

# **EXHIBIT 36**



[SPAMfighter](#)
[SERVER Solutions](#)
[VIRUSfighter](#)
[SPYWAREfighter](#)
[SLOW-PCfighter](#)
[FULL-DISKfighter](#)

Email

ShareThis

## British Police Arrested Couple for Spreading Zeus Trojan

British Police stated on November 18, 2009 that they had arrested two individuals for spreading Zbot or Zeus, an advanced **malware** capable of extracting sensitive details from a user's computer.

The duo, husband and wife, both aged 20, were arrested on November 3, 2009 in Manchester, England, stated the Metropolitan PCeU (Police's Central e-Crime Unit). Although the couple is currently free on bail, they will be eventually tried under the 1990 Computer Misuse Act along with the 2006 Fraud Act.

Talking about Zeus, it is a highly sophisticated **malware** that users frequently download on their computers unknowingly, following a social engineering tactic or phishing, which impersonates credit card companies, tax offices, banks, or some other entity known to victims, luring them to follow malevolent links or to go to malware-ridden websites. During one such assault, a variant of Zeus mimicked an e-mail of an organization's IT unit and directed the user that he must update his Web-mail configurations with Microsoft.

Once placed on a user's system, Zeus creeps inside IE or other browser of the victim where it monitors the traffic. Thereafter, it copies Social Security numbers, credit card details as well as credentials for online banking, other financial accounts and corporate login details that it then transmits to its remote controller, according to investigators at the security firm BitDefender.

Graham Cluley, Senior Technology Consultant at Sophos (an **antivirus** firm) states that Zeus isn't merely an isolated malware, rather it is a group consisting of several other members, each disguising differently and try to infect end-users as well as to steal their confidential data, which could enable attackers to hack into the victims' social-networking and bank accounts, as reported by TheRegister on November 18, 2009.

According to officials in London, individuals and organizations that were infected by Zbot suffered significant monetary losses while those responsible for spreading the **malware** enjoyed enormous financial gains.

Additionally, the arrest is the first of its kind in Europe and also across the globe in relation to the Zeus Trojan, they said.

Related article: [British Telecommunications Introduces New anti-spam System](#)

» SPAMfighter News - 27-11-2009

## Share and tell your friends!

0

0

ShareThis

New

0

### Read IT-Security News

#### 2012

[December](#)  
[November](#)  
[October](#)  
[September](#)  
[August](#)  
[July](#)  
[June](#)  
[May](#)  
[April](#)  
[March](#)  
[February](#)  
[January](#)

#### 2011

[December](#)  
[November](#)  
[October](#)  
[September](#)  
[August](#)  
[July](#)  
[June](#)  
[May](#)  
[April](#)  
[March](#)  
[February](#)  
[January](#)

#### 2010

[December](#)  
[November](#)  
[October](#)  
[September](#)  
[August](#)  
[July](#)  
[June](#)  
[May](#)  
[April](#)  
[March](#)  
[February](#)  
[January](#)

#### 2009

[December](#)  
[November](#)  
[October](#)

#### 2008

[December](#)  
[November](#)  
[October](#)

#### 2007

[December](#)  
[November](#)  
[October](#)

All SPAMfighter products offer a free trial!



SPAMfighter is a **free spam filter** for Outlook, Outlook Express, Windows Mail, Windows Live Mail and Thunderbird.



Optimize your **Slow PC** for better performance. Try **FREE scan** now



**Disk space recovery** and disk optimization. Try FULL-DISKfighter free



SPAMfighter Exchange Module is a **Spam filter for Exchange server** - Free 30 days trial.



**Remove Spyware** with SPYWAREfighter - Free 30 days trial



SPAMfighter is



Microsoft Partner  
Gold Independent Software Vendor (ISV)



[September](#)  
[August](#)  
[July](#)  
[June](#)  
[May](#)  
[April](#)  
[March](#)  
[February](#)  
[January](#)

[September](#)  
[August](#)  
[July](#)  
[June](#)  
[May](#)  
[April](#)  
[March](#)  
[February](#)  
[January](#)

[September](#)  
[August](#)  
[July](#)  
[June](#)  
[May](#)  
[April](#)  
[March](#)  
[February](#)  
[January](#)



**Antivirus software** for your  
Windows PC - Free 30 days trial

[<<<](#)

[>>>](#)

Be all you can be, be a SPAMfighter

(C) SPAMfighter 2003-2012  
All rights reserved.

[Privacy Statement](#)

# **EXHIBIT 37**

## Question

### My webroot can seem to remove this virus/malware - PWS:Win32/Zbot.gen!Y ? What else can I do?

Applies To: Windows | Windows 7 | Security, Privacy, and User Accounts

Microsoft safety scanner has detected this virus (listed below) and my anti virus software wont remove it!! Help  
PWS:Win32/Zbot.gen!Y -

May 1, 2011 | Reply with quote | Report abuse

Reply

Email me

**1** Person had  
this question Me Too



Was this helpful?

Yes

**1**

Vote

## Answer

Hi,

If you need to check for malware here are my recommendations - these will allow you to do a thorough check and removal without ending up with a load of spyware programs running resident which can cause as many issues as the malware and maybe harder to detect as the cause.

No one program can be relied upon to detect and remove all malware. Added that often easy to detect malware is often accompanied by a much harder to detect and remove payload. So its better to be overly thorough now than to pay the high price later. Check with these to an extreme overkill point and then run the cleanup only when you are very sure the system is clean.

These can be done in Safe Mode - repeatedly tap F8 as you boot however you should also run them in regular Windows when you can.

TDSSKiller.exe. - Download to the Desktop - then go to it and Right Click on it - RUN AS ADMIN it will show any infections in the report after running - if it will not run change the name from tdsskiller.exe to tdsskiller.com. Whether it finds anything or not does not mean you should not check with the other methods below.  
<http://support.kaspersky.com/viruses/solutions?qid=208280684>

Download malwarebytes and scan with it, run MRT, and add Prevx to be sure it is gone.  
(If Rootkits run UnHackMe)

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Malwarebytes - free  
<http://www.malwarebytes.org/>

Run the Microsoft Malicious Removal Tool

Start - type in Search box -> MRT find at top of list - Right Click on it - RUN AS ADMIN.

You should be getting this tool and its updates via Windows Updates - if needed you can download it here.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN  
(Then run MRT as above.)

Microsoft Malicious Removal Tool - 32 bit

<http://www.microsoft.com/downloads/details.aspx?FamilyID=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>

Microsoft Malicious Removal Tool - 64 bit

<http://www.microsoft.com/downloads/details.aspx?FamilyID=585D2BDE-367F-495E-94E7-6349F4E7FC74&displaylang=en>

also install Prevx to be sure it is all gone.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Prevx - Home - Free - small, fast, exceptional CLOUD protection, works with other security programs. This is a scanner only, VERY EFFECTIVE, if it finds something come back here or use Google to see how to remove.

<http://www.prevx.com/> <-- information

<http://info.prevx.com/downloadcsi.asp> <-- download

PCmag - Prevx - Editor's Choice

<http://www.pcmag.com/article2/0,2817,2346862,00.asp>

Try the trial version of Hitman Pro :

Hitman Pro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.).

<http://www.surfright.nl/en/hitmanpro>

-----  
If needed here are some online free scanners to help

<http://www.eset.com/onlinescan/>

-----  
Original version is now replaced by the Microsoft Safety Scanner

<http://onecare.live.com/site/en-us/default.htm>

Microsoft Safety Scanner

<http://www.microsoft.com/security/scanner/en-us/default.aspx>

-----  
<http://www.kaspersky.com/virusscanner>

Other Free online scans

<http://www.google.com/search?hl=en&source=hp&q=antivirus+free+online+scan&aq=f&oq=&aqi=g1>

-----  
**After removing any malware :**

**Also do these to cleanup general corruption and repair/replace damaged/missing system files.**

Start - type this in Search Box -> COMMAND find at top and RIGHT CLICK - RUN AS ADMIN

Enter this at the prompt - sfc /scannow

How to Repair Windows 7 System Files with System File Checker

<http://www.sevenforums.com/tutorials/1538-sfc-scannow-command-system-file-checker.html>

How to analyze the log file entries that the Microsoft Windows Resource Checker (SFC.exe) program generates in Windows Vista cbs.log

<http://support.microsoft.com/kb/928228>

Also run CheckDisk so we can rule out corruption as much as possible.

How to Run Disk Check in Windows 7

<http://www.sevenforums.com/tutorials/433-disk-check.html>

-----  
If any Rootkits are found use this thread and other suggestions. (Run UnHackMe)

<http://social.answers.microsoft.com/Forums/en-US/InternetExplorer/thread/a8f665f0-c793-441a-a5b9-54b7e1e7a5a4/>

=====

If needed AFTER you are sure the machine is clean of all malware.

How to Do a Repair Install to Fix Windows 7

<http://www.sevenforums.com/tutorials/3413-repair-install.html>


Hope this helps.

May 2, 2011 | Reply with quote | Report abuse

Reply

 MS MVP

 MVP

 Microsoft MVP - Windows Expert - Consumer : Bicycle - Mark Twain said it right.

Was this helpful?

Yes

1

Vote

Answer

Get rid of webroot and install something like MSSE. Update it then do a full scan

Disable system restore. Get trojan remover update it then click on scan. Then select all options under the utils menu. Dont use any passwords online till you remove this

May 1, 2011 | Reply with quote | Report abuse

Reply



MCC

All Replies (2)

More Help

Was this helpful?

Yes

1

Vote

Answer

Get rid of webroot and install something like MSSE. Update it then do a full scan

Disable system restore. Get trojan remover update it then click on scan. Then select all options under the utils menu. Dont use any passwords online till you remove this

May 1, 2011 | Reply with quote | Report abuse

Reply



MCC

Was this helpful?

Yes

1

Vote

Answer

Hi,

If you need to check for malware here are my recommendations - these will allow you to do a thorough check and removal without ending up with a load of spyware programs running resident which can cause as many issues as the malware and maybe harder to detect as the cause.

No one program can be relied upon to detect and remove all malware. Added that often easy to detect malware is often accompanied by a much harder to detect and remove payload. So its better to be overly thorough now than to pay the high price later. Check with these to an extreme overkill point and then run the cleanup only when you are very sure the system is clean.

These can be done in Safe Mode - repeatedly tap F8 as you boot however you should also run them in regular Windows when you can.

TDSSKiller.exe. - Download to the Desktop - then go to it and Right Click on it - RUN AS ADMIN it will show any infections in the report after running - if it will not run change the name from tdsskiller.exe to tdsskiller.com. Whether it finds anything or not does not mean you should not check with the other methods below.  
<http://support.kaspersky.com/viruses/solutions?qid=208280684>

Download malwarebytes and scan with it, run MRT, and add Prevx to be sure it is gone.  
(If Rootkits run UnHackMe)

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Malwarebytes - free  
<http://www.malwarebytes.org/>

Run the Microsoft Malicious Removal Tool

Start - type in Search box -> MRT find at top of list - Right Click on it - RUN AS ADMIN.

You should be getting this tool and its updates via Windows Updates - if needed you can download it here.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN  
(Then run MRT as above.)

Microsoft Malicious Removal Tool - 32 bit  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>

Microsoft Malicious Removal Tool - 64 bit  
<http://www.microsoft.com/downloads/details.aspx?FamilyId=585D2BDE-367F-495E-94E7-6349F4EFFC74&displaylang=en>

also install Prevx to be sure it is all gone.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Prevx - Home - Free - small, fast, exceptional CLOUD protection, works with other



security programs. This is a scanner only, VERY EFFECTIVE, if it finds something come back here or use Google to see how to remove.

<http://www.prevx.com/> <-- information

<http://info.prevx.com/downloadcsi.asp> <-- download

PCmag - Prevx - Editor's Choice

<http://www.pcmag.com/article2/0,2817,2346862,00.asp>

Try the trial version of Hitman Pro :

Hitman Pro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.).

<http://www.surfright.nl/en/hitmanpro>

-----  
If needed here are some online free scanners to help

<http://www.eset.com/onlinecan/>

-----  
Original version is now replaced by the Microsoft Safety Scanner

<http://onecare.live.com/site/en-us/default.htm>

Microsoft Safety Scanner

<http://www.microsoft.com/security/scanner/en-us/default.aspx>

-----  
<http://www.kaspersky.com/virusscanner>

Other Free online scans

<http://www.google.com/search?hl=en&source=hp&q=antivirus+free+online+scan&aq=f&oq=&aqi=g1>

-----  
**After removing any malware :**

**Also do these to cleanup general corruption and repair/replace damaged/missing system files.**

Start - type this in Search Box -> COMMAND find at top and RIGHT CLICK - RUN AS ADMIN

Enter this at the prompt - sfc /scannow

How to Repair Windows 7 System Files with System File Checker

<http://www.sevenforums.com/tutorials/1538-sfc-scannow-command-system-file-checker.html>

How to analyze the log file entries that the Microsoft Windows Resource Checker (SFC.exe) program generates in Windows Vista cbs.log

<http://support.microsoft.com/kb/928228>

Also run CheckDisk so we can rule out corruption as much as possible.

How to Run Disk Check in Windows 7

<http://www.sevenforums.com/tutorials/433-disk-check.html>

-----  
If any Rootkits are found use this thread and other suggestions. (Run UnHackMe)

<http://social.answers.microsoft.com/Forums/en-US/InternetExplorer/thread/a8f665f0-c793-441a-a5b9-54b7e1e7a5a4/>

=====

If needed AFTER you are sure the machine is clean of all malware.

How to Do a Repair Install to Fix Windows 7

<http://www.sevenforums.com/tutorials/3413-repair-install.html>

Hope this helps.


May 2, 2011 | Reply with quote | Report abuse

Reply

 MS MVP

 MVP



 Microsoft MVP - Windows Expert - Consumer : Bicycle - Mark Twain said it right.

---

## Question

### Z-bot tojan virus A.K.A ZEUS

Applies To: Windows | Windows Vista | Security, Privacy, and User Accounts

I have recently recieved a message from windows defender that my pc (WIN7) is infected with a zbot @ win32 does anyone know if that is real or not? and also there have been incidents on facebook about people clicking what appears to be youtube links but lead nowhere and by the time you notice, your pc is infected so as soon as you ave finished reading this scan your computer just to be sure.

also apparently a zbot uses a rootkit programm and it has been around since 2006 sooo...

.... whats a rootkit?

i really hope this helps and also please help me!

With kind regards: [REDACTED]

May 29, 2010 | Reply with quote | Report abuse

Reply

Email me

**3** People had  
this question Me Too



---

Was this helpful?

Yes

## Answer

A **rootkit** is a type of software that is designed to gain administrator-level control over a computer system without being detected.

<http://en.wikipedia.org/wiki/Rootkit>

Win32/Zbot is a family of password stealing trojans. Win32/Zbot also contains backdoor functionality that allows unauthorized access and control of an affected machine.

Scan your system with microsoft security essentials to remove these threats

[http://www.microsoft.com/security\\_essentials/](http://www.microsoft.com/security_essentials/)

Manual removal is not recommended for this threat. To detect and remove this threat and other malicious software that may have been installed, run a full-system scan with an up-to-date antivirus product such as the Microsoft online scanner (<http://safety.live.com> ).

PWS:Win32/Zbot attempts to steal sensitive and confidential information from affecters users in order to perpetrate fraud. If you believe that your personal financial information may have been compromised , visit <http://www.microsoft.com/athome/security/bank/PhishingVictim.mspx>

---

If this post helps to resolve your issue, please click the "Mark as Answer" or If you find it helpful , Mark it as helpful by clicking on "Helpful" button at the top of this message. By marking a post as Answered, or Helpful you help others find the answer faster.

May 29, 2010 | Reply with quote | Report abuse

Reply

**All Replies (5)**[More Help](#)

Was this helpful?

Yes

In reply to [REDACTED] post on May 29, 2010

Is there a way to get rid of a zbot?

Btw. i hae avira, norton, AVG, and mcafee and spybot search and destroy rning together and still it happened any ideas?

May 29, 2010 | [Reply with quote](#) | [Report abuse](#)[Reply](#)

[REDACTED]



Was this helpful?

Yes

In reply to [REDACTED] post on May 29, 2010

If Multiple anti-virus programs are running, your system may experience performance degradation and other problems caused by the conflict of two services providing real time protection simultaneously.

Please uninstall all security application and restart your computer. After that install microsfst security essential and scan your system

If you have further concerns and need help to remove threats/virus on your system , please go to

<https://consumersecuritysupport.microsoft.com/>

Hope the above information's helps you

Good luck

If this post helps to resolve your issue, please click the "Mark as Answer" or If you find it helpful , Mark it as helpful by clicking on "Helpful" button at the top of this message. By marking a post as Answered, or Helpful you help others find the answer faster.

May 29, 2010 | [Reply with quote](#) | [Report abuse](#)[Reply](#)

[REDACTED]



Was this helpful?

Yes

In reply to [REDACTED] post on May 29, 2010

ok i will but how can i rid the pc of the zbot and make sure it never comes back?

i tried a mirror program (a program that sends viruses back to their source) but that didn't work :( and a trojan removal tool but no luck there i even bought norton 360 and still nothing is there any way of manually finding and erasing the virus (critical OP system files are backed up on an external hard drive) also my main boot drive is affected by the looks of it coz i had to connect the external hard drive to boot the pc but i still have it.

could it be on the hard drive now?

May 29, 2010 | Reply with quote | Report abuse

Reply



Was this helpful?

Yes

In reply to [REDACTED] post on May 29, 2010

As i said please visit <https://consumersecuritysupport.microsoft.com/> if you have any questions on threat removal

You can get instant support through chat from experts.

- Enable a firewall on your computer.
- Get the latest computer updates for all your installed software.
- Use up-to-date antivirus software.
- Use caution when opening attachments and accepting file transfers.
- Use caution when clicking on links to Web pages.
- Avoid downloading pirated software.
- Protect yourself against social engineering attacks.
- Use strong passwords.

Use a third-party firewall product or turn on the Microsoft Windows Internet Connection Firewall.

- How to turn on the Windows Firewall in Windows 7
- How to turn on the Windows Firewall in Windows Vista
- How to turn on the Windows firewall in Windows XP

Updates help protect your computer from viruses, worms, and other threats as they are discovered. It is important to install updates for all the software that is installed in your computer. These are usually available from vendor Web sites.

You can use the Automatic Updates feature in Windows to automatically download future Microsoft security updates while your computer is on and connected to the Internet.

- How to turn on Automatic Updates in Windows 7
- How to turn on Automatic Updates in Windows Vista
- How to turn on Automatic Updates in Windows XP

Most antivirus software can detect and prevent infection by known malicious software. To help protect you from infection, you should always run antivirus software, such as Microsoft Security Essentials, that is updated with the latest signature files. For more information, see <http://www.microsoft.com/protect/computer/viruses/vista.mspx>.

Exercise caution with e-mail and attachments received from unknown sources, or received unexpectedly from known sources. Use extreme caution when accepting file transfers from known or unknown sources.

Exercise caution with links to Web pages that you receive from unknown sources, especially if the links are to a Web page that you are not familiar with, unsure of the destination of, or suspicious of. Malicious software may be installed in your system simply by visiting a Web page with harmful content.

Threats may also be bundled with software and files that are available for download on various torrent sites. Downloading "cracked" or "pirated" software from these sites carries not only the risk of being infected with malware, but is also illegal. For more information, see 'The risks of obtaining and using pirated software'.

While attackers may attempt to exploit vulnerabilities in hardware or software in order to compromise a system, they also attempt to exploit vulnerabilities in human behavior in order to do the same. When an attacker attempts to take advantage of human behavior in order to persuade the affected user to perform an action of the attacker's choice, it is known as 'social engineering'. Essentially, social engineering is an attack against the human interface of the targeted system. For more information, see 'What is social engineering?'.

Attackers may try to gain access to your Windows account by guessing your password. It is therefore important that you use a strong password – one that cannot be easily guessed by an attacker. A strong password is one that has at least 8 characters, and combines letters, numbers, and symbols. For more information, see <http://www.microsoft.com/protect/yourself/password/create.aspx>.

---

If this post helps to resolve your issue, please click the "Mark as Answer" or If you find it helpful , Mark it as helpful by clicking on "Helpful" button at the top of this message. By marking a post as Answered, or Helpful you help others find the answer faster.

May 29, 2010 | Reply with quote | Report abuse

Reply

[Redacted]

[Redacted]

## Question

### Windows Vista Start up message Virus in Win32?zbot.cre in c:\documents and settings\████████\application\data\vgeq\zeywk

Applies To: Windows | Windows Vista | Security, Privacy, and User Accounts

think I have a virus

When I logged onto my computer this morning I got the following message:

Virus in Win32?zbot.cre in c:\documents and settings\████████\application\data\vgeq\zeywk

I am using a computer that is networked to a Microsoft 2008 server at the office

September 21, 2010 | Reply with quote | Report abuse

Reply

Email me

**3** People had this question Me Too

████████



Was this helpful?

Yes

## Answer

Hi ██████████

You may try booting in Safe mode and check if the issue occurs

#### Step 1: Safe mode

You may refer the following links to boot in safe mode:

<http://windows.microsoft.com/en-US/windows-vista/Advanced-startup-options-including-safe-mode>

<http://windows.microsoft.com/en-US/windows-vista/Start-your-computer-in-safe-mode>

#### Step 2: Perform Clean boot

If you can boot in safe mode then try performing a clean boot to check if any third party software or startup item is causing this issue.

For more information on performing clean boot, you may refer the following link:

<http://support.microsoft.com/kb/929135>

If your issue is resolved after performing Clean Boot, then follow the steps mentioned in the above KB article to narrow down the exact source:

Also, after resolving the issue, see the section on how to return your computer to a Normal startup mode by following the steps under "Reset the computer to start as usual."

#### Step 3: You may also try running a live scan and antimalware scan.

Refer the following link:

<http://www.microsoft.com/security/malwareremove/default.aspx>

If nothing works, then you may get in touch with the system administrator.

If you need any further help, you may also post the issue here:

<http://social.technet.microsoft.com/Forums/en-us/itprovistasecurity/threads>

Hope this information is helpful.

Microsoft Answers Support Engineer

Visit our Microsoft Answers Feedback Forum and let us know what you think

If this post helps to resolve your issue, please click the "Mark as Answer" or "Helpful" button at the top of this message. By marking a post as Answered, or Helpful you help others find the answer faster.

September 22, 2010 | [Reply with quote](#) | [Report abuse](#)

Reply

  
Support Engineer



**All Replies (1)**

[More Help](#)



## Question

**zeus trogen**

Applies To: Microsoft Security Essentials | Getting Started and Upgrading

My compute appears to be highly infected with the ZEUS TROJEN and it has HIJACKED it. PLEASE HELP!!!

October 9, 2011 | Reply with quote | Report abuse

Reply

Email me

**1** Person had  
this question Me Too

Was this helpful?

Yes

**1**

Vote

Answer

Hi [REDACTED]

Zeus is AKA ZBot Trojan and here's more information about it:  
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fZbot>.

Please proceed as follows:

First, try the following programs if you haven't as they may help. I recommend you download, install, update, and run full scans with Malwarebytes:<http://www.malwarebytes.org/> and SuperAntiSpyware:<http://superantispyware.com/> and then run a full ESET online scan: <http://www.eset.com/us/online-scanner>. I'd also try Microsoft Safety Scanner as the article says it can deal with this infection: <http://www.microsoft.com/security/scanner/en-us/default.aspx>. These may or may not remove the infections, but will probably not repair any damage caused by them. Even if they or your current AV software seem to work or indicate you aren't infected, you shouldn't completely trust them and need to continue with the recommendations that follow (so it's up to you if you want to try them first or just skip over all of this and get the expert help you really need as described below).

Properly and completely removing such infections can be complex and often require manual removal procedures (which may or may not be entirely effective either). Even if they work, I'd suggest the following anyway, so we may as well start there (you can ignore the above removal methods if you want as this is really the way to go, but it won't hurt to try them).

Please follow these recommendations compliments of Stephen Boots - MVP:

**Are you running Microsoft Security Essentials?**

If so: **Start here** - <https://support.microsoftsecurityessentials.com/> and select the link that says - I think my computer is infected - and then select the support option for phone, chat or email (options will vary by Region)

If not using MSE:

You can start here: <https://consumersecuritysupport.microsoft.com/> or here:[http://support.microsoft.com/contactus/cu\\_sc\\_virsec\\_master?ws=support#tab0](http://support.microsoft.com/contactus/cu_sc_virsec_master?ws=support#tab0) for help and support for malware infections.

Whether you are or not, if you are in North America, you can call 866-727-2338 for free help from Microsoft for virus and spyware infections.

In other regions not served by the link above, go here: <http://Support.microsoft.com/security> and go to the "assisted support" or contact us menu.

If that doesn't work or they can't help, try one of the following malware-removal forums compliments of PA Bear - MVP:

*I can recommend the expert assistance offered in these forums:*<http://spywarehammer.com/simplemachinesforum/index.php?board=10.0>,<http://www.spywarewarrior.com/viewforum.php?f=5>,<http://www.dslreports.com/forum/cleanup>,<http://www.bluetack.co.uk/forums/index.php>, and <http://aumha.net/viewforum.php?f=30>

I hope this helps.

Good luck!

October 9, 2011 | Reply with quote | Report abuse

Reply

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

Join the community! Sign up for a free account to ask questions, share your knowledge, and connect with other experts.

Was this helpful?

Yes

1

Vote

Answer

In reply to [REDACTED] post on October 9, 2011

Hi [REDACTED]

If you are confused by them or how to deal with the results or they don't seem to be helping, then simply bypass them all, go to the bold section, and contact Microsoft Support using the provided links and numbers for expert advice and assistance. They will either guide you step-by-step or simply use remote desktop to connect to your computer and do it themselves while all you need to do is sit back and watch.

At this point, considering your confusion and your many different attempts, this is by far and away the best choice. Just in case, here again are those instructions:

**Start here** - <https://support.microsoftsecurityessentials.com/> and select the link that says - I think my computer is infected - and then select the support option for phone, chat or email (options will vary by Region)

If you are in North America, you can call 866-727-2338 for free help from Microsoft for virus and spyware infections.

In other regions not served by the link above, go here:<http://Support.microsoft.com/security> and go to the "assisted support" or contact us menu.

Please trust me on this and contact them and I assure you things will be easier, safer, simpler, more complete, and validated by a specialist. I'm confident they will resolve things and all you need to do for now is contact them as indicated above and then leave the rest up to them.

Good luck!

October 9, 2011 | Reply with quote | Report abuse

Reply

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

## All Replies (4) More Help

Was this helpful?

Yes

1

Vote

Answer

Hi [REDACTED]

Zeus is AKA ZBot Trojan and here's more information about it:  
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fZbot>.

Please proceed as follows:

First, try the following programs if you haven't as they may help. I recommend you download, install, update, and run full scans with Malwarebytes:<http://www.malwarebytes.org/> and SuperAntiSpyware:<http://superantispyware.com/> and then run a full ESET online scan: <http://www.eset.com/us/online-scanner>. I'd also try Microsoft Safety Scanner as the article says it can deal with this infection: <http://www.microsoft.com/security/scanner/en-us/default.aspx>. These may or may not remove the infections, but will probably not repair any damage caused by them. Even if they or your current AV software seem to work or indicate you aren't infected, you shouldn't completely trust them and need to continue with the recommendations that follow (so it's up to you if you want to try them first or just skip over all of this and get the expert help you really need as described below).

Properly and completely removing such infections can be complex and often require manual removal procedures (which may or may not be entirely effective either). Even if they work, I'd suggest the following anyway, so we may as well start there (you can ignore the above removal methods if you want as this is really the way to go, but it won't hurt to try them).

Please follow these recommendations compliments of [REDACTED] - MVP:

### Are you running Microsoft Security Essentials?

If so: **Start here** - <https://support.microsoftsecurityessentials.com/> and select the link that says - I think my computer is infected - and then select the support option for phone, chat or email (options will vary by Region)

If not using MSE:

You can start here: <https://consumersecuritysupport.microsoft.com/> or here:[http://support.microsoft.com/contactus/cu\\_sc\\_virsec\\_master?ws=support#tab0](http://support.microsoft.com/contactus/cu_sc_virsec_master?ws=support#tab0) for help and support for malware infections.

Whether you are or not, if you are in North America, you can call 866-727-2338 for free help from Microsoft for virus and spyware infections.

In other regions not served by the link above, go here: <http://Support.microsoft.com/security> and go to the "assisted support" or contact us menu.

If that doesn't work or they can't help, try one of the following malware-removal forums compliments of [REDACTED] - MVP:

*I can recommend the expert assistance offered in these forums:*  
*<http://spywarehammer.com/simplemachinesforum/index.php?board=10.0>, <http://www.spywarewarrior.com/viewforum.php?f=5>, <http://www.dslreports.com/forum/cleanup>, <http://www.bluetack.co.uk/forums/index.php>, and <http://aumha.net/viewforum.php?f=30>*

I hope this helps.

Good luck!

October 9, 2011 | Reply with quote | Report abuse

Reply



[REDACTED] MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

Was this helpful?

Yes

In reply to [REDACTED] post on October 9, 2011

Thank you for any advice given,  
I have tried to do a scan using 'SUPER ANTI SPYWARE', 'MALWAREBYTES ANTI-MALWARE' and 'MICROSOFT SECURITY SCANNER', as well as trying to generate a log with 'HIGHJACK THIS' and tried to run software called 'SPY HUNTER' which either shut down during the scan or like 'WINDOWS DEFENDER' don't even get a chance to start. I have been locked out of my control panel, system restore, program & file search, program files, etc. I tried to format my C drive and I have been locked out of that too. I have tried to reload WINDOWS from my XP HOME disk and my CD/DV drives don't work either. The program that has HIJACKED my computer is called 'GUARD ONLINE' and is operated by "B77ffEL9gTZqYCK.exe". I managed to get a Partial log from 'SUPER ANTI SPYWARE' but the scan shuts down before it gets to complete. There are over 100 infected areas and this virus seems to be a learning bug because when I try something that has worked in the past with other viruses, it starts to work then all access to that avenue gets shut down.

SUPERAntiSpyware Scan Log  
<http://www.superantispyware.com>

Generated 08/20/2008 at 08:46 AM

Application Version : 4.15.1000

Core Rules Database Version : 3540  
Trace Rules Database Version: 1529

Scan type : Complete Scan  
Total Scan Time : 01:54:32

Memory items scanned : 502  
Memory threats detected : 1  
Registry items scanned : 7694  
Registry threats detected : 9  
File items scanned : 163997  
File threats detected : 11

**Adware.IWinGames**

C:\PROGRA~1\WINGA~1\WINGA~1.DLL  
C:\PROGRA~1\WINGA~1\WINGA~1.DLL  
HKLM\Software\Classes\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}\InprocServer32  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}\InprocServer32#ThreadingModel  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}\ProgID  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}\Programmable  
HKCR\CLSID\{8CA5ED52-F3FB-4414-A105-2E3491156990}\VersionIndependentProgID  
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{8CA5ED52-F3FB-4414-A105-2E3491156990}  
C:\PROGRAM FILES\IWIN GAMES\IWINGAMESHOOKIE.DLL

**Adware.Tracking Cookie**

C:\Documents and Settings\██████████\Cookies\██████████@mediatrafic[1].txt  
C:\Documents and Settings\██████████\Cookies\\*\*\* Email address is removed for privacy \*\*\*[1].txt  
C:\Documents and Settings\██████████\Cookies\\*\*\* Email address is removed for privacy \*\*\*[2].txt  
C:\Documents and Settings\██████████\Cookies\██████████@doubleclick[1].txt  
C:\Documents and Settings\██████████\Cookies\██████████@clickbank[1].txt  
C:\Documents and Settings\██████████\Cookies\██████████@zedo[1].txt  
C:\Documents and Settings\██████████\Cookies\██████████@windowsmedia[2].txt  
C:\Documents and Settings\██████████\Cookies\\*\*\* Email address is removed for privacy \*\*\*[1].txt

**Adware.Mirar/NetNucleus**

C:\DOCUMENTS AND SETTINGS\██████████\LOCAL SETTINGS\TEMPORARY INTERNET FILES\CONTENT.IE5  
7XUUJD1Y\UNINSTALLER[1].EXE

I'm Completely PUZZLED and don't know what to do next!!!

October 9, 2011 | Reply with quote | Report abuse

Reply



Was this helpful?

Yes

1

Vote  
Answer

In reply to [REDACTED] post on October 9, 2011

Hi [REDACTED]

If you are confused by them or how to deal with the results or they don't seem to be helping, then simply bypass them all, go to the bold section, and contact Microsoft Support using the provided links and numbers for expert advice and assistance. They will either guide you step-by-step or simply use remote desktop to connect to your computer and do it themselves while all you need to do is sit back and watch.

At this point, considering your confusion and your many different attempts, this is by far and away the best choice. Just in case, here again are those instructions:

**Start here - <https://support.microsoftsecurityessentials.com/> and select the link that says - I think my computer is infected - and then select the support option for phone, chat or email (options will vary by Region)**

**If you are in North America, you can call 866-727-2338 for free help from Microsoft for virus and spyware infections.**

**In other regions not served by the link above, go here:<http://Support.microsoft.com/security> and go to the "assisted support" or contact us menu.**

Please trust me on this and contact them and I assure you things will be easier, safer, simpler, more complete, and validated by a specialist. I'm confident they will resolve things and all you need to do for now is contact them as indicated above and then leave the rest up to them.

Good luck!

October 9, 2011 | Reply with quote | Report abuse

Reply



[REDACTED] MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

Was this helpful?

Yes

1

Vote

Answer

In reply to [REDACTED] post on October 9, 2011

Sir, it's not really my place to offer help here, but youre using a very old version of superantispyware. i'd advise trying the portable version from here:

<http://www.superantispyware.com/portablescanner.html>

restart your computer into safe mode. info on how to do that here:

<http://www.bleepingcomputer.com/tutorials/how-to-start-windows-in-safe-mode/>

scan and remove all threats found by your scanners and reboot into normal mode.

good luck!

October 9, 2011 | [Reply with quote](#) | [Report abuse](#)

Reply

[REDACTED]



## Question

**PSW:Win32/Zbot.gen!Y How do I get rid of this?**

Applies To: Microsoft Security Essentials | Scanning, Detecting, and Removing Threats

How do I get rid of this? Each time I start up my laptop it says My computer is infected. Help

April 15, 2011 | Reply with quote | Report abuse

Reply

Email me

**1** Person had  
this question Me Too

Was this helpful?

Yes

**1**

Vote

## Answer

The following excerpts are from the Encyclopedia entry for PWSWin32-Zbot.gen!Y at the Microsoft Malware Protection Center:

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3aWin32%2fZbot.gen!Y>

"PWS:Win32/Zbot.gen!Y is a generic detection for a password stealer and remote access trojan."

The above means that you should not access any banking or other important web sites that require passwords on this PC until it has been completely cleaned of this infection.

[http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3aWin32%2fZbot.gen!Y#recovery\\_link](http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3aWin32%2fZbot.gen!Y#recovery_link)

"This threat may make lasting changes to a computer's configuration that are NOT restored by detecting and removing this threat."

This means that even once an anti-malware application has successfully removed the infection itself, the PC is still at high risk of reinfection by this same or other malware.

All of the above and other information in that same Encyclopedia entry indicate that this is a very difficult to remove and dangerous information stealing (identity theft) infection, which means you will likely require knowledgeable help to remove it properly.

You will also need to change any passwords for banking or other passworded web sites that you have used from this PC, especially if these passwords were saved on that PC, since this malware steals all of that information. You MUST do this from a different PC unless the malware has been fully removed, since the new passwords will be immediately stolen on this PC again if it hasn't.

April 15, 2011 | Reply with quote | Report abuse

Reply

MCC

Was this helpful?

Yes



## Answer

Hi,

If you need to check for malware here are my recommendations - these will allow you to do a thorough check and removal without ending up with a load of spyware programs running resident which can cause as many issues as the malware and maybe harder to detect as the cause.

No one program can be relied upon to detect and remove all malware. Added that often easy to detect malware is often accompanied by a much harder to detect and remove payload. So its better to be overly thorough now than to pay the high price later. Check with these to an extreme overkill point and then run the cleanup only when you are very sure the system is clean.

These can be done in Safe Mode - repeatedly tap F8 as you boot however you should also run them in regular Windows when you can.

TDSSKiller.exe. - Download to the Desktop - then go to it and Right Click on it - RUN AS ADMIN it will show any infections in the report after running - if it will not run change the name from tdsskiller.exe to tdsskiller.com. Whether it finds anything or not does not mean you should not check with the other methods below.  
<http://support.kaspersky.com/viruses/solutions?qid=208280684>

Download malwarebytes and scan with it, run MRT, and add Prevx to be sure it is gone.  
(If Rootkits run UnHackMe)

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Malwarebytes - free  
<http://www.malwarebytes.org/>

Run the Microsoft Malicious Removal Tool

Start - type in Search box -> MRT find at top of list - Right Click on it - RUN AS ADMIN.

You should be getting this tool and its updates via Windows Updates - if needed you can download it here.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN  
(Then run MRT as above.)

Microsoft Malicious Removal Tool - 32 bit  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>

Microsoft Malicious Removal Tool - 64 bit  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=585D2BDE-367F-495E-94E7-6349F4E7FC74&displaylang=en>

also install Prevx to be sure it is all gone.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Prevx - Home - Free - small, fast, exceptional CLOUD protection, works with other security programs. This is a scanner only, VERY EFFECTIVE, if it finds something come back here or use Google to see how to remove.

<http://www.prevx.com/> <-- information  
<http://info.prevx.com/downloadcsi.asp> <-- download

PCmag - Prevx - Editor's Choice  
<http://www.pcmag.com/article2/0,2817,2346862,00.asp>

Try the trial version of Hitman Pro :

Hitman Pro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.).  
<http://www.surfright.nl/en/hitmanpro>

-----  
If needed here are some online free scanners to help

<http://www.eset.com/onlinecan/>

Original version is now replaced by the Microsoft Safety Scanner  
<http://onecare.live.com/site/en-us/default.htm>

Microsoft Safety Scanner  
<http://www.microsoft.com/security/scanner/en-us/default.aspx>

<http://www.kaspersky.com/virusscanner>

Other Free online scans  
<http://www.google.com/search?hl=en&source=hp&q=antivirus+free+online+scan&aq=f&oq=&aqi=g1>

**After removing any malware :**

**Also do these to cleanup general corruption and repair/replace damaged/missing system files.**

Start - type this in Search Box -> COMMAND find at top and RIGHT CLICK - RUN AS ADMIN

Enter this at the prompt - sfc /scannow

How to Repair Windows 7 System Files with System File Checker  
<http://www.sevenforums.com/tutorials/1538-sfc-scannow-command-system-file-checker.html>

How to analyze the log file entries that the Microsoft Windows Resource Checker (SFC.exe) program generates in Windows Vista cbs.log  
<http://support.microsoft.com/kb/928228>

Also run CheckDisk so we can rule out corruption as much as possible.

How to Run Disk Check in Windows 7  
<http://www.sevenforums.com/tutorials/433-disk-check.html>

If any Rootkits are found use this thread and other suggestions. (Run UnHackMe)

<http://social.answers.microsoft.com/Forums/en-US/InternetExplorer/thread/a8f665f0-c793-441a-a5b9-54b7e1e7a5a4/>

If needed AFTER you are sure the machine is clean of all malware.

How to Do a Repair Install to Fix Windows 7  
<http://www.sevenforums.com/tutorials/3413-repair-install.html>

Hope this helps.

April 15, 2011 | Reply with quote | Report abuse

Reply

MS MVP

MVP

- Microsoft MVP - Windows Expert - Consumer : Bicycle - Mark Twain said it right.

**All Replies (3)**    More Help

Was this helpful?

Yes

## Answer

Hi,

If you need to check for malware here are my recommendations - these will allow you to do a thorough check and removal without ending up with a load of spyware programs running resident which can cause as many issues as the malware and maybe harder to detect as the cause.

No one program can be relied upon to detect and remove all malware. Added that often easy to detect malware is often accompanied by a much harder to detect and remove payload. So its better to be overly thorough now than to pay the high price later. Check with these to an extreme overkill point and then run the cleanup only when you are very sure the system is clean.

These can be done in Safe Mode - repeatedly tap F8 as you boot however you should also run them in regular Windows when you can.

TDSSKiller.exe. - Download to the Desktop - then go to it and Right Click on it - RUN AS ADMIN it will show any infections in the report after running - if it will not run change the name from tdsskiller.exe to tdsskiller.com. Whether it finds anything or not does not mean you should not check with the other methods below.

<http://support.kaspersky.com/viruses/solutions?qid=208280684>

Download malwarebytes and scan with it, run MRT, and add Prevx to be sure it is gone.  
(If Rootkits run UnHackMe)

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Malwarebytes - free

<http://www.malwarebytes.org/>

Run the Microsoft Malicious Removal Tool

Start - type in Search box -> MRT find at top of list - Right Click on it - RUN AS ADMIN.

You should be getting this tool and its updates via Windows Updates - if needed you can download it here.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN  
(Then run MRT as above.)

Microsoft Malicious Removal Tool - 32 bit

<http://www.microsoft.com/downloads/details.aspx?FamilyID=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>

Microsoft Malicious Removal Tool - 64 bit

<http://www.microsoft.com/downloads/details.aspx?FamilyId=585D2BDE-367F-495E-94E7-6349F4EFC74&displaylang=en>

also install Prevx to be sure it is all gone.

Download - SAVE - go to where you put it - Right Click on it - RUN AS ADMIN

Prevx - Home - Free - small, fast, exceptional CLOUD protection, works with other security programs. This is a scanner only, VERY EFFECTIVE, if it finds something come back here or use Google to see how to remove.

<http://www.prevx.com/> <-- information

<http://info.prevx.com/downloadcsi.asp> <-- download

PCmag - Prevx - Editor's Choice

<http://www.pcmag.com/article2/0,2817,2346862,00.asp>

Try the trial version of Hitman Pro :

Hitman Pro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.).

<http://www.surfright.nl/en/hitmanpro>

If needed here are some online free scanners to help

<http://www.eset.com/onlinescan/>

---

Original version is now replaced by the Microsoft Safety Scanner

<http://onecare.live.com/site/en-us/default.htm>

Microsoft Safety Scanner

<http://www.microsoft.com/security/scanner/en-us/default.aspx>

---

<http://www.kaspersky.com/virusscanner>

Other Free online scans

<http://www.google.com/search?hl=en&source=hp&q=antivirus+free+online+scan&aq=f&oq=&aqi=g1>

---

**After removing any malware :**

**Also do these to cleanup general corruption and repair/replace damaged/missing system files.**

Start - type this in Search Box -> COMMAND find at top and RIGHT CLICK - RUN AS ADMIN

Enter this at the prompt - sfc /scannow

How to Repair Windows 7 System Files with System File Checker

<http://www.sevenforums.com/tutorials/1538-sfc-scannow-command-system-file-checker.html>

How to analyze the log file entries that the Microsoft Windows Resource Checker (SFC.exe) program generates in Windows Vista cbs.log

<http://support.microsoft.com/kb/928228>

Also run CheckDisk so we can rule out corruption as much as possible.

How to Run Disk Check in Windows 7

<http://www.sevenforums.com/tutorials/433-disk-check.html>

---

If any Rootkits are found use this thread and other suggestions. (Run UnHackMe)

<http://social.answers.microsoft.com/Forums/en-US/InternetExplorer/thread/a8f665f0-c793-441a-a5b9-54b7e1e7a5a4/>

---

If needed AFTER you are sure the machine is clean of all malware.

How to Do a Repair Install to Fix Windows 7

<http://www.sevenforums.com/tutorials/3413-repair-install.html>

Hope this helps.

April 15, 2011 | Reply with quote | Report abuse

Reply

MS MVP

MVP

Microsoft MVP - Windows Expert - Consumer : Bicycle - Mark Twain said it right.

Was this helpful?

Yes

1

Vote

Answer

The following excerpts are from the Encyclopedia entry for PWSWin32-Zbot.gen!Y at the Microsoft Malware Protection Center:

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3aWin32%2fZbot.gen!Y>

"PWS:Win32/Zbot.gen!Y is a generic detection for a password stealer and remote access trojan."

The above means that you should not access any banking or other important web sites that require passwords on this PC until it has been completely cleaned of this infection.

[http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3aWin32%2fZbot.gen!Y#recovery\\_link](http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS%3aWin32%2fZbot.gen!Y#recovery_link)

"This threat may make lasting changes to a computer's configuration that are NOT restored by detecting and removing this threat."

This means that even once an anti-malware application has successfully removed the infection itself, the PC is still at high risk of reinfection by this same or other malware.

All of the above and other information in that same Encyclopedia entry indicate that this is a very difficult to remove and dangerous information stealing (identity theft) infection, which means you will likely require knowledgeable help to remove it properly.

You will also need to change any passwords for banking or other passworded web sites that you have used from this PC, especially if these passwords were saved on that PC, since this malware steals all of that information. You MUST do this from a different PC unless the malware has been fully removed, since the new passwords will be immediately stolen on this PC again if it hasn't.

April 15, 2011 | Reply with quote | Report abuse

Reply

MCC

Was this helpful?

Yes

How do I get rid of this? Each time I start up my laptop it says My computer is infected. Help

Are you running Microsoft Security Essentials? You have posted to a forum for users of Microsoft Security Essentials.

**If so:**

Start here - <https://support.microsoftsecurityessentials.com/>

and select the link that says - I think my computer is infected - and then select the support option for phone, chat or email (options will vary by Region)

**If not:**

You can start here: <https://consumersecuritysupport.microsoft.com/> or here:

[http://support.microsoft.com/contactus/cu\\_sc\\_virsec\\_master?ws=support#tab0](http://support.microsoft.com/contactus/cu_sc_virsec_master?ws=support#tab0) for help and support for malware infections.

If you are in North America, you can call 866-727-2338 for free help from Microsoft for virus and spyware infections. In other regions not served by the link above, go here: <http://Support.microsoft.com/security> and go to the "assisted support" or contact us menu.

[REDACTED]

April 15, 2011 | [Reply with quote](#) | [Report abuse](#)

Reply

[REDACTED]

[REDACTED]

MVP

[REDACTED]

Microsoft MVP Windows Live

## Question

### pws:win32/zbot- MSE is not removing it.

Applies To: Microsoft Security Essentials | Scanning, Detecting, and Removing Threats

Hello. "PWS:win32/zbot" keeps showing up in my MSE scans and MSE does not seem to be completely removing it. Can MSE handle this password stealer? If not, is there a tool to completely remove this? Thank you. Greg.

June 10, 2011 | Reply with quote | Report abuse

Reply

Email me

**1** Person had  
this question Me Too



Was this helpful?

Yes

### Answer

Saw your other post - glad to see you started a separate thread.

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=PWS:Win32/Zbot>

MSE **should** remove this threat and I have no explanation why it's not doing so.

Suggest you manually update MSE to get the latest definitions, disable system restore, scan with MSE, reboot the computer and then reenable system restore which should get rid of any malware in the system volume folder.

If that doesn't work your best option is to seek assistance from MSE Support:

Since you are using **Microsoft Security Essentials**, you can get help with malware removal here: <https://support.microsoftsecurityessentials.com/> Then select "**I think my computer is infected**". From there, select the email or phone option. You can also use <https://consumersecuritysupport.microsoft.com/eform.aspx?productKey=pcsafetymalware&ct=eformts&supportLink=eformts=E-mail>

If you are in North America, you can call MS Support at 866-727-2338 for help with virus and spyware infections.

For international information see your local subsidiary support site.

**OR**

Go to [www.malwarebytes.org](http://www.malwarebytes.org) and download, install, update and run the free version – just follow the prompts. You may need to rename the installation file to 123.exe or something similar to prevent the malware from disabling/blocking the installation.

and/or

Try Hitman Pro:

<http://www.surfright.nl/en/hitmanpro> This is a 30 day trial version of a pay product; if the program works and you like the program and decide to purchase it, that is your option.

and/or

Try TDSS Killer: <http://support.kaspersky.com/faq/?qid=208283363>

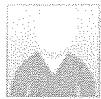
If the above steps are not successful, you could also seek assistance at Virtual Doctor Forums - they are quite good at malware removal: <http://discussions.virtualdr.com/forumdisplay.php?f=71>

Good luck...

[http://\[REDACTED\]/why\\_dont\\_antimalware\\_tools\\_work\\_better.html](http://[REDACTED]/why_dont_antimalware_tools_work_better.html)

June 10, 2011 | [Reply with quote](#) | [Report abuse](#)

Reply



**All Replies (1)**

[More Help](#)



## Question

**Zeus (zero-day)**

Applies To: Microsoft Security Essentials | Scanning, Detecting, and Removing Threats

Here is a recent test from Malware Research Group that shows MSE failed. Is a fix in the works?

**Threat Name:** Zeus (zero-day)**Threat Type:** KeyLogger**Risk Level:** Severe**Operating System:** Windows 7 32-bit Ultimate**Standalone Anti-Malware Applications**

Avira AntiVir Premium	Failed
Avast Antivirus Professional	Failed
AVG Antivirus	Failed
BitDefender Antivirus	Failed
BluePoint Security	Passed
Emsisoft Anti-Malware	Failed
Eset Nod32 Antivirus	Failed
F-Secure Antivirus	Failed
G Data Antivirus	Failed
Immunet Protect Plus	Failed
Kaspersky Antivirus	Failed
Microsoft Security Essentials	Failed
McAfee Antivirus Plus	Failed
Norton Antivirus	Passed
Panda Antivirus	Failed
PC Tools Spyware Doctor with Antivirus	Failed
Prevx	Passed
GFI/Sunbelt VIPRE Antivirus Premium	Passed

**Complementary Anti-Malware Applications**

Malwarebytes Anti-Malware	Passed
SUPERAntispyware Professional Edition	Failed

May 20, 2011 | Reply with quote | Report abuse

Reply

Email me

**2** People had this question Me Too

Was this helpful?

Yes

**1**

Vote

Answer

Hi [REDACTED]

Are you infected? It sounds more like you identified a threat MSE isn't detecting and are curious about how Microsoft is dealing with it. If infected, post back and I'll provide more detailed instructions on how to address the situation.

I'm tempted to automatically respond yes as the people who produce definitions and updates are hard at work on every bit of malware and virus they identify. According to the Microsoft Malware Protection Center <http://www.microsoft.com/security/portal/>, this particular threat does not seem to be included in their listing at this time so either they are unaware of it (unlikely) or they haven't produced an article concerning this threat yet (more likely). If you had

a sample, you could submit it at this site (but I assume your question is generic and that you aren't infected yourself and don't have a sample you can send them). One way to potentially bring this to their attention is via their blog at: <http://blogs.technet.com/b/mmpc/>.

As far as MSE goes, the only way I know to report a threat not covered by MSE (other than getting infected by it - LOL!) is through feedback here: <https://feedback.microsoftsecurityessentials.com/default.aspx?productkey=moor&mkt=en-us>. Presumably, they will get it to the right people (once they read it, if they read it, and if they do something about it - and we can only hope that works as well as we all want it to work). There's no specific place to report threats not caught by MSE (or any other Security product as far as I know) such as you've discovered with the posted report. But I'm willing to wager but can't guarantee they are well aware of that report and this threat.

Other than that, we don't really have access to the people who respond to these threats for MSE and other security products (like ForeFront or MSRT or Safety Scanner...). And they simply don't have the time to keep us informed on their progress with every threat they're working on (it would serve little purpose, it would divert their energies from working on the threats, and they probably can't predict a date of resolution anyway).

I realize this isn't really an answer to your question, but we don't have anyone to truly ask about it. We don't have any special inside contacts. We have no better way of reporting this stuff than anyone else. We have no way of finding out answers to their progress on specific threats (though I'm willing to bet they know about them before we do and before you did as well even if they don't immediately publish anything about it).

In the meantime, since Malwarebytes seems to have passed, if we find anyone so infected we can suggest they try using that (I generally do so anyway). There are also several information articles and suggested removal procedures out there: <http://www.bing.com/search?q=zeus%20keylogger&PQ=zeus&SP=2&QS=HS&SK=HS1&sc=8-4&form=BB07SH&pc=BB07>, and then, if all else fails (or perhaps in any case to be on the safe side), refer them to the MSE email support link or the Microsoft malware removal support number as usual for assistance.

I hope this helps.

Thanks and good luck!

May 21, 2011 | Reply with quote | Report abuse

Reply

[Redacted]

[Redacted]

[Redacted]

[Redacted] MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

## All Replies (6)

## More Help

Was this helpful?

Yes

Could you give us the URL or the reference for these information? First we should know is this a virus or false-positive.

If you have sample of it, I suggest to submit it to:

<https://www.microsoft.com/security/portal/Submission/Submit.aspx>

If it detect as Malware, then once you update MSE it will detect.

May 21, 2011 | Reply with quote | Report abuse

Reply

[Redacted]



Community Star

Was this helpful?

Yes

1

Vote

Answer

Hi [REDACTED]

Are you infected? It sounds more like you identified a threat MSE isn't detecting and are curious about how Microsoft is dealing with it. If infected, post back and I'll provide more detailed instructions on how to address the situation.

I'm tempted to automatically respond yes as the people who produce definitions and updates are hard at work on every bit of malware and virus they identify. According to the Microsoft Malware Protection Center <http://www.microsoft.com/security/portal/>, this particular threat does not seem to be included in their listing at this time so either they are unaware of it (unlikely) or they haven't produced an article concerning this threat yet (more likely). If you had a sample, you could submit it at this site (but I assume your question is generic and that you aren't infected yourself and don't have a sample you can send them). One way to potentially bring this to their attention is via their blog at: <http://blogs.technet.com/b/mmpc/>.

As far as MSE goes, the only way I know to report a threat not covered by MSE (other than getting infected by it - LOL!) is through feedback here: <https://feedback.microsoftsecurityessentials.com/default.aspx?productkey=morro&mkt=en-us>. Presumably, they will get it to the right people (once they read it, if they read it, and if they do something about it - and we can only hope that works as well as we all want it to work). There's no specific place to report threats not caught by MSE (or any other Security product as far as I know) such as you've discovered with the posted report. But I'm willing to wager but can't guarantee they are well aware of that report and this threat.

Other than that, we don't really have access to the people who respond to these threats for MSE and other security products (like ForeFront or MSRT or Safety Scanner...). And they simply don't have the time to keep us informed on their progress with every threat they're working on (it would serve little purpose, it would divert their energies from working on the threats, and they probably can't predict a date of resolution anyway).

I realize this isn't really an answer to your question, but we don't have anyone to truly ask about it. We don't have any special inside contacts. We have no better way of reporting this stuff than anyone else. We have no way of finding out answers to their progress on specific threats (though I'm willing to bet they know about them before we do and before you did as well even if they don't immediately publish anything about it).

In the meantime, since Malwarebytes seems to have passed, if we find anyone so infected we can suggest they try using that (I generally do so anyway). There are also several information articles and suggested removal procedures out there: <http://www.bing.com/search?q=zeus%20keylogger&PQ=zeus&SP=2&QS=HS&SK=HS1&sc=8-4&form=BB07SH&pc=BB07>, and then, if all else fails (or perhaps in any case to be on the safe side), refer them to the MSE email support link or the Microsoft malware removal support number as usual for assistance.

I hope this helps.

Thanks and good luck!

May 21, 2011 | Reply with quote | Report abuse

Reply

[REDACTED]



MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

Was this helpful?

Yes

In reply to [redacted] post on May 21, 2011

That's from Sunbelt Security News(Vipre) Vol 4 #115 May 18, 2011 "The Infamous CR Review"  
<http://www.sunbeltsecuritynews.com/>  
Take it for what it's worth.

May 21, 2011 | Reply with quote | Report abuse

Reply



MCC



My first computer was a Commodore 63 (1963) E-mail was twice as fast as regular mail.

Was this helpful?

Yes

In reply to [redacted] post on May 21, 2011

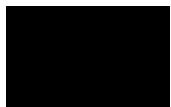
Hi [redacted]

Thanks for that. BTW, I'd like to talk to you privately and outside the forums (to get to know each other better and so forth) as I'm impressed by your work here and would like to know you better. [redacted] profile leads to an email address where you can contact him to get mine - I've already messaged him it's OK to give it to you. If interested, give me a shout.

Take care!

May 21, 2011 | Reply with quote | Report abuse

Reply



MCSE, MCSA, Network+, A+, ex-MCC. Mark helpful posts & answers - it thanks us & helps viewers.

Was this helpful?

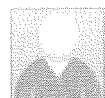
Yes

In reply to Cyber\_Defend\_Team post on May 21, 2011

See post below. It was indeed in a Vipre newsletter. Thanks.

May 21, 2011 | Reply with quote | Report abuse

Reply



MCC



Was this helpful?

Yes

In reply to [redacted] post on May 21, 2011

No, not infected, just curious. Thanks for the excellent response.



MCC

May 21, 2011 | Reply with quote | Report abuse



Reply

