Answered by:

JohnLenz

Longwood Associates, Inc.

60 Points 0 0 5

Consultant providing business development and delivery of networking, system selection and hardware/software support services. Conducted ERP and CRM strategy and selection, operational reviews focusing on technology operating costs, office solutions and supporting data/document retention and recovery. I have broad and deep career experience equally balanced over twenty-five years in industry and professional services. In industry, I have held all technical roles including turnaround and interim CIO. In professional services, I build trusted relationships with the "C-Suite" to help them better understand, direct and program manage the technology organization. I have extensive experience in eCommerce and was the COO of an Internet banking eAssociation portal.

JohnLenz's threads

View Profile

ZeroAccess.Rootkit removal

Windows Vista IT Pro forums > Windows Vista Security

Question

Win Vista home premium

Infected system I have removed most of Trojans except this particularly bad one ZeroAccess.rootkit.

0

Sign in to vote

To date - Cannot run Malwarebytes nor Spyhunet on system, Trojan intercepts - "corrupt image".

Removed system drive from laptop and added externally to a WinXP machine with Symantec Endpoint 11, Malwarebytes and Spyhunter. Ran spyhunter scans but Endpoint found files with "access denied".

Uninstalled endpoint and re-ran both Malwarebytes and Spyhunter until clean.

Re-installed drive in Vista system. Had corrupted desktop that troubleshooter cleaned up.

Ran ComboFix which found ZeroAcess.Rootkit. I can get desk top up but have no Internet connection. Properties come back with no IP connections for DNS, Gateway and system. Checked properties to ensure no LAN settings.

What can I do now?

John Lenz

Moved by Carey Frisch MVP, Moderator Monday, November 14, 2011 6:51 PM Moved to more appropriate forum category (From:Windows Vista Networking)

Monday, November 14, 2011 4:57 PM

Reply | Quote |

JohnLenz Longwood Associates, Inc. 60 Points

Top related threads

removed

Agent removal for ESX - No removal

Remove Server

Removing SBA

Removing replication

Answers

The stand alone sweeper was able to find and clean a Trojan embedded in Java. It did not restore networking; however, I then did a O/S recovery and am back up and working.

THX

John Lenz

0
Sign in to vote

Marked as answer by JohnLenz Wednesday, November 16, 2011 8:29 PM

Wednesday, November 16, 2011 8:29 PM

Reply | Quote |

JohnLenz Longwood Associates, Inc. 60 Points

All replies

Please review: Help: I Got Hacked. Now What Do I Do?

Carey Frisch

0
Sign in to vote

Monday, November 14, 2011 6:50 PM

Reply | Quote |

Moderator 

Carey Frisch Microsoft MVP since 2003 (MCC, Partner, MVP) 93,320 Points

You'll probably have to reinstall, but before you do, try Microsoft's Standalone System Sweeper. Although it's still at the beta testing stage, it runs very well indeed and I've removed rootkit infections with it.

0
Sign in to vote

On a working machine download the appropriate 32-bit or 64-bit version here https://connect.microsoft.com/systemsweeper and burn a CD. Boot from the CD and run a full scan.

Monday, November 14, 2011 7:04 PM

Reply | Quote |

BurrWalnut 8,170 Points

0
Sign in to vote

THX,

I'll trry this. I have a extensive set of tools but this trojan is VERY bad.
I got one of the 2 systems working and cleaned. Hopefully this standalone run will do the trick. I cna see the infected files "deny access" but did not have the toolo to kill them.

I'll post back results.

BTW, I do this as a living - keeping systems clean and running.

John Lenz

Monday, November 14, 2011 8:20 PM

Reply | Quote |

JohnLenz Longwood Associates, Inc. 60 Points

0
Sign in to vote

Hi,

I would like to provide the following suggestions:

1. You may specifically give the Administrator the full permissions on this folder and its subfolders and files, and then try to run the antivirus software to remove the virus again.

2. Please contact your antivirus program support to see if they have special update or tools to complete remove it.

3. Actually, the officially recommended method is still to format and re-install the compromised computer from a known good build (i.e. operating system CD + all security patches while disconnected from the network). For more information on hacking, please see these links:

Help: I Got Hacked. Now What Do I Do?
http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx

Help: I Got Hacked. Now What Do I Do? Part II
http://www.microsoft.com/technet/community/columns/secmgmt/sm0704.mspx

How A Criminal Might Infiltrate Your Network
http://www.microsoft.com/technet/technetmag/issues/2005/01/AnatomyofaHack/default.aspx

Malicious Software Removal Tool
http://www.microsoft.com/security/malwareremove/default.mspx

The Day After: Your First Reponse To A Security Breach
http://www.microsoft.com/technet/technetmag/issues/2005/01/IncidentResponse

4. You can also contact your antivirus vendor for assistance with identifying or removing virus or worm infections. If you need more help with virus-related issues, contact Microsoft Product Support Services.

For information about Security updates, visit the Microsoft Virus Solution and Security Center for resources and tools to keep your PC safe and healthy. If you are having issues with installing the update itself, visit Support for Microsoft Update for resources and tools to keep your PC updated with the latest updates.

I hope this helps. Thank you for your time and cooperation!

(Please note that the newsgroups are staffed weekdays by Microsoft Support professionals to answer your non-urgent, break/fix systems and applications questions. Our goal is to provide 24 hour response to all questions. If this response time does not meet your needs, please contact Customer Service and Support (CSS) for more immediate assistance. For more information on available CSS services, please click here: http://support.microsoft.com/default.aspx?scid=fh;EN-US;OfferProPhone#faq607.)

Regards,

Sabrina

TechNet Subscriber Support in forum

If you have any feedback on our support, please contact tnmff@microsoft.com.

This posting is provided "AS IS" with no warranties or guarantees, and confers no rights. |Please remember to click “Mark as Answer” on the post that helps you, and to click “Unmark as Answer” if a marked post does not actually answer your question. This can be beneficial to other community members reading the thread.

Edited by Sabrina Shen Friday, April 06, 2012 3:41 AM PCSafety Center update

Tuesday, November 15, 2011 2:19 AM

Reply | Quote |

Sabrina Shen 15,890 Points

The stand alone sweeper was able to find and clean a Trojan embedded in Java. It did not restore networking; however, I then did a O/S recovery and am back up and working.

THX

John Lenz

0
Sign in to vote

Marked as answer by JohnLenz Wednesday, November 16, 2011 8:29 PM

Wednesday, November 16, 2011 8:29 PM

Reply | Quote |

JohnLenz Longwood Associates, Inc. 60 Points

ZeroAccess troubled me a lot too but you should try out Mcafee's RootkitRemover.....
The tool worked flawlessly and save many of my office computer's asses.

Cheers

0
Sign in to vote

Thursday, January 05, 2012 4:42 PM

Reply | Quote |

SteveKanan 0 Points

Another great tool that i have found is combofix it can be found on bleepingcomputer.com and it will remove zeroaccess rootkit and restore your network back to normal and it works well for many other infections and problems such as a missing taskbar. Best of all its free to use.

0
Sign in to vote

Thursday, February 16, 2012 8:51 PM

Reply | Quote |

Cowboy24 0 Points

I encountered the same problem as you describe, but didn't want to reinstall Windows as the system contained a lot of proprietary software with complex settings to reconfigure. To fix (if anyone else has the same problem - this worked for me), firstly reboot into the Microsoft Windows Recovery Console, then (where D:\ is the Windows install CD-ROM); expand D:\i386\ipsec.sy_ c:\Windows\system32\drivers\ipsec.sys expand D:\i386\dnsapi.dl_ C:\Windows\system32\dnsapi.dll expand D:\i386\dnsrslvr.dl_ C:\Windows\system32\dnsrslvr.dll (See: http://www.osisecurity.com.au/blog/zeroaccess-rootkit-sirefef-no-internet-connectivity-dns) Then reboot. This should fix the no IP address error in addition to the unable to resolve DNS problem. Goodluck! -Patrick

0
Sign in to vote

Edited by www.osisecurity.com.au Friday, March 02, 2012 6:08 AM

Friday, March 02, 2012 6:07 AM

Reply | Quote |

www.osisecurity.com.au 0 Points