

Forum:[Hack Forums](#)

Thread: [What is a Rootkit and how do you remove it?](#)

Noahfallon - January 4, 2015, 4:33 pm

Hi guys -

I was just wondering what exactly a rootkit is and does to a computer. I'm also interested in knowing how to remove one just in case I need to do that some day for some reason. For example, what is the Ring-3 rootkit and what about the Ring-0 rootkit? What are the differences between them?

Thank you in advance!! :)

AruCard - January 4, 2015, 4:34 pm

stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
<https://en.wikipedia.org/wiki/Rootkit>

ask aura, he says i dont know what to do so PM him

Aura - January 4, 2015, 4:35 pm

(Jan 4, 2015 05:34 PM)AruCard Wrote: [\[CITE\]](#) stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Nice copy/paste : <https://en.wikipedia.org/wiki/Rootkit>

To be honest, Wikipedia have a pretty good article on "protection rings", even beginners should understand it:

https://en.wikipedia.org/wiki/Protection_ring

Also, there's a few tools that specializes in removing rootkits such as Malwarebytes Anti-Rootkit, RogueKiller, TDSSKiller, etc. But if you don't know how to use them, it's useless.

Awakened - January 4, 2015, 4:37 pm

(Jan 4, 2015 05:35 PM)Aur? Wrote: [\[CITE\]](#) Also, there's a few tools that specializes in removing rootkits such as Malwarebytes Anti-Rootkit, RogueKiller, TDSSKiller, etc. But if you don't know how to use them, it's useless.

+1 for Malwarebytes and their Anti-Rootkit!

Here's an explanation of the differences between some of the types of malicious software:

<http://www.guidingtech.com/8888/difference-between-malware-virus-rootkits-trojans-worm-spyware/>

Noahfallon - January 4, 2015, 4:51 pm

(Jan 4, 2015 05:35 PM)Aur? Wrote: [\[CITE\]](#) Nice copy/paste : -SNIP- no links until 50 posts.

To be honest, Wikipedia have a pretty good article on "protection rings", even beginners should understand it:

-SNIP- Can't post links ATM.

Also, there's a few tools that specializes in removing rootkits such as Malwarebytes Anti-Rootkit, RogueKiller, TDSSKiller, etc. But if you don't know how to use them, it's useless.

Thank you for the quick answers guys!!

About Malwarebytes Anti-Rootkit:

I actually had to use that program very recently (January 1st of 2015) because something, I never figured out what exactly caused it, opened a BUNCH of different, random Windows .exe's, such as FIXMAPAPI, DLLHOST (I think that one was present) and a few other processes. But the thing is, is that each process (About 3 or 4 of them) each had a bunch of their own processes open at the same time. (Multiple FIXMAPAPI.exe's and along with the other processes.) I had tried to end them via task manager with "End process tree" but they kept coming back. It slowed my computer down to the point where I could barely do anything, and it took so long. I had to be really patient and download MBAR and then it had to RUN, which took 45 minutes. Not to mention it literally made my CPU run at 90-100% usage constantly. It cleaned up everything, though and everything is back to normal so I'm thankful for that.

I'll definitely read up on that rootkit stuff as well. Thanks!!

Aura - January 4, 2015, 6:08 pm

(Jan 4, 2015 05:51 PM)Noahfallon Wrote: [\[CITE\]](#) Thank you for the quick answers guys!!

About Malwarebytes Anti-Rootkit:

I actually had to use that program very recently (January 1st of 2015) because something, I never figured out what exactly caused it, opened a BUNCH of different, random Windows .exe's, such as FIXMAPAPI, DLLHOST (I think that one was present) and a few other processes. But the thing is, is that each process (About 3 or 4 of them) each had a bunch of their own processes open at the same time. (Multiple FIXMAPAPI.exe's and along with the other processes.) I had tried to end them via task manager with "End process tree" but they kept coming back. It slowed my computer down to the point where I could barely do anything, and it took so long. I had to be really patient and download MBAR and then it had to RUN, which took 45 minutes. Not to mention it literally made my CPU run at 90-100% usage constantly. It cleaned up everything, though and everything is back to normal so I'm thankful for that.

I'll definitely read up on that rootkit stuff as well. Thanks!!

Malwarebytes Anti-Rootkit is quite useful, yes. If you want, that technology is now included in Malwarebytes Anti-Malware, so you don't have to install both products on your system in order to do a "Rootkit" scan.

Enthusiastic - January 4, 2015, 6:47 pm

basically you need to remove it from startup

Aura - January 4, 2015, 6:50 pm

(Jan 4, 2015 07:47 PM)Enthusiastic Wrote: [\[CITE\]](#) basically you need to remove it from startup

It's a bit more complicated than that to be honest. The ... "concept" of Startup is good, but it's bit more in-depth than that.