

Forum:[Hack Forums](#)

Thread: [?? \[INFO\] All about Malware - ROOTKITS ! \[INFO\] | Learning ??](#)

Madara-Uchiha - March 23, 2013, 5:41 am

ALL ABOUT MALWARE

- Rootkits -

Introduction:

Hey Guys, welcome to my second tutorial here on HF. Well, I planned to make a series about Malware. In my threads I will explain how they work, what they are, how you could protect yourself from the type of malware that I discuss in the thread. Well in this thread I like to explain you everything I know about rootkits. I hope I could help you with this tutorial and you will learn something from it ;) Enjoy!

Definition:

A rootkit is a stealthy type of malware which is used to hide processes, programs and registry keys from the user. A rootkit installation could be automatic or a hacker could install it on victims computer. Once they've obtained root/Administrator access, they start to hide something. A rootkit is not an exploit! A rootkit could get full control over a system and can modify everything, normally the system.

How does a rootkit work?

To explain how a rootkit works, I need to explain first how an application normally works on your computer. Let's take the timer application as an example.

[img]http://s14.directupload.net/images/130323/vyoxut2a.jpg[/img]

The timer shows you the current time.

[img]http://s14.directupload.net/images/130323/c83ka8gz.jpg[/img]

But to get the timer know what's the current time, the timer needs to know it from the system. But the timer is not allowed to get access to the system clock. But the timer is allowed to ask windows or better: the API (Application Programming Interface). Well our clock wants to know the time. The clock uses the function in the API to get time. The API can now access to the system clock to read out the current time.

[img]http://s14.directupload.net/images/130323/m2slh6c7.jpg[/img]

The system gives us the response over the API and our clock application can tell us the current time:

[img]http://s7.directupload.net/images/130323/ayqtjdig.jpg[/img]

Every application works like that. There's no exception.

Another example:

After clicking a folder we could see what files are into. It works the same way as above.

[img]<http://s14.directupload.net/images/130323/aydze3zt.jpg>[/img]

Our explorer wants to know what files are on C:\ so it has to ask the API. The API tells the system to list all files on C:\.

[img]<http://s1.directupload.net/images/130323/iuifytzw.jpg>[/img]

The system gives us the response over the API and our explorer can display us all files on C:\

[img]<http://s14.directupload.net/images/130323/hfrpp9sb.jpg>[/img]

**

Now let's see what happens when our system is infected with a rootkit. We take the same example as before, where the explorer displays us the files on C:\.

(The red bug in the image is the rootkit)

The rootkit makes just one thing at startup. It modifies the Enum-File API. The rootkit sets a "Jump-Point" at the Enum-Files-API. (The "Jump-Point" is the red area at the API)

[img]<http://s14.directupload.net/images/130323/33uzx8ca.jpg>[/img]

Now our explorer should display us the files on C:\ so it asks the Enum-Files API. But we know that our Enum-Files API has a new "Jump-Point" and the API did not ask the real system function to read out the files on C:\ instead it asks one of the rootkit DLL's.

[img]<http://s7.directupload.net/images/130323/ox2bbxia.jpg>[/img]

The rootkit DLL asks now the real Enum-Files-Function. And the real Enum-Files API gets the list of all files on C:\

[img]<http://s1.directupload.net/images/130323/29irdq94.jpg>[/img]

We could now see there are all Files and also the File named "Virus.exe".

This is the file the rootkit wants to hide from the User and also from the antivirus software. So it deletes the Virus.exe file from the list. (It does not delete the file itself it just deletes the entry in the list.)

The filtered List without the Virus.exe file goes back to the real Enum-Files API and the real Enum-Files API sends the filtered list back to our explorer. The explorer displays all files, but NOT the Virus.exe file!

I hope you could understand now how a rootkit works in general.

That's the same thing if you antivirus software scans your computer. If the computer is infected with a rootkit, the program could not detect the rootkit because he could not see it. The antivirus scans only a modified files by the rootkit.

[img]<http://s1.directupload.net/images/130323/exyh2tdh.jpg>[/img]

Types of rootkits

There are different Types of rootkits. Here is a list:

Kernel-Based:

Typically, kernel-based rootkits are codes that are able to mask themselves under the operating system's loadable modules and device drivers. Because these rootkits are incorporated inside important components, detecting them can be difficult. A kernel-based rootkit rewrites and modifies the kernel's code to stay hidden and manipulate every facet of the operating system. Because it is within the kernel, it has pretty much unrestricted movement within the system. Some popular malicious kernel-based rootkit examples in Windows are TR/Rootkit.Gen, W32.Focelto.A and Haxdoor rootkits.

Application-Based:

Application-based rootkits are pretty common. They find their way into a computer system through the installation or updating of software, such as word-processing, graphics-editing, gaming and other commonly used computer programs. These rootkits come in the form of an application library file that will be associated with the application installed. It will modify the behavior of the application to escape detection and do what it was written to do. For example, when using a Windows-based system, you will often encounter this threat by way of a suspicious .DLL file. The rootkit will then replicate certain processes to evade detection while it captures information in the system. Application-based rootkits are easier to manage than some other types, since most system-protection software constantly updates definitions to include these types of malicious codes.

Firmware-Based:

A firmware-based rootkit is a code specifically designed to create a permanent instance of the Trojan or malware in a device through its firmware--a combination of hardware and software, such as computer chips. For example, a simple residential DSL router uses firmware. If its firmware is compromised by a rootkit, there's really no way to detect it and the damage it can cause can be enormous, especially since all of the data you send and receive online passes through the router. Basically, there are only two ways a rootkit can embed itself in the firmware of a specific hardware--through a firmware update or through purchase, where the seller purposely installs the rootkit before selling it.

Virtual:

Considered to be low-level threats, virtual or virtualized rootkits hijack and modify a system and boot it up to appear as a virtual machine. This will allow the rootkit to capture data from the hardware as a guest machine requests it. While these types of rootkits aren't common, it is a vulnerability that Microsoft and Linux are aware of.

Source: [Rootkit Types](#)

The first rootkits:

Here is a short List with some of the first rootkits for windows ever made:

Year 2000 – he4hook

This tool was developed by a Russian programmer. It works in Kernel mode and hides files. The author itself doesn't say it's a rootkit.

Year 2002 – HackerDefender

The HackerDefender is also a tool, but a more powerful one. You can use it over a configuration file to hide files, processes, Services and registry keys. It also works in Kernel mode.

Year 2003 – Vanquish

The tool vanquish could also be used to hide files, directories, processes and registry keys. It could also record the passwords on a user's computer. This rootkit is usermode based.

How to detect rootkits?

There are different methods of detecting rootkits. But only a good antivirus software could do this, you as normal user are not able to find a rootkit if it's well hidden. You could never detect a rootkit and be 100% sure it is one. There are some plausibility tests to detect a rootkit.

Here are some methods the most antivirus software uses to detect rootkits on a computer:

Alternative trusted medium:

The best and most reliable method for operating-system-level rootkit detection is to shut down the computer suspected of infection, and then to check its storage by booting from an alternative trusted medium (e.g. a rescue CD-ROM or USB flash drive). The technique is effective because a rootkit cannot actively hide its presence if it is not running.

Behavior method:

This method is just looking for rootkit behavior which means hooking API to hide something. This method has a high rate of false positives.

Signature based:

The signature based method is using a stealth detector. If rootkit attempts to hide or unload itself during a virus scan the signature detection or fingerprinting can still find it. That's why the programmer of a rootkit often try's to implement counterattack methods into the rootkit which means to kill the antivirus process or service.

Sources:

<http://www.technibble.com/how-to-remove-a-rootkit-from-a-windows-system/>
<http://en.wikipedia.org/wiki/Rootkit#Detection>
http://www.ehow.com/info_8041976_list-rootkits.html
<http://www.ethicalhacker.net/content/view/10/2/>
<https://www.youtube.com/watch?v=bv2usm1zLko>
<http://www.techrepublic.com/blog/10things/10-things-you-should-know-about-rootkits/416>

Please leave a thanks if you've enjoyed my informative thread ?

Madara-Uchiha

y8tvkid - March 23, 2013, 8:25 am

EWWW i hate malware AVG is WAY better

Madara-Uchiha - March 23, 2013, 8:44 am

I'm not sure if you understand this thread?

It should explain you how a rootkit works in detail, and not a discussion about AVG .__.

Nephist - March 23, 2013, 8:49 am

(Mar 23, 2013 08:25 AM)y8tvkid Wrote: [\[CITE\]](#) EWWW i hate malware AVG is WAY better This is another HQ thread, not for you to be saying "EWW" in the comments.

Madara-Uchiha - March 23, 2013, 9:20 am

(Mar 23, 2013 08:49 AM)Nephist Wrote: [\[CITE\]](#) This is another HQ thread, not for you to be saying "EWW" in the comments.

Thank you very much ?

If you have any suggestions for improvement, please let me know.

Wires - March 23, 2013, 9:22 am

Haven't had a chance to read through ALL of this, taking my time with it. Looks good so far.

BlueShocks - March 23, 2013, 9:49 am

Looks Pretty Good, Shows a lot of work and time nice job.

Madara-Uchiha - March 23, 2013, 9:55 am

(Mar 23, 2013 09:49 AM)BlueShocks Wrote: [\[CITE\]](#) Looks Pretty Good, Shows a lot of work and time nice job.

Thank you! Yeah, it was a lot of work and a lot of reading webpages..

But now I finally put all information I've collected together in this thread :D

Ch1m4zz - March 23, 2013, 10:17 am

hey u EEW guy seriously u think we are talking about antivirus's

-_- N00b

Acroz - March 23, 2013, 10:21 am

Good thread. Great start on tutorials.

Almost Einstein - March 24, 2013, 8:15 am

Awesome tutorial, thanks alot of this! <3

Zatch11 - March 24, 2013, 9:01 am

Nice job, seems like alot though, I think I'll fully read this another time.

Cydp3 - March 24, 2013, 10:37 am

HQ thread, really good for learning!

Madara-Uchiha - March 24, 2013, 11:29 am

No, problem guys, your welcome!

I will make also a thread for other types of malware too in a week or so... ?

Klarion - March 24, 2013, 3:09 pm

just what I've been looking for :)

can you tell me what can I use rootkit for? can I bind it to my RAT server so it hides the server's process, startup key from registry?

lowkasen - March 24, 2013, 3:48 pm

wow nice guide on malware!!! thanked!

Madara-Uchiha - March 24, 2013, 3:58 pm

I'll highly recommend you to use HackerDefender. Just spread your Rat-Server normally and after you got access to the victims computer install the configured HackerDefender.

With HackerDefender you can hide your Servers Process, registry key, msconfig entry and its service.

Madara-Uchiha

HighARc - March 24, 2013, 9:27 pm

Great thread, good info, Learned alot from reading this! Thanks for contributing!

Madara-Uchiha - March 25, 2013, 1:51 am

No Problem, I am glad you like it ?

Huziwara - March 25, 2013, 3:55 am

Wow, nice tutorial !

Gives me a lot of ideas for the PoC backdoor/rootkit I am doing.

Thank you !

mmgun66 - March 25, 2013, 6:38 am

Looks Pretty Good, Shows a lot of work and time nice job.

yfinley - March 27, 2013, 6:41 pm

Hey thanks! This is a really informative thread.

Madara-Uchiha - March 28, 2013, 5:05 pm

(Mar 27, 2013 06:41 PM)yfinley Wrote: [\[CITE\]](#) Hey thanks! This is a really informative thread.

I am glad you like it. I hope it helped you ?

on-silo - March 28, 2013, 5:11 pm

Great info and you actually listed sources, please hang around... we need more people like you.

Angryflash - March 28, 2013, 10:23 pm

I was confused about exactly what rootkits are and how they work. Thank you for clearing that up for me.

Madara-Uchiha - March 30, 2013, 3:42 am

That's the reason why I made this thread ;D

I've now finished my thread about computer worms..

Leon_V._Metcalf - March 30, 2013, 11:39 am

(Mar 23, 2013 08:25 AM)y8tvkid Wrote: [\[CITE\]](#) EWWW i hate malware AVG is WAY better

??? Seriously? I have nothing to say to you.

OP: This is a great post. I hope it educates users better about the functionality of rootkits. Keep up the good work!

tho475 - March 30, 2013, 11:59 am

thanks for the help i apprecieted :)

Lane_Stalker - March 30, 2013, 12:01 pm

the ultimate thread for understanding Rootkits and Malwares..
nice thread OP

ahsan001 - April 2, 2013, 1:50 pm

So far i found 3 malware infections the scan is still going on i had no idea what malware/rootkit is, until u posted in my thread about blue screen error thanks alot, i will keep u updated.

Madara-Uchiha - April 2, 2013, 1:55 pm

No problem I am glad I could help you.
Rootkits often causes BSOD's on x64 systems.
Maybe you could post the scanresult after the scan is finished?:)

Klarion - April 2, 2013, 4:32 pm

hey mate, I have a problem, I can't double click to open my drives (C:, D:) and also some other folders. Do you think this is caused by a rootkit? And if yes how do I remove it? I've searched for malicious processes with Security Task Manager but haven't found any... The double click problem goes away when I remove the registry entry called 'mountpoints2', but it always comes back after couple of minutes...

Madara-Uchiha - April 2, 2013, 4:49 pm

I am on my mobile now and very sleepy, so excuse grammar fails :D

- 1) Rootkits normally just hide something (Regkeys, Processes, Files and Services.
- 2) I don't think its a rootkit cuz if the problem depends on the registry key mountpoints2 that means you are able to see this regkey. If it is a rk it would hide it.
- 3) Try to open the drives with a double click on the right mouse button (maybe you got ratted and the hacker swapped your mouse buttons.
- 4) Try to access your drive with arrow keys and the enter key.
- 5) Run a full scan with Malwarebytes Anti malware and one with Malwarebytes Anti Root kit. They are free just download them.
- 7) have a look for suspect startup entry's .

I don't think this is a rootkit and if it is malware than it is a rat. Do a fullscan with Malwarebytes. If the problem still stays contact me tomorrow and I will try to help you out.

soul rebel - April 2, 2013, 6:29 pm

HQ thread, thanks for the good info. without those pics i wouldnt have understood it lol.

(Apr 2, 2013 04:32 PM)satryiasis19 Wrote: [\[CITE\]](#) hey mate, I have a problem, I can't double click to open my drives (C:, D:) and also some other folders. Do you think this is caused by a rootkit? And if yes how do I remove it? I've searched for malicious processes with Security Task Manager but haven't found any... The double click problem goes away when I remove the registry entry called 'mountpoints2', but it always comes back after couple of minutes...

my advice is to instal ubuntu! fuck windows and virus's! something like that happened to me and i decided i didnt want to put up with malware, never using windows again

ahsan001 - April 2, 2013, 8:43 pm

(Apr 2, 2013 01:55 PM)Madara-Uchiha Wrote: [\[CITE\]](#) No problem I am glad I could help you.
Rootkits often causes BSOD's on x64 systems.
Maybe you could post the scanresult after the scan is finished?:)
found 6 infections :P so far so good no BSOD yet. thnx

scan logSpoiler ([Click to View](#))Malwarebytes Anti-Rootkit BETA 1.01.0.1022

Database version: v2013.04.02.13

Windows 7 x64 NTFS (Safe Mode/Networking)

Internet Explorer 8.0.7600.16385

Ahsan :: AHSAN-PC [administrator]

4/2/2013 22:25:29

mbar-log-2013-04-02 (22-25-29).txt

Scan type: Quick scan

Scan options enabled: Memory | Startup | Registry | File System | Heuristics/Extra |
Heuristics/Shuriken | PUP | PUM | P2P

Scan options disabled:

Objects scanned: 31667

Time elapsed: 42 minute(s), 45 second(s)

Memory Processes Detected: 0

(No malicious items detected)

Memory Modules Detected: 0

(No malicious items detected)

Registry Keys Detected: 4

HKLM\SOFTWARE\WOW6432NODE\CLASSES\CLSID\{537C9B79-38B5-AB8F-FFCF-0A7DA9E641A8} (Adware.MultiPlug) -> Delete on reboot.

HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\BROWSER_HELPER_OBJECTS\{537C9B79-38B5-AB8F-FFCF-0A7DA9E641A8}
(Adware.MultiPlug) -> Delete on reboot.

HKLM\SOFTWARE\WOW6432NODE\CLASSES\CLSID\{DE62DE1C-E938-0E32-3025-3100331BDD09} (Adware.MultiPlug) -> Delete on reboot.

HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\BROWSER_HELPER_OBJECTS\{DE62DE1C-E938-0E32-3025-3100331BDD09}
(Adware.MultiPlug) -> Delete on reboot.

Registry Values Detected: 0

(No malicious items detected)

Registry Data Items Detected: 0

(No malicious items detected)

Folders Detected: 0

(No malicious items detected)

Files Detected: 2

c:\ProgramData\Browse22save\51547299d2d79.dll (Adware.MultiPlug) -> Delete on reboot.

c:\ProgramData\SeaRcchy-NewTTab\515472d731281.dll (Adware.MultiPlug) -> Delete on reboot.

(end)

Phoeni? - April 4, 2013, 2:55 pm

High Quality thread, Keep it up. ?

XmysteriousX - April 4, 2013, 3:24 pm

thanks for tuto i didn't know much about Malware :)

Madara-Uchiha - April 4, 2013, 3:32 pm

Thank you guys. I'll keep my work up :) The next informative thread will be about Keyloggers I think :)

_Renegade - April 4, 2013, 4:08 pm

This Thing Is Awesome! I Use It Most Of The Time Really Helpful

Orochimaru - April 4, 2013, 7:56 pm

You should also write down about Ring-0/Ring-3 Rootkits etc, and how ring0 affects Kernel Mode of a PC and all that information, good job with the information though!

Madara-Uchiha - April 5, 2013, 4:46 pm

Yeah I will add this these days...

Thx for reminding me :)

DesuDesu - April 5, 2013, 10:35 pm

Very interesting, thanks for putting the time in to write it :).

Dude4019 - April 6, 2013, 12:02 pm

This is really informative and I've learned a lot from this. Thank you for posting this! ?

Madara-Uchiha - April 6, 2013, 3:59 pm

Thank you guys. If you have any questions, feel free to ask me ;)

sasue11 - April 21, 2013, 1:53 pm

How would you remove one without av/reformatting?

Madara-Uchiha - April 21, 2013, 1:59 pm

It's hard. Because normally you won't detect it without AV.

Maybe you can look if it does not hide a port. Then it would be suspicious: an application which "doesn't exist" but using a port...

But hard to find without good software and also hard to remove.

Sucker for pain - September 17, 2013, 11:34 am

really HQ post, thanks for this :)

hope u make some more :)

huff - September 17, 2013, 11:35 am

Wow Pretty HQ bro Keep it up! ?

Madara-Uchiha - September 17, 2013, 12:27 pm

I am glad u liked it.

It should explain the structure how rootkits work.

I made a thread for worms too, u can look there if u are interested how worms work ;)

SIM-1456245 - November 10, 2013, 11:45 am

Sorry for making this thread by grave digging it, but it's just the thing that I needed. Thank you bro, it's awesome.

Madara-Uchiha - November 11, 2013, 2:57 pm

I am glad you learned something:) enjoy it^^