

Forum:[Hack Forums](#)

Thread: [Guide to Removal of Malware \(Detailed\)](#)

Agent Shark - November 24, 2010, 8:52 pm

Hello everyone today I will be discussing some stuff about removal of Malware along with tips to keep your computer in tip top shape.

So lets begin:

Tips:

Never have two or more anti viruses or firewalls on one computer as it can cause failure of functions of each program.

To fix this do the following:

Start > Control Panel > Add/Uninstall a program

Step One:

If you ever feel your infected, the best step to start checking is running a malware removal program known as [Malware Anti Malware](#).

What Is Malware Anti-Malware?

Spoiler ([Click to View](#)) Malwarebytes' Anti-Malware is an anti-malware application that can thoroughly remove even the most advanced malware. It includes a number of features, including a built in protection monitor that blocks malicious processes before they even start.

Steps to Usage:

- Proceed with Installation and Update.
 - Select "Full Scan" and select ALL Drivers
- After completion if infections are found remove all.
(Restart May Occur)

Step 2: As another scanner to use, I suggest [Super Anti Spyware](#)

What is Super Anti Spyware?

Spoiler ([Click to View](#)) Detect and Remove Spyware, Adware and Remove Malware, Trojans, Dialers, Worms, KeyLoggers, HiJackers, Parasites, Rootkits, Rogue Security Products and many other types of threats.

Light on System Resources and won't slow down your computer like many other anti-spyware products. Won't conflict with your existing anti-spyware or anti-virus solution!

* Repair broken Internet Connections, Desktops, Registry Editing and more with our unique Repair System!

Usage of this tool:

- After download do the following:
- Select the tab known as "Check For Updates"

- After updates are completed hit the tab "Scan Your Computer"
- Next Select "Complete Scan"

After completion to find your log look under preferences > statistics and logs > Select Latest Log > Copy/Paste To NotePad

ESET Online Scanner

To download this program click [here](#).

Usage of this program:

- Select Yes to ToS
- Allow ActiveX to install

For additional information select the following:

- Remove found threats and the option Scan unwanted applications

To Locate your log please look here: C:\Program Files\ESET\ESET Online Scanner\log.txt

Now this is my guide to using the WHH area.

For professional help with the usage and support with these tools you may go to the [HiJackThis Log Analysis](#)

Thank you for reading about the usage of the most common tools used for removal of viruses.

Note: I did not know how to use OTL very well so I did not post about it as I could have been considered a noob for not knowing it's complete usage.

Regards,
Disruption

Xenochrist - November 24, 2010, 8:53 pm

Nice tutorial just make it easier to read. Make the section titles bold, etc. ?

Agent Shark - November 24, 2010, 8:56 pm

(Nov 24, 2010 09:53 PM)Rizing Tide Wrote: [\[CITE\]](#) Nice tutorial just make it easier to read. Make the section titles bold, etc. ?

I made the titles bold along with the steps italicized.

Thanks for the comment.

Regards,
Disruption

iDuL - November 24, 2010, 10:17 pm

Amazing post man, keep it up. Seriously.

Agent Shark - November 24, 2010, 11:03 pm

(Nov 24, 2010 11:17 PM)iDuL Wrote: [\[CITE\]](#) Amazing post man, keep it up. Seriously.

Thank you for the feedback

Eminent - November 24, 2010, 11:45 pm

Nice post. Haha, I always feel like a broken record in the white hat section, because almost every thread here is fixed by one of these scans.

Agent Shark - November 24, 2010, 11:47 pm

(Nov 25, 2010 12:45 AM)acid_fall Wrote: [\[CITE\]](#) Nice post. Haha, I always feel like a broken record in the white hat section, because almost every thread here is fixed by one of these scans.

Well when new tools come out people tend to analyze it's abilities.

Shinkirou - November 24, 2010, 11:57 pm

(Nov 25, 2010 12:45 AM)acid_fall Wrote: [\[CITE\]](#) Nice post. Haha, I always feel like a broken record in the white hat section, because almost every thread here is fixed by one of these scans.

To be honest, you should feel like a broken record. Only posting those scans is pointless, most problems here don't need those scans. Yet everyone seems to think their helping when they all post the same advice 6 times in the same thread.

Agent Shark - November 25, 2010, 12:00 am

(Nov 25, 2010 12:57 AM)Shinkirou Wrote: [\[CITE\]](#) To be honest, you should feel like a broken record. Only posting those scans is pointless, most problems here don't need those scans. Yet everyone seems to think their helping when they all post the same advice 6 times in the same thread. So is this thread considered "worthless" in your perspective?

Shinkirou - November 25, 2010, 12:03 am

(Nov 25, 2010 01:00 AM)Disruption Wrote: [\[CITE\]](#) So is this thread considered "worthless" in your perspective?

You read to deep into my post. Did I ever say that? No I don't believe I did.

Whats worthless is all these people that go around saying nothing but "Scan with MBAM" and think that their actually helping. Hate to burst their bubble, but nine out of ten times; they aren't.

Agent Shark - November 25, 2010, 12:07 am

(Nov 25, 2010 01:03 AM)Shinkirou Wrote: [\[CITE\]](#) You read to deep into my post. Did I ever say that? No I don't believe I did.

Whats worthless is all these people that go around saying nothing but "Scan with MBAM" and think that their actually helping. Hate to burst their bubble, but nine out of ten times; they aren't. Oh my apologies on that I misunderstood what you said.

Well what do you think of the thread? I need comments and suggestions.

Shinkirou - November 25, 2010, 12:16 am

Well I can't say more detail, because the only more detail I can think of is scanners which are potentially dangerous to be used without "guidance".

You could include prevention tips (virtual machines, drive encryption if you wanna be fancy, don't do Sandboxie though it's outdated and more dangerous then what its worth since it's fairly easily bypassed nowadays).

If you want to go fancier, you could talk about exploit testing your own machine and learning how to patch/close up certain vulnerabilities instead of having to wait for a security update.

Just a few random ideas I had.

Agent Shark - November 25, 2010, 12:18 am

(Nov 25, 2010 01:16 AM)Shinkirou Wrote: [\[CITE\]](#) Well I can't say more detail, because the only more detail I can think of is scanners which are potentially dangerous to be used without "guidance".

You could include prevention tips (virtual machines, drive encryption if you wanna be fancy, don't do Sandboxie though it's outdated and more dangerous then what its worth since it's fairly easily bypassed nowadays).

If you want to go fancier, you could talk about exploit testing your own machine and learning how to patch/close up certain vulnerabilities instead of having to wait for a security update.

Just a few random ideas I had.

I think that will be a new topic I will further look into it and see what I can come up with.

I have been using the Virtual Machines a ton as it is perfect to identify files and study files.

The part I lost you at is Drive encryption could you describe to me what that is by any chance?

Shinkirou - November 25, 2010, 12:27 am

(Nov 25, 2010 01:18 AM)Disruption Wrote: [\[CITE\]](#) I think that will be a new topic I will further look into it and see what I can come up with.

I have been using the Virtual Machines a ton as it is perfect to identify files and study files.

The part I lost you at is Drive encryption could you describe to me what that is by any chance?

http://en.wikipedia.org/wiki/Full_disk_encryption

That link can explain more in depth then I can. The basics though are pretty much encrypting all the contents of a drive and requiring a password to read and write files to (and in the read case; that are already on) the drive. It renders most viruses useless as they cannot write their files to the drive because they get denied access.

Agent Shark - November 25, 2010, 12:30 am

(Nov 25, 2010 01:27 AM)Shinkirou Wrote: [\[CITE\]](#) http://en.wikipedia.org/wiki/Full_disk_encryption

That link can explain more in depth then I can. The basics though are pretty much encrypting all the contents of a drive and requiring a password to read and write files to (and in the read case; that are already on) the drive. It renders most viruses useless as they cannot write their files to the drive because they get denied access. Oh I see so when doing this a virus cannot bypass the encryption?

Also is this a program or could anyone do this by simply a click of a button?

Shinkirou - November 25, 2010, 12:33 am

(Nov 25, 2010 01:30 AM)Disruption Wrote: [\[CITE\]](#) Oh I see so when doing this a virus cannot bypass the encryption?

Also is this a program or could anyone do this by simply a click of a button?

Basically, unless viruses have means of bypassing drive encryption (which to my knowledge they don't).

Yeah it is something anyone can do, one of the more popular programs to do it with is called "[TrueCrypt](#)" which allows you to encrypt drives or only create certain "directories" (a "non-physical" hard drive I guess you could say) that are encrypted (and all the contents of course) that you have to know the password to mount.

Agent Shark - November 25, 2010, 12:37 am

(Nov 25, 2010 01:33 AM)Shinkirou Wrote: [\[CITE\]](#) Basically, unless viruses have means of bypassing drive encryption (which to my knowledge they don't).

Yeah it is something anyone can do, one of the more popular programs to do it with is called "[TrueCrypt](#)" which allows you to encrypt drives or only create certain "directories" (a "non-physical" hard drive I guess you could say) that are encrypted (and all the contents of course) that you have to know the password to mount. Ah I understand it now. I seem to learn a bit more everyday. So

would you assume drive encryption is better than a virtual machine.

I know there are huge differences in both but they seem to do the same: "Protect" the user.

Shinkirou - November 25, 2010, 12:45 am

(Nov 25, 2010 01:37 AM)Disruption Wrote: [\[CITE\]](#) Ah I understand it now. I seem to learn a bit more everyday. So would you assume drive encryption is better than a virtual machine.

I know there are huge differences in both but they seem to do the same: "Protect" the user. Actually the two working "hand in hand" so to speak would be really helpful. Say you were testing something in a VM, with an encrypted drive there would be no chance of you getting infected by anything that "leaked" out of the VM. Though highly unlikely, theres still a chance.

Agent Shark - November 25, 2010, 12:47 am

(Nov 25, 2010 01:45 AM)Shinkirou Wrote: [\[CITE\]](#) Actually the two working "hand in hand" so to speak would be really helpful. Say you were testing something in a VM, with an encrypted drive there would be no chance of you getting infected by anything that "leaked" out of the VM. Though highly unlikely, theres still a chance. So has anyone researched the likely hood of obtaining a virus from a Virtual Machine and what type of viruses can come out of it?

flAmingw0rm - November 25, 2010, 12:51 am

These are steps used by HJT Team as well, but this wouldn't completely remove the trojan, because there are many trojans which bypass anti viruses and they are fully undetectable.

Shinkirou - November 25, 2010, 12:51 am

(Nov 25, 2010 01:47 AM)Disruption Wrote: [\[CITE\]](#) So has anyone researched the likely hood of obtaining a virus from a Virtual Machine and what type of viruses can come out of it?

Not to my knowledge, I haven't done much research on that myself.

I would think it's really unlikely that a virus could leak from a VM, if it's even possible.

I did find [this thread](#) on Kaspersky's forum, which says that it is possible due to bugs in the coding of the program (ex: VMWare) but I would assume a major flaw like that would be patched really quickly.

(Going to sleep now, if you have any questions or anything you can PM them to me, and I'll answer/reply when I wake up.)

Agent Shark - November 25, 2010, 7:01 am

I see that most people tend to "freak out" when a virus gets on there Virtual Machine.

If you wanted to mess with the file you could I assume disassemble it and analyze the files inside of it. Also you could just simply remove the hard disk from the computer and then your set.

Am I correct?

Shinkirou - November 25, 2010, 11:26 am

(Nov 25, 2010 08:01 AM)Disruption Wrote: [\[CITE\]](#) I see that most people tend to "freak out" when a virus gets on there Virtual Machine.

If you wanted to mess with the file you could I assume disassemble it and analyze the files inside of it. Also you could just simply remove the hard disk from the computer and then your set.

Am I correct?

Assuming your talking about the VM HD, then yeah, you can just delete the VM and you should be fine.

Herakleitos - November 25, 2010, 12:32 pm

I need help for remove cybergate rat :(infected today hacked all from me computer :(

Agent Shark - November 25, 2010, 12:34 pm

(Nov 25, 2010 01:32 PM)Herakleitos Wrote: [\[CITE\]](#) I need help for remove cybergate rat :(infected today hacked all from me computer :(

Can you please rephrase what you said?

Also look at the beginning of my thread and also look in the HJT Area.

Regards,
Disruption

Agent Shark - November 25, 2010, 7:26 pm

I see alot of views but not a lot of comments :(

\$ zS \$ - November 26, 2010, 6:38 pm

What would really be amazing if that you made this into an AIO program!

Shinkirou - November 26, 2010, 7:36 pm

Malware Bytes Anti Malware, SAS and ESET Online Scanner are all copyrighted, which means that putting them all into a program would most likely cause numerous copyright violations and potentially a lawsuit or a fine.

Crxnkz - November 27, 2010, 1:39 am

Nice guide, keep up the good work and the high quality posts

Langleyyy - November 27, 2010, 1:41 am

Great post OP. I used this in the past to get some kids bot off my shit. Thanks!

Agent Shark - November 27, 2010, 12:55 pm

(Nov 27, 2010 02:41 AM)Langleyyy Wrote: [\[CITE\]](#) Great post OP. I used this in the past to get some kids bot off my shit. Thanks!

Anytime and thanks to all for the positive feedback ?

Charmz - November 27, 2010, 1:53 pm

Nice tutorial. I think you should add more. Also format the post so it looks better. :)

Agent Shark - November 27, 2010, 1:56 pm

(Nov 27, 2010 02:53 PM)Charmz Wrote: [\[CITE\]](#) Nice tutorial. I think you should add more. Also format the post so it looks better. :)Well with some of the tools, we white hats are not qualified to use so I cannot really use them in this thread.

If you have some tools that are allowed to be used by us pm me and I can make a procedure with it.

Regards,
Disruption