

Forum: [Hack Forums](#)

Thread: [Rootkit bins would anyone buy?](#)

kingroot - January 2, 2014, 7:55 pm

Would anyone buy a rootkit module for their malware? I will be able to execute your file in the memory space of another process no RUNPE this will inject into an existing process
Works both on x64 and x86.

This rootkit will hide your file from explorer, cmd, task mgr, regedit. You also have an option to create a 'system wide injection' where it will inject into every x64 & x86 process. It will check if the process is hooked first before injecting the code.

I'm looking for around \$100 a bin.

Tackled - January 2, 2014, 7:56 pm

what price would you be looking for, this sounds quite good

kingroot - January 2, 2014, 8:05 pm

(Jan 2, 2014 08:56 PM)MastersLobbies Wrote: [\[CITE\]](#) what price would you be looking for, this sounds quite good

Around \$100 a bin, it works on all x86 processes and x64 processes.

Also forgot to mention if the file is not executed via admin it will prompt them with UAC to open up command prompt, similar to betabot. I mean this is an ingenious way to manipulate the victim

Crake - January 2, 2014, 8:10 pm

You'd need a L33t or Ub3r to sell for you, of course. \$100 might be a bit much for this market, though, they don't tend to have that much loose change.

kingroot - January 2, 2014, 8:14 pm

(Jan 2, 2014 09:10 PM)emanb29 Wrote: [\[CITE\]](#) You'd need a L33t or Ub3r to sell for you, of course. \$100 might be a bit much for this market, though, they don't tend to have that much loose change. If i get positive feedback i myself will purchase l33t and sell this

Uncle Ruckus - January 2, 2014, 9:54 pm

(Jan 2, 2014 09:10 PM)emanb29 Wrote: [\[CITE\]](#) You'd need a L33t or Ub3r to sell for you, of course. \$100 might be a bit much for this market, though, they don't tend to have that much loose change. Why would he need an upgraded member to? You're encouraging him to proxy sell which isn't allowed.

?ain - January 2, 2014, 9:58 pm

\$100 is a bit overpriced. Does it come with anything else?

kingroot - January 2, 2014, 10:15 pm

(Jan 2, 2014 10:58 PM)G0dOf4ll Wrote: [\[CITE\]](#) \$100 is a bit overpriced. Does it come with anything else?

I personally think \$100 is underpriced. ? Well i mean it acts as a 'crypter' with a rootkit.

xhflhkeuhwguu34 - January 2, 2014, 10:19 pm

You're not trusted at all, so you'll need to work on your stats a bit before trying this...

Honestly if you can do this, without c+ping code from the internet, \$75 per bin is reasonable.

kingroot - January 2, 2014, 10:19 pm

(Jan 2, 2014 11:19 PM)Xenon Wrote: [\[CITE\]](#) You're not trusted at all, so you'll need to work on your stats a bit before trying this...

Honestly if you can do this, without c+ping code from the internet, \$75 per bin is reasonable.
Well can't really copy and paste heaven gate methods

xhflhkeuhwguu34 - January 2, 2014, 10:20 pm

(Jan 2, 2014 11:19 PM)kingroot Wrote: [\[CITE\]](#) Well can't really copy and paste heaven gate methods
<http://www.ic0de.org/archive/index.php/t-11525.html>

?ain - January 2, 2014, 10:21 pm

(Jan 2, 2014 11:15 PM)kingroot Wrote: [\[CITE\]](#) I personally think \$100 is underpriced. ? Well i mean it acts as a 'crypter' with a rootkit.

Crypter? So this FUDs your file (or at least UD), and also gives it rootkit? Not bad. I'd like to see this in action first.

kingroot - January 2, 2014, 10:22 pm

(Jan 2, 2014 11:20 PM)Xenon Wrote: [\[CITE\]](#) <http://www.ic0de.org/archive/index.php/t-11525.html>
That's just an example, which seems to be in ASM. You'd have to understand what the concept is at hand to apply it to major functions. Yet alone an ENTIRE pe. MSDN is an exemplar.

Crake - January 2, 2014, 10:23 pm

(Jan 2, 2014 11:19 PM)Xenon Wrote: [\[CITE\]](#) You're not trusted at all, so you'll need to work on your stats a bit before trying this...

Honestly if you can do this, without c+ping code from the internet, \$75 per bin is reasonable. This is exactly why, in response to whoever was asking

kingroot - January 2, 2014, 10:26 pm

I don't mind providing live demos to prove this programs legitimacy. I'm just curious if there would be any buyers for this price.

betamonkey - January 2, 2014, 10:29 pm

Is this a user mode or kernel mode rootkit? In either case, how will it know what file(s) and process(es) and thread(s) to protect? I'm assuming whatever it is packaged with will need to be altered (by the author no doubt) to work with your product? If that is the case, for this to be successful, you need to be very proactive in having people work with you on this.

kingroot - January 2, 2014, 10:35 pm

(Jan 2, 2014 11:29 PM)betamonkey Wrote: [\[CITE\]](#) Is this a user mode or kernel mode rootkit? In either case, how will it know what file(s) and process(es) and thread(s) to protect? I'm assuming whatever it is packaged with will need to be altered (by the author no doubt) to work with your product? If that is the case, for this to be successful, you need to be very proactive in having people work with you on this.

user mode, i deem a kernel rootkit useless unless you have some bypass methods for a licensed certificate.. also patchguard is a problem too, sure you can create kernel hooks without bypassing patchguard but it's just too much. for now i'm just making sure the hook is in place for both x86 and x64 processes, if not then proceed to inject. This isn't efficient but i'm working at ease. The files i'm

protecting only use the imagename for now (can easily be bypassed by changing the filename, the average person won't know this) but i'm going to have to make this more secure to prevent future cleanup. I can take up this project by myself for now that is. I've been working on it for the past four days so don't expect much at this point. I'm not using any third party software for these hooks, no mhook, no detours. As for the injection, i'm copying the entire pe image over to memory i've allocated, handling relocation of pointers and imports then creating a remote thread for my function which would be located from my (distance from base)(Function - ModuleBase) + (otherprocessesnewmodulebase)(added onto the allocated memories base for the address to point at our function). As for the hooks, i'm currently hooking ntquerysysteminformation and ntquerydirectoryfile & findnextfile

betamonkey - January 2, 2014, 10:43 pm

CreateRemoteThread isn't going to go over well with decent antivirus solutions' HIPS. Also, how can you protect bots who install using random filenames? Most malware does that.

Honestly dude, this isn't worth much unless it can provide wide protection for more than just a static file name. And it needs effective HIPS bypass. This thing has 1 function, and that's to inject code systemwide and hook relevant functions to protect payload resources. You can't possibly justify a higher price for something that doesn't perform its sole function very well.

kingroot - January 2, 2014, 10:48 pm

(Jan 2, 2014 11:43 PM)betamonkey Wrote: [\[CITE\]](#) CreateRemoteThread isn't going to go over well with decent antivirus solutions' HIPS. Also, how can you protect bots who install using random filenames? Most malware does that.

Honestly dude, this isn't worth much unless it can provide wide protection for more than just a static file name. And it needs effective HIPS bypass. This thing has 1 function, and that's to inject code systemwide and hook relevant functions to protect payload resources. You can't possibly justify a higher price for something that doesn't perform its sole function very well.

Well yet again, don't see anything on these forums that go beyond this project. As for the malware, i'll be executing it in memory of another processes memory space that being said.. i'd only have to protect the stub. If that said malware has drops, it's not my problem. The person using this rootkit can provide multiple file names if needed

betamonkey - January 2, 2014, 10:54 pm

(Jan 2, 2014 11:48 PM)kingroot Wrote: [\[CITE\]](#) Well yet again, don't see anything on these forums that go beyond this project. As for the malware, i'll be executing it in memory of another processes memory space that being said.. i'd only have to protect the stub. If that said malware has drops, it's not my problem. The person using this rootkit can provide multiple file names if needed

Ok, well here, take this for example: Plasma, which doesn't inject into anything is binded with your kit. Upon installation, where it would normally install fine, your injection causes the AV to start bitching and removing files. You just made an otherwise working bot less reliable. That's really why effective HIPS bypass is necessary here.

You're right, there is nothing else here that is the same as your project. But that doesn't mean you're going to get rave reviews and lots of sales if you release something that doesn't work well or as intended.

Anyway good luck with your project.

kingroot - January 2, 2014, 10:58 pm

(Jan 2, 2014 11:54 PM)betamonkey Wrote: [\[CITE\]](#) Ok, well here, take this for example: Plasma, which doesn't inject into anything is binded with your kit. Upon installation, where it would normally

install fine, your injection causes the AV to start bitching and removing files. You just made an otherwise working bot less reliable. That's really why effective HIPS bypass is necessary here.

You're right, there is nothing else here that is the same as your project. But that doesn't mean you're going to get rave reviews and lots of sales if you release something that doesn't work well or as intended.

Anyway good luck with your project.

I've actually never intended this project to protect from AVs but i'll have a look at mcafee for now and see if i can find any methods to overcome HIPS then move onto the next av. that being said i'd be increasing the price. I've read this article

<http://rce.co/why-usermode-hooking-sucks-bypassing-comodo-internet-security/> and already feel like shit

betamonkey - January 2, 2014, 11:10 pm

(Jan 2, 2014 11:58 PM)kingroot Wrote: [\[CITE\]](#) I've actually never intended this project to protect from AVs but i'll have a look at mcafee for now and see if i can find any methods to overcome HIPS then move onto the next av. that being said i'd be increasing the price. I've read this article <http://rce.co/why-usermode-hooking-sucks-bypassing-comodo-internet-security/> and already feel like shit

You misunderstood me.. I didn't say protect FROM avs. I said that by you using CreateRemoteThread and other very well known and detected injection methods, you actually cause a reliable piece of software to get detected when it otherwise wouldn't.

That's why I kept bringing up HIPS bypass.

kingroot - January 2, 2014, 11:17 pm

(Jan 3, 2014 12:10 AM)betamonkey Wrote: [\[CITE\]](#) You misunderstood me.. I didn't say protect FROM avs. I said that by you using CreateRemoteThread and other very well known and detected injection methods, you actually cause a reliable piece of software to get detected when it otherwise wouldn't.

That's why I kept bringing up HIPS bypass.

i mean it's 2013, what would you reckon i do at the user mode level

betamonkey - January 2, 2014, 11:19 pm

(Jan 3, 2014 12:17 AM)kingroot Wrote: [\[CITE\]](#) i mean it's 2013, what would you reckon i do at the user mode level

Huh? There are ways of injecting code without setting of antiviruses. Lots of bots, mine included, do it. I'm just saying you need to do similar things.

The entire purpose of your product relies around injecting code, so don't you think if that is it's only real job, it should do it well?

kingroot - January 2, 2014, 11:30 pm

(Jan 3, 2014 12:19 AM)betamonkey Wrote: [\[CITE\]](#) Huh? There are ways of injecting code without setting of antiviruses. Lots of bots, mine included, do it. I'm just saying you need to do similar things.

The entire purpose of your product relies around injecting code, so don't you think if that is it's only real job, it should do it well? I have a few ideas.

I'll be looking into using ZwQueueApcThread

Qmz_ - January 3, 2014, 12:30 am

I personally wouldn't buy it. But if you build around it a basic herding bot with just few "features", a lot of people would probably buy it.

Tackled - January 3, 2014, 8:42 am

(Jan 3, 2014 12:17 AM)kingroot Wrote: [\[CITE\]](#) i mean it's 2013, what would you reckon i do at the user mode level

Sorry to disappoint you, but it is 2014 :p

kingroot - January 3, 2014, 12:52 pm

(Jan 3, 2014 09:42 AM)MastersLobbies Wrote: [\[CITE\]](#) Sorry to disappoint you, but it is 2014 :pahhh that new years.... i've been no lifing for too long my friend ?

Anyways i can confirm what i have so far works on vista x64, windows 8, windows 7

Tackled - January 3, 2014, 12:53 pm

(Jan 3, 2014 01:52 PM)kingroot Wrote: [\[CITE\]](#) ahhh that new years.... i've been no lifing for too long my friend ?

Anyways i can confirm what i have so far works on vista x64, windows 8, windows 7

With Rootkit, it is extremely hard to remove the file? Correct?

kingroot - January 3, 2014, 12:56 pm

(Jan 3, 2014 01:53 PM)MastersLobbies Wrote: [\[CITE\]](#) With Rootkit, it is extremely hard to remove the file? Correct?

I've disabled ntquerydirectoryfile and ntquerysysteminformation from locating your file. This is any process. x86 & x64. And of course i don't hook every application. Just the ones that are necessary. That is untrusted applications, and task manager, explorer etc. The only way i can see you removing the file is if you unhook these hooks, you'd need some asm knowledge. which is how proper botkillers work

Tackled - January 3, 2014, 12:57 pm

(Jan 3, 2014 01:56 PM)kingroot Wrote: [\[CITE\]](#) I've disabled ntquerydirectoryfile and ntquerysysteminformation from locating your file. This is any process. x86 & x64. And of course i don't hook every application. Just the ones that are necessary. That is untrusted applications, and task manager, explorer etc. The only way i can see you removing the file is if you unhook these hooks, you'd need some asm knowledge.

Sounds like something I could be interested in then, cause in my botnet, the file I send out when to my bots after they connect, can easily be removed and detected.

Flaxpicker - January 3, 2014, 1:01 pm

Sounds like a great product

But if you want more customers I would suggest selling under \$100

kingroot - January 3, 2014, 7:45 pm

(Jan 3, 2014 02:01 PM)F.R.I.E.N.D.S Wrote: [\[CITE\]](#) Sounds like a great product

But if you want more customers I would suggest selling under \$100

Will probably lower the price. I need some beta testers for this soon.

Tackled - January 3, 2014, 8:00 pm

(Jan 3, 2014 08:45 PM)kingroot Wrote: [\[CITE\]](#) Will probably lower the price. I need some beta testers for this soon.

Me and a friend will be willing to test this out if you ever need the help, hope it turns out well.

ccman - *January 5, 2014, 7:55 am*

There is no more information about programming, but I there is a clear purpose.

And if it can last longer to the target for that purpose, consider purchasing depending on the price.

I've spent a lot of cost for the express purpose.

Please excuse me shit my Google Translate.