

Forum:[Hack Forums](#)

Thread: [Need help, virus!](#)

mrddare360 - November 29, 2012, 8:09 am

I downloaded a Skype resolver, I think it was made by someone called StayOS and now my UAC has be set to minimal, there is a file that can't be ran on 64 bit windows in a folder named system32 which is named stayserver6.exe, and that file isn't even visible to the system, it's obviously a virus even though scanning with Malwarebytes doesn't pick it up. I'm trying Avast as of now but I have my doubts, when I delete the file it is created again. The thread which I downloaded it from is now deleted and I have no idea what to do. Please help me! D:

FireStorM1337 - November 29, 2012, 8:11 am

check your taskmanager, may there are some suspicious tasks there?

rinor4ever - November 29, 2012, 8:13 am

Try kaspersky or maybe this isn't virus. Something else bllocked.

Waffle - November 29, 2012, 8:15 am

Hi, sounds like you have an obvious trojan to me, and one that's persistent. Open up command prompt then type these two commands;

Spoiler ([Click to View](#))

Code tasklistCode netstat -ano

PM the copy and pasted results to me in between [/code] tags please. I can then find the trojan's malicious connection and find the linked process(es).

mrddare360 - November 29, 2012, 8:22 am

(Nov 29, 2012 09:15 AM)KiliJac Wrote: [\[CITE\]](#) Hi, sounds like you have an obvious trojan to me, and one that's persistent. Open up command prompt then type these two commands;

Spoiler ([Click to View](#))

Code tasklistCode netstat -ano

PM the copy and pasted results to me in between [/code] tags please. I can then find the trojan's malicious connection and find the linked process(es).

Alrighty:

<http://paste.ubuntu.com/1397193/>

<http://paste.ubuntu.com/1397195/>

Waffle - November 29, 2012, 8:48 am

I don't see any malicious connections, assuming that you have skype running at this time;

Download, install and run [MBAR](#).

Download and run [TDSSKiller](#).

Download, install and run [SuperAntiSpyware](#) quick scan.

You don't have to keep these, but I recommend keeping them even after checks :)

If they do not pick anything up then write a batch file like so;

Code del ### stayserver6.exe /FEDIT: Replace ## with the path for stayserver6. Where is this system32 folder located? Is it in appdata, windows, or what?

Save it to your desktop as 'del.bat'

Reboot in safe mode, run 'del.bat' as administrator, and see what happens. When you're in safe mode, use a program like [Infested Cleaner](#) to view startup keys, and delete any suspicious entries.

Hope I helped you in some way or other. Report back with some results

mrdare360 - November 29, 2012, 9:24 am

(Nov 29, 2012 09:48 AM)KiliJac Wrote: [\[CITE\]](#) I don't see any malicious connections, assuming that you have skype running at this time;

Download, install and run [MBAR](#).

Download and run [TDSSKiller](#).

Download, install and run [SuperAntiSpyware](#) quick scan.

You don't have to keep these, but I recommend keeping them even after checks :)

If they do not pick anything up then write a batch file like so;

Code del ## stayserver6.exe /FEDIT: Replace ## with the path for stayserver6. Where is this system32 folder located? Is it in appdata, windows, or what?

Save it to your desktop as 'del.bat'

Reboot in safe mode, run 'del.bat' as administrator, and see what happens. When you're in safe mode, use a program like [Infested Cleaner](#) to view startup keys, and delete any suspicious entries.

Hope I helped you in some way or other. Report back with some results

MBAR picked up some items and removed them, none of them being stayserver6.exe, TDSSKiller found nothing and SuperantiSpyware found:

Restarting computer now for removals to take effect, also the system32 folder is being created in Users/Joanne.

(Nov 29, 2012 09:48 AM)KiliJac Wrote: [\[CITE\]](#) I don't see any malicious connections, assuming that you have skype running at this time;

Download, install and run [MBAR](#).

Download and run [TDSSKiller](#).

Download, install and run [SuperAntiSpyware](#) quick scan.

You don't have to keep these, but I recommend keeping them even after checks :)

If they do not pick anything up then write a batch file like so;

Code del ## stayserver6.exe /FEDIT: Replace ## with the path for stayserver6. Where is this system32 folder located? Is it in appdata, windows, or what?

Save it to your desktop as 'del.bat'

Reboot in safe mode, run 'del.bat' as administrator, and see what happens. When you're in safe mode, use a program like [Infested Cleaner](#) to view startup keys, and delete any suspicious entries.

Hope I helped you in some way or other. Report back with some results

All seems good now, when I delete STAYSERVER6.exe it stays deleted. Although I do not see the system32 folder in Users/Joanne either. Thanks for your help! I would give you +rep but I can't(What does one have to do to give rep?). Thanks alot :)

Waffle - November 29, 2012, 9:33 am

In that case, make the batch file delete the whole folder, then reboot and run it as administrator. Report back with superantispyware logs and mbar logs if you can, so I can get a better idea of what it's done

(Nov 29, 2012 09:15 AM)KiliJac Wrote: [\[CITE\]](#) Hi, sounds like you have an obvious trojan to me, and one that's persistent. Open up command prompt then type these two commands;

Spoiler [\(Click to View\)](#)

Code tasklistCode netstat -ano

PM the copy and pasted results to me in between `[/code]` tags please. I can then find the trojan's malicious connection and find the linked process(es). Good to hear that it seems fixed :) Can you just repeat the quoted steps please, for a final check. To give reputation to people you need to buy I33t or ub3r, but it doesn't matter, glad problem seems fixed

mrddare360 - November 29, 2012, 10:55 am

(Nov 29, 2012 10:33 AM)KiliJac Wrote: [\[CITE\]](#) In that case, make the batch file delete the whole folder, then reboot and run it as administrator. Report back with superantispyware logs and mbar logs if you can, so I can get a better idea of what it's done

Good to hear that it seems fixed :) Can you just repeat the quoted steps please, for a final check. To give reputation to people you need to buy I33t or ub3r, but it doesn't matter, glad problem seems fixed

<http://paste.ubuntu.com/1397496/>

<http://paste.ubuntu.com/1397497/>

Once again, thanks a lot :).

Waffle - November 29, 2012, 11:16 am

(Nov 29, 2012 11:55 AM)mrddare360 Wrote: [\[CITE\]](#) <http://paste.ubuntu.com/1397496/>
<http://paste.ubuntu.com/1397497/>

Once again, thanks a lot :). Looks good. You're welcome, stay safe

NoodleBot™ - November 29, 2012, 10:49 pm

Think you're INFECTED? Here is what you can do:

Firstly, you want to restart your computer and disconnect from the internet. Also, when I say disconnect, I mean turn off your router, just in case you ARE actually infected.

Look for the suspicious infected file and delete it.

Then, look through your process list, check to see if there are any unusual processes running that are taking a lot of CPU power. If found, end the process tree.

Make sure to use ApiTrap, which removes DarkComet, BlackShades, CyberGate, and other RATs.

[ApiTrap](#)

If that doesn't work, open up Ccleaner and Disk Defragment and start cleaning up your PC.

Defragging usually helps in cases of files not opening up due to computer LAG.

If the problem persists, check your recent files, if nothing is there, run a system restore.

If the System Restore function doesn't work or is being blocked by the virus/infection on your computer, shutdown and run in safe mode.

If you cannot shutdown, unplug your computer from the wall or if it is a laptop, take out the battery. Be sure to make the system restore 2 days prior to when you think this problem began.

After restoring, repeat the above process. If the problem persists, PM Phyber on HF. He is a professional White Hat and knows a lot about computer security.

On the side, get AVG Anti-Virus Free 2012 Edition, it's the best out there at the moment.

If you know yourself, and somehow want to have a secondary protection besides your own mental capabilities, look for a good Anti-Virus.

Here are a few I can recommend:
AVG Anti-Virus Free 2012 Edition

AVG advances in catching infectious tools and Remote Administration Tools.

Avast! Home Edition

Avast! Home Edition is great for catching the average worm or standardized virus, but it lacks much in the field of Remote Administration Tools.

Malware Bytes Anti-Malware 2012

Malware Bytes Anti-Malware 2012 catches and is able to remove majority of malware found on standardized computers today.

Hope this helped. If it didn't, I do apologize. :(

This was provided to you by NuudleRow, but credits go to Mind Control™!

Waffle - November 30, 2012, 8:11 am

(Nov 29, 2012 11:49 PM)NuudleRow Wrote: [\[CITE\]](#) Think you're INFECTED? Here is what you can do:

Firstly, you want to restart your computer and disconnect from the internet. Also, when I say disconnect, I mean turn off your router, just in case you ARE actually infected.

Look for the suspicious infected file and delete it.

Then, look through your process list, check to see if there are any unusual processes running that

are taking a lot of CPU power. If found, end the process tree.

Make sure to use ApiTrap, which removes DarkComet, BlackShades, CyberGate, and other RATs.

[ApiTrap](#)

If that doesn't work, open up Ccleaner and Disk Defragment and start cleaning up your PC.

Defragging usually helps in cases of files not opening up due to computer LAG.

If the problem persists, check your recent files, if nothing is there, run a system restore.

If the System Restore function doesn't work or is being blocked by the virus/infection on your computer, shutdown and run in safe mode.

If you cannot shutdown, unplug your computer from the wall or if it is a laptop, take out the battery. Be sure to make the system restore 2 days prior to when you think this problem began.

After restoring, repeat the above process. If the problem persists, PM Phyber on HF. He is a professional White Hat and knows a lot about computer security.

On the side, get AVG Anti-Virus Free 2012 Edition, it's the best out there at the moment.

If you know yourself, and somehow want to have a secondary protection besides your own mental capabilities, look for a good Anti-Virus.

Here are a few I can recommend:
AVG Anti-Virus Free 2012 Edition

AVG advances in catching infectious tools and Remote Administration Tools.

Avast! Home Edition

Avast! Home Edition is great for catching the average worm or standardized virus, but it lacks much in the field of Remote Administration Tools.

Malware Bytes Anti-Malware 2012

Malware Bytes Anti-Malware 2012 catches and is able to remove majority of malware found on standardized computers today.

Hope this helped. If it didn't, I do apologize. :(

This was provided to you by NuudleRow, but credits go to Mind Control™! I don't mean to be annoying, but read the thread before you c&p. Problem was resolved already :)

