

Forum:[Hack Forums](#)

Thread: [\[TUT\] An easy way to disinfect yourself](#)

b570r - March 24, 2011, 9:50 pm

Most of the time it isn't that difficult to remove an infection. The problem is that a lot of the RATs disables the Task Manager and Regedit. In this example I'll use Security Task Manger on Windows XP.

Grab Security Task Manager from <http://www.neuber.com/taskmanager/taskmanager.html> (Any advanced task manager should work - Google it)

Install and run the task manager.

[img]<http://s2.postimage.org/43oj67v9o/taskman.jpg>[/img]

Spoiler ([Click to View](#))Image Backup

<http://postimage.org/image/k2lgesdg/>

- 1) Sort the tasks by "Rating".
- 2) Take note of the filenames.

Files that are in any of the Temp folders are 99% of the time an infection as are files with weird filenames like "asdYww8.exe". In this example I've infected myself with DarkComet and as you can see on line one of the screenshot the filename is twunk32.exe .The correct filename for this Windows file is twunk_32.exe in that same folder so I suggest that you get to know the process names on your PC.

- 3) Take note of the process details.

Normal programs are a lot more open and descriptive so pay attention. Look at some of the other processes to see what the differences are.

- 4) Look at the properties.

As you can see in this example DarkComet doesn't have visible windows, has no description, is an unknown file in the widows folder, is not a windows system file, starts when the computer starts and have some very suspicious functions like monitor and record input. These are all signs of a RAT. Once again compare the properties from different processes and you'll quickly learn the difference.

- 5) Click on the "Remove" button and select "Move file to quarantine".

Be careful not to quarantine the wrong files though, it could cause more problems than intended.

Play around with the task manager of your choice and you will be able to disinfect yourself in record time. I only have a Windows XP VM running but the same goes for Vista and Windows 7.

Note: All the motivational credit for writing this tut goes to the dumbass who tricked me on youtube when I first started working with RATs. Nice work @ssh0le!

phybe? - March 24, 2011, 9:53 pm

This is useful when infecting yourself by accident, nice work.

Jaxon - March 24, 2011, 10:16 pm

yea thanks. very useful if i ever get infected :P

Daveyjones - March 25, 2011, 12:43 am

Thanks, nice post, that will help some people :)

Kamehamehaaaa - March 25, 2011, 12:45 am

Looks cool thank you =) i love the warning% of processes

Corsican - March 25, 2011, 1:55 am

Excellent post! Gonna try it right now.