

Forum:[Hack Forums](#)

Thread: [Voodoo HTTP | C++ Loader with a Ring 3 Rootkit](#)

Sanch - September 12, 2015, 1:46 pm

Voodoo HTTP

So I have finally recoded my bot!

Voodoo HTTP is a loader written in C++ it will run on Windows 2000 to Windows 10.

It's main feature is a ring 3 rootkit meaning that is totally hidden from most software!

It has been thoroughly tested and is proven to be very stable with thousands of bots.

Features: Small 45 KB stub size

Basic commands Download and execute

CMD Command

Exit

Remove / Update

Ring 3 x86/x64 rootkit (Injection in a system process and hidden registry key even in safe mode)

Runtime FUD

Prevent auto sleep and hibernate

Obfuscated communication

Basic Persistence

Clean and functional panel

Multiple domain support

Function calls and strings are obfuscated

Panel Screenshots:

<http://vgy.me/KdDDPn.png>

<http://vgy.me/SnWqZt.png>

<http://vgy.me/U0dL8D.png>

The panel is not obfuscated and I encourage you to modify it.

Price:

\$100 BTC.

Add antiav@xmpp.jp on Jabber or neojesus2 on skype or PM me if you want to buy or test!

?Cyber - September 12, 2015, 1:48 pm

Vouch for sanch, one of the best coders on HF.

Sanch - September 12, 2015, 1:58 pm

(Sep 12, 2015 01:48 PM)?Cyber Wrote: [\[CITE\]](#) Vouch for sanch, one of the best coders on HF. Thank you for the vouch as for me being one of the best coders on HF I doubt it.

Netwxrk - September 12, 2015, 2:02 pm

Vouch for Sanch, his HTTP Bot works like a charm.

Spoiler [\(Click to View\)](#)

Sanch - September 12, 2015, 2:03 pm

(Sep 12, 2015 02:02 PM)Netwxrk Wrote: [\[CITE\]](#) Vouch for Sanch, his HTTP Bot works like a charm.

Spoiler [\(Click to View\)](#)

Thank you for the vouch <3

The Sly - September 12, 2015, 2:20 pm

Big Vouch for Sanch, this is 1 of the few ppl here on HF who actually know their shit and arent just reselling other ppl's stuff.

I've seen it in Action and that is some truly amazing botnet, u wont regret investing in it

Cibor - September 12, 2015, 2:25 pm

Looks good, good luck with sales

r00tard - September 12, 2015, 5:08 pm

No price? If ur giving away send me a pm

Sanch - September 13, 2015, 3:20 am

I love people who down vote this without even commenting! I would love some criticism it might help me improve it :)

Sanch - September 13, 2015, 4:01 am

(Sep 13, 2015 03:55 AM)Pajser Wrote: [\[CITE\]](#) Here we go.

Do you use DLL injection that dan wrote?

I really hope that you dont use NT native api to create null terminated reg key and calling it a rootkit?

In what process do you inject your dlls. Explorer?

The stub is quite large for only those function.

I offered you to beta test this you even sent me a PM and I told you to add me on jabber. But no I

don't use dll injection. As for the stub size: compile a Hello World in any version of visual studio that is > 7.0 and it will be at least 50 KB if you look at my todo I say compile with vs 6.0.

Sanch - September 13, 2015, 4:14 am

(Sep 13, 2015 04:13 AM)Pajser Wrote: [\[CITE\]](#) I have sent you a PM but I haven't received any response from you so I figured that you have found enough beta testers.

As for compiling, ofc the hello world will be 50kb when you use CRT functions like printf etc.

What about persistence, how is it achieved? How does your ring3 rootkit works exactly?

I have sent you a PM but I haven't received any response from you so I figured that you have found enough beta testers.

As for compiling, ofc the hello world will be 50kb when you use CRT functions like printf etc.

What about persistence, how is it achieved? How does your ring3 rootkit works exactly?

I sent you a PM but even without the CRT you will get at least 50 kb if statically link. Look at the feature list I inject into a system process and I have a hidden registry key.

Mr. Dr. Prof. Patrick - September 13, 2015, 5:00 am

(Sep 13, 2015 04:01 AM)Sanch Wrote: [\[CITE\]](#) I offered you to beta test this you even sent me a PM and I told you to add me on jabber. But no I don't use dll injection. As for the stub size: compile a Hello World in any version of visual studio that is > 7.0 and it will be at least 50 KB if you look at my todo I say compile with vs 6.0.

If VS is spiting out Big files then just take things into your own hand compile from the CMD line(or pragma), and change your entry point from main or winmain they both come with overheads

Sanch - September 13, 2015, 5:19 am

(Sep 13, 2015 05:00 AM)Mr. Dr. Prof. Patrick Wrote: [\[CITE\]](#) If VS is spiting out Big files then just take things into your own hand compile from the CMD line(or pragma), and change your entry point from main or winmain they both come with overheads

When I will compile with VS 6 the size will be 1/3 of what it is now.

Darksidefox - September 13, 2015, 5:20 am

I received a Beta Tester copy, here a short review about the bot:

- [+] The installation is pretty simple and you can setup the bot very fast
- [+] Bot is simple, no junk functions that increase the file size
- [+] The panel looks nice, is smooth and pretty fast. I had no problems
- [+] The bot has a Ring 3 Rootkit, which is great for a stable bot with a lot of bots
- [+] Bot receives a plugin system
- [+] Panel isn't obfuscated, can be extended
- [+] Commands work good and don't have a delay of a few minutes
- [-] Had a little problem with the CMD Command Task

Overall: Nice bot and thanks for giving me a copy. Keep up the good work! :p

Screenshots:

Spoiler [\(Click to View\)](#)

NightAng3L - September 13, 2015, 5:58 am

1 - Does the rootkit work on 64 bit ?

2 - Rootkit able to inject and hook 64 bit process ?

3 - Loader drop's any files on hard disk ?

(One of my friend needs to buy this and he cant post here so i'm asking on behalf of him)
good luck with sales

Xsal_Ice - September 13, 2015, 6:03 am

Looks nice really nice. I will keep an eye on this.

I wish u GLWS mate!

Sanch - September 13, 2015, 6:12 am

(Sep 13, 2015 05:58 AM)NightAng3L Wrote: [\[CITE\]](#) 1 - Does the rootkit work on 64 bit ?

2 - Rootkit able to inject and hook 64 bit process ?

3 - Loader drop's any files on hard disk ?

(One of my friend needs to buy this and he cant post here so i'm asking on behalf of him)
good luck with sales

It works on 64 systems it does not drop any files on disk. You can contact me to get a test copy to verify this.

rezzex - September 13, 2015, 8:04 am

So i wanna vouch for this Product. All Commands perfect, bot is stable as fuck, it doesnt drop any Files, other than that you can change the Panel as you want. The Bot is runtime FUD, its really nice. I had some Problems with my Bin, he helped me out really quick.

Some Improvments:

- A User Managment / Permissions System would be great to have
- MD5 Check if its the real executable/if its the same executable
- And a Scanner like in BB would be really nice to have.
- Ah and a Basic Botkiller would be nice :)

Reality_Skid__Scam_Buster - September 13, 2015, 8:04 am

Working in SysWOW64 is different theory BUT

Your loader rootkit able to inject and hook 64 bit process to hide process etc ?

Don't PM me,More you or anyone PM's me the more i will stay on your topic.

Simply post in the thread in front of all.

(And i'm not allowed to access PM as new member)

Sanch - September 13, 2015, 8:14 am

(Sep 13, 2015 08:04 AM)Reality_Skid__Scam_Buster Wrote: [\[CITE\]](#) Working in SysWOW64 is different theory BUT

Your loader rootkit able to inject and hook 64 bit process to hide process etc ?

Don't PM me,More you or anyone PM's me the more i will stay on your topic.

Simply post in the thread in front of all.

(And i'm not allowed to access PM as new member)

My loader is hidden on x64 and x86 systems contact me if you want to see it for yourself.

Reality_Skid__Scam_Buster - September 13, 2015, 8:15 am

(Sep 13, 2015 08:14 AM)Sanch Wrote: [\[CITE\]](#) My loader is hidden on x64 and x86 systems contact me if you want to see it for yourself.

No need,i just needed above official confirmation from the seller i.e you

gl with sales ?

Sanch - September 14, 2015, 6:37 am

(Sep 13, 2015 08:23 AM)Pajser Wrote: [\[CITE\]](#) Here is my review of this bot. I will try to keep it short :)

Quick overview

This bot is fairly simple. It has a few functions that are crucial for a loader but the bin size is really huge for a loader.

Static Analysis

I have received the bin from Sanch that weighs 84kb. The file size is big because the coder use a CRT and static links it at a compile time. (This is not a good way to make a loader or any other malware). The coder should of have used native WINAPI instead of certain CRT function.

This loader lacks of a string encryption, all of the external api calls are shown in the plain text. The author should have use the dynamic api calls and encrypt them.

Loader contains another Portable Executable in the resources that is compressed with UPX to lower the overall loader size but its not encrypted. See the picture below.

[img]<http://s10.postimg.org/4oievcbvh/bin.png>[/img]

Compressed PE weighs 30kb and when decompressed it is around 60kb.

[img]<http://s10.postimg.org/sqz8q7sll/compressed.png>[/img]

In this PE strings are not encrypted and all external api calls are visible in plain text.

Behavioral Analysis

When executed this loader copy itself to "Application Data\Microsoft\RcdIzCFP.exe", runs that instance and uses this as a melt function "ping 1.1.1.1 -n 1 -w 500 & del "%s"". Then it open svchost.exe process and inject the PE that is located in the resources. It use NtCreateKey to create a hidden regkey that contains a null byte terminator. Its the same technique used by poweliks malware to hide registry keys. This is simple to bypass, just use NtDeleteKey to remove it.

Go here for more info :

http://read.pudn.com/downloads111/sourcecode/windows/system/460388/REGHIDE.C_.htm

I wouldn't really recommend of doing this as there are scanners that pick up these kind of registry entries.

This loader doesn't have a system wide injection and it only injects into single process. To kill it you just have to identify the process and suspend it or kill it and you can use a Registry Dumper to remove the registry key.

The thread says that this loader contains a ring3 rootkit but the only thing that I saw is the process injection and null terminated registry key and I wouldn't classify that as a rootkit. When you try to open a registry key windows will even warn you about it and it will be suspicious to the end user (if he has some knowlede).

Loader lacks of anti debug methods and it is really easy to debug it.

When you extract the PE from resources you can run it and it will connect to the panel.

[img]<http://s10.postimg.org/uy3he4xvt/Capture.png>[/img]

Here is the execution flow of the payload:

Code NtCreateMutant --> RcdlzCFP

NtOpenKey --> \Registry\Machine\System\CurrentControlSet\Control\ComputerName // Gets the PC name

NtOpenKey --> \Software\Microsoft\Windows\CurrentVersion\Run

NtSetValueKey --> \x00RcdlzCFP // Create a hidden reg key

NtCreateFile --> C:\Documents and Settings\User\Local Settings\Application Data\Microsoft\RcdlzCFP.exe

InternetConnectA --> 127.0.0.1 // This is the connection part

HttpOpenRequestA --> /client.php // Script that handles the data

HttpSendRequestA --> sends the post data

CreateThread // Creates a new thread

//New thread

InternetConnectA --> 127.0.0.1 // This is the connection part

HttpOpenRequestA --> /client.php // Script that handles the data

RegOpenKeyExA --> Software\Microsoft\Windows\CurrentVersion\Run // Check for the reg key

HttpSendRequestA --> sends the post data

NtDelayExecution --> 45000 ms

LOOP

Network Analysis

There is not much to say about this part. It send a http request with post data and receives the response. The only notable thing here is that it uses a very weak encryption to secure the data being send.

Conclusion

This is a simple piece of malware and it is really easy to reverse it and remove it completely from the infected system.

However, this malware works as described and all mentioned functions are working correctly and nothing is missing unlike other HTTP bots being currently sold here.

Oh and a few words about the panel. I haven't spent much time looking at it but it seems good.

Anyway thanks for the test bin!

Thank you for your review the bot has been updated to make it harder to reverse it!

rezzex - September 14, 2015, 6:54 am

How we can get that update? Should i write you on Skype?

Sanch - September 14, 2015, 7:04 am

(Sep 14, 2015 06:54 AM)GET_MONEY Wrote: [\[CITE\]](#) How we can get that update? Should i write you on Skype?

PM me I will sort it out ;)

Uiqueblhats - September 19, 2015, 3:36 pm

Seller not online for days and ignoring my pms and for the testing of his bot i bought new hosting + domain but its useless now