

Forum:[Hack Forums](#)

Thread: [How to update Stub when Crypted ?](#)

Dezinator - April 15, 2018, 11:08 am

Hey Guys,

Got a little Question. Most Botnets got a Function to update the Botnet Stub. Good Idea for sure but how is it possible to use this?

If I crypt my Stub the Bot is working. When the stub now would get detected how could I remove the Old stub and update with the new one without losing the Bot ? When I would use something like Botkill all process which are not connected with the Bot would get killed. If this happend how can I update the new one ? Seems like this is not possible or did I missed something ? Also after Crypting and Injection the new Stub would not get accepted if the old Bot Stub is still running. Hope I got my point clear.

Greetings

Raoul Duke - April 15, 2018, 5:23 pm

You need to update your stub very often BEFORE it gets detected. Once you get detected the remote connection will be blocked and you will loose any control you had on this target.

GlobalLine - April 15, 2018, 5:53 pm

(Apr 15, 2018 11:08 AM)Dezinator Wrote: [\[CITE\]](#) Hey Guys,

Got a little Question. Most Botnets got a Function to update the Botnet Stub. Good Idea for sure but how is it possible to use this?

If I crypt my Stub the Bot is working. When the stub now would get detected how could I remove the Old stub and update with the new one without losing the Bot ? When I would use something like Botkill all process which are not connected with the Bot would get killed. If this happend how can I update the new one ? Seems like this is not possible or did I missed something ? Also after Crypting and Injection the new Stub would not get accepted if the old Bot Stub is still running. Hope I got my point clear.

Greetings

Lol. What?

If your stub gets detected by an AV, the AV doesn't just mark it as detected. It wipes that shit off the hard drive.

If your stub gets detected, then your bot is gone on that computer. Period. You can't update it unless they manually install a fresh copy of it.

sssniperwolf - April 15, 2018, 6:47 pm

(Apr 15, 2018 05:53 PM)GlobalLine Wrote: [\[CITE\]](#) Lol. What?

If your stub gets detected by an AV, the AV doesn't just mark it as detected. It wipes that shit off the hard drive.

If your stub gets detected, then your bot is gone on that computer. Period. You can't update it

unless they manually install a fresh copy of it.

Yes the AV will remove the detected stub but the new updated undetected stub will remain on his computer

Dezinator - April 15, 2018, 6:49 pm

Okay get this but how do i update this with out my stub get removed when its crypted ?

Also not every botkill remove stubs which are Injected in some major Process ?

Its not possible to update stub when the main process of the Bot (for example Betabot is still running on the System)

sssniperwolf - April 15, 2018, 7:05 pm

(Apr 15, 2018 06:49 PM)Dezinator Wrote: [\[CITE\]](#) Okay get this but how do i update this with out my stub get removed when its crypted ?

Also not every botkill remove stubs which are Injected in some major Process ?

Its not possible to update stub when the main process of the Bot (for example Betabot is still running on the System)

You say you cant update the stub because there is already a stub running on their system? I haven't used betabot in over 3 years but im pretty sure it has a basic update / download / uninstall option you are probably running a cracked betabot which is completely useless

AnonTri - April 15, 2018, 7:08 pm

(Apr 15, 2018 07:05 PM)sssniperwolf Wrote: [\[CITE\]](#) You say you cant update the stub because there is already a stub running on their system? I haven't used betabot in over 3 years but im pretty sure it has a basic update / download / uninstall option you are probably running a cracked betabot which is completely useless

He didn't mention BB.

OP If you are using startup on your bot just run update. Otherwise run update and if the old bot reconnects uninstall it. Simple as that.

Dezinator - April 15, 2018, 7:21 pm

Buddy its just one Question. If my Stub is crypted with a Injection in a Normal Process, it is not possible to kill it with Botkill.If it gets detected from AV it will be removed. So I will lost the bot. So how do I update the Bot with Killing the Old Process and Update with the new one ?

If I update it with the new stub and the old one is not removed with the Botkill the new FUD Stub will not be accepted from the System

sssniperwolf - April 15, 2018, 7:38 pm

(Apr 15, 2018 07:21 PM)Dezinator Wrote: [\[CITE\]](#) Buddy its just one Question. If my Stub is crypted with a Injection in a Normal Process, it is not possible to kill it with Botkill.If it gets detected from AV it will be removed. So I will lost the bot. So how do I update the Bot with Killing the Old Process and Update with the new one ?

If I update it with the new stub and the old one is not removed with the Botkill the new FUD Stub will not be accepted from the System

I understand what your saying, which bot are you running and version#

Dezinator - April 16, 2018, 11:24 am

For Example Betabot

25 Characters..

MrPatterson - April 18, 2018, 7:46 pm

I'm guessing you should look at using a better bot than Betabot, I think it would solve the problem you're describing.

Zettabit - April 19, 2018, 12:47 pm

The update function of most bots purposely uninstalls the old bot from the system, and then starts the new bot. If it's injected into a process, it should exit that process and remove all traces of the old file from the system.

If your bot isn't doing this, then I don't know what the fuck you're using but it's trash.

sssniperwolf - April 19, 2018, 4:46 pm

(Apr 19, 2018 12:47 PM)Zettabit Wrote: [\[CITE\]](#) The update function of most bots purposely uninstalls the old bot from the system, and then starts the new bot. If it's injected into a process, it should exit that process and remove all traces of the old file from the system.

If your bot isn't doing this, then I don't know what the fuck you're using but it's trash.
He keeps saying betabot which is probably a cracked version so the update feature doesn't work.

MrPatterson - April 19, 2018, 7:33 pm

(Apr 19, 2018 12:47 PM)Zettabit Wrote: [\[CITE\]](#) The update function of most bots purposely uninstalls the old bot from the system, and then starts the new bot. If it's injected into a process, it should exit that process and remove all traces of the old file from the system.

If your bot isn't doing this, then I don't know what the fuck you're using but it's trash.
Out of interest, what bot would you recommend?

Dezinator - April 21, 2018, 3:51 pm

(Apr 19, 2018 04:46 PM)sssniperwolf Wrote: [\[CITE\]](#) He keeps saying betabot which is probably a cracked version so the update feature doesn't work.

You dont understand. How should the Update Function in Betabot know where I inject my FUD Stub ? And If the Update Function is not able to delete my Stub, the System will reject a new Stub a

Dezinator - April 27, 2018, 8:26 pm

Any suggestions about Stubs which are Injected and dont are able to update ?

Zettabit - April 28, 2018, 6:44 pm

(Apr 21, 2018 03:51 PM)Dezinator Wrote: [\[CITE\]](#) You dont understand. How should the Update Function in Betabot know where I inject my FUD Stub ? And If the Update Function is not able to delete my Stub, the System will reject a new Stub a

No, you don't understand. The bot knows every place that it resides on the system. The update command will know which processes / files to delete.

DarkTitan - January 31, 2020, 4:14 pm

(Apr 28, 2018 06:44 PM)Zettabit Wrote: [\[CITE\]](#) No, you don't understand. The bot knows every place that it resides on the system. The update command will know which processes / files to delete.

Also if this is an old thread curious to know the answer from you.

What if the Stub is crypted and therefore injected into another process (for example for startup etc.)

? Then the "old" Stub knows where it's injected but doesn't know where the crypter places the startup and injected it, so the new stub would again be rejected by the system (as it were not removed completely)

How did you solve this on LiteHTTP ? The update function therefore would only work if crypter and botnets know from each other where it can be found on the system (and where it was injected)

Zettabit - February 1, 2020, 7:59 am

(Jan 31, 2020 05:14 PM)DarkTitan Wrote: [\[CITE\]](#) Also if this is an old thread curious to know the answer from you.

What if the Stub is crypter and therefore injected into another process (for example for startup etc.) ? Then the "old" Stub knows where it's injected but doesn't know where the crypter places the startup and injected it, so the new stub would again be rejected by the system (as it were not removed completely)

How did you solve this on LiteHTTP ? The update function therefore would only work if crypter and botnets know from each other where it can be found on the system (and where it was injected)

I don't know of any crypter that injects a .NET exe into a process other than itself. It's more work than it's worth. If LiteHTTP was a native bot then that would be an issue.

EDIT: One more thing I might add is if you're crypting a bot to begin with, you shouldn't use startup on the crypter anyway. You should always let the bot use its own startup to avoid problems like this.

Zinx™ - February 1, 2020, 10:10 am

Update every 20-36 hours if you're not hitting High detection rates.