue has been resolved, I hope someone closes this thread soon. ?

Aura - December 23, 2014, 11:03 pm

(Dec 23, 2014 11:50 PM)Brandenx781 Wrote: [\[CITE\]](#) Hi,

Just wanted to drop in to say something.

PnkBstrA.exe is a legitimate file. It is part of an anti-cheat program thingymabob. ?

Whattttt, is that it?!?! I'm seeing tons of malicious stuff in his temp folder! ?

But anyways, since the issue has been resolved, I hope someone closes this thread soon. ?

You might want to harass Paradoxum for that, or one of the original three ?

Shadow™ - December 24, 2014, 9:14 am

Haha just got l33t :D. Can close threads ?