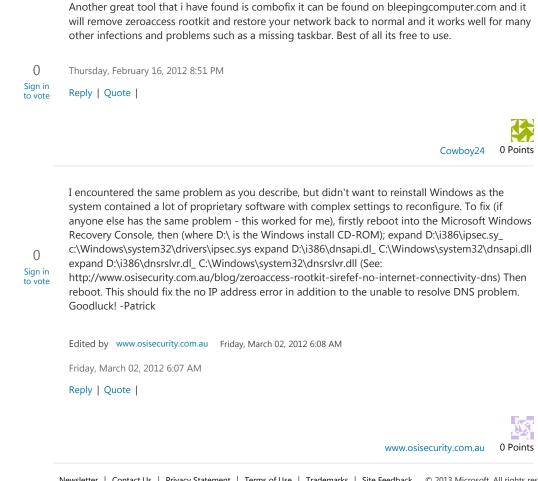


Answers	
	The stand alone sweeper was able to find and clean a Trojan embedded in Java. It did not restore networking; however, I then did a O/S recovery and am back up and working.
0	ТНХ
0 Sign in to vote	John Lenz
	Marked as answer by JohnLenz Wednesday, November 16, 2011 8:29 PM
	Wednesday, November 16, 2011 8:29 PM
	Reply Quote
	JohnLenz Longwood Associates, Inc. 60 Poir
All replies	
	Please review: Help: I Got Hacked. Now What Do I Do?
	Carey Frisch
0	Monday, November 14, 2011 6:50 PM
Sign in to vote	Reply Quote
	Moderator 🧲
	Carey Frisch Microsoft MVP since 2003 (MCC, Partner, MVP) 93,320 Poin
	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 Poir

	THX,
0 Sign in to vote	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

	Hi,
	I would like to provide the following suggestions:
0 Sign in to vote	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

a ma	posting is provided "AS IS" with no warranties or guarantees, and confers no rights. Please mber to click "Mark as Answer" on the post that helps you, and to click "Unmark as Answer" in rked post does not actually answer your question. This can be beneficial to other community bers reading the thread.
Edited	by Sabrina Shen Friday, April 06, 2012 3:41 AM PCSafety Center update
Tuesc	lay, November 15, 2011 2:19 AM
Reply	Quote
	Sabrina Shen 15,890 Point
0 Sign in to vote	John Lenz Marked as answer by JohnLenz Wednesday, November 16, 2011 8:29 PM Wednesday, November 16, 2011 8:29 PM
	Reply Quote
	Reply Quote JohnLenz Longwood Associates, Inc.
0	JohnLenz Longwood Associates, Inc. ZeroAccess troubled me a lot too but you should try out Mcafee's RootkitRemover
0 Sign in to vote	JohnLenz Longwood Associates, Inc. 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.



Newsletter | Contact Us | Privacy Statement | Terms of Use | Trademarks | Site Feedback © 2013 Microsoft. All rights reserved.