EXHIBIT 32

[redacted]

Log in or Sign up

Home | Forums | Members

Search Forums Recent Posts

Can NOT fully remove Win32 Dorkbot virus

[redacted]

Please help! I'm in Peace Corps so my response time may lag, but I plan to check back here as much as possible.

I received a "RECYCLER" virus some days ago on my flash drive which hides files on my USB and created shortcuts or new folders. When running Microsoft Security Essentials, it shows that the virus itself is called "Win32 Dorkbot." It is able to locate the virus, but never fully deletes it.

I'm not even sure if it's deleted from my USB completely, other than checking it on a friend's PC and them running Essentials on it. How can I know if it's clean? I'm not sure what is infecting what, though I do feel it's more likely I just haven't deleted it fully from my computer.

Judging from [redacted] about the virus, it's exactly what I have.

I'm now stuck because I've run EVERYTHING on this page... [redacted] with no success. In addition, the ROOTREPEAL program never even could open, stating there was a problem

I would upload logs, but I can't even open my application data folder...

However... Superantispyware, malwarebytes, combofix, and MGTools have not fixed the problem : (

PLEASE HELP!!!

Attached Files:

RootRepeal_crash_091611.093252.txt	
File size:	189 bytes
Views:	1

[redacted], Sep 16, 2011 #1

[redacted]

I would upload logs, but I can't even open my application data folder...

However... Superantispyware, malwarebytes, combofix, and MGTools have not fixed the problem : (

I need to be able to see those logs before I can give you a fix.

[redacted] Sep 17, 2011 #2

[redacted]

Ok I've found how to attach the logs.

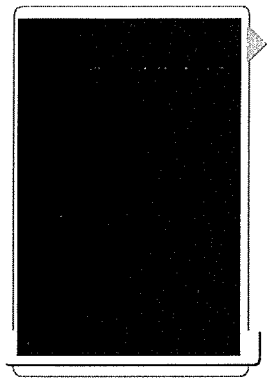
like I said, I can run everything BUT Rootrepeal, but I've attached the error log.

Thanks so much!

Attached Files:

[redacted], Sep 17, 2011 #3

[redacted] <--- delete this file if it exists.



Insert your flash drive before we begin. **Hold down the Shift key** when inserting the flash drive until Windows detects it to bypass the autorun feature. This will keep the autorun.inf from executing automatically.

Please have all your removable storage devices ready for disinfection.

Download **Flash Disinfector by sUBs** and save it to your desktop.

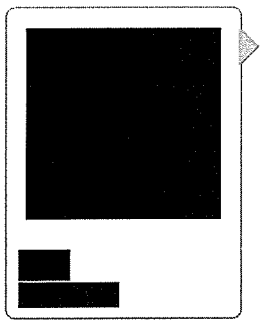
- Double-click Flash_Disinfector.exe to run it.
- Your desktop and icons may disappear. This is normal.
- It will do a cleanup of removable storage devices, and write a protected **Autorun.inf** file to help prevent re-infection.
- Follow any prompts that may appear.
- The utility may ask you to insert your flash drive and/or other removable drives including your mobile phone. Please do so and allow the utility to clean up those drives as well.
- Wait until it has finished scanning and then exit the program.
- There will be no GUI interface or log file produced.
- Reboot your computer when done.

Note: Flash_Disinfector will create a hidden folder named autorun.inf in each partition and every USB drive plugged in when you ran it. Don't delete this folder. It will help protect your drives from future infection.

Does this help you? You might also try giving this a run:

Microsoft Safety Scanner

[redacted], Sep 17, 2011 #4



The Antqtq file doesn't exist, at least not in that location (or any other that I can tell)

I inserted my flash drive (which i cleaned on another computer) holding shift like you said, and then WATCHED as the RECYCLER file and a bunch of short cuts magically appeared after a little time. This seems to show that the computer keeps giving it to the USB drive, and not the other way around.

I downloaded the two programs but they won't run!

I click "run" for the Flash Disinfector and then NOTHING happens

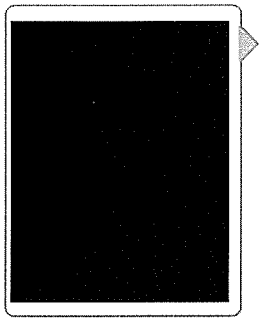
As for the Windows Security Scanner program, I click "run" and I get an error message saying that it is not a valid Win32 application...

what do I do now??? Nothing will run!

Oh, and it is worth mentioning that I also tried running them in Safe mode with no luck either.

Last edited by a moderator: Sep 17, 2011

[redacted], Sep 17, 2011 #5



The Antqtq file doesn't exist, at least not in that location (or any other that I can tell)

I inserted my flash drive (which i cleaned on another computer) holding shift like you said, and then WATCHED as the RECYCLER file and a bunch of short cuts magically appeared after a little time. This seems to show that the computer keeps giving it to the USB drive, and not the other way around.

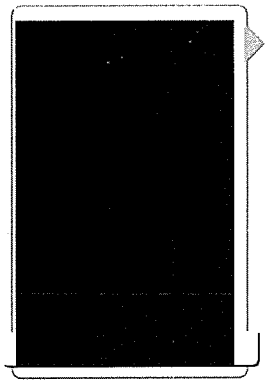
I downloaded the two programs but they won't run!

I click "run" for the Flash Disinfector and then NOTHING happens

As for the Windows Security Scanner program, I click "run" and I get an error message saying that it is not a valid Win32 application...

what do I do now??? Nothing will run!

[redacted], Sep 17, 2011 #6



> *When running Microsoft Security Essentials, it shows that the virus itself is called "Win32 Dorkbot." It is able to locate the virus, but never fully deletes it.*

Give me the exact locations of the threats being found?

Download this file to your desktop

Kaspersky Virus Removal Tool

Run the program you have just downloaded to your desktop (it will be randomly named)

First we will run a virus scan.

- On the first tab select all elements down to Computer and then select start scan.
- Once it has finished select report and post that.

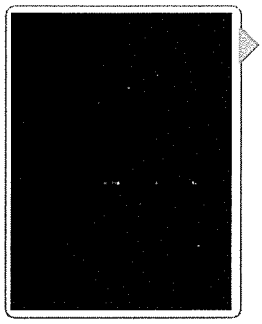
Do not close AVPTool or it will self uninstall, if it does uninstall - then just rerun the setup file on your desktop.

Now an analysis scan

- Select the **Manual Disinfection** tab
- Press the **Gather System Information** button
- Once done Open the last report saved folder then attach the zip file to your next post.
- The file is located at C[redacted]

Please attach that too.

[redacted], Sep 17, 2011 #7



I think that actually worked! At the very least, the antivirus sites are no longer blocked.

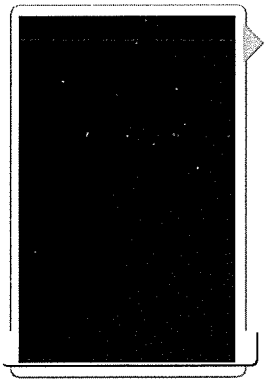
I have attached the system log file, but majorgeeks kept showing an error message about a security file missing so I can't even post them simply copied. there are two. One is from the first complete scan, but for some reason my computer restarted so I redid the scan again.

Thanks for all your help I really appreciate it.

Is it safe to say that my USBs are still infected even if cleaned with Microsoft Security Essentials?

What anitvirus program should I get to make sure this doesn't happen again? Because it seems that even though Essentials can identify it, it couldn't delete it.

[redacted], Sep 18, 2011 #8

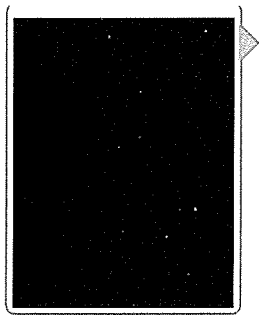


Can you run Combofix again please and attach the log? Also I would really like to see the avptool_sysinfo.zip

Now run the [redacted] file by double clicking on it. (Right click and run as admin if using [redacted] or [redacted] Then attach the new [redacted] file that will be created by running this.

[redacted], Sep 19, 2011 #9

I've attached the Combofix log and the MG log file.



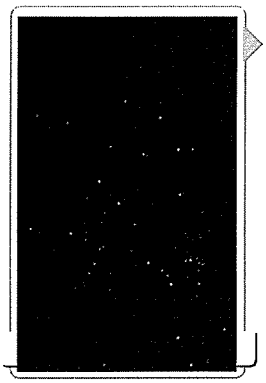
I can't seem to locate the avptool_sysinfo.zip file. Do you know where the file would be located.

Thanks a lot for you're help!

I still would like to know what you would recommend to avoid this again, especially since it's quite possible that my USBs still have the virus. I want to completely fix my computer and install some sort of antivirus program before I try to connect them again.

Thanks!

[redacted], Sep 19, 2011 #10



> *I've attached the Combofix log and the MG log file.*

They did not attach.

> *I can't seem to locate the avptool_sysinfo.zip file. Do you know where the file would be located.*

Yes, here: [redacted]

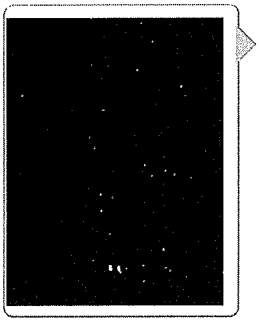
> *Thanks a lot for you're help!*

You're welcome!

> *I still would like to know what you would recommend to avoid this again, especially since it's quite possible that my USBs still have the virus. I want to completely fix my computer and install some sort of antivirus program before I try to connect them again.*

I will address this once I have seen the latest logs.

[redacted], Sep 19, 2011 #11



I've attached the Combofix log and the MG log file.

I can't seem to locate the avptool_sysinfo.zip file. Do you know where the file would be located.

Thanks a lot for you're help!

I still would like to know what you would recommend to avoid this again, especially since it's quite possible that my USBs still have the virus. I want to completely fix my computer and install some sort of antivirus program before I try to connect them again.

Thanks!

Attached Files:

ComboFix.txt	
File size:	18.4 KB
Views:	2

MGlogs.zip	
File size:	310.2 KB
Views:	1

[redacted], Sep 19, 2011 #12

[redacted]

Yes, here: [redacted]

Ah, the problem is that the "setup" is an application not a folder, the Kapersky virus removal tool

[redacted], Sep 19, 2011 #13

[redacted]

SystemLook

Please download **SystemLook** from one of the links below and save it to your Desktop.
Download Mirror #1
Download Mirror #2

- Double-click **SystemLook.exe** to run it.
- Copy the content of the following codebox into the main textfield:

Code:

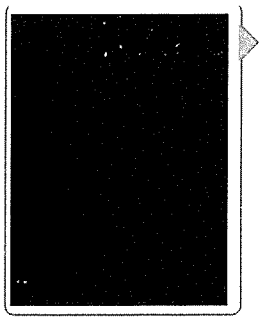
```
:filefind
avptool_sysinfo.zip
```

- Click the **Look** button to start the scan.
- When finished, a notepad window will open with the results of the scan. Please post this log in your next reply.

Note: The log can also be found on your Desktop entitled **SystemLook.txt**

[redacted], Sep 19, 2011 #14

Done :)

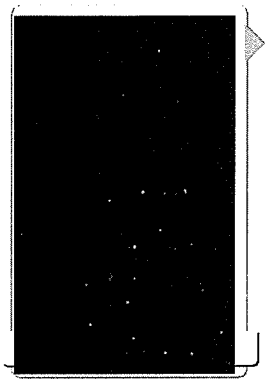


Perhaps this file was deleted when I ran the Kapersky?

Attached Files:

SystemLook.txt	
File size:	444 bytes
Views:	1

[redacted], Sep 19, 2011 #15



Please disable all anti-virus and anti-spyware programs while we do the following **(re-enable when you are finished):**

Run C:\MGtools**analyse.exe** by double clicking on it (Note: if using Vista, don't double click, use right click and select Run As Administrator). This is really HijackThis (select Do a system scan only) and select the following lines but DO NOT CLICK FIX until you exit all browser sessions including the one you are reading in right now:

- O4 - Startup: _uninst_.lnk = [redacted]

After clicking **Fix** exit HJT.

Now we need to use ComboFix by sUBs

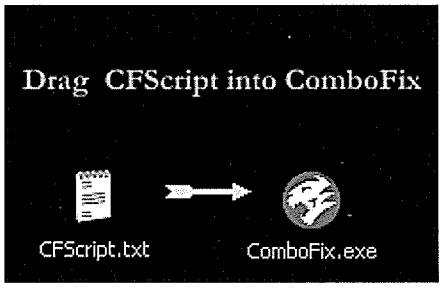
- Make sure that combofix.exe that you downloaded while doing the READ & RUN ME is on your Desktop but **Do not run it!**
  - If it is not on your Desktop, the below will not work.
- **Also make sure you have shut down all protection software (antivirus, antispyware...etc) or they may get in the way of allowing ComboFix to run properly.**
- If ComboFix tells you it needs to update to a new version, **make sure you allow it to update.**
- Open Notepad and copy/paste the text **in** the below quote box. Ensure you scroll down to select ALL the lines:

Code:

```
KILLALL::

File::
[redacted]
```

- Save the above as CFscript.txt and make sure you save it to the same location (should be on your Desktop) as ComboFix.exe
- At this point, you MUST EXIT ALL BROWSERS NOW before continuing!
- You should have both the ComboFix.exe and CFScript.txt icons on your Desktop.
- Now use your mouse to drag CFscript.txt on top of ComboFix.exe



- Follow the prompts.
- When it finishes, a log will be produced named c:\combofix.txt
- I will ask for this log below

Note:

Do not mouseclick combofix's window while it is running. That may cause it to stall.

If after running Combofix you discover none of your programs will open up, and you recieve the following error: **"Illegal operation attempted on a registry key that has been marked for deletion".** Then the answer is to **REBOOT** the machine, and all will be corrected.

Could you please get this: **54266884.sys** into a zipped file and attach it for me in your next post? To do this, see the below:

Please go to start > Run and paste in the following:

[redacted]

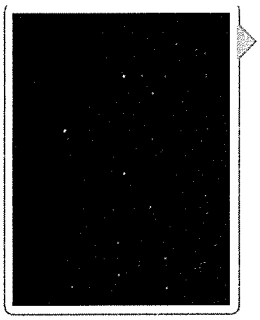
log retrievable @ C:**collect.zip**

Please go to **virustotal** and upload the following files for analysis, and **let me know the results.**

- [redacted]

Now run the [redacted] file by double clicking on it. (Right click and run as admin if using Vista or Windows7) Then attach the new [redacted] file that will be created by running this.

[redacted] Sep 19, 2011 #16



1. I followed the instructions to the letter for MGtools by making the document and dragging it, updating MGTools etc, but unforunately I accidentally closed the window when it said it was preparing the log file and that it would be located on my C drive because I mistakenly thought it had finished. Should I run it again and attach the log? sorry about that. My computer did restart during the process, but I never got the error message you wrote about.

2. the file, 54266884.sys, does not exist under the file name you gave me.

3. I have attached the new mglogs zip

4. Question: Under users..[redacted] I have a bunch of ntuser files that I can't delete because it says the system is using them. what are they?

Attached Files:

MGlogs.zip	
File size:	311.3 KB
Views:	4

EntJ, Sep 20, 2011 #17

Download and run OTM.

Download **OTM** by **Old Timer** and save it to your Desktop.

[redacted]

- Right-click OTM.exe And select " Run as administrator " to run it.
- Paste the following code under the Paste Instructions for Items to be Moved area. Do not include the word Code.

Code:

[redacted]

```
:Commands
[emptytemp]
[Reboot]
```

- Return to OTM, right click in the Paste List of Files/Folders to Move window (**under the yellow bar**) and choose Paste.
- Push the large MoveIt! button.
- OTM may ask to reboot the machine. Please do so if asked.
- Copy everything in the Results window (under the green bar), and paste it into notepad, save it as something appropriate and attach it into your next reply.

NOTE: If you are unable to copy/paste from this window (as will be the case if the machine was rebooted), open Notepad (**Start->All Programs->Accessories->Notepad**), click **File->Open**, in the File Name box enter *.log and press the Enter key, navigate to the C:_OTM\MovedFiles folder, and open the newest .log file present, and **attach** the contents of that document back here in your next post.

Now run the C:\MGtools**GetLogs.bat** file by double clicking on it. (Right click and run as admin if using [redacted] or [redacted] Then attach the new C:**MGlogs.zip** file that will be created by running this.

Last edited: Sep 20, 2011

[redacted] Sep 20, 2011 #18

Also, once we have made some more progress, we can try having you run a complete scan with Malware Bytes and SUPERantispyware with the flashdrive plugged in. I can then check the log.

[redacted]

Please tell me what this is: C:**removerecycler.exe**

Last edited: Sep 20, 2011

[redacted] Sep 20, 2011 #19

[redacted]

the recycler.exe is a program i downloaded to delete the folder on my USB

I can't find its URL, but it opens a program that does some commands on the black screen and deletes it.

Attached Files:

OTM .log	
File size:	3.7 KB
Views:	2

MGlogs.zip	
File size:	313.4 KB
Views:	2

[redacted] Sep 21, 2011 #20

1 2 Next >

(You must log in or sign up to reply here.)

Share This Page

[redacted]