

Forum:[Hack Forums](#)

Thread: [Brotherhood Helpdesk: Post Here For Help If Infected](#)

-Hyperion - August 27, 2015, 6:33 am

Hey guys it's -Hyperion ?

I am currently a technician for a fortune 500 company and running my own pentesting business. As well as leader of the Brotherhood Computing Sector, also known as BHCPU.

I have been away the past few months working on other projects and apparently this section has gone to shit. Instead of going through and answering a bunch of posts, if you need help and think you are infected then please post here using this format:

Code OS:

What is happening:

What have you done: Do not take help from anyone else unless they are listed on this post.

-Hyperion

Roger Waters

Help is first come first serve and check out some of these useful links first.

[Am I Infected](#)

[Doing A Basic Cleanup](#)

[File Analysis](#)

[Anti Virus Recommendations](#)

Trigger3lite - August 27, 2015, 10:03 am

OS: Win7 sp1

What is happening: Virus not going away, infecting other files.

What have you done: AVG, Malware bytes and ComboFix(pastebin.com/BhAKjttL)

YungTrigz - August 27, 2015, 2:07 pm

(Aug 27, 2015 10:03 AM)Trigger3lite Wrote: [\[CITE\]](#) ComboFix(pastebin.com/BhAKjttL)
nononononononono NEVER use combifix unless a pro tells you too.

-Hyperion - August 27, 2015, 4:21 pm

(Aug 27, 2015 10:03 AM)Trigger3lite Wrote: [\[CITE\]](#) OS: Win7 sp1

What is happening: Virus not going away, infecting other files.

What have you done: AVG, Malware bytes and ComboFix(pastebin.com/BhAKjttL)

why do you think you have a virus and never run combifix.

lawton111 - August 28, 2015, 4:04 am

Sorry - apparently the referral I was given asked me to post in the wrong section and redirected me here :)

Here goes :

Hi there,

I have been referred to you through the forums as I have a Macbook and maybe you can help with the removal of a RAT?? I will copy you my original post to see what I am up against :) Any help you

can over would be much appreciated and am happy to compensate you for your time.

Hi there,

I thought I already posted this but here goes for a second time.

I have an ex girlfriend who seems to have gained access to my MacBook and/or my Iphone. These include my email, Facebook, Skype, email and Ebay, further the programs on my Iphone 6 including complete access to Viber.

I have repeatedly changed passwords including my login access on my Mac. She seems to have access to all my information - blatantly telling me whats going on in my life and who I am talking to, how much I paid for things on Ebay even when the programs are not running - quite honestly its a little scary. I am not looking to hack anyone just stop what she is doing.

Any ideas on this and any remedial action? I am using a Macbook Pro running Yosemite, and also an Iphone 6

Many Thanks

-Hyperion - August 28, 2015, 10:33 am

(Aug 28, 2015 04:04 AM)lawton111 Wrote: [\[CITE\]](#) Sorry - apparently the referral I was given asked me to post in the wrong section and redirected me here :)

Here goes :

Hi there,

I have been referred to you through the forums as I have a Macbook and maybe you can help with the removal of a RAT?? I will copy you my original post to see what I am up against :) Any help you can over would be much appreciated and am happy to compensate you for your time.

Hi there,

I thought I already posted this but here goes for a second time.

I have an ex girlfriend who seems to have gained access to my MacBook and/or my Iphone. These include my email, Facebook, Skype, email and Ebay, further the programs on my Iphone 6 including complete access to Viber.

I have repeatedly changed passwords including my login access on my Mac. She seems to have access to all my information - blatantly telling me whats going on in my life and who I am talking to, how much I paid for things on Ebay even when the programs are not running - quite honestly its a little scary. I am not looking to hack anyone just stop what she is doing.

Any ideas on this and any remedial action? I am using a Macbook Pro running Yosemite, and also an Iphone 6

Many Thanks

Is your Iphone jailbroken and what scans etc have you run?

Kimi Räikkönen - August 28, 2015, 10:47 am

OS: Windows 7

What is happening: When I startup my PC first 5-10 minutes it's really slow and Task Manager crashes 1-3 times and Programs wont open up or they're not responding. This started happening about 3 days ago. I've run Malwarebytes scan for 4 times and it doesn't detect any viruses.

What have you done:

Honestly I have no idea how this possibly virus has come to my PC, I've only downloaded few files from sites that I deem trusted. Only have downloaded one file from Graphic designer 1 week ago.

Thank you in advance!

-Hyperion - August 28, 2015, 10:51 am

(Aug 28, 2015 10:47 AM)Kimi Räikkönen Wrote: [\[CITE\]](#) OS: Windows 7

What is happening: When I startup my PC first 5-10 minutes it's really slow and Task Manager crashes 1-3 times and Programs wont open up or they're not responding. This started happening about 3 days ago. I've run Malwarebytes scan for 4 times and it doesn't detect any viruses.

What have you done:

Honestly I have no idea how this possibly virus has come to my PC, I've only downloaded few files from sites that I deem trusted. Only have downloaded one file from Graphic designer 1 week ago.

Thank you in advance!screen shot your processes please so I can see what all is running.

Kimi Räikkönen - August 28, 2015, 11:06 am

It doesn't let me take screenshot with either windows tool or Lightshot, both not responding when starting up...

-Hyperion - August 28, 2015, 2:06 pm

(Aug 28, 2015 11:06 AM)Kimi Räikkönen Wrote: [\[CITE\]](#) It doesn't let me take screenshot with either windows tool or Lightshot, both not responding when starting up...

Please run rkill>tdsskiller and emsisoft in that order from

<https://hackforums.net/showthread.php?tid=4558828> here and post the logs.

lawton111 - August 28, 2015, 10:22 pm

Thanks for your reply.

My Iphone 6 is jailbroken and is less than 1 year old, I have now deleted FB and Messenger off it but she still has access to the Programs through the Mac. I have now deleted temp deactivated my FB account until i get this resolved. As I mentioned she still has complete access to anything over the Internet, Skype, Imessage, Viber etc.

I have no idea what scans I should run on a Mac as I wouldnt know what to run. Really appreciate your help.

Thanks

Also she even joked the other day after I changed some passwords that me changing the passwords wouldnt help, so she knew that too.

-Hyperion - August 28, 2015, 11:02 pm

(Aug 28, 2015 10:22 PM)lawton111 Wrote: [\[CITE\]](#) Thanks for your reply.

My Iphone 6 is jailbroken and is less than 1 year old, I have now deleted FB and Messenger off it but she still has access to the Programs through the Mac. I have now deleted temp deactivated my FB account until i get this resolved. As I mentioned she still has complete access to anything over the Internet, Skype, Imessage, Viber etc.

I have no idea what scans I should run on a Mac as I wouldnt know what to run. Really appreciate your help.

Thanks

Also she even joked the other day after I changed some passwords that me changing the passwords wouldnt help, so she knew that too.run this to start
<https://itunes.apple.com/us/app/bitdefender-virus-scanner/id500154009?mt=12> I will look tomorrow

Kimi Räikkönen - August 29, 2015, 5:17 am

<http://prntscr.com/8a7uyr>

That's screenshot of my processes, atiedxx.exe cannot be stopped and can't locate it at all.

lawton111 - August 29, 2015, 8:17 am

Hello,

Well i ran Bitdefender first scanning critical locations - it ran for 65minutes but declared my Mac clean of Malware. I then ran Deep system clean and again after 20 minutes it declared my Mac clean. I hope you dont think I am making this up but today she texted me to report on something else I had done on Facebook!

Many thanks in advance

-Hyperion - August 29, 2015, 10:15 am

(Aug 29, 2015 05:17 AM)Kimi Räikkönen Wrote: [\[CITE\]](#) <http://prntscr.com/8a7uyr>

That's screenshot of my processes, atiedxx.exe cannot be stopped and can't locate it at all.run this
<http://www.bleepingcomputer.com/download/roguekiller/>

Quit all running programs

Wait until the pre-scan is completed.

Accept the EULA and click Scan.

A report will be generated after the scan (you can publish it on the appropriate forum).

Click Remove.

also that is part of your graphics driver suite

(Aug 29, 2015 08:17 AM)lawton111 Wrote: [\[CITE\]](#) Hello,

Well i ran Bitdefender first scanning critical locations - it ran for 65minutes but declared my Mac clean of Malware. I then ran Deep system clean and again after 20 minutes it declared my Mac clean. I hope you dont think I am making this up but today she texted me to report on something else I had done on Facebook!

Many thanks in advance

something you had done private or something she could have seen public?

please follow these instructions

<http://www.cnet.com/how-to/how-to-use-facebooks-new-security-checkup-feature/> and setup 2FA if you have not.

lawton111 - August 29, 2015, 1:14 pm

It was a private conversation some friends and i were having on Facebook messenger - no chance she could have seen unless she had access. I have now deactivated my account until i get this sorted

Also Viber on my Iphone and Skype, and the other programs I mentioned before

Thanks

-Hyperion - August 29, 2015, 3:57 pm

(Aug 29, 2015 01:14 PM)lawton111 Wrote: [\[CITE\]](#) It was a private conversation some friends and i were having on Facebook messenger - no chance she could have seen unless she had access. I

have now deactivated my account until i get this sorted

Also Viber on my Iphone and Skype, and the other programs I mentioned before

Thanks

do what I said and enable 2fa and change all passwords that tool lets you see who is logged in

Grievous????? - August 29, 2015, 4:07 pm

OS : Windows 8.1

What is happening : My internet isn't working on my PC, it is working perfectly on my phone.

What have you done : I was messing around with my RAT, I got someone to crypt my stub and I ran it to see if it worked. It did, but when I uninstalled myself from my RAT some cmd thing kept popping up every 5 seconds for like 1 second and then disappeared again.

I have no anti virus on my pc, only my firewall.

I have no internet connection to my Pc, its being blocked or something.

-Hyperion - August 29, 2015, 5:13 pm

(Aug 29, 2015 04:07 PM)Sosuke• Wrote: [\[CITE\]](#) OS : Windows 8.1

What is happening : My internet isn't working on my PC, it is working perfectly on my phone.

What have you done : I was messing around with my RAT, I got someone to crypt my stub and I ran it to see if it worked. It did, but when I uninstalled myself from my RAT some cmd thing kept popping up every 5 seconds for like 1 second and then disappeared again.

I have no anti virus on my pc, only my firewall.

I have no internet connection to my Pc, its being blocked or something.

run rkill first found here <http://www.bleepingcomputer.com/download/rkill/>

then

run this

<http://www.bleepingcomputer.com/download/roguekiller/>

Quit all running programs

Wait until the pre-scan is completed.

Accept the EULA and click Scan.

A report will be generated after the scan (you can publish it on the appropriate forum).

Click Remove.

Post the log here

lawton111 - August 29, 2015, 10:03 pm

Hi there,

I have done as you suggested on FB, I already know she can access my FB and I know the pc she does it from is in Europe. I am trying to stop her - how will this help just knowing she can login other than reporting her to FB?

Secondly how does she have access to my Viber on my Iphone? along with the other programs I mentioned on my Mac - forgive me I am new at this but does she have a keylogger or a password breaker - am i to assume now after the Bitdefender run I dont have a RAT?

Many thanks

And now she called me to say I have visited this hack forum - unbelievable

Ethan_hunt - August 30, 2015, 4:38 am

OS: Windows 7 32-bit

What is happening: ".eml" files flooded in every folder of C: drive.

What have you done: Have tried to delete it but it comes back after some time. 1000+ files are present right now in my pc. It's size is 14.5 kb.

-Hyperion - August 30, 2015, 7:11 pm

(Aug 30, 2015 04:38 AM)Ethan_hunt Wrote: [\[CITE\]](#) OS: Windows 7 32-bit

What is happening: ".eml" files flooded in every folder of C: drive.

What have you done: Have tried to delete it but it comes back after some time. 1000+ files are present right now in my pc. It's size is 14.5 kb.

run rkill>mwb and emsisoft in order and post the logs

<https://hackforums.net/showthread.php?tid=4558828>

Mad76e - September 3, 2015, 1:16 pm

Hi -Hyperion. This is a nice gesture to the community. I do miss good ol Brotherhood :)

Nobody- - September 3, 2015, 3:34 pm

Someone keeps ratting me. I have no clue how to remove it I cant seem to find it when I go into safe mode.

-Hyperion - September 3, 2015, 3:55 pm

(Sep 3, 2015 03:34 PM)Nobody- Wrote: [\[CITE\]](#) Someone keeps ratting me. I have no clue how to remove it I cant seem to find it when I go into safe mode.

please boot into safe mode with networking and use these instructions to run Please run rkill>tdsskiller and roguekiller in that order from <https://hackforums.net/showthread.php?tid=4558828> here and post the logs.

CodZillas - September 3, 2015, 6:38 pm

Main problem: Computer freezing up and needed to be switched off at the mains, after performing simple tasks such as running a video on youtube, ustream e.g.

Other problems going along with the main problem:

Task Bar moved up by 3 for no reason.

I cannot activate the task manager.

Is my computer infected?

If so, what should I do?

?

I don't want to factory reset my computer as I have so many important files on my computer.