

Forum:[Hack Forums](#)

Thread: [Remove a JRAT? - SOLVED!!!](#)

Av?!?r - June 11, 2015, 6:43 pm

Anyone gotta a clue as to how I get this thing off of my PC? I got it around 2 days ago, and it's gotten to the point that I can't use my computer unless I start it in Safe Mode with Networking. I know that there's probably a section specifically for this on HF, but I don't know where it is, and I haven't ever posted in any of the other sections.

and dun call me stoopid. I ran a scan on the file before using it and it came up clean for some reason.

Yeah, and then some other guy did a scan on the same file on the same website and found that it had RAT in it. Fml...

I'm actually willing to do a complete wipe of my hard drive and reinstall Windows 8.1, but it won't accept my Product ID for some reason. I guess getting a computer with Windows pre-installed complicates things. :/

c\$sh - June 11, 2015, 6:46 pm

Curious, what file was it?

Kotlin - June 11, 2015, 6:49 pm

I'm not entirely sure this is the right section. Even though it's Java, it belongs in the Whitehat section.

<https://hackforums.net/forumdisplay.php?fid=110>

Anyways, you tried scanning with Malwarebyte?

Av?!?r - June 11, 2015, 6:57 pm

(Jun 11, 2015 06:49 PM)S. M. Archer Wrote: [\[CITE\]](#) I'm not entirely sure this is the right section. Even though it's Java, it belongs in the Whitehat section.

<https://hackforums.net/forumdisplay.php?fid=110>

Anyways, you tried scanning with Malwarebyte?

Tried just about every freakin antivirus ever. So like 6. But yeah, Malwarebyte was one of them. All it did was a 5 hour scan that had no effect on the virus that was actually causing all of the problems. It just found shit like trojans and adware in Internet Explorer, which I don't even use.

Oh and I forgot.

Somewhere along the lines, I managed to stop the virus for a few hours. It was only after I ran a scan from Kaspersky, then started a 30 day free trial where it would protect your computer in real time, like most other antivirus software does. I then uninstalled and reinstalled Java. After that, it was working fine for a few hours, and then it just stopped working.

And now when I start up my PC normally, I can't do anything because it's lagging so hard, with 40 instances of Java Environment... something running in the background, making pop-up windows n

shit one after the other.

(Jun 11, 2015 06:46 PM)WontonZ Wrote: [\[CITE\]](#) Curious, what file was it?
Supposed to be an "installer" in this link for Flare 3.3.
http://www.2shared.com/file/HS40LLVy/Flare_33_Cracked_by_Saladman.html

The actual thing has been leaked now though. I've heard the font rendering has some issues...

Also, here's the link of the working leak. Because the guy who cracked it felt like deobfuscating the RAT, so I guess it might help.
<http://hentaiandecchi.#.com/forums/attachment.php?aid=13>

Kotlin - June 11, 2015, 7:08 pm

(Jun 11, 2015 06:57 PM)TheWallsPlayer Wrote: [\[CITE\]](#) - snip -
I suggest you delete those links because:

A:) The dev sells the product on the forums
B:) It's not allowed.

Ashley? - June 11, 2015, 7:09 pm

<https://github.com/redpois0n/jrat-remover>

There are build instructions in the readme. Made by the guy who made jRAT.

le edgy fag - June 11, 2015, 7:40 pm

Holy shit redpois0n, now that's a name I haven't seen in a while

Av?!?r - June 11, 2015, 7:45 pm

(Jun 11, 2015 07:09 PM)poop nugget Wrote: [\[CITE\]](#) <https://github.com/redpois0n/jrat-remover>

There are build instructions in the readme. Made by the guy who made jRAT.
u w0t m8? That sounds too good to be true, lol. But I'll try it.

My problem is that I literally cannot do anything once I log into my computer in regular mode. I get like a 1 minute time window to be able to do anything. After that, it becomes too laggy to accomplish anything.

afk0 - June 11, 2015, 7:46 pm

(Jun 11, 2015 07:45 PM)TheWallsPlayer Wrote: [\[CITE\]](#) u w0t m8? That sounds too good to be true, lol. But I'll try it.

My problem is that I literally cannot do anything once I log into my computer in regular mode. I get like a 1 minute time window to be able to do anything. After that, it becomes too laggy to accomplish anything.

Sounds like your computer is being used to mine Bitcoins.

I reported your post for being in the wrong section so staff should move it soon.

Av?!?r - June 11, 2015, 7:52 pm

(Jun 11, 2015 07:46 PM)?aron Wrote: [\[CITE\]](#) Sounds like your computer is being used to mine Bitcoins.

I reported your post for being in the wrong section so staff should move it soon.

I hope I know where to find it when it gets there, haha.

(Jun 11, 2015 07:09 PM)poop nugget Wrote: [\[CITE\] https://github.com/redpois0n/jrat-remover](#)

There are build instructions in the readme. Made by the guy who made jRAT.
How do I run this program again? In the readme it's saying something about double-clicking "Remover.jar", but that didn't come with the file on that page. :/

The Scarabian - June 11, 2015, 7:55 pm

Why the hell is this in the Griefing Section?

Av?!?r - June 11, 2015, 7:57 pm

Goddamn, the Whitehat section just looks f-ing sad. All those people with the same problems. Durn.

(Jun 11, 2015 07:55 PM)Manuel Neuer Wrote: [\[CITE\]](#) Why the hell is this in the Griefing Section?
werkin on et.

m8002342342345

c\$sh - June 11, 2015, 8:07 pm

Are you sure it is a jRAT?

Could really be about any RAT on the market considering it was an EXE

Av?!?r - June 11, 2015, 8:35 pm

(Jun 11, 2015 08:07 PM)WontonZ Wrote: [\[CITE\]](#) Are you sure it is a jRAT?

Could really be about any RAT on the market considering it was an EXE

Naw, it was a .jar alright. Every time I start up my computer, my desktop gets spammed with Java Environment errors n shit.

Also, gotta love contacting Microsoft for help on resetting your computer, and the bitch says this:

"That is great

LEt's get started

Windows 8.1 will cost you \$119.99 and you will have this one for a life time"

I already payed for the shit when I got it pre-installed along with this poop of a laptop. Last time I contacted them and told them I had a virus, they wanted me to buy a subscription or some crap that was \$40 a month. T_T

Do they not have enough \$\$\$\$\$\$?

Knautschtabak - June 11, 2015, 10:44 pm

Hi TheWallsPlayer.

Are you now able to get into normal mode? If so, please do that and proceed with the following steps.

Please read through the points below to ensure this process moves as quickly and efficiently as possible.Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please do not run any tools or take any steps other than those I provide for you. Independent efforts may make matters worse, and will affect my ability in providing the best set of instructions for

you.

Please backup important files before proceeding with my instructions. Malware removal can be unpredictable at times.

If you come across any issues whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

Step 1: Farbar Recovery Scan Tool (FRST) ScanPlease download [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run.

Right-Click FRST.exe or FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to [pastebin.com](#). Post the link here.

Step 2: RogueKillerDownload [RogueKiller \(32 bit\)](#)/[RogueKiller \(64 bit\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download the first (32-bit) if you're unsure.

Close any running programs.

Right-Click RogueKiller.exe and select Run as administrator to run the program.

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to [pastebin.com](#), click Submit and

paste the link to it in your next reply.

Av?I?r - June 12, 2015, 5:48 am

(Jun 11, 2015 10:44 PM)Knautschtabak Wrote: [\[CITE\]](#) *snip

I'm not able to use my computer in normal mode. Will this work in Safe Mode?

Edit: It's working

Knautschtabak - June 12, 2015, 6:39 am

Proceed with safe mode then.

Av?I?r - June 12, 2015, 6:56 am

I wasn't able to use pastebin because of the file size limit, so I put the logs on File Dropper.

Farbar Recovery Scan Tool

FRST.txt: <http://www.filedropper.com/frst>

Addition.txt: <http://www.filedropper.com/addition>

RogueKiller

Report: <http://www.filedropper.com/rkreportscn06122015095000>

FINALLY something detected the rat on my computer! :D

Knautschtabak - June 12, 2015, 7:27 am

RogueKiller FixClose any running programmes.

Right-Click RogueKiller.exe and select Run as administrator to run the programme.

Allow the Prescan to complete.

A browser window may open. Close the browser window.

Click .

Upon completion, do the following:

Click and place a checkmark next to all VT.Backdoor.Java.JRat items. Ensure any other items are unchecked.

Click .

Click .

Copy the contents of the log and paste in your next reply.

Also check if you can access normal mode after that.

Immoral Collective - June 12, 2015, 7:34 am

Just saying remove java for now and it will make the virus unable to run until you reinstall. Though it gives you time to send the .jar into virustotal and in about 4/5 days your av should be detecting it.

Av?!?r - June 12, 2015, 7:52 am

(Jun 12, 2015 07:27 AM)Knautschtabak Wrote: [\[CITE\]](#) *snip
Awesome, I'll try that. :)

(Jun 12, 2015 07:34 AM)Immoral Collective Wrote: [\[CITE\]](#) Just saying remove java for now and it will make the virus unable to run until you reinstall. Though it gives you time to send the .jar into virustotal and in about 4/5 days your av should be detecting it.

I'll completely uninstall Java if/when I can, but I'm not sure when I should reinstall it.

When I first got this virus, it just slowed everything down a little bit. I could still do things on my computer, but typing was really slow, so I thought someone was logging my keystrokes. Also, my webcam came on once, and I changed all of my passwords since then. On a different computer of course.

When I was still able to use my PC in normal mode, I ran a scan by Kaspersky. It didn't find the rat, but for some reason the 30-day free trial for protecting my PC in real time worked, and everything was running like normal. Then I uninstalled and reinstalled Java with the antivirus still on, but a few hours later the virus came back and this time completely crippled my computer.

So how long should I wait before reinstalling Java again? And should I change my passwords a 3rd time?

Alright, here it is. <http://www.filedropper.com/rkreportdel06122015114734>

Knautschtabak - June 12, 2015, 8:52 am

Can you access normal mode now?

Av?!?r - June 12, 2015, 9:00 am

(Jun 12, 2015 08:52 AM)Knautschtabak Wrote: [\[CITE\]](#) Can you access normal mode now?
I'll try now.

btw, you had 1337 posts before that one just now. :D rip

Nope. ./ There's still pop-ups when I start up, and it's still really laggy.

Anything else I should try? I figured out that uTorrent worked in Safe Mode and I got a Windows 8.1 .iso. I was thinking of resetting my PC that way, since I don't have my own disc.

Knautschtabak - June 12, 2015, 11:29 am

Reinstalling the operating system is always the safest option if infected with a backdoor/RAT.

It is up to you. Post a fresh FRST log (without Addition) if you want me to proceed with removal.

Av?!?r - June 12, 2015, 11:41 am

(Jun 12, 2015 11:29 AM)Knautschtabak Wrote: [\[CITE\]](#) Reinstalling the operating system is always

the safest option if infected with a backdoor/RAT.

It is up to you. Post a fresh FRST log (without Addition) if you want me to proceed with removal.

Yeah, I was prepared to reinstall my operating system, but I have a problem with that as well. When trying to reset Windows, it tells me that I need some missing information, like on a disc or USB. My computer came with Windows 8 pre-installed, so I didn't get a disc. I've updated to 8.1 since then.

I used a Third-Party program called NirSoft's ProduKey to get the key for Windows 8.1. When my computer was still able to run normally, I tried entering in the key to reset my OS, because there was an option that would allow me to do that without needing a disc. However, the key didn't work.

I tried contacting Windows about it, to see if they would give me my correct key if the last one was wrong. But all wanted was my computer's Product ID so they could send me a Windows 8.1 disc for \$119! Christ almighty.

Knautschtabak - June 12, 2015, 11:45 am

Yes, that sucks. Do you still want to reformat? Or can I help you with anything else?

Av?!?r - June 12, 2015, 11:47 am

(Jun 12, 2015 11:45 AM)Knautschtabak Wrote: [\[CITE\]](#) Yes, that sucks. Do you still want to reformat? Or can I help you with anything else?

Yes, please. If you can think of any way I can reformat my PC, that would be awesome. :)

Knautschtabak - June 12, 2015, 11:54 am

Not sure if this is what you tried and were the key did not work, but take a look at this:

<http://www.bleepingcomputer.com/tutorials/how-to-perform-a-clean-install-of-windows-8/>

Av?!?r - June 12, 2015, 12:01 pm

(Jun 12, 2015 11:54 AM)Knautschtabak Wrote: [\[CITE\]](#) Not sure if this is what you tried and were the key did not work, but take a look at this:

<http://www.bleepingcomputer.com/tutorials/how-to-perform-a-clean-install-of-windows-8/>

Yeah. When I get to the part "Remove everything and reinstall Windows", I click Get Started, and this comes up:

"Insert media

Some files are missing. Your Windows installation or recovery media will provide these files."

Edit: And the part where I said that it would let me reinstall Windows without any recovery media only showed up in normal mode, which I can't access anymore. It asked for the Windows key and a USB drive with at least 3GB of space.

UnknownRaz - June 12, 2015, 12:15 pm

(Jun 12, 2015 11:54 AM)Knautschtabak Wrote: [\[CITE\]](#) senpai<3

BTW bro since i cannot pm i had to post here to remind u on my post

Knautschtabak - June 12, 2015, 12:17 pm

I see this possibility for you to proceed now. You can ask in the Windows section here on HF if the others know any way to reformat your system.

If they can't help you, you come back here and I will proceed with cleaning your machine as good as I can.

(Alternatively switch to Linux ;P)

Av?I?r - June 12, 2015, 12:20 pm

(Jun 12, 2015 12:17 PM)Knautschtabak Wrote: [\[CITE\]](#) I see this possibility for you to proceed now. You can ask in the Windows section here on HF if the others know any way to reformat your system.

If they can't help you, you come back here and I will proceed with cleaning your machine as good as I can.

(Alternatively switch to Linux ;P)
Alright.

Thank you very much for your help. :))

Null Byte - June 12, 2015, 12:35 pm

WHY ARE YOU ASKING HIM TO REINSTALL? It's an easy removal

Also holy fuck that is a poorly programmed rat. Look at all those startup keys.

OP, if nobody knows how to make a fixlist for this (rly knautschtabak?) then I will make one for you. Just give me the word.

Knautschtabak - June 12, 2015, 12:39 pm

(Jun 12, 2015 12:35 PM)Null Byte Wrote: [\[CITE\]](#) WHY ARE YOU ASKING HIM TO REINSTALL? It's an easy removal

Also holy fuck that is a poorly programmed rat. Look at all those startup keys.

OP, if nobody knows how to make a fixlist for this (rly knautschtabak?) then I will make one for you. Just give me the word.

I did not ask him. It was his decision. I always gave the option to remove the malware.

? PROFIT ? - June 12, 2015, 12:51 pm

I think i have the same thing on my PC.

hopefully a fix can be found for us both.

<https://www.virustotal.com/en/file/190b457a3242030c5d24cfefea4c586a80a16cfe8c380426e7f960c8f964029a/analysis/>

^ scan of the infected file

Av?I?r - June 12, 2015, 12:54 pm

(Jun 12, 2015 12:35 PM)Null Byte Wrote: [\[CITE\]](#) WHY ARE YOU ASKING HIM TO REINSTALL? It's an easy removal

Also holy fuck that is a poorly programmed rat. Look at all those startup keys.

OP, if nobody knows how to make a fixlist for this (rly knautschtabak?) then I will make one for you. Just give me the word.

Hey dude, if you know how to fix this, I'm all for it. At this point, I don't really care how, I just want it gone. :P

(Jun 12, 2015 12:39 PM)Knautschtabak Wrote: [\[CITE\]](#) I did not ask him. It was his decision. I always gave the option to remove the malware.

I say we do both at once. I doubt anyone from the Windows section is gonna be able to find a way to reset my PC when I can't even run Windows normally, lol.

Hit me with round 2 if ya got it. ?

Knautschtabak - June 12, 2015, 12:58 pm

(Jun 12, 2015 12:54 PM)TheWallsPlayer Wrote: [\[CITE\]](#) Hey dude, if you know how to fix this, I'm all for it. At this point, I don't really care how, I just want it gone. :P

I say we do both at once. I doubt anyone from the Windows section is gonna be able to find a way to reset my PC when I can't even run Windows normally, lol.

Hit me with round 2 if ya got it. ?

?

I always gave you the option that I fix it.

Post fresh FRST logs.

Av?!?r - June 12, 2015, 1:05 pm

(Jun 12, 2015 12:58 PM)Knautschtabak Wrote: [\[CITE\]](#) ?

I always gave you the option that I fix it.

Post fresh FRST logs.

Okie dokie, I'm 000n et.

.....

(Jun 12, 2015 12:51 PM)Austin72 Wrote: [\[CITE\]](#) I think i have the same thing on my PC.

hopefully a fix can be found for us both.

<https://www.virustotal.com/en/file/190b457a3242030c5d24cfefea4c586a80a16cfe8c380426e7f960c8f964029a/analysis/>

^ scan of the infected file

omg, exactly! I scanned that exact same file and it came up "clean" like in that one.

? PROFIT ? - June 12, 2015, 1:13 pm

(Jun 12, 2015 01:05 PM)TheWallsPlayer Wrote: [\[CITE\]](#) Okie dokie, I'm 000n et.

.....

omg, exactly! I scanned that exact same file and it came up "clean" like in that one.
yea ive been trying to get rid of it for a few days.

i found a way to stall it. not fix it tho. i deleted all the .jar files it made in my startup folder.

Av?!?r - June 12, 2015, 1:17 pm

(Jun 12, 2015 01:13 PM)Austin72 Wrote: [\[CITE\]](#) yea ive been trying to get rid of it for a few days.

i found a way to stall it. not fix it tho. i deleted all the .jar files it made in my startup folder.
lkr, same. Except my computer's not the best, so mine just freezes up now.

Also, here's that next scan: http://www.filedropper.com/frst_1

I haven't even gotten a reply from the guys at the Windows section yet. xD

? PROFIT ? - June 12, 2015, 1:22 pm

<https://www.virustotal.com/en/file/d0018aba175174cbfaeb31a81867baf4295770d01cc75c10c9e4068510921be0/analysis/1434140421/>

heres a scan of one of the files it puts in the startup.

Null Byte - June 12, 2015, 1:22 pm

Download attached fixlist.txt file and save it to the same directory as FRST.exe.

Download link: <https://d.maxfile.ro/dmbeutaywz.txt> (Right click --> Save as... Then rename to fixlist.txt)

Save all work before running this! Your computer will be rebooted.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work!

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally.
After that let the tool complete its run.

When finished FRST will reboot your computer and generate a log on the Desktop (Fixlog.txt).
Please post it to your reply.

After your reboot I want you to do another FRST scan. So the two logs I need form you are:

- FRST.txt
- Fixlog.txt

?

Null Byte

Av?!?r - June 12, 2015, 1:34 pm

(Jun 12, 2015 01:22 PM)Null Byte Wrote: [\[CITE\]](#) Download attached fixlist.txt file and save it to the same directory as FRST.exe.

Download link: <https://d.maxfile.ro/dmbeutaywz.txt> (Right click --> Save as... Then rename to fixlist.txt)

Save all work before running this! Your computer will be rebooted.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work!

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally.
After that let the tool complete its run.

When finished FRST will reboot your computer and generate a log on the Desktop (Fixlog.txt).

Please post it to your reply.

After your reboot I want you to do another FRST scan. So the two logs I need from you are:

- FRST.txt
- Fixlog.txt

?

Null Byte

Ok nice. Hold on, I'll try this in a bit. I'm talking to a friend who has some suggestions as well.

? PROFIT ? - June 12, 2015, 1:38 pm

I think i just fixed it on my own.....

no more java.exe or javaw.exe processes running after restarting my computer!

I deleted all the jar files in C:\users\Austin & in the startup folder

i also removed all scheduled tasks that would put the jar files there on startup.

:D

I hope its gone for good!

Null Byte - June 12, 2015, 1:38 pm

(Jun 12, 2015 01:34 PM)TheWallsPlayer Wrote: [\[CITE\]](#) Ok nice. Hold on, I'll try this in a bit. I'm talking to a friend who has some suggestions as well.

Okay. Keep in mind that if you continue delaying, Jrat could keep replicating (potentially). So you may want to run this soon.

Av?!?r - June 12, 2015, 1:43 pm

(Jun 12, 2015 01:38 PM)Null Byte Wrote: [\[CITE\]](#) Okay. Keep in mind that if you continue delaying, Jrat could keep replicating (potentially). So you may want to run this soon.

O_o You're kidding. Why isn't this guy curing cancer?

(Jun 12, 2015 01:38 PM)Austin72 Wrote: [\[CITE\]](#) I think i just fixed it on my own.....

no more java.exe or javaw.exe processes running after restarting my computer!

I deleted all the jar files in C:\users\Austin & in the startup folder

i also removed all scheduled tasks that would put the jar files there on startup.

:D

I hope its gone for good!

tell tell tell tell tell tell tell tell tell

how how how how how how how how how

? PROFIT ? - June 12, 2015, 1:53 pm

(Jun 12, 2015 01:38 PM)Null Byte Wrote: [\[CITE\]](#) Okay. Keep in mind that if you continue delaying, Jrat could keep replicating (potentially). So you may want to run this soon.

it sure as hell does replicate.

i deleted like 200 .jar files(made by it).

Av?!?r - June 12, 2015, 2:10 pm

Wow. This is the first time I've been able to run normally for days. Stuff like website cookies and saved log-in information was deleted. I actually had to request a new randomly generated password so I could sign in, because the old one wasn't working for some reason.

Alright, here we gooo!

FRST.txt: http://www.filedropper.com/frst_2

Fixlog: <http://www.filedropper.com/fixlog>

And I forgot to turn off the "Addition" option in FRST, so I have that too:

http://www.filedropper.com/addition_1

I hope that doesn't break things. :3

Null Byte - June 12, 2015, 4:54 pm

(Jun 12, 2015 02:10 PM)TheWallsPlayer Wrote: [\[CITE\]](#) Wow. This is the first time I've been able to run normally for days. Stuff like website cookies and saved log-in information was deleted. I actually had to request a new randomly generated password so I could sign in, because the old one wasn't working for some reason.

Alright, here we gooo!

FRST.txt: http://www.filedropper.com/frst_2

Fixlog: <http://www.filedropper.com/fixlog>

And I forgot to turn off the "Addition" option in FRST, so I have that too:

http://www.filedropper.com/addition_1

I hope that doesn't break things. :3

Looks much better! Is your computer running OK now?

Av?!?r - June 12, 2015, 6:19 pm

(Jun 12, 2015 04:54 PM)Null Byte Wrote: [\[CITE\]](#) Looks much better! Is your computer running OK now?

Yes! Just like normal! Thank you Knautschtabak and Null Byte for your help!

PS: What would you guys recommend for cleaning up my PC? I'm talking Grade-A stuff here; I must have a lot of crap on my PC that I don't want. :3

YekiM - June 12, 2015, 6:36 pm

(Jun 12, 2015 12:51 PM)Austin72 Wrote: [\[CITE\]](#) I think i have the same thing on my PC.

hopefully a fix can be found for us both.

<https://www.virustotal.com/en/file/190b457a3242030c5d24cfefea4c586a80a16cfe8c380426e7f960c8f964029a/analysis/>

^ scan of the infected file
Hi Austin,

Fixes, fixlists and removal advice are on a case-by-case basis, and using the same fixlist found in this thread may render your system inoperable as the nature of your problem (although might seem to be the same issue) could be different. I would suggest you make a new thread with fresh FRST.txt, addition.txt and rkreport.txt. Refer to the spoiler below if you need help with the instructions. Furthermore, deleting the entries in both MSCONFIG (or just the start-up folder) & the services does not remove the malware completely from your system, as the entries will remain dormant until it can find a way to activate itself again (usually through human error, system restoring or antivirus conflicts.)

Spoiler ([Click to View](#))

Before we start please note the following: Analysis and research take some time, so please be patient. If your helper doesn't respond for more than 24 hours, PM them.

Please follow their instructions exactly as they are posted and do not run any tools on your own.

Stay with them to the very end, the absence of symptoms doesn't mean that your machine is fully operational.

They can't foresee everything, so if anything unexpected happens, please stop and inform them.

If you have any questions, please don't hesitate to ask your helper.

Category: Discovery

Step 1: Farbar Recovery Scan Tool (FRST) ScanDownload [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run

Right-Click FRST.exe or FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

When it has finished, it will alert you in separate pop-ups that both FRST.txt and addition.txt has been saved to the desktop. Go ahead and press Ok

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

Step #2: RogueKillerDownload [RogueKiller \(x64\)](#) and save the file to your Desktop.

Close any running programs.

Right-Click RogueKiller.exe and select Run as administrator to run the program.

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to pastebin.com, click Submit and paste the link to it in your next reply.

In your next reply:FRST.txt

Addition.txt

RKreport.txt

Knautschtabak - June 12, 2015, 9:00 pm

(Jun 12, 2015 01:22 PM)Null Byte Wrote: [\[CITE\]](#) Download attached fixlist.txt file and save it to the same directory as FRST.exe.

Download link: <https://d.maxfile.ro/dmbeutaywz.txt> (Right click --> Save as... Then rename to fixlist.txt)

Save all work before running this! Your computer will be rebooted.

NOTE: It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work!

Run FRST/FRST64 and press the Fix button just once and wait.

If for some reason the tool needs a restart, please make sure you let the system restart normally. After that let the tool complete its run.

When finished FRST will reboot your computer and generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

After your reboot I want you to do another FRST scan. So the two logs I need from you are:

- FRST.txt
- Fixlog.txt

?

Null Byte

Don't you think it is a bit impolite to just hijack another helper's thread? Especially after I told you that I am still helping?

@TheWallsPlayer There is still malware on your computer. The fix did not remove it all and your problem is faraway from being solved. I can continue with assistance, but I want you to decide for

ONE helper first and stick to that one. Because now it is really confusing who is helping here and I am not in the mood to prepare a fix just to see that you have followed instructions of other helpers in the meanwhile. That is not only annoying, it can also be dangerous with conflicting instructions.

Null Byte - June 12, 2015, 9:06 pm

(Jun 12, 2015 09:00 PM)Knautschtabak Wrote: [\[CITE\]](#) Don't you think it is a bit impolite to just hijack another helper's thread? Especially after I told you that I am still helping?

@TheWallsPlayer There is still malware on your computer. The fix did not remove it all and your problem is faraway from being solved. I can prepare a new one, but I want you do decide for ONE helper first and stick to that one. Because now it is really confusing who is helping here and I am not in the mood to prepare a fix just to see that you have followed instructions of other helpers in the meanwhile. That is not only annoying, it can also be dangerous with conflicting instructions.

Considering you wanted him to format, I had to intervene. Impolite or not, it's most important that OP gets the help he needs.

Retribute - June 12, 2015, 9:49 pm

(Jun 12, 2015 09:06 PM)Null Byte Wrote: [\[CITE\]](#) Considering you wanted him to format, I had to intervene. Impolite or not, it's most important that OP gets the help he needs.

Do you even have proper training under your belt? No offence as I have previously seen you help in this section, but you have never revealed the answer to this question before.

Null Byte - June 12, 2015, 10:25 pm

(Jun 12, 2015 09:49 PM)Retribute Wrote: [\[CITE\]](#) Do you even have proper training under your belt? No offence as I have previously seen you help in this section, but you have never revealed the answer to this question before.

Yeah, I like to think I'm pretty good at removing malware.

@knaut - what is the malware remaining on his system? Can you show me the fixlist you would administer here?

? PROFIT ? - June 12, 2015, 10:36 pm

(Jun 12, 2015 06:36 PM)YekiM Wrote: [\[CITE\]](#) Hi Austin,

Fixes, fixlists and removal advice are on a case-by-case basis, and using the same fixlist found in this thread may render your system inoperable as the nature of your problem (although might seem to be the same issue) could be different. I would suggest you make a new thread with fresh FRST.txt, addition.txt and rkreport.txt. Refer to the spoiler below if you need help with the instructions. Furthermore, deleting the entries in both MSCONFIG (or just the start-up folder) & the services does not remove the malware completely from your system, as the entries will remain dormant until it can find a way to activate itself again (usually through human error, system restoring or antivirus conflicts.)

Spoiler [\(Click to View\)](#)

Before we start please note the following: Analysis and research take some time, so please be patient. If your helper doesn't respond for more than 24 hours, PM them.

Please follow their instructions exactly as they are posted and do not run any tools on your own.

Stay with them to the very end, the absence of symptoms doesn't mean that your machine is fully operational.

They can't foresee everything, so if anything unexpected happens, please stop and inform them.

If you have any questions, please don't hesitate to ask your helper.

Category: Discovery

Step 1: Farbar Recovery Scan Tool (FRST) ScanDownload [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run

Right-Click FRST.exe or FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

When it has finished, it will alert you in separate pop-ups that both FRST.txt and addition.txt has been saved to the desktop. Go ahead and press Ok

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

Step #2: RogueKillerDownload [RogueKiller \(x64\)](#) and save the file to your Desktop.

Close any running programs.

Right-Click RogueKiller.exe and select Run as administrator to run the program.

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to pastebin.com, click Submit and paste the link to it in your next reply.

In your next reply:FRST.txt

Addition.txt

RKreport.txt

for now, its fixed, if i see anything suspicious at all in the future i will post here.

Knautschtabak - June 13, 2015, 1:19 am

(Jun 12, 2015 09:06 PM)Null Byte Wrote: [\[CITE\]](#) Considering you wanted him to format, I had to intervene. Impolite or not, it's most important that OP gets the help he needs.

Firstly reformat is the recommended action for backdoors. Every helper of reputable malware removal forums will say the same and inform the user about this fact.

Secondly I reacted upon him telling me he considered reformatting and he already downloaded a Windows torrent. I wanted him to decide before I proceed, so I don't prepare a fix for nothing. I always told him to post FRST scans if he wants to proceed. Thirdly, your fix came after the decision to proceed with removal. That was not necessary, nor professional.

We helpers in this section look out for each other, which is great. But this should be done in a professional way that does not create confusion for the user or creates the danger of proposing two conflicting fixes to the user.

If I have any problem with a (trained!) helper's fix in the section, I write a PM. So do the other helpers if they see a problem with my fix. That avoids confusion in the thread and that is also what I would like you to do if you see something troubling. I take any criticism seriously. So please, keep watching out, but don't hijack threads.

(Jun 12, 2015 10:25 PM)Null Byte Wrote: [\[CITE\]](#) @knaut - what is the malware remaining on his system? Can you show me the fixlist you would administer here?

Look into the One Month Created files section of the last FRST.txt and you will see remaining .jar files of the RAT.

You will also see that there is lots of adware on the system that needs to be fixed as well, or he will get other infections very soon through malvertising and the remaining security holes on the system.

Av?I?r - June 13, 2015, 2:23 am

(Jun 13, 2015 01:19 AM)Knautschtabak Wrote: [\[CITE\]](#) *snip

Look into the One Month Created files section of the last FRST.txt and you will see remaining .jar files of the RAT.

You will also see that there is lots of adware on the system that needs to be fixed as well, or he will get other infections very soon through malvertising and the remaining security holes on the system.

Ok, so how do you want me to do that? :P

Also, I uninstalled Kaspersky and reinstalled what I had before that whole mess had happened, which was Avast!. I did a scan with it, and it found somewhere around 650 of those jrat files, even though they weren't doing anything. So I "fixed" them, (that's what one of the options said, I don't necessarily know what it means), and then did a "boot-scan"; something I've never heard of. Basically all it did was delete the files 1 by 1 before restarting my PC.

(Jun 12, 2015 09:06 PM)Null Byte Wrote: [\[CITE\]](#) Considering you wanted him to format, I had to intervene. Impolite or not, it's most important that OP gets the help he needs.

Yeah trust me, I was the one who wanted to reformat. In fact if it were possible for me to reformat, I would have done that instead of all of this. That would have certainly fixed everything, lol.

Knautschtabak - June 13, 2015, 4:02 am

Since you did a lot of changes to your system in the meanwhile I will need a fresh FRST scan.

Farbar Recovery Scan Tool (FRST) ScanRight-Click FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

Av?I?r - June 13, 2015, 7:07 am

(Jun 13, 2015 04:02 AM)Knautschtabak Wrote: [\[CITE\]](#) Since you did a lot of changes to your system in the meanwhile I will need a fresh FRST scan.

Farbar Recovery Scan Tool (FRST) ScanRight-Click FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

FRST.txt: http://www.filedropper.com/frst_3

Addition.txt: http://www.filedropper.com/addition_2

Knautschtabak - June 13, 2015, 12:27 pm

Step 1: Uninstall SoftwarePress the Windows Key + r on your keyboard at the same time. Type appwiz.cpl and click OK.

Search for the following programs, right-click and click Uninstall.uTorrent (See: <https://torrentfreak.com/utorrent-quietly-installs-riskware-bitcoin-miner-users-report-150306/>)

Smart Saver (adware)

YoutubeAdBlocke (adware)

Follow the prompts.

Note: If you are offered the choice to install additional software, ensure you decline.

Reboot if necessary.

Step 2: Farbar Recovery Scan Tool (FRST) Script Press the Windows Key + r on your keyboard at the same time. Type Notepad and click OK.

Copy the entire contents of the codebox below and paste into the Notepad document.

Code start

CreateRestorePoint:

C:\Users\Zack\14*.jar

Task: {88956D3D-1EB8-4A58-83FD-58CA2C66B3EE} - \GPUP No Task File <==== ATTENTION

Folder: C:\Users\Zack

end

Click File, Save As and type fixlist.txt as the File Name.

Important: The file must be saved in the same location as FRST.exe.

NOTICE: This script is intended for use on this particular machine. Do not use this script on any other machine; doing so may cause damage to your Operating System. Right-Click FRST.exe and select Run as administrator to run the program.

Click Fix.

A log (Fixlog.txt) will open on your desktop. Copy the contents of the log to pastebin.com and paste the link to it in your next reply.

Step 3: Junkware Removal Tool (JRT) Please download [Junkware Removal Tool](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Right-Click JRT.exe and select Run as administrator to run the program.

Follow the prompts and allow the scan to run uninterrupted.

Upon completion, a log (JRT.txt) will open on your desktop.

Re-enable your anti-virus software

Copy the contents of JRT.txt to pastebin.com and paste the link in your next reply.

Step 4: AdwCleaner Please download [AdwCleaner](#) and save the file to your Desktop.

Right-Click AdwCleaner.exe and select Run as administrator to run the program.

Follow the prompts.

Click Scan.

Upon completion, click Report. A log (AdwCleaner[R0].txt) will open. Briefly check the log for anything you know to be legitimate.

Ensure anything you know to be legitimate does not have a checkmark, and click Clean.

Follow the prompts and allow your computer to reboot.

After rebooting, a log (AdwCleaner[S0].txt) will open. Copy the contents of the log to pastebin.com and paste the links in your next reply.

-- File and folder backups are made for items removed using this tool. Should a legitimate file or folder be removed (otherwise known as a 'false-positive'), simple steps can be taken to restore the item. Please do not overly concern yourself with the contents of AdwCleaner[R0].txt.

Av?!?r - June 13, 2015, 7:51 pm

Fixlog.txt: http://www.filedropper.com/fixlog_2

JRT log: <http://pastebin.com/KaCCpmRB>

AdwCleaner: <http://pastebin.com/Yk0bnBAv>

Knautschtabak - June 14, 2015, 11:42 am

ESET Online Scan

Note: This scan may take a long time to complete. Please do not browse the Internet whilst your Anti-Virus is disabled. Please download [ESET Online Scan](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Double-click esetsmartinstaller_enu.exe to run the programme.

Agree to the EULA by placing a checkmark next to Yes, I accept the Terms of Use. Then click Start.

Agree to the Terms of Use once more and click Start. Allow components to download.

Place a checkmark next to Enable detection of potentially unwanted applications.

Click Advanced settings. Place a checkmark next to: Scan archives

Scan for potentially unsafe applications

Enable Anti-Stealth technology

Ensure Remove found threats is unchecked.

Click Start.

Wait for the scan to finish. Please be patient as this can take some time.

Upon completion, click

[img]http://billy-oneal.com/Canned%20Speeches/speechimages/eset/esetListThreats.png[/img]. If no threats were found, skip the next two bullet points.

Click [img]http://billy-oneal.com/Canned%20Speeches/speechimages/eset/esetExport.png[/img] and save the file to your Desktop, naming it something such as "MyEsetScan".

Push the Back button.

Place a checkmark next to

[img]http://3-ps.googleusercontent.com/x/forums.whatthetech.com/i.imgur.com/xKN1w2nv.png.page speed.ic.JWqlaEgZi7.png[/img] and click
[img]http://1-ps.googleusercontent.com/x/forums.whatthetech.com/i.imgur.com/SzOC1p0.png.pagespeed.ce.OWDP45O6oG.png[/img].

Re-enable your anti-virus software.

Copy the contents of the log and paste in your next reply.

Av?I?r - June 15, 2015, 5:07 am

Nice. Sorry it took so long to reply. I was gonna wait until I could have it scan overnight. :)

C:\Program Files\Sony\Vegas Pro 11.0\sony.vegas11_64bit_keygen-patch.exe a variant of Win32/HackTool.Patcher.T potentially unsafe application

C:\Users\Zack\Desktop\Windows_8.1_Pro_X64_Activated.iso MSIL/HackTool.IdleKMS.C potentially unsafe application

Knautschtabak - June 15, 2015, 5:55 am

Looks good. The two files are detected, because they are "Hacktools"/grayware.
We are done, congratulations! ?

DelFixPlease download [DeIFix](#) and save the file to your Desktop.

Double-click DelFix.exe to run the programme.

Place a checkmark next to the following items:Remove disinfection tools

Create registry backup

Click the Run button.

-- This will remove the specialised tools we used to disinfect your system. Any leftover logs, files,

folders or tools remaining on your Desktop which were not removed can be deleted manually (right-click the file + delete).

Av?I?r - June 15, 2015, 9:13 am

(Jun 15, 2015 05:55 AM)Knautschtak Wrote: [CITE](#) Looks good. The two files are detected, because they are "Hacktools"/grayware.

We are done, congratulations! ?

DelFixPlease download [DelFix](#) and save the file to your Desktop.

Double-click DelFix.exe to run the programme.

Place a checkmark next to the following items:Remove disinfection tools

Create registry backup

Click the Run button.

-- This will remove the specialised tools we used to disinfect your system. Any leftover logs, files, folders or tools remaining on your Desktop which were not removed can be deleted manually (right-click the file + delete).

Yaaaaaasss thanks a bunch!