

Forum:[Hack Forums](#)

Thread: [\[Remove Rats/Check\] TCPViewer](#)

Velocity™ - August 31, 2015, 4:23 pm

So I have come across a nifty program that may help some noobies out if they believe they are being ratted or put under some virus.

Just look for any shady programs and especially using any unusual ports that the program should not be using. Also looking for default ports like 9003 (imminent) and others...

Here is a picture of a rat on my PC.

yes.exe is obviously not legit and the port is being used by something shady, So lets locate the file (for startup)

And there is the location for the rat.

This can be done through task manage, but I find this much more easier to manage and use more efficiently.

I hope I helped some newbies, fix there rat/keylogger related problems :)

note: this is not a full tutorial on removal of the rat, this just helps with a temporary solution, there may be startup and injection methods taking place.

Those who wants to download original TCPView program from Microsoft hosted website visit below website URL link.

Download TCPView:

<https://technet.microsoft.com/en-us/sysi...s/bb897437>

Burakku Kenshi - August 31, 2015, 4:24 pm

I use this method a lot :P

Velocity™ - August 31, 2015, 5:24 pm

Yeahh, it works very well, real efficient ;3

-Hyperion - August 31, 2015, 5:38 pm

This is pretty good for users who do not know how to use CMD

Freebooter - August 31, 2015, 5:39 pm

Are you trying to hide download link for Sysinternals famous TCPView program why are you not giving the original download URL link which then you don't have to make every HF member believe that your uploaded TCPView program is malware free very strange.

Those who wants to download original TCPView program from Microsoft hosted website visit below website URL link.

"Download TCPView"

<https://technet.microsoft.com/en-us/sysinternals/bb897437>

Velocity™ - August 31, 2015, 6:22 pm

(Aug 31, 2015 05:39 PM)Freebooter Wrote: [\[CITE\]](#) Are you trying to hide download link for Sysinternals famous TCPView program why are you not giving the original download URL link which then you don't have to make every HF member believe that your uploaded TCPView program is malware free very strange.

Those who wants to download original TCPView program from Microsoft hosted website visit below website URL link.

"Download TCPView"

<https://technet.microsoft.com/en-us/sysinternals/bb897437>

Apologies.

Added the correct link/description ?

bobbobbybobman - August 31, 2015, 7:04 pm

Thanks I had this some time ago and couldn't find it because forgot the name.

Velocity™ - August 31, 2015, 7:09 pm

(Aug 31, 2015 07:04 PM)bobbobbybobman Wrote: [\[CITE\]](#) Thanks I had this some time ago and couldn't find it because forgot the name.

My pleasure mate, enjoy. ?

freemium - September 1, 2015, 12:32 am

yep good one, it has "who is" too :)

Velocity™ - September 3, 2015, 12:44 am

Thanks guys for the excellent feedback