

Forum:[Hack Forums](#)

Thread: [PURE CRYPTER FUD HELP WINDOWS DEFENDER](#)

viio - September 2, 2022, 4:42 am

I use Async Rat and Pure Crypter

I get 2/26 on avcheck.net this includes windows 10 defender being clean.

But when i put encrypted file on windows 10. It get detected immediately by windows defender

Kindly let me know what i am doing wrong. Below my setting

prnt.sc/aUVkBZVz3GfE

Sorry about my English.

Thanks in advance

Frost Crypt - September 2, 2022, 5:14 am

you probably have a cloud detection that needs internet connection hence why it shows clean on antiscan

contact the owner for support privately , he knows his crypter better than anyone

viio - September 2, 2022, 6:01 am

(Sep 2, 2022 05:14 AM)Nano Shield Wrote: [\[CITE\]](#) you probably have a cloud detection that needs internet connection hence why it shows clean on antiscan

contact the owner for support privately , he knows his crypter better than anyone

Please what do you mean by cloud detection that need internet connection. Is it on crypter or AsyncRAT

I ask because i did not use any setting on AsyncRAT just build stub

Thanks very much

trojohn - September 2, 2022, 10:44 am

(Sep 2, 2022 06:01 AM)viio Wrote: [\[CITE\]](#) Please what do you mean by cloud detection that need internet connection. Is it on crypter or AsyncRAT

I ask because i did not use any setting on AsyncRAT just build stub

Thanks very much

Windows defender has a cloud protection feature. When enabled, it can cross reference your executable with an online database of threats. Sometimes this catches threats that it wouldn't otherwise until the next defender update.

This is enabled by default but a lot of gamers turn it off because they don't like any unnecessary connections going on in the background. So if GPUs are your target, it's probably not a big problem short term.

viio - September 2, 2022, 10:13 pm

(Sep 2, 2022 10:44 AM)trojohn Wrote: [\[CITE\]](#) Windows defender has a cloud protection feature. When enabled, it can cross reference your executable with an online database of threats. Sometimes this catches threats that it wouldn't otherwise until the next defender update.

This is enabled by default but a lot of gamers turn it off because they don't like any unnecessary connections going on in the background. So if GPUs are your target, it's probably not a big problem short term.

Any solution to bypass Windows defender with cloud protection feature on?

Thanks

AlmightyK - September 9, 2022, 11:49 pm

(Sep 2, 2022 10:13 PM)viio Wrote: [\[CITE\]](#) Any solution to bypass Windows defender with cloud protection feature on?

Thanks

Get a private crypt.

JoeyMax - September 16, 2022, 5:03 pm

(Sep 2, 2022 10:13 PM)viio Wrote: [\[CITE\]](#) Any solution to bypass Windows defender with cloud protection feature on?

Thanks

man ya gots to add to /exclusions/..... for file directory \appdata\roaming\temp is fine for root that as fast as possible then unpack/decrypt downloader and grab the botnet.exe from http host Zonelfidnet doesn't care then

dav323232 - September 21, 2022, 5:04 am

Please what the site for the Pure Crypter?

FUD Master - September 21, 2022, 9:34 pm

Share your exe (raw stub without any encryption) with me. let me try to bypass WD for you

?BADMAN? - September 22, 2022, 8:48 am

Try to change the pe resources like filename and version , it helps bypass cloud detections.

HiddenEyE - September 25, 2022, 10:09 pm

cloud protection you experience is defenders latest defence against malware etc.

to bypass it you need the crypter seller to give you a private build with sophisticated technique otherwise the private build will be detected in one day at most in another system(or even yours) that you are spreading.

using online check is just scantime not runtime most time.

ADVICE- the best way to check defender for runtime is to take they cryted malware to download folder and run it from there.

FUD Master - September 26, 2022, 2:53 am

(Sep 2, 2022 04:42 AM)viio Wrote: [\[CITE\]](#) I use Async Rat and Pure Crypter

I get 2/26 on avcheck.net this includes windows 10 defender being clean.

But when i put encrypted file on windows 10. It get detected immediately by windows defender

Kindly let me know what i am doing wrong. Below my setting

prnt.sc/aUVkBZVz3GfE

Sorry about my English.

Thanks in advance

1. Scan time and runtime FUD are different issues and has different ways to FUD. Most of the people believes in scantime FUD.
2. run time FUD is important for results.
3. Testing your stub has proper methods. you have to save your metadata, file signatures, file Behavior, logs etc etc etc from sharing to AV database.

44happy - *October 19, 2022, 7:25 pm*

(Sep 21, 2022 05:04 AM)dav323232 Wrote: [\[CITE\]](#) Please what the site for the Pure Crypter?

Hey, I this offer still up jittt itd be a blessing. Shit i just copped Byte Crypter v3 and it dont get past cloud AV. I tried to DM u but i couldn't so hit me back manee all luvv