

Forum:[Hack Forums](#)

Thread: [CLOSED](#)

?IvNet™ - February 19, 2013, 8:37 am

CLOSED, please delete.

CLOSED, please delete.

CLOSED, please delete.

CLOSED, please delete.

CLOSED, please delete.

CLOSED, please delete.

Pendalum - February 19, 2013, 8:39 am

Great tutorial you dork keep it up ;]

?IvNet™ - February 19, 2013, 8:41 am

(Feb 19, 2013 09:39 AM)Pendalum Wrote: [\[CITE\]](#) Great tutorial you dork keep it up ;)Thanks, I actually just picked this up from a tutorial on how to see your startup and testing around with my RAT

kambatta - February 19, 2013, 9:47 am

You didn't address the persistence part of the problem. It does not matter if you delete the entry from the startup or delete the executable from the location. Until you have dealt with its persistence files, they will keep coming back.

?IvNet™ - February 19, 2013, 10:14 am

(Feb 19, 2013 10:47 AM)kambatta Wrote: [\[CITE\]](#) You didn't address the persistence part of the problem. It does not matter if you delete the entry from the startup or delete the executable from the location. Until you have dealt with its persistence files, they will keep coming back.Im not sure what you mean but I added if theres an error when deleting the source stop the process in task manager and then delete it.

Stev - February 19, 2013, 10:15 am

Looks like a decent tutorial, but it belongs in the White Hat section.

Jim Newman - February 19, 2013, 10:16 am

Thanks for this great tutorial should help many users on the forums. ?

?IvNet™ - February 19, 2013, 10:32 am

(Feb 19, 2013 11:15 AM)Kohsti Wrote: [\[CITE\]](#) Looks like a decent tutorial, but it belongs in the White Hat section.Well its mostly about RAT's. But if admin decides its the wrong section then if they can move it would be great :)

?IvNet™ - February 20, 2013, 2:04 pm

I got another method which I wont right. If you think you have a RAT and cant find it contact me.

teonanacalt - February 22, 2013, 12:13 am

Good guide and information, very useful guide.

Nice tutorial, thanks OP...appreciate.

Tiszy - February 22, 2013, 6:12 am

Nice tutorial, but keep in mind that there is binders around here, and you can also bind your server into a specific proc., which means it can be binded with all proc., and then you can't use this methods :/ All the new rats does have this function.

But overall, nice tutorial.

Vir2ListiX - February 22, 2013, 6:22 am

Nice tutorial for those who don't know or are new to this stuff.

?IvNet™ - February 22, 2013, 11:43 am

(Feb 22, 2013 07:12 AM)Tiszy Wrote: [\[CITE\]](#) Nice tutorial, but keep in mind that there is binders around here, and you can also bind your server into a specific proc., which means it can be binded with all proc., and then you can't use this methods :/ All the new rats does have this function.

But overall, nice tutorial. True, I will make another thread in a couple days or so about detecting viruses. And other stuff.

Wafflemonger - February 22, 2013, 11:44 am

Eh ... this tutorial is okay, but it won't remove the difficult RATs. Also, disconnecting your internet just stops the owner from connecting to the PC. The RAT doesn't need internet to stop you from opening up processes. Furthermore, as another poster has said, you didn't touch on the persistent factor. When you delete it, almost ALL RATs will re-add themselves and re-create themselves. Just deleting the .exe is almost pointless. Plus, there are legit processes that are those names you mentioned as well. Thanks for the most though :).