

Forum:[Hack Forums](#)

Thread: [Pure Crypter, Pure Loader and Raccoon](#)

Resident3vil - August 27, 2022, 7:59 pm

I have Pure Crypter and Raccoon which I don't think work together very well. Testing goes fine sometime but other than that my installs all deliver empty logs. Both real installs and bot installs deliver empty logs. I think both products are good and I'll be testing new Crypter soon tonight for raccoon.

Pure Coder has a shitty attitude but a great product so I try not to ask her any questions any more lol. When stub isn't FUD the detections are normally very low (0-2) which I like. Can any of you guys make suggestions on which software you've found to work best with Pure Crypter as I would like to test it. Also, if any of you have worked with the Pure Log software what are the pros and cons you've encountered. I'm thinking it might be best to use his software with his Crypter in stead of Raccoon.

Thanks!

Frost Crypt - August 28, 2022, 2:27 am

sounds a lot like your loggers are outdated and unable to grab logs from latest updated browsers and this has nothing to do with the crypter you are using

VGO - August 28, 2022, 2:34 am

Some Crypters damages the features of the prog's which is normal!

to make a proper test, make some logs @ ur VM and save them then take a snapshot.

Now execute unencrypted file, check your panel if it got the logs then next step is roll back the snapshot and execute the crypted file, check your panel if it got the logs.

If no logs were found when you tested unencrypted then yes your software is fucked.

If you got logs when tested the Unencrypted file BUT NO logs were found when you tested Crypted file then your crypter is making the problem, simply if this happen record a video in action and report to the Crypter coder I'm sure he will fix it for you.

Resident3vil - August 28, 2022, 8:54 am

(Aug 28, 2022 02:34 AM)VGO Wrote: [\[CITE\]](#) Some Crypters damages the features of the prog's which is normal!

to make a proper test, make some logs @ ur VM and save them then take a snapshot.

Now execute unencrypted file, check your panel if it got the logs then next step is roll back the snapshot and execute the crypted file, check your panel if it got the logs.

If no logs were found when you tested unencrypted then yes your software is fucked.

If you got logs when tested the Unencrypted file BUT NO logs were found when you tested Crypted file then your crypter is making the problem, simply if this happen record a video in action and report to the Crypter coder I'm sure he will fix it for you.

Yes this exactly how I perform my tests. I'm sure crypt is the problem for software I'm using. Again, Cryptor has shitty attitude so I'm sure he will not correct. He does refud stub a few times a day so I'm looking for feedback on his log software to use with his cryptor. I think it will be best for me to find new crypt for raccoon.

Thanks for your help. It confirms what I was thinking.

(Aug 28, 2022 02:27 AM)Nano Shield Wrote: [\[CITE\]](#) sounds a lot like your loggers are outdated and unable to grab logs from latest updated browsers and this has nothing to do with the crypter you are using

If you read the response below you'll see why I believe and member below believes crypter is the issue. My logger grabs logs from every browser it's supposed to without crypt. With crypt it grabs nothing. Thanks for your input though!

Resident3vil - August 28, 2022, 9:21 am

(Aug 28, 2022 09:04 AM)Dyne Wrote: [\[CITE\]](#) Hello,

Have you considered spreading the loader directly instead?

Then dropping a UAC exploit and adding the entire C:\ to antivirus exclusions after?

This ensures you keep your client, then you can drop your stealer or other malware how you intend it.

Loader stub > crypt > spread with your method / delivery method > Stub connects > drop Exclusions/or do by remote shell after UAC exploit via D&E or plugin > then drop stealer > review logs > drop tool you need to use the high volume logs.

Understand?

I haven't quite wrapped my head around the loader stub yet. I did use and test loader config (not knowing what I was doing) yesterday but again I'm not even sure how spreading loader stub works.

When crypt loader gave me jpg I hosted that and took the direct link and dropped back in crypter. When crypter was finished I took stub and hosted that and took direct link which I used to spread. I'm sure this isn't right way to spread loader stub but you asked did I understand lol.

Thanks for you guys help. For awhile the biggest obstacle was trying to figure out how to spread to valuable targets. I can see them opening my email and using my short link so I believe my spread is good. Just have to overcome this issue now. About to have my coffee and start studying the tips above!

Resident3vil - August 28, 2022, 9:42 am

(Aug 28, 2022 09:34 AM)Dyne Wrote: [\[CITE\]](#) Ah, loader stub is slang for a botnet stub. A botnet is for holding clients.

Once the client connects to your botnet stub and connection is established, to prevent AV from continuously scanning the runtime behaviors of the .exe, you drop (Via Download&Execute task) a UAC exploit or a WD exclusions .reg or pwrshell script which adds your entire C:\ to exclusions from being scanned.

After this, anything dropped to the PC doesn't have to be crypted and can often run like normal without risking encryption messing up the \dir\ drop and pack of your stealer.

The key benefit of this method is ability to use the logs you pull from a stealer (whether it be reverse proxy, hVNC or just straight up remote desktop)

So in my case the loader configuration gives me a .jpg to upload and get download link which I paste in crypter before crypter spits out an .exe for me. Do I upload the exe and spread exe download link or do I spread download link for the .jpg that crypter creates before creating exe?

(Aug 28, 2022 09:34 AM)Dyne Wrote: [\[CITE\]](#) Ah, loader stub is slang for a botnet stub. A botnet is for holding clients.

Once the client connects to your botnet stub and connection is established , to prevent AV from continuously scanning the runtime behaviors of the .exe, you drop(Via Download&Execute task) a UAC exploit or a WD exclusions .reg or pwrshell script which adds your entire C:\ to exclusions from being scanned.

After this, anything dropped to the PC doesn't have to be crypted and can often run like normal without risking encryption messing up the \dir\ drop and pack of your stealer.

The key benefit of this method is ability to use the logs you pull from a stealer (whether it be reverse proxy, hVNC or just straight up remote desktop)

If you have telegram I can send you a video of crypter software running. It's only about a minute long.

YAK_CODER - August 28, 2022, 11:53 am

Just use self inject

will solve most recovery and proxy problems

Resident3vil - August 28, 2022, 12:22 pm

(Aug 28, 2022 11:53 AM)YAK_CODER Wrote: [\[CITE\]](#) Just use self inject

will solve most recovery and proxy problems

Thanks. I will test this. Are you familiar with Loader features? It produces a .jpg that I need to host and get download link for Crypter to finish crypting the build and to produce the exe.

If you are familiar with this feature, my question is do I spread the .jpg download link or do I upload exe to host at this point and spread the download link for exe? I guess I'm just lost on the use of .jpg after crypt is complete.

Ph4n70M Phr34K - August 28, 2022, 12:35 pm

(Aug 28, 2022 12:22 PM)Resident3vil Wrote: [\[CITE\]](#) Thanks. I will test this. Are you familiar with Loader features? It produces a .jpg that I need to host and get download link for Crypter to finish crypting the build and to produce the exe.

If you are familiar with this feature, my question is do I spread the .jpg download link or do I upload exe to host at this point and spread the download link for exe? I guess I'm just lost on the use of .jpg after crypt is complete.

first of you have confused a botnet loader with "loader mode" in PureCrypter.

In PureCrypter you need to enable "loader mode" then click "get php files". It will show you loader.zip archive which you need to extract and upload to your webserver, you can use cpanel for example, then you need to put the direct link to upload.php file, you can see example in PureCrypter. Now you can click test to see if it works.

If it works then you will be able to crypt your file, it will produce normal executable file, unless you choose another extension. Thats the file you can spread.

Resident3vil - August 28, 2022, 12:50 pm

(Aug 28, 2022 12:35 PM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) first of you have confused a botnet loader with "loader mode" in PureCrypter.

In PureCrypter you need to enable "loader mode" then click "get php files". It will show you

loader.zip archive which you need to extract and upload to your webserver, you can use cpanel for example, then you need to put the direct link to upload.php file, you can see example in PureCrypter. Now you can click test to see if it works.

If it works then you will be able to crypt your file, it will produce normal executable file, unless you choose another extension. Thats the file you can spread.

Bruh thank you. This is the explanation I needed of this feature. Thanks.

jason123 - August 28, 2022, 1:08 pm

(Aug 28, 2022 12:35 PM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) first of you have confused a botnet loader with "loader mode" in PureCrypter.

In PureCrypter you need to enable "loader mode" then click "get php files". It will show you loader.zip archive which you need to extract and upload to your webserver, you can use cpanel for example, then you need to put the direct link to upload.php file, you can see example in PureCrypter. Now you can click test to see if it works.

If it works then you will be able to crypt your file, it will produce normal executable file, unless you choose another extension. Thats the file you can spread.

Great?

Resident3vil - September 2, 2022, 2:42 pm

UPDATE:

So after continuing to test the suggestions here I still didn't have any success which led me to believe maybe it's just the Crypter incompatible with the software. I then purchased a crypt from a referral I got in the raccoon group and all tests have been flawless.

But I still have Pure Crypter and I'd like to put that to work. So I purchased Pure Miner. It also has a loader feature which I'm hoping works good but I've been having trouble getting even a test worker to show up on the dashboard. I've hired someone from this forum who's vouched for setup but we haven't yet figured out why my test stubs aren't giving me any workers when I run the program. This guy has been very responsive so I'm hoping we figure it out soon but if you guys have any experience with Pure Miner and have had similar issues when testing please offer any tips you have that got you up and running.

Thanks!