

Forum:[Hack Forums](#)

Thread: [How do I bypass Trojan.TR/Dropper.Gen with runPE?](#)

ArcticSlay - April 11, 2020, 3:16 am

I've currently got my crypter and program down to 3/26 using a refud of runPE and cannot bypass Trojan.TR/Dropper.Gen.

<https://antiscan.me/scan/new/result?id=ma24fHL8xn1j>

Chameleon - April 11, 2020, 4:25 am

it's so hard i remember back in the day web avira was the bastard that no one could bypass but these days it has seemed to have died down

CROW - April 11, 2020, 4:45 am

Hey, man at least you're bypassing Avast. That's a plus.

ArcticSlay - April 11, 2020, 5:14 am

(Apr 11, 2020 04:45 AM)TechaOG Wrote: [\[CITE\]](#) Hey, man at least you're bypassing Avast. That's a plus.

True, I could look at the ups, just I thought I was doing well by changing the information and so on, but I cannot seem to add the registry startup properly in the injection either... But it sends past av's which is a plus.

CROW - April 11, 2020, 5:42 am

Yeah, i'm having trouble with the registry as well. It adds to the Current User but not into the "run" part.

But i know why that is, because my file does not get dropped on the disk it's going straight to memory so when the target executes it, i'll have to add it by hand.
Which sucks.

Wish i was friends with a programmer so i could get some help but when you ask for help anywhere on the internet you get yelled at hahaha.

I just look at other code and try to add it to my code the best way i can, but sometimes it does not work out cause i don't have enough arguments in the code.

youlded - has1 - April 11, 2020, 6:47 am

Most of those methods aren't going to be free, with that knowledge you can sell a crypter on here.

I have a method that will remove any scantime detection of your runPE, startup, & similar methods for 100\$.

VisualSoft - April 11, 2020, 7:04 am

(Apr 11, 2020 04:45 AM)TechaOG Wrote: [\[CITE\]](#) Hey, man at least you're bypassing Avast. That's a plus.

Avast is much easier to bypass than avira.

(Apr 11, 2020 06:47 AM)youlded - has1 Wrote: [\[CITE\]](#) Most of those methods aren't going to be free,

with that knowledge you can sell a crypter on here.

I have a method that will remove any scantime detection of your runPE, startup, & similar methods for 100\$.

I agree with you my friend.

CROW - April 11, 2020, 8:03 am

(Apr 11, 2020 07:04 AM)VisualSoft Wrote: [\[CITE\]](#) Avast is much easy to bypass then avira.

I agree with you my friend.

I kinda figured avast would be really hard to bypass haha but yet again i hardly know what i'm doing, but i am getting better.

I just need to learn some technique's. I'm scared to buy a crypter on here cause i got a lot of feed back, saying "crypters on HF's don't do much.

But that's just what i heard.

I love messing around with base64 strings. If i can figure out some new technique's i'll be good to go. I just need to learn a bit more.

It's just really hard learning on you're own cause you don't know where to start hahaha.

NYANxCAT - April 11, 2020, 11:18 am

(Apr 11, 2020 03:16 AM)ArcticSlay Wrote: [\[CITE\]](#) I've currently got my crypter and program down to 3/26 using a refud of runPE and cannot bypass Trojan.TR/Dropper.Gen.

<https://antiscan.me/scan/new/result?id=ma24fHL8xn1j>

I don't think someone will give you free tutorial on how to refud or how to bypass specific av otherwise no one will sell private stubs or public crypter on HF....

post here [Service Requests](#) and you will get help within a day or two

n0\$f3ratu\$ - April 11, 2020, 12:21 pm

(Apr 11, 2020 03:16 AM)ArcticSlay Wrote: [\[CITE\]](#)

Are you positive that detection is from runpe?

Are you sure is not from Assembly.Load or resources?

Redrum - April 11, 2020, 5:49 pm

You could try zipping the Binary in the res instead of just encrypting?

I've bypassed it before using passworded zip files to hold binary in res before

ArcticSlay - April 11, 2020, 9:42 pm

(Apr 11, 2020 11:18 AM)??` NYAN CAT `?? Wrote: [\[CITE\]](#) I don't think someone will give you free tutorial on how to refud or how to bypass specific av otherwise no one will sell private stubs or public crypter on HF....

post here [Service Requests](#) and you will get help within a day or two

Thanks, yeah I don't need help on the refud, just wondering basically what that antivirus detection was basically, so if I know what it is, I can find a way around it without exploiting people for free services.

(Apr 11, 2020 05:49 PM)Redrum Wrote: [\[CITE\]](#) You could try zipping the Binary in the res instead of

just encrypting?

I've bypassed it before using passworded zip files to hold binary in res before

Thank you for the feedback, I will try.

(Apr 11, 2020 12:21 PM)n0\$f3ratu\$ Wrote: [\[CITE\]](#) Are you positive that detection is from runpe?
Are you sure is not from Assembly.Load or resources?

I am not to be honest. I'll check other ways around, ty.

(Apr 11, 2020 08:03 AM)TechaOG Wrote: [\[CITE\]](#) I kinda figured avast would be really hard to
bypass haha but yet again i hardly know what i'm doing, but i am getting better.

I just need to learn some technique's. I'm scared to buy a crypter on here cause i got a lot of feed
back, saying "crypters on HFs don't do much.

But that's just what i heard.

I love messing around with base64 strings. If i can figure out some new technique's i'll be good to
go. I just need to learn a bit more.

It's just really hard learning on you're own cause you don't know where to start hahaha.

I am a noob when it comes to that too man, it's a cool learning experience. HMU on discord for
some ideas to share lol Arctic#3060

zataeta - April 12, 2020, 11:51 pm

tell me in Dis,c-0rd -> Quebe\$h#3858 and i can put it fud 100% for you

finalexception - April 15, 2020, 4:42 pm

bro it says dropper, just stop droppin