

Forum: [Hack Forums](#)

Thread: [Where can I get a heavily detected virus \(PE\) from?](#)

ObscureCoder - October 4, 2014, 9:25 am

I really need a virus for a project I'm working on... I just need it to be detected as a virus by almost all AVs.

I'm not sure how easy something like this would be to obtain but it's fine since I'm developing on Linux right now so it's all good. I'm also not sure if the spreading of malware is allowed on HF but if anyone can point me in the right direction that'd be great ;) Thanks.

Da? ?ae - October 4, 2014, 9:27 am

I mean.. all you'd need to do is download DarkComet, and output a random ass stub xD
Like enable Keylogger, Enable AV killer, enable the shit that you WOULDN'T want to happen to your PC.

Most AVs will recognize this in a heartbeat.

EDIT: 300 posts yay

s1r_n0z - October 4, 2014, 9:35 am

old timers rats will do the job for you. Trojanfrance had very old ones. That i can remember some are:

sub7/beast/poisonivy/win-spy/ and some more. Good luck and i hope i help a little.

PS: another ver detected malware is Ardamax Keylogger.

ObscureCoder - October 4, 2014, 9:42 am

Thanks guys for the suggestions. I'll look for some. It can't be too hard to find some good old viruses xD

Tiny Hippo - October 4, 2014, 11:14 am

Take a look at the EICAR test file. It's a fake virus that will not do anything harmful to your system, but most anti viruses will recognize it as a virus. It was made specifically for testing the capability of anti viruses. Even my Mac detected it as a virus.

Info: <http://www.f-secure.com/v-descs/eicar.shtml>

DL: <http://www.f-secure.com/virus-info/eicar.com>

Here's a scan:

<https://www.virustotal.com/en/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd0f/analysis/1412446280/>

Anyone can make this virus by pasting the following onto a text editor and save it as filename.com
Code X5O!P%#@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

ObscureCoder - October 4, 2014, 11:56 am

(Oct 4, 2014 11:14 AM)Tiny Hippo Wrote: [\[CITE\]](#) Take a look at the EICAR test file. It's a fake virus

that will not do anything harmful to your system, but most anti viruses will recognize it as a virus. It was made specifically for testing the capability of anti viruses. Even my Mac detected it as a virus.

Info: <http://www.f-secure.com/v-descs/eicar.shtml>

DL: <http://www.f-secure.com/virus-info/eicar.com>

Here's a scan:

<https://www.virustotal.com/en/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f/analysis/1412446280/>

Anyone can make this virus by pasting the following onto a text editor and save it as filename.com
Code X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Yeah, I checked it out. Basically, I discovered how easy crypters were to make xD

joneh heil - October 4, 2014, 1:33 pm

Lol, please tell me why you need this! ?

ObscureCoder - October 4, 2014, 1:52 pm

(Oct 4, 2014 01:33 PM)joneh heil Wrote: [\[CITE\]](#) Lol, please tell me why you need this! ?

Testing crypter development.

Using Java and C++ w/ JNI.

Niely - October 4, 2014, 1:53 pm

EICAR is the only virus stimulator I can find:

<http://www.eicar.org/86-0-Intended-use.html>

You can also download a script-kiddie tool from Mediafire like DoSer.exe and bind that to your project using a binder.

EICAR is the most best solution though, I think you also have to bind it.

<https://hackforums.net/showthread.php?tid=3354709>

(Oct 4, 2014 01:52 PM)ObscureCoder Wrote: [\[CITE\]](#) Testing crypter development.

Using Java and C++ w/ JNI.

In that case,

Try to download malware on a VM (tools like DoSer.exe); then crypt that malware with your crypter and see if the Anti-Viruses on your VM detect it, if not; you've got a decent crypter. :)

ObscureCoder - October 4, 2014, 1:56 pm

(Oct 4, 2014 01:53 PM)?Niely Wrote: [\[CITE\]](#) EICAR is the only virus stimulator I can find:

<http://www.eicar.org/86-0-Intended-use.html>

You can also download a script-kiddie tool from Mediafire like DoSer.exe and bind that to your project using a binder.

EICAR is the most best solution though, I think you also have to bind it.

<https://hackforums.net/showthread.php?tid=3354709>

In that case,

Try to download malware on a VM (tools like DoSer.exe); then crypt that malware with your crypter and see if the Anti-Viruses on your VM detect it, if not; you've got a decent crypter. :)

Thanks for the ideas mate ;) Will do so.