

Forum:[Hack Forums](#)

Thread: [how to bypass Trojan:Win32/Wacatac.D!ml](#)

notahackerman - April 25, 2020, 3:39 am

hello guys, how to bypass this thing?

Trojan:Win32/Wacatac.D!ml

it's the result on scan on antiscan.me for Windows Defender..

some1 have an idea?

VisualSoft - April 25, 2020, 3:48 am

Its simple, replace the code which is causing that detection.

notahackerman - April 25, 2020, 7:49 am

(Apr 25, 2020 03:48 AM)VisualSoft Wrote: [\[CITE\]](#) Its simple, replace the code which is causing that detection.

yeah, ofc lmao you're mastermind, thank you help wtf..

should i replace with? lol

Shadow_Cloud - April 25, 2020, 8:36 am

(Apr 25, 2020 07:49 AM)notahackerman Wrote: [\[CITE\]](#) yeah, ofc lmao you're mastermind, thank you help wtf..

should i replace with? lol

You really aren't giving us enough info. Do you even know which code is causing the detection? If you break this down to smallest possible form of which code flags the detection, we might be able to help. But without any idea of the code causing this, how should we know what to replace it with?

VisualSoft - April 25, 2020, 9:15 am

(Apr 25, 2020 07:49 AM)notahackerman Wrote: [\[CITE\]](#) yeah, ofc lmao you're mastermind, thank you help wtf..

should i replace with? lol

What should you replace?

Untill and unless we dont have the code you used Only GOD Can tell what to replace ?

notahackerman - April 25, 2020, 10:28 am

(Apr 25, 2020 08:36 AM)Shadow_Cloud Wrote: [\[CITE\]](#) You really aren't giving us enough info. Do you even know which code is causing the detection? If you break this down to smallest possible form of which code flags the detection, we might be able to help. But without any idea of the code causing this, how should we know what to replace it with?

(Apr 25, 2020 09:15 AM)VisualSoft Wrote: [\[CITE\]](#) What should you replace?

Untill and unless we dont have the code you used Only GOD Can tell what to replace ?

i'm using this one,

<https://github.com/NYAN-x-CAT/Bitcoin-Grabber/blob/master/Bitcoin-Grabber/Program.cs>

thx nyan cat

what should i replace to avoid that detection guys?

Shadow_Cloud - April 25, 2020, 10:57 am

(Apr 25, 2020 10:28 AM)notahackerman Wrote: [\[CITE\]](#) i'm using this one,
<https://github.com/NYAN-x-CAT/Bitcoin-Grabber/blob/master/Bitcoin-Grabber/Program.cs>

thx nyan cat

what should i replace to avoid that detection guys?

Can you tell us which part is being detected?

notahackerman - April 25, 2020, 11:50 am

(Apr 25, 2020 10:57 AM)Shadow_Cloud Wrote: [\[CITE\]](#) Can you tell us which part is being detected?
how could i find out?

it's the whole source and if you google the Wacatac meaning it's something like:

<https://malwarefixes.com/threats/trojanwin32-wacatac-dml/>

Shadow_Cloud - April 25, 2020, 11:52 am

(Apr 25, 2020 11:50 AM)notahackerman Wrote: [\[CITE\]](#) how could i find out?

it's the whole source and if you google the Wacatac meaning it's something like:

<https://malwarefixes.com/threats/trojanwin32-wacatac-dml/>

Typically you can narrow this down to a file/class based on the description of the detection. But we don't have your code, its going to be very hard for us to divine this.

notahackerman - April 25, 2020, 12:00 pm

(Apr 25, 2020 11:52 AM)Shadow_Cloud Wrote: [\[CITE\]](#) Typically you can narrow this down to a file/class based on the description of the detection. But we don't have your code, its going to be very hard for us to divine this.

nevermind, the confuserEx made it, thank you anyway

VisualSoft - April 25, 2020, 12:14 pm

In case you are using that Rat, I would suggest you to use a Crypter,

In case you plan to use that particular Feature, then I suggest you to Comment functions of that project and see at which point the detection goes.

(Apr 25, 2020 12:00 PM)notahackerman Wrote: [\[CITE\]](#) nevermind, the confuserEx made it, thank you anyway

It wont be for long, SO I would suggest you to find some other option to FUD.

__Digital__ - April 25, 2020, 12:47 pm

(Apr 25, 2020 11:50 AM)notahackerman Wrote: [\[CITE\]](#) how could i find out?

it's the whole source and if you google the Wacatac meaning it's something like:

<https://malwarefixes.com/threats/trojanwin32-wacatac-dml/>

You sir are retarded, its called comment out the code piece by piece until its undetected. thats how you figure out whats getting flagged. it is not rocket science to figure it out.

confuserex is not always needed, learn to protect your code in other ways

notahackerman - April 25, 2020, 1:00 pm

(Apr 25, 2020 12:47 PM)___Digital___ Wrote: [\[CITE\]](#) You sir are retarded, its called comment out the code piece by piece until its undetected. thats how you figure out whats getting flagged. it is not rocket science to figure it out.

confuserex is not always needed, learn to protect your code in other ways
anyway, the problem is fixed, some junk codes added and stop using confuserx and WD is bypassed...

but on ILSPY i still can see my source, what should i do ?

(Apr 25, 2020 12:47 PM)___Digital___ Wrote: [\[CITE\]](#) You sir are retarded, its called comment out the code piece by piece until its undetected. thats how you figure out whats getting flagged. it is not rocket science to figure it out.

confuserex is not always needed, learn to protect your code in other ways
maybe Dotfuscator is more good or NETreactor? i have to protect the code ?

Accord - April 25, 2020, 8:59 pm

(Apr 25, 2020 01:00 PM)notahackerman Wrote: [\[CITE\]](#) anyway, the problem is fixed, some junk codes added and stop using confuserx and WD is bypassed...
but on ILSPY i still can see my source, what should i do ?

maybe Dotfuscator is more good or NETreactor? i have to protect the code ?
Use netguard, theyre offering excellent service for cheaper price.

notahackerman - April 26, 2020, 1:44 am

(Apr 25, 2020 08:59 PM)Accord Wrote: [\[CITE\]](#) Use netguard, theyre offering excellent service for cheaper price.
i'm using code dom as builder to compile the source from source.cs

if i'll buy netguard and then crypt the builder, the source compiled will be crypted too or?

Accord - April 26, 2020, 2:34 am

(Apr 26, 2020 01:44 AM)notahackerman Wrote: [\[CITE\]](#) i'm using code dom as builder to compile the source from source.cs

if i'll buy netguard and then crypt the builder, the source compiled will be crypted too or?
No, i thought you only have one binary, if you have builder and you want output to be obfuscated (not crypted) then you need to obfuscate it with netguard everytime.

If youre working with malware, netguard will terminate your account

If youre working with malware, netguard will terminate your account

notahackerman - April 26, 2020, 10:45 pm

(Apr 25, 2020 08:59 PM)Accord Wrote: [\[CITE\]](#) Use netguard, theyre offering excellent service for cheaper price.
i need something which offer me to protect that exe for each client for each time

Shadow_Cloud - April 26, 2020, 11:32 pm

(Apr 26, 2020 10:45 PM)notahackerman Wrote: [\[CITE\]](#) i need something which offer me to protect that exe for each client for each time

Change the paradigm so nothing sensitive is on the exe.

You could easily create the exe so it fetches code at runtime. Assuming you aren't injecting anything retarded that gets flagged, you'll have all the flexibility you need.

If you get creative with this it will be quite hard to block the source. Don't have this fetch from an IP or Domain directly that a sure way to get reported for abuse.