

Forum:[Hack Forums](#)

Thread: [How can I disguise my RAT?](#)

IlyaDeev - November 7, 2024, 9:09 am

I'm using NjRat, and I need it for individual purposes, meaning I'll be sending it personally in messages. I've already used obfuscation and encoded the RAT using The Enigma Protector, but I still got detected by 35 antivirus programs on VirusTotal. How else can I improve the result so that the file functions properly as an executable? Or should I consider switching to a different tool altogether?

Ren And Stimpy - November 7, 2024, 10:10 am

NJRAT... wow haven't hard about that in like 8 years Always Crypt then Exploit. Don't scan on VT...

<https://hackforums.net/showthread.php?tid=6245000>

DramaKing - November 7, 2024, 10:24 am

(Nov 7, 2024 10:09 AM)IlyaDeev Wrote: [\[CITE\]](#) I'm using NjRat, and I need it for individual purposes, meaning I'll be sending it personally in messages. I've already used obfuscation and encoded the RAT using The Enigma Protector, but I still got detected by 35 antivirus programs on VirusTotal. How else can I improve the result so that the file functions properly as an executable? Or should I consider switching to a different tool altogether?

NjRat is legacy malware today. You have three problems that I see. 1. Using a very-well analyzed piece of malware that isn't written to modern standards. 2. Using a public crypter that probably is only for anti-reverse-engineering. 3. Uploading to VirusTotal like a n00b. The fastest known way to get AV signatures for your file.

Biggy_Asian - November 7, 2024, 11:24 am

There's alot of ways avs detect malware. Just obfuscating it/using protectors will do jack nower days. Change the behaviour/functionality of the rat. Thats one way.

Some good points:

(Nov 7, 2024 11:24 AM)DramaKing Wrote: [\[CITE\]](#) NjRat is legacy malware today. You have three problems that I see. 1. Using a very-well analyzed piece of malware that isn't written to modern standards. 2. Using a public crypter that probably is only for anti-reverse-engineering. 3. Uploading to VirusTotal like a n00b. The fastest known way to get AV signatures for your file.

IlyaDeev - November 8, 2024, 11:19 am

(Nov 7, 2024 11:24 AM)DramaKing Wrote: [\[CITE\]](#) NjRat is legacy malware today. You have three problems that I see. 1. Using a very-well analyzed piece of malware that isn't written to modern standards. 2. Using a public crypter that probably is only for anti-reverse-engineering. 3. Uploading to VirusTotal like a n00b. The fastest known way to get AV signatures for your file.

OK, thanks, I changed the virus to DcRat and installed plugins to hide the file. Can you suggest where you can safely check the virus and which cryptographers can you recommend?

PitbulIT0r - November 8, 2024, 12:21 pm

I always recommend AsyncRAT because its open source and you can find it on GitHub.

Move from njRat too old!

DramaKing - November 8, 2024, 3:40 pm

(Nov 8, 2024 12:19 PM)IlyaDeev Wrote: [\[CITE\]](#) OK, thanks, I changed the virus to DcRat and installed plugins to hide the file. Can you suggest where you can safely check the virus and which cryptographers can you recommend?

I recommend a hand crypt from [etizolamvendor](#) if you want something that lasts. Even so-called "private crypts" may not actually be private. "FUD" is just a marketing term. I definitely wouldn't put any stock in a plugin that "hides" a file.

IlyaDeev - November 12, 2024, 3:02 am

(Nov 8, 2024 01:21 PM)PitbullT0r Wrote: [\[CITE\]](#) I always recommend AsyncRAT because its open source and you can find it on GitHub.

Move from njRat too old!

Thanks for the offer, but I have a question, how exactly did you open ports for AsyncRAT? I used to use Playit.gg, but after opening the port I was immediately banned for using Async, and I don't use ngroj because it requires my bank card.

PitbullT0r - November 12, 2024, 4:37 am

(Nov 12, 2024 04:02 AM)IlyaDeev Wrote: [\[CITE\]](#) Thanks for the offer, but I have a question, how exactly did you open ports for AsyncRAT? I used to use Playit.gg, but after opening the port I was immediately banned for using Async, and I don't use ngroj because it requires my bank card.

Buy a cheap bulletproof VPS or use a VPN with port forwarding.

IlyaDeev - November 12, 2024, 10:19 am

(Nov 12, 2024 05:37 AM)PitbullT0r Wrote: [\[CITE\]](#) Buy a cheap bulletproof VPS or use a VPN with port forwarding.

Thanks for the advice, but if it's not too much trouble can you roughly explain how to use a VPS server (I bought it on myihc) to route the necessary tunnel, if that's what I'm thinking about. The server is on ubuntu. Just as I understood I need to establish a connection from my computer to the server and from the server to the victim, in builder specifying the white IP server and the port opened by me, but tried a lot of methods so to the end and did not understand what I did wrong.

PitbullT0r - November 12, 2024, 12:35 pm

(Nov 12, 2024 11:19 AM)IlyaDeev Wrote: [\[CITE\]](#) Thanks for the advice, but if it's not too much trouble can you roughly explain how to use a VPS server (I bought it on myihc) to route the necessary tunnel, if that's what I'm thinking about. The server is on ubuntu. Just as I understood I need to establish a connection from my computer to the server and from the server to the victim, in builder specifying the white IP server and the port opened by me, but tried a lot of methods so to the end and did not understand what I did wrong.

Sorry i dont understand what are you trying to do.

Please tell us wich RAT are you using and also why on Ubuntu?

motor2024 - November 12, 2024, 1:17 pm

Ilya send me your TG in DM

Can help you

DramaKing - November 12, 2024, 1:21 pm

(Nov 12, 2024 11:19 AM)IlyaDeev Wrote: [\[CITE\]](#) Thanks for the advice, but if it's not too much trouble can you roughly explain how to use a VPS server (I bought it on myihc) to route the necessary tunnel, if that's what I'm thinking about. The server is on ubuntu. Just as I understood I need to establish a connection from my computer to the server and from the server to the victim, in builder specifying the white IP server and the port opened by me, but tried a lot of methods so to the end and did not understand what I did wrong.

The trick is not to forward ports. Get a WINDOWS VPS and run your C2 on it. If that just isn't an agreeable option, use SSH local port forwarding or set up a WireGuard VPN (the latter would require some iptables rules and some research to get working).

(Nov 12, 2024 02:17 PM)motor2024 Wrote: [\[CITE\]](#) Ilya send me your TG in DM
Can help you

He can't. He's too new like you. The messaging restrictions are to protect new users or to protect from new users. Keep your discussion in the open and DO NOT message off-platform to avoid moderation.

narubasu - November 13, 2024, 4:47 am

Just buy a good private crypt private rat and dedicated rdp