

Forum:[Hack Forums](#)

Thread: [Things allowed to be requested and not requested](#)

Agent Shark - December 18, 2010, 5:19 pm

Hello Reader,

I didn't find anything about this so I am making a little guide to what you can request and what you cannot request.

Table of ContentsIntroduction (What this thread is about)

Tools allowed to be requested

Tools NOT allowed to be requested

Introduction

I made this thread to describe the tools allowed to be used in the White Hat Section and the tools not allowed. If you are an undergraduate or up on the HJT Team, you can request any type of log/tool to be used. As for undergraduates, everything requested is analyzed by an expert. So for those of you who are NOT HJT members like myself, then I suggest reading this so you do not mess up or feel like a fool in the process of assisting a user.

Tools Allowed To Be Requested

In this next couple of sentences, I will describe and list some tools that are allowed for regular members to use and request others to download. So lets being.

Malwarebytes Anti-Malware

SUPERAntiSpyware

ESET Online Scanner

RKill

Note: If there are more tools please tell me via pm with a description of the tool.

[Malwarebytes Anti-Malware](#)

Spoiler ([Click to View](#))- Malwarebytes Anti Malware is dedicated to removal of viruses such as Trojans, Worms, Keyloggers, RATS and so forth. The usage of Malware Anti Malware is pretty simple and quite user friendly.

Some other useful information about Malwarebytes Anti Malware:

- Safe Mode Friendly: This means if you want to boot into safe mode you can with this tool and it makes the scan more sufficient upon the removal process.

- User Friendly: Big Friendly buttons make users interface useful.

Features Of Malwarebytes Anti Malware:

- Updated just about everyday
- Uses installation for updates.

[SUPERAntiSpyware](#)

SUPERAntiSpyware is a program that specializes in the removal of spyware. It's database is constantly updated and contains tons of viruses/adware. When using this tool note that it looks mostly for Spyware and not as much for other viruses.

Features:

Spoiler ([Click to View](#))Quote:* 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!

Real-Time Blocking of threats! Prevent potentially harmful software from installing or re-installing

First Chance Prevention examines over 50 critical points of your system each time your system starts up and shuts down to eliminate threats before they have a chance to infect and infiltrate your system.

* Schedule either Quick, Complete or Custom Scans Daily or Weekly to ensure your computer is free from harmful software. Remove spyware automatically.

Taken From Here: <http://superantispyware.com/>

[ESET Online Scanner](#)

What is ESET?

ESET is an online scanner that allows you to scan your computer without doing an install and provides very high results. In that matter, it also locates suspicious files and so forth.

[RKill.](#)

Rkill is a program used to kill malicious process. It doesn't delete programs or restore anything, it just terminates processes, and it is quite effective against rogues if they are being associated with running processes.

Tools Not Allowed to be Requested From Members

In this next group, these tools are NOT allowed to be requested. (No Download Links Will Be Provided)

ComboFix

- A tool used for very difficult malware removal and without expert assistance can damage your computer permanently. This tool is not recommended unless the HJT Team requests it for you. Otherwise if you see someone post it report it and ignore it.

System Restore/Format: Although this is not a tool, I see this NUMEROUS times and it's only a LAST resort to any log or infection. When reformatting you are losing ALL files and everything valuable to you. When performing a System Restore, this brings your computer back to an earlier stage but this could bring the virus along to.

GMER RootKit Scan

- This is a scanner to detect Rootkits in the users computer. When using this, there are specific things needed to be checked for the right procedure. Using this on your own or requesting members to use it is very bad and can lead to severe computer problems and wasting of time.

OTL/HJT Logs

- These tools are used to identify running processes, services, toolbars , and so forth located in the users computer. Specialized people understand this and that is why Regular users cannot tell others to download this for the safety of the infected and the community. If people used this commonly, then accidents could occur and required services would be disabled/deleted.

Note: If there are more please tell me and give me a description.

Credits:

Peter Chao - Read over and gave me some pointers to place inside the thread

Epidemic - For giving info on RKill

Now that's all to my list if you have more feel free to pm them to me and I will give you credit for it towards the end of my topic.

Thank you for reading and I do hope this clears issues upon tools.

Regards,

Disruption

Please rate and comment to keep this thread alive!!!

Moralitas - December 18, 2010, 5:43 pm

This is a great thread, mostly new helpers ask to download things they shouldn't be asking. I've seen Paradoxum tell members several times to not instruct someone on using Combofix, but when do people listen right?

I would also like to point out that if a HJT member that isn't an undergraduate yet asks for these logs, the post should be reported. There's a very strict policy for this, if a HJT member is found doing logs before they are eligible too, they will be expelled from the program.

Agent Shark - December 18, 2010, 5:44 pm

(Dec 18, 2010 06:43 PM)Peter Chao Wrote: [\[CITE\]](#) This is a great thread, mostly new helpers ask to download things they shouldn't be asking. I've seen Paradoxum tell members several times to not instruct someone on using Combofix, but when do people listen right?

I would also like to point out that if a HJT member that isn't an undergraduate yet asks for these log, the post should be reported as well. There's a very strict policy for this, if a HJT member is found doing logs before they are eligible too, they will be expelled from the program.

Thank you for your feedback and I am glad I put your input into my thread.

Xerotic - December 18, 2010, 5:45 pm

Thank you very much. Now I know if someone suggests other than recommended in the thread, to not use it, and get another opinion.

Xch4ng3 - December 18, 2010, 5:46 pm

Well done. Maybe people will learn not to recommend something like ComboxFix. Last thing we need is a bunch of unusable machines.

Agent Shark - December 18, 2010, 5:52 pm

Thank you all for your positive feedback and everyone please continue to post and rate if you could.

-Disruption

Minnesota Nice - December 18, 2010, 5:58 pm

This is great, I really like the thread.

I laughed at combo fix. :D

I sort of want to join the HJT team but I don't have time for it.

Agent Shark - December 18, 2010, 6:01 pm

(Dec 18, 2010 06:58 PM)Minnesota Nice Wrote: [\[CITE\]](#) This is great, I really like the thread.

I laughed at combo fix. :D

I sort of want to join the HJT team but I don't have time for it.

Thank you for your feedback upon my thread.

I do hope some day I get in :)

Minnesota Nice - December 18, 2010, 6:02 pm

(Dec 18, 2010 07:01 PM)Disruption Wrote: [\[CITE\]](#) Thank you for your feedback upon my thread.

I do hope some day I get in :)

It's quite a challenge! I bet you could get in!

Agent Shark - December 18, 2010, 6:03 pm

(Dec 18, 2010 07:02 PM)Minnesota Nice Wrote: [\[CITE\]](#) It's quite a challenge! I bet you could get in!! have been trying :)

I applied 4mths Ago so I hope my app gets looked at soon :)

Mermaid - December 18, 2010, 6:19 pm

Good thread, I personally like Malwarebytes the best and use that the most yet combofix comes in handy as a last resort malware removal program ?

Agent Shark - December 18, 2010, 6:20 pm

(Dec 18, 2010 07:19 PM)Tyler8746 Wrote: [\[CITE\]](#) Good thread, I personally like Malwarebytes the best and use that the most yet combofix comes in handy as a last resort malware removal program ? Thank you for your feedback :)

Epidemic - December 18, 2010, 8:57 pm

I once ran Combofix on my old computer the next day it wouldn't turn on. Bad thing is I didn't have a virus. I was just testing it out. Wtf >.<

Good thing not to request using combofix if you don't know what your doing.

Its sucks though because after it didn't turn on, I continued to stomp it and slam it agasnt my bathtub hoping it would turn on but all it did was catch on fire.

But this is a great thread. I usually request a lot more than ESET, Malwarebytes and SuperAntispyware, its just those are the main ones I use. :p

DestinyOnly - December 18, 2010, 10:15 pm

(Dec 18, 2010 09:57 PM)Epidemic Wrote: [\[CITE\]](#) I once ran Combofix on my old computer the next day it wouldn't turn on. Bad thing is I didn't have a virus. I was just testing it out. Wtf >.<

Good thing not to request using combifix if you don't know what your doing.

Its sucks though because after it didn't turn on, I continued to stomp it and slam it agasnt my bathtub hoping it would turn on but all it did was catch on fire.

But this is a great thread. I usually request a lot more than ESET, Malwarebytes and SuperAntispyware, its just those are the main ones I use. :p

That's strange. Every time I've tried the stomping and slamming approach it's fixed my computer.

MouseDesign - December 19, 2010, 12:43 am

Good job, this should be a sticky imo.

The Janitor - December 19, 2010, 3:38 am

Hey there,

I think Rkill should be in there too.

Rkill kills the common processes that Rogue AV's And other stuff use.

So you can scan your computer after using Rkill.

Agent Shark - December 19, 2010, 5:15 am

Thanks everyone for there feedback.

Maybe Valiant will consider this a sticky one day :)

MouseDesign - December 19, 2010, 6:55 am

I'll refer this towards Valiant. We never thought of making a thread like this, I assume hence it didn't get created yet.

Agent Shark - December 19, 2010, 7:02 am

(Dec 19, 2010 07:55 AM)Volenar Wrote: [\[CITE\]](#) I'll refer this towards Valiant. We never thought of making a thread like this, I assume hence it didn't get created yet.

Thanks Volenar!

If you did do this I would be very happy as it would make me seem like I am contributing to the White Hat Area.

-Disruption

Eminent Fate - December 19, 2010, 12:15 pm

I think Comodo deserves a chance proving itself worthy in by beating both Avira and Avast in a mid-size test.

http://www.youtube.com/watch?v=YRreh8G4bLw&feature=mfu_in_order&list=ULwww.youtube.com/my_subscriptions?feature=mhum

http://www.youtube.com/watch?v=vbtdeIFcTfc&feature=mfu_in_order&list=UL

Agent Shark - December 19, 2010, 12:20 pm

(Dec 19, 2010 01:15 PM)Cocopara Wrote: [\[CITE\]](#) I think Comodo deserves a chance proving itself worthy in by beating both Avira and Avast in a mid-size test.

http://www.youtube.com/watch?v=YRreh8G4bLw&feature=mfu_in_order&list=ULwww.youtube.com/my_subscriptions?feature=mhum

http://www.youtube.com/watch?v=vbtdeIFcTfc&feature=mfu_in_order&list=UL

That has nothing to do with this thread ?

Eminent Fate - December 19, 2010, 12:25 pm

It does, it states that Eset online scanner is the anti virus to be suggested. OR atleast thats how I interperate it.

Agent Shark - December 19, 2010, 12:30 pm

(Dec 19, 2010 01:25 PM)Cocopara Wrote: [\[CITE\]](#) It does, it states that Eset online scanner is the anti virus to be suggested. OR atleast thats how I interperate it.

ESET is an online/on demand scanner.

Avira and Comodo are Anti Viruses.

See the difference ?

-Disruption

Epidemic - December 19, 2010, 12:37 pm

(Dec 19, 2010 01:25 PM)Cocopara Wrote: [\[CITE\]](#) It does, it states that Eset online scanner is the anti virus to be suggested. OR atleast thats how I interperate it.

ESET is not a Anti-virus it is an Online scanner used to scan your computer.

Agent Shark - December 19, 2010, 1:14 pm

Thank you everyone for feedback I appreciate if we keep this thread alive and so forth.

Thanks,
Disruption

Infallible - December 19, 2010, 4:53 pm

A nice thread. Thank you for this.

Agent Shark - December 19, 2010, 4:58 pm

Thank you for all the feedback it's well appreciated :)

Agent Shark - December 20, 2010, 7:51 am

A well needed .

I noticed more people requesting GMER and one person for Combofix.

The Janitor - December 20, 2010, 8:14 am

(Dec 19, 2010 04:38 AM)gtaclick Wrote: [\[CITE\]](#) Hey there,

I think Rkill should be in there too.

Rkill kills the common processes that Rogue AV's And other stuff use.

So you can scan your computer after using Rkill.

At least read it mate.

Link : <http://www.technibble.com/rkill-repair-tool-of-the-week/>

Download link is somewhere in there too.

Agent Shark - December 20, 2010, 8:16 am

(Dec 20, 2010 09:14 AM)gtaclick Wrote: [\[CITE\]](#) At least read it mate.

Link : <http://www.technibble.com/rkill-repair-tool-of-the-week/>

Download link is somewhere in there too.It's a tool only HJT members can request.

airjosh97 - December 20, 2010, 8:27 am

Personally i think [dr.web](#) should be added into the list, i've had a lot more success with it than malware bytes.

Agent Shark - December 20, 2010, 8:30 am

Hi Josh please pm me that tool with a descriptive information upon it.

Thanks,
Disruption

The Janitor - December 20, 2010, 8:35 am

(Dec 20, 2010 09:14 AM)gtaclick Wrote: [\[CITE\]](#) At least read it mate.

Link : <http://www.technibble.com/rkill-repair-tool-of-the-week/>

Download link is somewhere in there too.

I don't get it , why would this simple program only be able to be used by HJT Trainees?

Agent Shark - December 20, 2010, 8:36 am

(Dec 20, 2010 09:35 AM)gtaclick Wrote: [\[CITE\]](#) I don't get it , why would this simple program only be able to be used by HJT Trainees?Hi gtaclick,

Please pm me that tool with a description and usage of it.

I will ask an HJT member if were allowed to use it.

-Disruption

MouseDesign - December 20, 2010, 9:40 am

(Dec 20, 2010 09:36 AM)Disruption Wrote: [\[CITE\]](#) Hi gtaclick,

Please pm me that tool with a description and usage of it.

I will ask an HJT member if were allowed to use it.

-Disruption
What tool are we talking about?

Eminent Fate - December 20, 2010, 9:42 am

(Dec 19, 2010 01:37 PM)Epidemic Wrote: [\[CITE\]](#) ESET is not a Anti-virus it is an Online scanner used to scan your computer.
The same thing.

An anti virus is a program used to detect viruses, that is an online anti virus scanner, not much of a difference.

Agent Shark - December 20, 2010, 9:57 am

They are discussing RKILL

Epidemic - December 20, 2010, 10:56 am

(Dec 20, 2010 10:42 AM)Cocopara Wrote: [\[CITE\]](#) The same thing.

An anti virus is a program used to detect viruses, that is an online anti virus scanner, not much of a difference.

No they are not the same thing.

In simple terms

Anti-Virus program is a module that protects your whole system and monitors everything being, downloaded, ran, viewed and stored. It offers, protections, scanning, fire wall, virus chest, virus definitions etc.

The Scanner is what exactly it sounds like. It scans. That is oly what it does. You download it, it scans, it gives you the log, you analyze. Easy as that.

ESET is not an Anti-Virus program It is an online scanner used to detect viruses. Difference

(Dec 20, 2010 10:57 AM)Disruption Wrote: [\[CITE\]](#) They are discussing RKILL

We can use Rkill. There was no problems made before when using it.

airjosh97 - December 20, 2010, 12:34 pm

I've pm'd you a short description of Dr.web cure it

Eminent Fate - December 20, 2010, 12:37 pm

(Dec 20, 2010 11:56 AM)Epidemic Wrote: [\[CITE\]](#) No they are not the same thing.

In simple terms

Anti-Virus program is a module that protects your whole system and monitors everything being, downloaded, ran, viewed and stored. It offers, protections, scanning, fire wall, virus chest, virus definitions etc.

The Scanner is what exactly it sounds like. It scans. That is oly what it does. You download it, it scans, it gives you the log, you analyze. Easy as that.

ESET is not an Anti-Virus program It is an online scanner used to detect viruses. Difference

(Dec 20, 2010 10:57 AM)Disruption Wrote: [\[CITE\]](#) They are discussing RKILL

We can use Rkill. There was no problems made before when using it.

I suggest disallowing Eset for poor performance. Just having ran it on a friend's PC I am amazed, the PC came out clean. MBAM found 23 infections whereas 5 where .exe :), I am amazed...

Isn't Rkill just a program used to kill everything on the desktop and restore it?, effective vs some rouges?.

Agent Shark - December 20, 2010, 12:42 pm

I will be updating this shortly when I obtain some more time.

RKILL is being added and I am undergoing Dr. Cureit.

ESET will not be removed.

If you have questions or queries about this tool contact an HJT Member.

Epidemic - December 20, 2010, 2:00 pm

(Dec 20, 2010 01:37 PM)Cocopara Wrote: [\[CITE\]](#) We can use Rkill. There was no problems made before when using it.

I suggest disallowing Eset for poor performance. Just having ran it on a friend's PC I am amazed, the PC came out clean. MBAM found 23 infections whereas 5 where .exe :), I am amazed...

Isn't Rkill just a program used to kill everything on the desktop and restore it?, effective vs some rouges?.

[/quote]

Eset is a good scanner. Malwarebytes is just better and probably had a more updated virus definitions. All scanners will not pick up the same thing. Thats a fact.

Rkill is a program sued to kill malicious process. It doesn't delete programs or restore anything, it just terminates processes, and it is quite effective against rouges if they are being associated with running processes,

Agent Shark - December 20, 2010, 2:39 pm

I have updated the tools list.

RKill is added.

Dr.CureIt is still being analyzed for further analysis.

Keep posting on here please to keep this thread alive.

airjosh97 - December 21, 2010, 6:25 am

Bump to keep this thread alive, How's the analysis of dr.web going?

Agent Shark - December 21, 2010, 6:26 am

(Dec 21, 2010 07:25 AM)airjosh97 Wrote: [\[CITE\]](#) Bump to keep this thread alive, How's the analysis of dr.web going?

Honestly,

I do not like it to much.

If an HJT Member recommends it then I will put it otherwise it's a no sorry :(

Thanks for ing :D

Eminent Fate - December 21, 2010, 6:29 am

Disruption. You should use Dr.web but only in severe cases.

However Airjosh97 do not understand the strengths of Dr.Web. To actually utilize DR.Web in a nice manner you need to download it to a rescue CD as their ordinary program is rather obsolete.

(Dec 20, 2010 03:00 PM)Epidemic Wrote: [\[CITE\]](#) I suggest disallowing Eset for poor performance. Just having ran it on a friend's PC I am amazed, the PC came out clean. MBAM found 23 infections whereas 5 where .exe :), I am amazed...

Isn't Rkill just a program used to kill everything on the desktop and restore it?, effective vs some rouges?.

Eset is a good scanner. Malwarebytes is just better and probably had a more updated virus

definitions. All scanners will not pick up the same thing. Thats a fact.

Rkill is a program used to kill malicious process. It doesn't delete programs or restore anything, it just terminates processes, and it is quite effective against rogues if they are being associated with running processes,
[/quote]

I seen newer Rouges be very persisent to Rkill..

Eset online scanner was not obsolete, it ran its updating scheme but it failed terribly not removing any of the infections which were a very old worm, rat and some trojans.

airjosh97 - December 21, 2010, 8:05 am

(Dec 21, 2010 07:29 AM)Cocopara Wrote: [\[CITE\]](#) Disruption. You should use Dr.web but only in severe cases.

However Airjosh97 do not understand the strengths of Dr.Web. To actually utilize DR.Web in a nice manner you need to download it to a rescue CD as their ordinary program is rather obsolete. Actually, Dr.web cure it is updated like 5 times a day

Agent Shark - December 21, 2010, 1:18 pm

(Dec 21, 2010 09:05 AM)airjosh97 Wrote: [\[CITE\]](#) Actually, Dr.web cure it is updated like 5 times a dayI will look at it via Virtual Box again later.

Eminent Fate - December 21, 2010, 2:23 pm

Great thread showing what programs can be suggested.

Those softwares given in the thread should be sufficient to remove most malware.

Agent Shark - December 22, 2010, 8:04 am

Bumping for new White Hat Helpers.