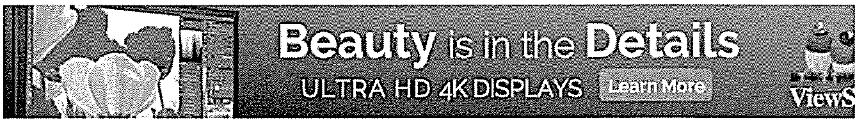
EXHIBIT 31

[redacted] → Security → Virus, Trojan, Spyware, and Malware Removal Logs



Register a free account to unlock additional features at BleepingComputer.com

Welcome to **BleepingComputer**, a free community where people like yourself come together to discuss and learn how to use their computers. Using the site is easy and fun. As a guest, you can browse and view the various discussions in the forums, but can not create a new topic or reply to an existing one unless you are logged in. Other benefits of registering an account are subscribing to topics and forums, creating a blog, and having **no ads** shown anywhere on the site.

Click here to Register a free account now! or read our **Welcome Guide** to learn how to use this site.

Infected with Worm:Win32/Dorkbot.I - Need of Recovering External USB data

Started by [redacted] Sep 17 2013 12:19 AM

[redacted]

Posted 17 September 2013 - 12:19 AM

Hi everyone!

Last week I used a pendrive in a public computer at my university, and when I tried to enter to my folders, all of them were instant access. I was able to reach my files anyways, but I was scared because obviosly this was because some kind of malware, so I formatted the pendrive.

The next day I conected the same pendrive to my personal computer, and a message popped up saying that my computer was infected with this **"Worm:Win32/Dorkbot.I". I searched how to delete it, and I found this program called "Microsoft Sofware Malicious Sofware Removal Tool". I used it and I tought I was done with this Dorkbot, so the next day I connect another pendrive, this one with very important stuff, and I realize that now this pendrive got the same problem (all of the folders converted into instant access). I continued my research to delete this malware and I found another program called "Malwarebytes Anti-Malware" So I used it and I finally was able to delete this malware from my computer and all of my pendrives. The thing is that now I try to access the files from my important pendrive and this dialog shows to me:**

"Windows cannot find 'I/.Trashes/8f9538f1.exe'. Make sure you typed the name correctly, and then try again".

The information in this pendrive is really important for me, and I need some help to get it back.
Thank you all for your time, please help!

Attached Files

[redacted]

BC AdBot (Login to Remove)

[redacted]

Posted 17 September 2013 - 07:35 PM

[redacted]

Welcome to BC forums!

Please do the following...

① To stop the Autorun feature, download and run the following:
Microsoft Fix It 50471:
http://support.microsoft.com/kb/967715 (http://support.microsoft.com/kb/967715)
Scroll down to: How to disable or enable all Autorun features in Windows 7 and other operating systems
Click Run in the File Download dialog box, and follow the steps of the wizard.
Note: There is an option to enable Autorun automatically. You can do so later, if you wish.
Reboot the system after applying the Microsoft FixIt.

② Please click on the Windows 7 *Start* button and then on *Control Panel*
In Control Panel, select the *Folder Options* link.
Click on the *View* tab in the Folder Options window.
In the Advanced settings: area, locate the *Hidden files and folders* category.
Check: *Show hidden files, folders, and drives*
Uncheck: *Hide protected operating system files (Recommended)*
Click Apply and OK at the bottom of the Folder Options window.

③ Next, download **UsbFix:**
http://www.infospyware.com/utiles/usbfix/ (http://www.infospyware.com/utiles/usbfix/)
It is a Spanish language website, but the program is in English.
To download. press the button that says: Descagar (It means: Download)
Save to the Desktop.

④ Connect the problem USB drive!

⑤ Next, right-click the downloaded USBFix file and select: Run as Administrator
Press: *Research*
When done, the program closes on its own, and a report appears.
(The report file is also found at C:\UsbFix.txt)
>> Please post the *UsbFix.txt (Research Mode)* report in your reply.

⑥ Once again, run *USBFix* as Administrator, but, this time, press: *Listing*
>> Also post the *UsbFix.txt (Listing Mode)* report in your reply.

Note 1: If USBFix does not run in normal Windows, please run in Safe Mode:
Restart your computer.
When the computer starts, tap the F8 key on the keyboard repeatedly until presented with the Advanced Boot Options menu
Using the arrow keys, select: Safe Mode
Press the Enter key on your keyboard to boot into the selected mode.

Note 2: If your AntiVirus program detects USB as malware, either let the AV program allow USBFix to run, or, temporarily disable your AntiVirus program:
Info - http://www.bleepingcomputer.com/forums/t/114351/how-to-temporarily-disable-your-anti-virus-firewall-and-anti-malware-programs/ (http://www.bleepingcomputer.com/forums/t/114351/how-to-temporarily-disable-your-anti-virus-firewall-and-anti-malware-programs/)
When done with USBFix, re-enable your AV!

⑦ Last, please download the **Farbar Recovery Scan Tool**
Download: http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/ (http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/)
Select the version that applies to your system.
Save it to your Desktop.
Double-click the downloaded file to run it.
When the tool opens click *Yes* to the disclaimer.
Press the **Scan** button.
The tool makes a log (*FRST.txt*) in the same directory from which the tool is run (Desktop).

>> Please provide the *FRST.txt* in your reply.

The first time the tool is run, it also makes another log: *Addition.txt*
>> Also post the *Addition.txt* in your reply.

[redacted]

Edited by Aaflac, 17 September 2013 - 07:37 PM.

[redacted]

Posted 17 September 2013 - 08:22 PM

Here are all the files you asked for. Thanks!

Attached Files

[redacted]

Edited by [redacted] 17 September 2013 - 08:22 PM.

[redacted]

Posted 17 September 2013 - 09:45 PM

[redacted]

Thanks for the reports.

Let's press on with *FRST*...

① Please open Notepad (Start > All Programs > Accessories > Notepad)
Copy the entire contents of the code box below
Save it to the Desktop, and name it: *fixlist.txt*

```
start
HKLM-x32\...\Runonce: [] - [x]
[redacted]
HKCU\...\Winlogon: [Shell] Explorer.exe <==== ATTENTION
HKLM-x32\...\Run: [] - [x]
end
```

Once again, double-click *FRST* to run it.
When the tool opens click *Yes* to disclaimer.
Press the **Fix** button.
When done, FRST produces *Fixlog.txt* on the Desktop.
>> Please provide the *Fixlog.txt* on your reply.

② Next, please press the W*indows* Key and the *R* key at the same time for the Run prompt to appear.
In the Run prompt, type the following in the Open area, and press Enter: **cmd**

When the Command Prompt opens, copy/paste (with the mouse) the following, and press: *Enter*

```
attrib -h -s -r -a /s /d X:\*.*
```

(Change the drive letter X to the letter corresponding to the problem USB removable drive.)

③ Now, please run *USBFix* once again
Press: ***Deletion***
When done, the program closes on its own, and a report appears.

The report file is also found at C:\UsbFix.txt
>> Please post the *UsbFix.txt (Deletion Mode)* report in your reply.

Note: As before, if your AntiVirus program detects USB as malware, either let the AV program allow USBFix to run, or, temporarily disable your AntiVirus program.

Check the USB drive and see if the shortcuts are gone.

Edited by [redacted] 17 September 2013 - 09:49 PM.

[redacted]

Posted 17 September 2013 - 10:03 PM

Totally worked! You did an amazing job. Thank you alot... for real! ☺

Attached Files

[redacted]

[redacted]

Posted 18 September 2013 - 08:14 AM

Good job, [redacted] ☺

Need to focus on both your computer and the pendrives...

: ① With the pen drives connected, please run **Malwarebytes Anti-Malware**:
Download: http://www.bleepingcomputer.com/download/malwarebytes-anti-malware/ (http://www.bleepingcomputer.com/download/malwarebytes-anti-malware/)
Save to the Desktop
Double-click the downloaded MBAM file to run it.

When the installation begins, follow the prompts in the setup process.
DO NOT make any changes to default settings and when the program has finished installing, make sure only the following options are checked:
>Update Malwarebytes' Anti-Malware
>Launch Malwarebytes' Anti-Malware
Uncheck:
>Enable free trial of Malwarebytes Anti-Malware PRO
Click on the *Finish* button.

If an update is found, the program automatically updates itself.
At the program console, on the *Scanner* tab, and select: *Perform Full Scan*

When the *Select the Drives to scan* prompt appears, make sure **all** drives (except: CD-Rom/DVD) are selected.
Next, click on the **Scan** button.

When the Malwarebytes scan is completed, click on: *Show Results*
When presented with a screen showing the malware detected, make sure everything is Checked, and click on: *Remove Selected*

When removal is completed, a report opens in Notepad.
>> Please copy/paste the entire contents of the MBAM report in your reply.

Note: If MBAM encounters a file that is difficult to remove, you are asked to reboot the computer so MBAM can proceed with the disinfection process. If asked to restart the computer, please do so immediately. Failure to reboot normally (not into safe mode) prevents MBAM from removing all the malware.

② Also, ddownload **RogueKiller:**

[redacted]

http://tigzy.geekstogo.com/roguekiller.php (http://tigzy.geekstogo.com/roguekiller.php)
Select the version that applies to the system.
Save to the Desktop.

After closing all windows and browsers, right-click the downloaded *RogueKiller* file and select: *Run as Administrator*
At the program console, wait for the Prescan to finish. (Under Status, it says: Prescan finished.)
Press: **SCAN**
When done, a report opens on the Desktop: *RKreport.txt*
>> Please provide the *RKreport.txt (Mode: Scan)* in your reply.

③ Last, run the *Farbar Recovery Scan Tool* once again, and post its report.

[redacted]

[redacted]

Posted 18 September 2013 - 02:44 PM

I completed all the steps you asked me to do. I accidentally pressed the "delete" button after I scanned my computer using Roge Killer. Is there any trouble? Thanks.

Attached Files

[redacted]

[redacted]

Posted 18 September 2013 - 09:01 PM

On RogueKiller, there should be an RKreport Mode : Delete -- Date : 09/18/2013 HH:MM:SS
It should be on the Desktop.

Please post it if you find it.

MBAM showed:
[redacted]

However, it was Quarantined and deleted successfully. None of the other reports showed it.

Are you having any more malware problems?

[redacted]

Posted 18 September 2013 - 09:22 PM

I found this report in my desktop of Rogue Killer. Anyways, my computer and my pendrives are doing fine. Thanks for your help.

Attached Files

[redacted]

[redacted]

[redacted]

Posted 21 September 2013 - 06:45 PM

My apology for the delay.

Since the issue with the USB drives is solved, let's wrap up and remove the following tools and their reports, which are no longer needed.
These tools are updated frequently, and, if outdated, will not produce accurate results.

You can remove from the Desktop:
Microsoft Fix It 50471
UsbFix
Farbar Recovery Scan Tool, as well as any *fixlist* and *fixlog*. Also remove the *FRST* (or FRST64) folder, found normally on *C:\FRST*
RogueKiller and its RKreports

Keep Malwarebytes Anti-Malware (MBAM), and use it regularly.
Any USB pendrives, SD cards, or External drives connected to someone else's computer, and then connected back to your computer should have a *Full Scan* performed. MBAM has the option of selecting which drives to scan, and includes removable drives.

If you are no longer having malware problems, you are good to go!

Thanks for following all the instructions and providing the reports!!

Have a great week, and, buena suerte, [redacted]

[redacted]

Posted 22 September 2013 - 12:16 AM

[redacted] I'm taking a very good image from this forum because of you. Thanks for your help.

[redacted]

Posted 22 September 2013 - 07:52 PM

Mi placer!

Back to Virus, Trojan, Spyware, and Malware Removal Logs

[redacted] → Security → Virus, Trojan, Spyware, and Malware Removal Logs