

Forum:[Hack Forums](#)

Thread: [Crypter for Razor Rat](#)

tyjesws - April 18, 2025, 11:27 am

hello

i tried many crypters from the market and all were detected by either wd or smartscreen
a few posts on here recommended private crypts made by a forum user named Z***
i sent him a private message weeks ago but was never answered

does anyone know how i can reach him?
or do you know of a working crypting service that offers private stubs?

thanks

Hopsin - April 18, 2025, 12:56 pm

(Apr 18, 2025 11:27 AM)tyjesws Wrote: [\[CITE\]](#) hello

i tried many crypters from the market and all were detected by either wd or smartscreen
a few posts on here recommended private crypts made by a forum user named Z***
i sent him a private message weeks ago but was never answered

does anyone know how i can reach him?
or do you know of a working crypting service that offers private stubs?

thanks

What's his profile link or UID ? Also, what is your budget ?

DramaKing - April 18, 2025, 2:42 pm

Python scripts are supposed to be invisible to antivirus.

tyjesws - April 19, 2025, 2:04 am

(Apr 18, 2025 11:27 AM)tyjesws Wrote: [\[CITE\]](#) hello

i tried many crypters from the market and all were detected by either wd or smartscreen
a few posts on here recommended private crypts made by a forum user named Z***
i sent him a private message weeks ago but was never answered

does anyone know how i can reach him?
or do you know of a working crypting service that offers private stubs?

thanksthe thanks for the reply

sent you a pm

(Apr 18, 2025 12:56 PM)Hopsin Wrote: [\[CITE\]](#) What's his profile link or UID ? Also, what is your budget ?

thanks for the reply
but i dont see how its relevant
maybe i misunderstood
razor is written in c++ and asm

Sand Ferret - April 20, 2025, 11:45 pm

You're unlikely to find any good crypting service on this forum - it's unfortunate, but that's the reality.

That applies to all malware, not specifically Razor.

Razor is not hard to crypt, the problem that people face when trying to crypt it is they do not know how Razor works internally; Razor drops copies of itself during certain tasks, such as auto elevation and for startup - if that copy is not properly crypted, then the AV kills it. The majority of crypter coders on this site are too lazy to even bother testing the malware before agreeing to crypt.

tyjesws - April 21, 2025, 1:30 am

(Apr 20, 2025 11:45 PM)Sand Ferret Wrote: [\[CITE\]](#) You're unlikely to find any good crypting service on this forum - it's unfortunate, but that's the reality. That applies to all malware, not specifically Razor.

Razor is not hard to crypt, the problem that people face when trying to crypt it is they do not know how Razor works internally; Razor drops copies of itself during certain tasks, such as auto elevation and for startup - if that copy is not properly crypted, then the AV kills it. The majority of crypter coders on this site are too lazy to even bother testing the malware before agreeing to crypt.thanks for that

so do you know where i could find someone who properly crypts malware?
in the case of razor, maybe i could use its static output option and have the crypter take care of startup and elevation. usually the crypter is responsible for these functions anyhow, no?

7 - April 21, 2025, 1:38 am

(Apr 20, 2025 11:45 PM)Sand Ferret Wrote: [\[CITE\]](#) You're unlikely to find any good crypting service on this forum - it's unfortunate, but that's the reality. That applies to all malware, not specifically Razor.

Razor is not hard to crypt, the problem that people face when trying to crypt it is they do not know how Razor works internally; Razor drops copies of itself during certain tasks, such as auto elevation and for startup - if that copy is not properly crypted, then the AV kills it. The majority of crypter coders on this site are too lazy to even bother testing the malware before agreeing to crypt.
Same problem with amadey loader. It drops unencrypted dlls which instantly get detected.

Crypting is a very diffucult probelm to face these days due to hueristic scans anyway you can pay up to 5k for a crypt and still hit heuritic protection.
Ratting now is the final step in the attack not the initial payload like it once was.

I cannot really give [tyjesws](#) advice on crypting Razor Rat. Actually I have never seen it until today. If you hoping to just mass spread and hope for the best result you will find a solution but you want 100% success, your starting off the wrong way.

tyjesws - April 21, 2025, 1:57 am

(Apr 21, 2025 01:38 AM)7 Wrote: [\[CITE\]](#) Same problem with amadey loader. It drops unencrypted dlls which instantly get detected.

Crypting is a very diffucult probelm to face these days due to hueristic scans anyway you can pay up to 5k for a crypt and still hit heuritic protection.
Ratting now is the final step in the attack not the initial payload like it once was.

I cannot really give [tyjesws](#) advice on crypting Razor Rat. Actually I have never seen it until today. If you hoping to just mass spread and hope for the best result you will find a solution but you want 100% success, your starting off the wrong way.thanks, very eye-opening
what then is the initial payload for 100% success?
im not interested in mass spreading

7 - April 21, 2025, 7:36 am

I would start with a c2 shell MSF or personally I prefer havoc and work on getting that passed AV's first.

It's a learning curve but you will soon start to catch on and also much more educational

Yokobovich - May 5, 2025, 11:12 am

I won't be mentioning the unmentionable (Z) for various reasons. ?

But,

Through extensive use of Razor, I can reveal this:

1. The recent versions of Razor doesn't drop anything during auto elevation, likely a different UAC method.

2. Razor does NOT drop the bot in static mode or persistence-less mode. The static mode was explained to be a solution for those using the simpler Run-PE style crypters.

3. If a non-static bot (injecting) has persistence ENABLED, then the bot is dropped ONLY at the exact moment of system reboot and shutdowns. Never before or during execution.

4. If a non-static bot (injecting) has persistence DISABLED, then NO dropping is done, EVER.

My advice to people using the most primitive crypters: A good approach is to enable the static mode because such bots can run from anywhere without any extra noise. If persistence is needed, just enable it in the crypter.

Or you can use the unmentionables crypter stubs if you have rich parents and don't mind being yelled at. ???