

Forum:[Hack Forums](#)

Thread: [Infect a PC with a rat](#)

Idonthackalot - May 19, 2019, 1:54 pm

Im wondering how i can infect a rat onto the target computer without having access to the remote laptop wich im trying to RAT.

I have an old laptop wich i wanna try and learn a program like webmonitor but infecting the laptop manually while having access to it would bypass the challenge im looking for so this is why im asking to try and learn more about the PC world or w/e.

Fluox - May 19, 2019, 2:12 pm

(May 19, 2019 01:54 PM)Idonthackalot Wrote: [\[CITE\]](#) Im wondering how i can infect a rat onto the target computer without having access to the remote laptop wich im trying to RAT.

I have an old laptop wich i wanna try and learn a program like webmonitor but infecting the laptop manually while having access to it would bypass the challenge im looking for so this is why im asking to try and learn more about the PC world or w/e.

You could send the rat over to the target? Via any form of social media or messaging service, if you crypt it they will be non the wiser and if you wish to go ahead and do a little extra, you could bind the rat to any for of software the target is likly to download and then send it to them. ?

Kind regards,
Fluox.

Idonthackalot - May 19, 2019, 2:14 pm

(May 19, 2019 02:12 PM)Fluox Wrote: [\[CITE\]](#) You could send the rat over to the target? Via any form of social media or messaging service, if you crypt it they will be non the wiser and if you wish to go ahead and do a little extra, you could bind the rat to any for of software the target is likly to download and then send it to them. ?

Kind regards,
Fluox.

Thank you, this is what i've understood to be the best options but i have no idea how to actually embed a RAT into a software, link or a message and need help doing this.

eFriend - May 19, 2019, 5:54 pm

Hi,

Most ways rats are executed on systems is by a client downloading and executing it, mostly from thinking that they are files that they want like a game cheat or a free program but really contain a rat. If you want to try and test ratting your other computer without bypassing the challenge, the way I would test that would be to keep all the setting on the computer standard as if it were another persons, (ex antivirus and firewall enabled) and downloading it and seeing if it works. You would need to crypt your rat stub with a crypter for this to work of course.

If your goal is to rat the computer without touching it, that is very challenging and is not how people normally do it if they are not specifically targeting one person and just want it to spread. The only way I could think to do that would be spreading it through a network or usb spreading with auto

run on, which are all hard to be able to do. If you were to target a specific person, the best way in my opinion would be to use social engineering and trick them into downloading it and running it, and it would have to be without setting off any red flags (like if their antivirus detected it). Good luck and only use this for ethical purposes.

Also to embed a rat into software like you said, a crypter would be your best option. With a good crypter, you have multiple options including binding the rat with another program, so for example getting a game cheat and binding it with the rat, so when executed by a client the game cheat will run making it look legit, but as well as the game cheat the rat would run. A crypter also makes the rat undetectable to antivirus which is its main function, depending on how good it is.

Idonthackalot - May 19, 2019, 7:27 pm

(May 19, 2019 05:54 PM)eFriend Wrote: [\[CITE\]](#) Hi,

Most ways rats are executed on systems is by a client downloading and executing it, mostly from thinking that they are files that they want like a game cheat or a free program but really contain a rat. If you want to try and test ratting your other computer without bypassing the challenge, the way I would test that would be to keep all the setting on the computer standard as if it were another persons, (ex antivirus and firewall enabled) and downloading it and seeing if it works. You would need to crypt your rat stub with a crypter for this to work of course.

If your goal is to rat the computer without touching it, that is very challenging and is not how people normally do it if they are not specifically targeting one person and just want it to spread. The only way I could think to do that would be spreading it through a network or usb spreading with auto run on, which are all hard to be able to do. If you were to target a specific person, the best way in my opinion would be to use social engineering and trick them into downloading it and running it, and it would have to be without setting off any red flags (like if their antivirus detected it). Good luck and only use this for ethical purposes.

Also to embed a rat into software like you said, a crypter would be your best option. With a good crypter, you have multiple options including binding the rat with another program, so for example getting a game cheat and binding it with the rat, so when executed by a client the game cheat will run making it look legit, but as well as the game cheat the rat would run. A crypter also makes the rat undetectable to antivirus which is its main function, depending on how good it is.

Thank you this is kinda the answer i been looking for, do you know any legit Crypters here on HF? I can pay but not too much since i just wanna test it out etc and a crypter that has a good ammount of vouches to it.

eFriend - May 19, 2019, 8:44 pm

Np, yeah there are some good crypters on hf that are verified. If you can't spend too much money than that's not too big of a problem but be aware that crypters aren't cheap. Also the more expensive the crypter, the less people that have it, which means the detection rate will be lower and the amount of time before the crypted file will get detected is also significantly lower.

For you I would recommend bytencrypter. it is cheap for a crypter (30 dollars for 3 months and 50 dollars for lifetime), has a ton of features, and has a very low detection rate. I don't know why but I can't find the thread for it right now, and be aware there is a scam site for it so ONLY MAKE PURCHAS

ES THROUGH HACKFORUMS. A good demo of it is here: <https://youtu.be/NeRYkQW6DBI>

The best crypter I know of is called cyber seal. Obviously the detection rate is next to nothing, has the most features I've seen in a crypter, even with a extension spoofer so instead of exe you can change it to png or something, and it has been around for like 10 years. It's great but is expensive af

so I wouldn't recommend it to you if your just starting out testing system exploitation. Here is the thread for it: <https://hackforums.net/showthread.php?tid=5776088> (remove spaces) and here is a demo of it: https://youtu.be/_jhlJ4Ktl8Q

And for testing, you can try lime crypter by nyan. It's alright as it bypasses most free antivirus programs such as avg, avast, windows defender, etc but is detected by actual antivirus companies. It also does not have a startup option which is essential, so this is why I recommend it only for testing. I would not use this for purposes other than testing. Here is the link for it on github, go to releases and download the latest zip file if you want to try it: <https://github.com/NYA-N-x-CAT/Lime-Crypter>

If you end up using crypters, you should know that when you crypt your stub and you want to test the detection rate, DO NOT use virus total. The reason why is because they distribute all files sent to antivirus companies, and if antivirus companies detect anything when distributed to them, especially files that are obfuscated, they will find ways to decompile them thus making it detectable by more antivirus programs. Good no distribute scanners are spyral scanner, antiscan.me, and no distribute scanner, but for me no distribute won't let me upload a file. So just use spyral and antiscan. Make sure they are verified not to distribute.

Also, if you hear the word "FUD" a lot, it means fully undetectable. Always make sure your stubs (rat) have startup enabled so they comeback when the computer is reset, and one more important thing to know is if you are going to use a crypter, when making the rat do not select any features, like startup for example (unless it is a feature for the rat like keylogging). Let the crypter handle that, and use its options. Otherwise it might mess up everything if both the rat settings and the crypter settings are enabled. Let the crypter do the work.

There are a lot of factors for making a stub undetectable when you crypt it. The encryption is the most important which is handled by the crypter, but also it is important that the assembly is set up so it seems legitimate, and that there is a startup delay, I would recommend at least 45 seconds. Modifying these will help evade detection to antivirus programs. You can edit these settings in the crypter settings. The demo vid I put for cyberseal explains this in depth.

Good luck and if you have anymore questions feel free to ask. Use this for ethical purposes only.