Microsoft

Sign in

Community

Find answers | Ask a question

We'll search this forum for an answer

Virus and Malware

Applies To: Virus and Malware | Other | Scanning, Detecting, and Removing Threats

Question

1 Had this question Me Too

Randyleepierce asked on August 12, 2012

Reveton virus

I have been infected by this virus (FBI scam) on my browser and it has locked my screen. I am unable to return to my home page as it comes up locked out every time. I am on my wife's browser and it seems to be fine. How can I remove it or return to my home page.
<Windows 7>

Reply | Reply with quote | Report abuse | Email updates

Answer

0 Found this helpful Me Too

Le Boule replied on August 12, 2012

Community Star

> I have been infected by this virus (FBI scam) on my browser and it has locked my screen. I am unable to return to my home page as it comes up locked out every time. I am on my wife's browser and it seems to be fine. How can I remove it or return to my home page.
> <Windows 7>

Have you sought assistance from your antimalware provider?

See http://www.bleepingcomputer.com/virus-removal/remove-fbi-monkeypak-ransomware

Alternatively suggest try the advice in the following link compliments of **Brian-** who is one of the Answers Forum users:
http://www.selectrealsecurity.com/remove-ransomware

Reply | Reply with quote | Report abuse

All Replies (3)

0 Found this helpful Me Too

George222(2) replied on August 12, 2012

Community Star

Ive not had the attack so Ive not tried this, but from a google:

http://www.f-secure.com/v-descs/trojan_w32_reveton.shtml from http://gcn.com/articles/2012/08/10/reveton-drive-by-fbi-extortion-scam.aspx

May assist. Thankfully Seems simple enough.

Also, download, install, update *(update by right-clicking its icon and 'run as admin' then go to its <update> tab)* and run a full scan with free Malwarebytes, **and** update your AV checker and run a full scan with that as well.

As its possible that this type of attack can download other nasties, it may be wise to also get the free version of http://www.superantispyware.com/downloadfile.html?productid=superantispywarefree and scan with that as well, as a double check.

Related Threads

Reveton Virus is in desktop and IE 9

Virus: .... Trojan:Win32/Reveton.N... Help!

Infected by the ransom virus (Reveton)

screen freeze reveton virus

Reveton virus

More Microsoft Resources

Help and Support for Security Essentials

Using Windows Defender

Learn about current top threats

Virus and Security Solution Center

Get Micrososft Security Essentials

English

Reply | Reply with quote | Report abuse

Answer

0 Found this helpful Me Too

Le Boule replied on August 12, 2012

Community Star

I have been infected by this virus (FBI scam) on my browser and it has locked my screen. I am unable to return to my home page as it comes up locked out every time. I am on my wife's browser and it seems to be fine. How can I remove it or return to my home page.
<Windows 7>

Have you sought assistance from your antimalware provider?

See http://www.bleepingcomputer.com/virus-removal/remove-fbi-monkeypak-ransomware

Alternatively suggest try the advice in the following link compliments of **Brian-** who is one of the Answers Forum users:
http://www.selectrealsecurity.com/remove-ransomware

Reply | Reply with quote | Report abuse

0 Found this helpful Me Too

fishman35 replied on October 26, 2012

In reply to Le Boule post on August 12, 2012

This one is a Flash exploit and is really weak. To disable it, boot into Safe Mode and disable all on the startup tab, (or simply uncheck the bogus entry. Anyone who spends time in MSCONFIG will notice it). Or discconect your NIC cable. This exploit cannot launch with an internet connection. Then you can run any malware scanner to get rid of it.
I use this version of Reveton to teachmalware removal classes.

It basically loads 3 files: a pointer, (MSCONFIG startup entry in HKLM\SW\MS\WND\CV\RUN), a loader, (usually in the hidden directory C:\ProgramData in Windows 7, and a painter, (which usually resides in the user\appdata\temp folder). The one I use to train uses a fake CFTMON for the startup, a fake lsass in ProgramData, and a Notepad.dll to paint the screen. This will always change, as will directories if you are using XP.

Now the damage afterwords can be bad, depending on level of root. Your Windows Firewall may go bye-bye, or your homepage may be hijacked. This is due to a second payload that comes in after the intital infection. Running ComboFix will usually do the job, but you should really read up on it's usage. You can do some damage unless you know what you are doing.

I use this version of Reveton to teachmalware removal classes.

Hope this helps

Reply | Reply with quote | Report abuse

Microsoft

Sign in

Community

Find answers | Ask a question

We'll search this forum for an answer

Windows

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

Question

3 Had this question Me Too

tonydownard asked on March 13, 2012

how do i remove trojan:win32/reveton.a virus

already ran microsoft security scan and parcialy removed it any sugestions to remove it completely

Reply | Reply with quote | Report abuse | Email updates

All Replies (7)

José Antonio Pontón Posada CEO replied on March 13, 2012

Community Star

1 Found this helpful Me Too

1. Open IE 32-bit (only) to https://consumersecuritysupport.microsoft.com/
2. Click on **I think my computer is infected**
3. On the resulting page, click on Run the Microsoft Safety Scanner
4. Select appropriate bit-service

Download now - 32 bit
Download now - 64 bit
then click on CONTINUE

I.- Clear out your Temporary files
Click **Start** > **All Programs** > **Accessories** > **System Tools** > **Disk Cleanup**

II.- Have your system scanned by the installed antivirus/security suite.

III.- Run this tool from Kaspersky: How to remove malware belonging to the family **Rootkit**.Win32.TDSS
<<http://support.kaspersky.com/viruses/solutions?qid=208280684>>

IV.- Download, install, update, and run scans with both of these free anti-malware tools:
MalwareBytes AntiMalware (**MBAM**)
<<http://www.malwarebytes.org/products/malwarebytes_free>>
SUPERAntiSpyware (**SAS**)
<<http://superantispyware.com/superantispywarefreevspro.html>>

*V.- **Mcafee's Stinger Virus Rem°ver***
<<http://vil.nai.com/vil/stinger/>>

-=-
UTC/GMT is 23:33 on Tuesday, March 13, 2012

Reply | Reply with quote | Report abuse

Brian M- replied on March 13, 2012

Community Star

1 Found this helpful Me Too

Related Threads

There are no related threads.

More Microsoft Resources

Windows Vista Help & How-to
Windows Vista Solution Center
Get Help Now For Windows Vista
Can my PC run Windows 7?
Microsoft Store

English Hi,

If the above suggestions do not work, try following **Step 1** and **2** in this virus/malware removal guide:
http://www.selectrealsecurity.com/malware-removal-guide

It contains instructions that will remove most malware infections. If you have any questions, just ask me. I hope this helps you.

Brian

Reply | Reply with quote | Report abuse

Joy Sarcar replied on September 10, 2012

0 Found this helpful Me Too

already ran microsoft security scan and parcialy removed it any sugestions to remove it completely

Whatever Windows based operating system version you use there are chances that some malware can bring back your PC to its knees. My Windows PC was infected with Trojan:Win32/Reveton.F couple of months ago. My PC was freezing most often than not and most of the applications were not working properly. I use Microsoft Security Essential and when I ran a scan of my hard drive it detected a worm by the name of Trojan:Win32/Reveton.F and then I moved it to the quarantine. I stopped the process of the worm from the Task Manager and deleted entries from the Windows Registry Editor.

I read a post online about how to troubleshoot Windows PC from Trojan:Win32/Reveton.F infection and you can have a look also:

http://www.howtofixerror.com/fixerror/remove-trojan%3awin32reveton.f-how-to-delete-trojan%3awin32reveton.f/882

All the Best

Reply | Reply with quote | Report abuse

vinodmalhotra1 replied on September 30, 2012

0 Found this helpful Me Too

In reply to Joy Sarcar post on September 10, 2012

The Microsoft seurity tool did not get rid of the Revton virus on my computer. The Antimalware bytes and the Superantivirus programs did not find the infected files. I found in another forum that advised downloading and running the Hitman Pro.

I downloaded the Hitman Pro for removing it. The program got rid of the virus but now my computer does not shut off windows properly and I have to turn off the computer by turning of the power. On restart I get an error message saying "The program cant start because credui.dll is missing from ur computer. try reinstalling the program to fix this problem".

What should I do to overcome this problem?

Please help.

Thanks

Reply | Reply with quote | Report abuse

Madeni K N replied on October 3, 2012

Forum Moderator

0 Found this helpful Me Too

In reply to vinodmalhotra1 post on September 30, 2012

Hi **vinodmalhotra1**,

I would suggest you to create a new thread for your issue in the Microsoft Community instead of replying to this old thread. That will help your issue get a better visibility and will draw more helpful replies from the community. The community will need some information from your computer in order to guide you on the issue and you can read the following article in order to know what information needs to be posted in your query :

Suggestions for asking a question on help forums
http://support.microsoft.com/kb/555375

Reply | Reply with quote | Report abuse

John_683 replied on October 13, 2012

0 Found this helpful
Me Too

In reply to Madeni K N post on October 3, 2012

Hi,

Trojan:Win32/Reveton.A is very aggressive and can lock the computer, I think the following removal guide will help you a lot.

http://removevirushelp.com/how-to-completely-remove-reveton-trojan-virus.html

Reply | Reply with quote | Report abuse

jacob55_923 replied on December 14, 2012

0 Found this helpful
Me Too

Hey guys, I have been hit with the new version of Trojan.Reveton i.e. **Trojan.Reveton.O**. It has simply made my PC unresponsive and obstructed to initiate several applications like Photoshop MS Word and several others. I was really in a mess. I searched a lot about this Trojan but got the right information and its proper removal information here at -

http://www.combatpcviruses.com/how-to-remove-trojan-reveton-o-from-pc-easily

If your PC also encountered with the same Trojan then you can consult the same link. I am sure you will be helped.

All the best!

Reply | Reply with quote | Report abuse

Microsoft

Sign in

Community

Find answers | Ask a question

We'll search this forum for an answer

Virus and Malware

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

Question

1 Had this question Me Too

popsiyz asked on April 17, 2012

my computer has been locked out by a ransomware scam how do I unlock it

my computer has been locked out by a ransomware scam how do I unlock it and why didtn microsoft security essentials protect my computer. The scam is the one where they ask for money and accuse you of viewing illegal stuff and comes in the form of a police criminal intelligence unit scotland yard warning.

Reply | Reply with quote | Report abuse | Email updates

Answer

2 Found this helpful Me Too

Stephen Boots replied on April 17, 2012

MVP Community Moderator Community Star

Unfortunately, these type of malware attacks are difficult to keep up with because they trick you into letting them install. They usually come from an infected web site, and usually through an advertisement. You get a pop-up from the infection and you click it to close the pop-up - which allows the infection to install. They can also be delivered in a "drive-by" fashion with no action needed by the user due to the system being unpatched, no matter what security software is running.

When you encounter one of these fake virus pop-ups while browsing, immediately do the following:

-Do not touch any browser window to close it or browse further.
-Immediately press Ctrl-Alt-Del and bring up Task Manager and forcibly end all instances of iexplore.exe, if using Internet Explorer, or the executable for your browser for any other web browser.
--or--
-Go to Start/Shut Down and restart the PC without touching any browser windows.
-If you used task manager to close browser instances, reboot the machine.
-Then go to Control Panel/Internet Options and delete all temporary Internet Files and cookies. If you are using an alternate web browser, open the browser settings to do the same - delete the local cached files and cookies.
-Perform a full scan with MSE.

The above steps should prevent the infection from taking hold.
Start here - https://support.microsoftsecurityessentials.com/
and select the link that says - I think my computer is infected. Options will vary by region, but phone support leads you to Microsoft Answer Desk (http://www.answerdesk.com/) **in the US at this time.** After an initial free consultation, a fee will be charged for assistance, based on the details of the case.

This web site - http://www.bleepingcomputer.com - contains details for many of these common infections, often immediately after they began to appear in the wild, and instructions are provided for how to remove the infections using their malware removal guides. They also have forums where you can seek help from people who specialize in malware removal.

Besides MSE, the following recommendations will assist in protecting the PC from infection:
-Make sure that the Windows Firewall is enabled.
-Make sure that all important/critical updates, including service packs for the operating system and programs are installed from Microsoft Update (Windows Update).
-Make sure Internet Explorer is at version 8 or 9 and updated with all patches.
-In Internet Explorer 8 or 9, use the SmartScreen Filter.
-Make sure that IE Internet Security settings are at least set to medium-high (default).
-Enable the pop-up blocker in IE.
-On Vista and Windows 7 make sure that User Account Control (UAC) ON and not running with elevated privileges.
-Make sure that Windows Automatic Updates are set to at least notify, but the preferred setting is to download and install automatically. If you update manually, be sure to update as soon as possible after being notified of available updates.

Related Threads

My computer has been locked by someone demanding ukash vouchers to...

More Microsoft Resources

Help and Support

Common questions about malicious software

Security Essentials solution center

Virus and Security Solution Center

Get Micrososft Security Essentials

English

-**Make sure that installed applications, especially Adobe Acrobat, Adobe Flash, and Java are at their latest versions. Many vendors are regularly updating and patching for security holes.**
-Never click through links from unknown sources and use caution even if they are from a "trusted" source.
-Never open unsolicited email attachments.
-Practice safe web browsing.

-steve

Microsoft MVP

Reply | Reply with quote | Report abuse

Answer

1 Found this helpful Me Too

rhabdomantist replied on April 17, 2012

The following references may be of use.
Trojan:Win32/Reveton.A (see Recovery section)
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan:Win32/Reveton.A#recovery_link
Police Themed Ransomware Continues
http://www.f-secure.com/weblog/archives/00002344.html
HitmanPro against police themed Ransomware
http://hitmanpro.wordpress.com/2012/04/12/hitmanpro-against-police-themed-ransomware/
When you say "locked out', is it because of file encryption?
-rhab

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

Reply | Reply with quote | Report abuse

All Replies (5)

0 Found this helpful Me Too

Cyber_Defend_Team replied on April 17, 2012
Community Star

If you have access to your system update MSE and run full system scan and if that didn't resolve your issue, then contact support:
https://support.microsoftsecurityessentials.com/
And chose:
I think my computer is infected

Reply | Reply with quote | Report abuse

Answer

2 Found this helpful Me Too

Stephen Boots replied on April 17, 2012
MVP Community Moderator Community Star

Unfortunately, these type of malware attacks are difficult to keep up with because they trick you into letting them install. They usually come from an infected web site, and usually through an advertisement. You get a pop-up from the infection and you click it to close the pop-up - which allows the infection to install. They can also be delivered in a "drive-by" fashion with no action needed by the user due to the system being unpatched, no matter what security software is running.

When you encounter one of these fake virus pop-ups while browsing, immediately do the following:

-Do not touch any browser window to close it or browse further.
-Immediately press Ctrl-Alt-Del and bring up Task Manager and forcibly end all instances of iexplore.exe, if using Internet Explorer, or the executable for your browser for any other web browser.
--or--
-Go to Start/Shut Down and restart the PC without touching any browser windows.
-If you used task manager to close browser instances, reboot the machine.
-Then go to Control Panel/Internet Options and delete all temporary Internet Files and cookies. If you are using an alternate web browser, open the browser settings to do the same - delete the local cached files and cookies.
-Perform a full scan with MSE.

The above steps should prevent the infection from taking hold.
Start here - https://support.microsoftsecurityessentials.com/
and select the link that says - I think my computer is infected. Options will vary by region, but phone support leads you to Microsoft Answer Desk (http://www.answerdesk.com/) **in the US at this time.** After an initial free consultation, a fee will be charged for assistance, based on the details of the case.

This web site - http://www.bleepingcomputer.com - contains details for many of these common infections, often immediately after they began to appear in the wild, and instructions are provided for how to remove the infections using their malware removal guides. They also have forums where you can seek help from people who specialize in malware removal.

Besides MSE, the following recommendations will assist in protecting the PC from infection:
-Make sure that the Windows Firewall is enabled.
-Make sure that all important/critical updates, including service packs for the operating system and programs are installed from Microsoft Update (Windows Update).
-Make sure Internet Explorer is at version 8 or 9 and updated with all patches.
-In Internet Explorer 8 or 9, use the SmartScreen Filter.
-Make sure that IE Internet Security settings are at least set to medium-high (default).
-Enable the pop-up blocker in IE.
-On Vista and Windows 7 make sure that User Account Control (UAC) ON and not running with elevated privileges.
-Make sure that Windows Automatic Updates are set to at least notify, but the preferred setting is to download and install automatically. If you update manually, be sure to update as soon as possible after being notified of available updates.
-**Make sure that installed applications, especially Adobe Acrobat, Adobe Flash, and Java are at their latest versions. Many vendors are regularly updating and patching for security holes.**
-Never click through links from unknown sources and use caution even if they are from a "trusted" source.
-Never open unsolicited email attachments.
-Practice safe web browsing.

-steve

Microsoft MVP

Reply | Reply with quote | Report abuse

Answer

1 Found this helpful
Me Too

rhabdomantist replied on April 17, 2012

The following references may be of use.
Trojan:Win32/Reveton.A (see Recovery section)
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan:Win32/Reveton.A#recovery_link
Police Themed Ransomware Continues
http://www.f-secure.com/weblog/archives/00002344.html
HitmanPro against police themed Ransomware
http://hitmanpro.wordpress.com/2012/04/12/hitmanpro-against-police-themed-ransomware/
When you say "locked out', is it because of file encryption?
-rhab

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

Reply | Reply with quote | Report abuse

0 Found this helpful
Me Too

popsiyz replied on April 27, 2012

In reply to Stephen Boots post on April 17, 2012

sorry that it has taken some time to respond to the answers to my question/problem on my pc.
this was because I had to use another pc to read the answers as my pc was locked out.
when I eventually turned on the infected pc (after about 1 week) I found that the pc was unlocked and the ransomscam virus did not appear has soon as the pc was switched on. straight away I followed the advice given and carried out a scan, I dont known whether this virus only hangs around for a week or so and then goes or whether my continued attempts at the time of intial infection by switching off and rebooting the pc enabled the pc to quaranteen part of the virus that locked me out just so that I could get in and carry out a scan to finally remove it.
I have sent a report to MSE.
Many thanks to all of you who took the time to help me . Very much appreciated.

Reply | Reply with quote | Report abuse

rhabdomantist replied on April 27, 2012

1 Found this helpful
Me Too

In reply to popsiyz post on April 27, 2012

popsiyz,
Glad to learn you didn't become infected. Your actions of not clicking on any part of the fake pop-up window in the browser and turning off the computer prevented the malware from taking over.
As Steve suggested ensure that your browser cache (Temporary Internet Files and Cookies) has been cleared.
How to Clear Your Browser's Cache
http://www.wikihow.com/Clear-Your-Browser's-Cache
Also very important ***Make sure that installed applications, especially Adobe Acrobat, Adobe Flash, and Java are at their latest versions. Many vendors are regularly updating and patching for security holes.***
There is a third-party browser plugin to assist is keeping these applications up to date.
Qualy's BrowserCheck FAQ's
https://community.qualys.com/docs/DOC-1542
Qualy's BrowserCheck Demo
https://community.qualys.com/docs/DOC-1311
Qualy's BrowserCheck
https://browsercheck.qualys.com/
Alternatively if you prefer an installed program,
Secunia PSI
http://secunia.com/vulnerability_scanning/personal/
Your reply is appreciated.
-rhab

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

Reply | Reply with quote | Report abuse

Microsoft

Sign in

Community

Find answers | Ask a question

We'll search this forum for an answer

Virus and Malware

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

Question

1 Had this question Me Too

MikeJFoley asked on August 12, 2012

Security failure

How did Microsoft Security Essestials let the Reveton trojan onto my computer? It took me over 4 hours to clean it.

Reply | Reply with quote | Report abuse | Email updates

Answer

1 Found this helpful Me Too

Le Boule replied on August 12, 2012

Community Star

> How did Microsoft Security Essestials let the Reveton trojan onto my computer? It took me over 4 hours to clean it.

I'm not employed by Microsoft and have no interest in defending MSE other than to try and answer your question.
No antimalware program can provide 100% protection. All AV vendors (whether free or paid versions) fight a constant battle to stay ahead of the authors of malware and keep their databases updated and current...in fact we sometimes receive complaints on these forums regarding failure of other AV programs to adequately protect computers...see these threads: http://answers.microsoft.com/en-us/protect/forum/protect_scanning/how-do-i-get-rid-of-the-smart-internet-protection/2d19448c-7cc7-451d-88c6-c9db9b2f7a3e#e5a340d7-0ee2-4335-a357-291d1989f26e, http://answers.microsoft.com/en-us/protect/forum/protect_scanning/pack-win107-2121/7e7385e1-c5db-4d1a-9aa5-b0279af0849c and http://answers.microsoft.com/en-us/protect/forum/protect_scanning/smart-hdd-virus/f0f6f6b9-1568-4188-80f3-4c338702b645. MSE is not perfect but it seems to be doing as good a job against malware as any of the AV programs.

Here's a comprehensive list of suggestions on handling such "attacks" by Stephen Boots, MSE Forum Moderator:

Unfortunately, these type of malware attacks are difficult to keep up with because they trick you into letting them install. They usually come from an infected web site, and usually through an advertisement. You get a pop-up from the infection and you click it to close the pop-up - which allows the infection to install. They can also be delivered in a "drive-by" fashion with no action needed by the user due to the system being unpatched, no matter what security software is running.

When you encounter one of these fake virus pop-ups while browsing, immediately do the following:

-**Do not touch any browser window to close it or browse further**.
-Immediately press Ctrl-Shift-Esc and bring up Task Manager and forcibly end all instances of iexplore.exe, if using Internet Explorer, or the executable for the browser you are using.
--or--
-Go to Start/Shut Down and restart the PC without touching any browser windows.
-If you used task manager to close browser instances, reboot the machine.
-Then go to Control Panel/Internet Options and delete all temporary Internet Files and cookies. If you are using an alternate web browser, open the browser settings to do the same - delete the local cached files and cookies.
-Perform a full scan with your antimalware program.

The above steps should prevent the infection from taking hold.

Besides using an antimalware program, the following recommendations will assist in protecting the PC from infection:

Related Threads

Installation failure of Definition update for MS Security...

Security Essentials virus and spyware definition update failure.

Security Essentials certification failure's

security essentails failure

Windows security essentials update failure

More Microsoft Resources

Help and Support

Common questions about malicious software

Security Essentials solution center

Virus and Security Solution Center

Get Micrososft Security Essentials

English

-Make sure that the Windows Firewall is enabled.
-Make sure that all important/critical updates, including service packs for the operating system and programs are installed from Microsoft Update (Windows Update).
-Make sure Internet Explorer is at version 8 or higher and updated with all patches.
-In Internet Explorer 8 or 9, use the SmartScreen Filter.
-Make sure that IE Internet Security settings are at least set to medium-high (default).
-Enable the pop-up blocker in IE.
-On Vista and Windows 7 make sure thatUser Account Control (UAC) ON and not running with elevated privileges.
-Make sure that Windows Automatic Updates are set to at least notify, but the preferred setting is to download and install automatically. If you update manually, be sure to update as soon as possible after being notified of available updates.
-Make sure that installed applications, especially Adobe Acrobat, Adobe Flash, and Java are at their latest versions. Many vendors are regularly updating and patching for security holes.
-Never click through links from unknown sources and use caution even if they are from a "trusted" source.
-Never open unsolicited email attachments.

http://voices.washingtonpost.com/securityfix/2009/09/what_to_do_when_rogue_anti-vir.html#more

http://ask-leo.com/why_dont_antimalware_tools_work_better.html

Reply | Reply with quote | Report abuse

All Replies (3)

TenMilesHigh replied on August 13, 2012

0 Found this helpful Me Too

In reply to Le Boule post on August 12, 2012

Like the above, I have an XP machine with sp3 and a fully updated MSE's. In came Reveton and Citadel. Not comfortable or knowledgable about removing them, I took my machine to a local pc fix-it shop, and for $65 they removed it. They also removed MSEs and put in a 30 day copy of 'Bitdefender'. "Much better than MSEs. Besides MSEs doesn't have a malware defender component, nor able to deal with this sort of ransomware. For only $68 a year (to us) it'll keep you clear of these things". Am I getting smoke wafted up my tighty-whitey's ? Or can I forgo their generous offer and reload MSEs? Or, in terms of safety, does it make a difference?
Any opinions out there will be greatly appreciated..
thanks, Al.

Reply | Reply with quote | Report abuse

Le Boule replied on August 13, 2012
Community Star

1 Found this helpful Me Too

In reply to TenMilesHigh post on August 13, 2012

Like the above, I have an XP machine with sp3 and a fully updated MSE's. In came Reveton and Citadel. Not comfortable or knowledgable about removing them, I took my machine to a local pc fix-it shop, and for $65 they removed it. They also removed MSEs and put in a 30 day copy of 'Bitdefender'. "Much better than MSEs. Besides MSEs doesn't have a malware defender component, nor able to deal with this sort of ransomware. For only $68 a year (to us) it'll keep you clear of these things". Am I getting smoke wafted up my tighty-whitey's ? Or can I forgo their generous offer and reload MSEs? Or, in terms of safety, does it make a difference?
Any opinions out there will be greatly appreciated..
thanks, Al.

http://www.techsupportalert.com/best-free-anti-virus-software.htm

http://www.av-comparatives.org/

http://www.dslreports.com/forum/r25776413-2011-Anti-Virus-Poll

http://ask-leo.com/i_run_antivirus_software_why_do_i_still_sometimes_get_infected.html

http://www.westcoastlabs.com/realTimeTesting/article/?articleID=1

And if you decide to replace Bitdefender with MSE recommend you **thoroughly** review the following guide:
Microsoft Security Essentials – Installation Checklist and Frequently Asked Questions

Regards...

Reply | Reply with quote | Report abuse