

Forum:[Hack Forums](#)

Thread: [Netflix and Amazon account compromised.](#)

Henning B - April 26, 2016, 10:02 am

Both my Netflix and Amazon account got compromised, I only use one computer for those two services.

Should I post my journalctl log and systemd services?

Annoited - April 26, 2016, 3:19 pm

Get some logs so that people can see what's wrong. Here are the recommended programs from ProtectNull:

Download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Farbar Recovery Scanning Tool Right click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce a log called FRST.txt in the same directory the tool is run from.

Please copy and paste the log back here

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

TDSSKiller Please download [TDSSKiller](#) and save the file to your Desktop.

Right-Click TDSSKiller.exe and select Run as Administrator

Click Change parameters. Place a checkmark next to Detect TDLFS file system and Verify file digital signatures.

Click Start Scan. Do not use the computer during the scan.

If objects are found, change the action to skip.

Click Continue and close the window.

A log will be created and saved to the root directory (usually C:\). Paste the file contents to [pastebin.com](#) and post the link in your next reply.

ProtectNull™ - April 26, 2016, 4:47 pm

(Apr 26, 2016 03:19 PM)Annointed Wrote: [\[CITE\]](#) Get some logs so that people can see what's wrong. Here are the recommended programs from ProtectNull:

Download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Farbar Recovery Scanning Tool Right click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce a log called FRST.txt in the same directory the tool is run from.

Please copy and paste the log back here

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

TDSSKiller Please download [TDSSKiller](#) and save the file to your Desktop.

Right-Click TDSSKiller.exe and select Run as Administrator

Click Change parameters. Place a checkmark next to Detect TDLFS file system and Verify file digital signatures.

Click Start Scan. Do not use the computer during the scan.

If objects are found, change the action to skip.

Click Continue and close the window.

A log will be created and saved to the root directory (usually C:\). Paste the file contents to [pastebin.com](#) and post the link in your next reply.

Yes, do this an I will assist you too. ?

Henning B - April 27, 2016, 6:06 am

(Apr 26, 2016 04:47 PM)ProtectNull™ Wrote: [\[CITE\]](#) Yes, do this an I will assist you too. ?
YEAH, ill do that on my linux box.

I said I could give you journalctl logs: (warning huge)
<http://paste.fedoraproject.org/360191/62367146/>

ProtectNull™ - April 27, 2016, 6:23 am

(Apr 27, 2016 06:06 AM)Henning B Wrote: [\[CITE\]](#) YEAH, ill do that on my linux box.

I said I could give you journalctl logs: (warning huge)
<http://paste.fedoraproject.org/360191/62367146/>

Are you just using the normal Linux Distro or other distro such as Ubuntu, CentOS etc?

Henning B - April 27, 2016, 6:27 am

(Apr 27, 2016 06:23 AM)ProtectNull™ Wrote: [\[CITE\]](#) Are you just using the normal Linux Distro or other distro such as Ubuntu, CentOS etc?

It is running arch linux.

ProtectNull™ - April 27, 2016, 7:14 am

(Apr 27, 2016 06:27 AM)Henning B Wrote: [\[CITE\]](#) It is running arch linux.

Reserved, will assist soon.

Hello, I'm going to check if you have a rootkit

Please open terminal and type1) sudo apt-get install chkrootkit

2) sudo chkrootkit

3) sudo chkrootkit -x | less

Please let me know if it finds any RK, if it does not.

Go back into terminal;

1) sudo apt-get install rkhunter

2) sudo rkhunter --check

And if it finds anything let me know.

Henning B - April 27, 2016, 10:45 pm

(Apr 27, 2016 07:14 AM)ProtectNull™ Wrote: [\[CITE\]](#) Reserved, will assist soon.

Hello, I'm going to check if you have a rootkit

Please open terminal and type1) sudo apt-get install chkrootkit

2) sudo chkrootkit

3) sudo chkrootkit -x | less

Please let me know if it finds any RK, if it does not.

Go back into terminal;

1) sudo apt-get install rkhunter

2) sudo rkhunter --check

And if it finds anything let me know.

Do you know Linux at all?

ProtectNull™ - April 27, 2016, 10:46 pm

(Apr 27, 2016 10:45 PM)Henning B Wrote: [\[CITE\]](#) Do you know Linux at all?
I use CentOS and Kali Linux and Ubuntu.

Henning B - April 27, 2016, 11:23 pm

(Apr 27, 2016 10:46 PM)ProtectNull™ Wrote: [\[CITE\]](#) I use CentOS and Kali Linux and Ubuntu.
Aptitude is only for debian based distros, I'll run the program, but you can't run those commands on anything but debian.

ProtectNull™ - April 27, 2016, 11:51 pm

(Apr 27, 2016 11:23 PM)Henning B Wrote: [\[CITE\]](#) Aptitude is only for debian based distros, I'll run the program, but you can't run those commands on anything but debian.
So is your one yum install?

Henning B - April 28, 2016, 1:33 am

(Apr 27, 2016 11:51 PM)ProtectNull™ Wrote: [\[CITE\]](#) So is your one yum install?
Arch: 'pacman -S firefox'

ProtectNull™ - April 28, 2016, 1:35 am

(Apr 28, 2016 01:33 AM)Henning B Wrote: [\[CITE\]](#) Arch: 'pacman -S firefox'
Oh alright. ?

Henning B - April 28, 2016, 7:52 am

None of the tools found anything

ProtectNull™ - April 28, 2016, 4:56 pm

(Apr 28, 2016 07:52 AM)Henning B Wrote: [\[CITE\]](#) None of the tools found anything
Are your passwords easy to crack?

Henning B - April 29, 2016, 12:46 am

(Apr 28, 2016 04:56 PM)ProtectNull™ Wrote: [\[CITE\]](#) Are your passwords easy to crack?
example of one of my passwords with all changed into similar chars:

Gb137689tdrsewq137689gt##

ProtectNull™ - April 29, 2016, 1:10 am

(Apr 29, 2016 12:46 AM)Henning B Wrote: [\[CITE\]](#) example of one of my passwords with all changed into similar chars:

Gb137689tdrsewq137689gt##

Do you use them in other sites?

Henning B - April 29, 2016, 6:09 am

(Apr 29, 2016 01:10 AM)ProtectNull™ Wrote: [\[CITE\]](#) Do you use them in other sites?
every site uses unique password.

ProtectNull™ - April 29, 2016, 6:29 am

(Apr 29, 2016 06:09 AM)Henning B Wrote: [\[CITE\]](#) every site uses unique password.
I would try getting ClamAV using pacman -S clamtk

I'm not too familiar with Archlinux using pacman, I'm more on apt-get and yum install.

?

