

Forum:[Hack Forums](#)

Thread: [How the fuck do I get rid of these dumb generic detections?](#)

DafforDucc - August 11, 2018, 1:02 am

No matter what RAT I use, or what crypter, or what settings, I get the same amount of detections (16-18), all with the same detection spammed across the results. Gen:Variant.Razy.*insert a random number*.

I have learned through the Crypter Bible that this is simply a matter of assembly information and icon? If this is the case, then what magic assembly or fucking icon must I use to get past these detections? No matter what I use, it is still detected across the board. What happened to RATs being easy :/? It used to be all you needed was fucking DarkComet and a random crypter and you were good to go.

Don't these AV companies have better things to do than going after RATs, like finding real scammers and real viruses, like ransomware and things that destroy infrastructure? ???

Cød3ing - August 11, 2018, 1:16 am

Sorry to break it to you but there's this thing called the runtime and if you thought bypassing scantime detections with assembly info & icon changes was complex you're in for a real treat.

As soon as that stuff is popped on a system with any decent AV it's going to be shot down pretty quick. Good AV's are active at ring 0 while your stuff is in ring 3 or 2 at best. It's also incredibly hard to maintain persistence since AVs are now turning to using ELAM.

No detections across "all" (or realistically most) top AVs is why those sort of builds can cost a real pretty penny.

DafforDucc - August 11, 2018, 1:41 am

(Aug 11, 2018 01:16 AM)Cod3ing® Wrote: [\[CITE\]](#) Sorry to break it to you but there's this thing called the runtime and if you thought bypassing scantime detections with assembly info & icon changes was complex you're in for a real treat.

As soon as that stuff is popped on a system with any decent AV it's going to be shot down pretty quick. Good AV's are active at ring 0 while your stuff is in ring 3 or 2 at best. It's also incredibly hard to maintain persistence since AVs are now turning to using ELAM.

No detections across "all" (or realistically most) top AVs is why those sort of builds can cost a real pretty penny.

lol you sound like a cuck for the AV companies, or an undercover AV employee on HF. Well, I did something pretty simple and figured out how to get rid of those generic detections, and the RAT is 100% functional. Got it down to 8 detections out of 30, compared to the 16-18 before due to generic shit. Some of the legit detections that is from the code itself is still there, but they are more obscure/expensive AV's picking up on it. Shit like AVG, Avast and Windows Defender aren't picking up on them, so gg mate.

FuxXER - August 11, 2018, 1:42 am

This will solve your generic detection issue.

[>\[1#\] ReFUD Gen:Variant,Razy, Bary,Zusy,Kazy,Conjor,Win32:Evo-gen \[Susp\]](#)

DafforDucc - August 11, 2018, 1:44 am

(Aug 11, 2018 01:42 AM)FuxXER Wrote: [\[CITE\]](#) This will solve your generic detection issue.

[>\[1#\] ReFUD Gen:Variant,Razy, Bary,Zusy,Kazy,Conjor,Win32:Evo-gen \[Susp\]](#)

The thing that I figured out for free is probably the same thing this dude is selling for \$25. Like anyone with a brain is gonna pay for that shit, come on man. I should release my own tutorial for free on how I did it.

FuxXER - August 11, 2018, 1:52 am

(Aug 11, 2018 01:44 AM)DafforDucc Wrote: [\[CITE\]](#) The thing that I figured out for free is probably the same thing this dude is selling for \$25. Like anyone with a brain is gonna pay for that shit, come on man. I should release my own tutorial for free on how I did it.

Fuck you!

DafforDucc - August 11, 2018, 1:56 am

(Aug 11, 2018 01:52 AM)FuxXER Wrote: [\[CITE\]](#) Fuck you!

You know I saw your thread earlier when I was trying to figure this out, and I considered buying it, but \$25 is ridiculous. I already spent that much on my crypter, I don't want to spend that much more on some basic ass method. If it was \$10-\$15 I would've bought it probably.

3DES - August 11, 2018, 4:52 am

If your crypt isnt FUD without icon/assembly you have terrible crypt.

(Aug 11, 2018 01:44 AM)DafforDucc Wrote: [\[CITE\]](#) The thing that I figured out for free is probably the same thing this dude is selling for \$25. Like anyone with a brain is gonna pay for that shit, come on man. I should release my own tutorial for free on how I did it.

You cant bypass shit, nobody gives a shit about your shitty .NET crapware, dyncheck with internet you mentally challenged idiot if you dont believe me.

DecAnn - August 11, 2018, 5:08 am

(Aug 11, 2018 01:44 AM)DafforDucc Wrote: [\[CITE\]](#) The thing that I figured out for free is probably the same thing this dude is selling for \$25. Like anyone with a brain is gonna pay for that shit, come on man. I should release my own tutorial for free on how I did it.

When are you releasing ur own tutorial? could you plz pm about this. would appreciate it, thanks

Twistd - August 11, 2018, 8:44 am

The detections you describe are heuristic detections, they are based on behaviour which can be either codeflow or api chains being detected scantime.

If you wish to get rid of these detections you need to change the main codeflow codeflow. Another cheap way that can help is adding a string table to the executable in resources, just clone from a different legit file.

Like mentioned above, scantime isnt really the challenge here, the challenge is full runtime bypass.

People claiming you need to use an "HQ" icon are just simply wrong. You shouldnt need to use an icon at all.

My experience with removing detections comes from asm and c/c++, if you're using programming managed code it might be different.

joleyman22 - August 11, 2018, 11:21 pm

You're saying you've tried a slew of RAT/Crypter combinations and end up with the same cruddy results? Sounds like you're using cruddy programs with cruddy crypters. 8/30 detections is still

terrible. If your getting tons of detections scantime, the second your file drops/is executed, it will be almost instantly deleted. I recommend investing more than \$25 in a crypter. A private stub crypter is ideal, but there are decent and affordable crypters out there like DataProtector.

DafforDucc - August 12, 2018, 4:44 am

(Aug 11, 2018 11:21 PM)joleyman22 Wrote: [\[CITE\]](#) You're saying you've tried a slew of RAT/Crypter combinations and end up with the same cruddy results? Sounds like you're using cruddy programs with cruddy crypters. 8/30 detections is still terrible. If your getting tons of detections scantime, the second your file drops/is executed, it will be almost instantly deleted. I recommend investing more than \$25 in a crypter. A private stub crypter is ideal, but there are decent and affordable crypters out there like DataProtector.

How about donating to my crypter fund? I don't have fifty fucking dollars to drop on some dude's recoding of another crypter. Nothing that the kids on HF release is worth more than thirty dollars. It's all the same recodes, and I could do it myself with ease if I had the free time to make my own.

Unfortunately I have classes, and a life to live. ?

Tyler Durden. - August 12, 2018, 4:58 am

You are a fucking idiot - get the hell off this forum.

DafforDucc - August 12, 2018, 5:16 am

(Aug 12, 2018 04:58 AM)Tyler Durden. Wrote: [\[CITE\]](#) You are a fucking idiot - get the hell off this forum.

Okay but why though? What's your argument for that? Or are you just going to say words without any reasoning to back it up, cause you're a fucking idiot yourself?

r4nd0mdvr - August 12, 2018, 8:30 am

(Aug 11, 2018 01:44 AM)DafforDucc Wrote: [\[CITE\]](#) The thing that I figured out for free is probably the same thing this dude is selling for \$25. Like anyone with a brain is gonna pay for that shit, come on man. I should release my own tutorial for free on how I did it.

How did you do it? ?

narc0tic - August 12, 2018, 8:49 am

(Aug 11, 2018 01:44 AM)DafforDucc Wrote: [\[CITE\]](#) The thing that I figured out for free is probably the same thing this dude is selling for \$25. Like anyone with a brain is gonna pay for that shit, come on man. I should release my own tutorial for free on how I did it.

Well you're not wrong.

Have you tried not using a icon or assembly?

Twistd - August 13, 2018, 1:37 pm

(Aug 13, 2018 12:08 PM)Phobophile Wrote: [\[CITE\]](#) If you refuse to invest the time to learn yourself then you don't deserve to have your problem fixed. So go off and "live your life" and stop asking for everything to be handed to you.

Totally support this. Some people are just beyond saving :)

NotAFed - August 13, 2018, 6:53 pm

Imagine paying for a rat that isn't fud lul. This is why I make my own, and they're FUD and always will be :)

Enjoy dropping 60 on a garbage rat 300+ people use

wiwiki - August 30, 2018, 3:44 pm

try changing assemble and icon.

ANoBody - August 30, 2018, 9:36 pm

Bro you really rude to people, all the people replying here are just trying to help you, so give them the fucking decency of being nice to them you may not like their idea but you can atleast politely say that not what your looking for particular.

Get some respect kid

FuxXER - August 31, 2018, 9:34 am

(Aug 12, 2018 08:49 AM)narc0tic Wrote: [\[CITE\]](#) Well you're not wrong.

Have you tried not using a icon or assembly?

Not only icon/assembly will cause generic detections and \$25 bucks is not teaching U how to change icon/assembly aswell.

narc0tic - August 31, 2018, 10:34 am

(Aug 31, 2018 09:34 AM)FuxXER Wrote: [\[CITE\]](#) Not only icon/assembly will cause generic detections and \$25 bucks is not teaching U how to change icon/assembly aswell.

Like, but seriously.

You have to be a serious dumbass to spend \$25 on something you can just ask your crypter owner to help you with.

? BL4ZE - August 31, 2018, 11:56 am

(Aug 31, 2018 10:34 AM)narc0tic Wrote: [\[CITE\]](#) Like, but seriously.

You have to be a serious dumbass to spend \$25 on something you can just ask your crypter owner to help you with.

I agree with you, if you asked crypter owner they'll definitely help and you don't have to pay extra \$25

FuxXER - August 31, 2018, 12:38 pm

I loose \$36.50 cause by asking for support.

<https://hackforums.net/showthread.php?tid=5843284&pid=57151148#pid57151148>

narc0tic - August 31, 2018, 1:08 pm

(Aug 31, 2018 12:38 PM)FuxXER Wrote: [\[CITE\]](#) I loose \$36.50 cause by asking for support.

<https://hackforums.net/showthread.php?tid=5843284&pid=57151148#pid57151148>

Imao, you called the guy gay for fucks sake.

He has a right to ban you if you are being rude.

? BL4ZE - August 31, 2018, 2:27 pm

(Aug 31, 2018 01:08 PM)narc0tic Wrote: [\[CITE\]](#) Imao, you called the guy gay for fucks sake.

He has a right to ban you if you are being rude.

You should read whole thread before saying anything!

He clearly means "guy" not "gay".

and in third message, you can clearly see no' is the first one to being rude!

after that he said "gay" accidentally!.

FeelsBadMan!

narc0tic - September 1, 2018, 5:10 am

(Aug 31, 2018 02:27 PM)? BL4ZE Wrote: [CITE](#) You should read whole thread before saying anything!

He clearly means "guy" not "gay".

and in third message, you can clearly see no' is the first one to being rude!

after that he said "gay" accidentally!.

FeelsBadMan!

Hmm, should have read the thread better.

Sorry about that.

No\$ is known to have bit of a temper.

Still, I suggest finding a crypter with nicer support than spending \$25.