

Forum:[Hack Forums](#)

Thread: [Misconceptions about dependencies](#)

Slavoj Žižek - November 18, 2016, 10:27 am

There is a lot of incorrect information going around hf, I want to slightly change that

What is a dependency?

A dependency for example java or .net that needs to be installed for the file to execute. if you have a no dependencies file it will more than likely have a quite high execution rate.

C++ is non-dependant right?

No, not necessarily sometimes some C++ files use Visual C++ which need the visual C++ framework installed. but most of the time C++ will be native.

I was told .net was running on 98% of computers?

I'm not sure about the 98% number but yes there is a quite high percentage of computers that have .net pre-installed

One problem .net is not fully reverse compatible, for example if I have .net 2.0 malware it will only execute (without installing extra updates) on windows 7 machines

leaving 8, 8.1, 10, vista and XP out of the picture whereas if I had .net 4.0 malware it will execute on windows 10 (without installing extra updates) but nothing else

(some frameworks come packaged with other ones, for example the .net 2.0 installer also installs 3.5)

when it comes to windows XP its best to have non-dependant malware since its pre-installed with no .net frameworks.

so just because 98% of computers have .net installed does not mean you will have a 98% execution rate, there are many variables

If I crypt a .net file with A native crypter that makes it native right?

You would seriously be surprised with the amount of people that actually think this but it is completely incorrect

a .net file will always be .net there is nothing you can do about that and if you crypt a .net file with a native crypter the execution rate will be held back because they still need the correct .net framework installed for the file to work.

crypting native malware with a .net crypter is a pretty bad Idea, since your malware is native you might as well go with a native crypter - get the whole XP - 10 execution range.

What about java then?

java is a cool language and all but nothing comes pre-installed with java (the odd linux distro does) and the only people I have ran into running java were either developers or minecrafters.

Personally I would stay away from java, for execution rate reasons (the actual malware its self might be good)

Ok then, what OS'es come pre-installed with these?

Windows XP - .NET 1.0

Windows vista - .NET 2.0

Windows 7 - .NET 3.5 (which includes 2.0)

Windows 8 / 8.1 - .NET 4.0+

Windows 10 - .NET 4.5+ (backwards compatible with 4.0)

(Thanks quicksilver!)

some linux distros - java (pls no java malware)

Languages and their dependencies

C++ - most of the time native, could be VC++ though

C - Native

Assembly (FASM, NASM, MASM etc) - Native

Delphi - Native

AutoIT - Native but quite large file size compared to c, cpp etc

Go - Native but absolutely massive file size 3mb+ generally.

vb.net - .net

C# - .net

F# - .net

python - you need to install python (please, never write malware in python, unless you use pyinstaller)

tl:dr don't crypt native malware with .net crypter

just because there is apparently 98% of computers have .net installed does not mean anything, .net is not completely reverse compatible

if you want as high execution rate go with something native like C++, C, assembly etc

There might be some incorrect information / spelling or grammar mistakes - I'm open to constructive crit

regards, blez ?

7 - November 18, 2016, 10:32 am

Good post. I know this is obvious for a lot of us users but there are many who still do not get it. Very useful.

SIM-297877 - November 18, 2016, 10:34 am

Go is fully native, also cross-platform.

7 - November 18, 2016, 10:37 am

(Nov 18, 2016 11:34 AM)SaturnsVoid Wrote: [\[CITE\]](#) Go is fully native, also cross-platform.

Yeah??? Nice. Look into that. Your botnet is Go ?

SIM-297877 - November 18, 2016, 10:38 am

(Nov 18, 2016 11:37 AM)NulldB Wrote: [\[CITE\]](#) Yeah??? Nice. Look into that. Your botnet is Go ?

Yeah, i switched to only coding in Go. Love it vary powerful just needs more people to adopt it.

Check out Go here: <https://golang.org/>

Slavoj Žižek - November 18, 2016, 10:40 am

(Nov 18, 2016 11:38 AM)SaturnsVoid Wrote: [\[CITE\]](#) Yeah, i switched to only coding in Go. Love it vary powerful just needs more people to adopt it.

I heard it once or twice until I saw your thread, how big are the file size? like AutoIT? ?

SIM-297877 - November 18, 2016, 10:44 am

(Nov 18, 2016 11:40 AM)Blezzedd Wrote: [\[CITE\]](#) I heard it once or twice until I saw your thread, how big are the file size? like AutoIT? ?

Yeah about, Though they drop about 5-10% each compiler update it seems.... Most large-scale applications will be around 5mb, but they compress good.

bzr? - November 18, 2016, 10:46 am

Nice thread that is really informative. Will hopefully educate a lot of users about this area.

Purple Kief - November 18, 2016, 10:52 am

If you made this you did a really good job.

Hope to see more of this.

Slavoj Žižek - November 18, 2016, 10:58 am

(Nov 18, 2016 11:52 AM)Purple Kief Wrote: [\[CITE\]](#) If you made this you did a really good job.

Hope to see more of this.

thanks m80, its all mine

Qismon - November 18, 2016, 11:09 am

I agree with everything you said except for the python malware.....I have one that is written in python, very stable, and no need for python to be installed on client PC.....compiled with pyinstaller.....works on XP - Win10.

Slavoj Žižek - November 18, 2016, 11:40 am

(Nov 18, 2016 12:09 PM)pdapentester Wrote: [\[CITE\]](#) I agree with everything you said except for the python malware.....I have one that is written in python, very stable, and no need for python to be installed on client PC.....compiled with pyinstaller.....works on XP - Win10.

You have a point, I have changed it ?

QU?CKSILVER - November 18, 2016, 4:10 pm

(Nov 18, 2016 11:27 AM)Blezzedd Wrote: [\[CITE\]](#) (some frameworks come packaged with other ones, for example the .net 2.0 installer also installs 3.5)

It's actually the other way around. 3.5 includes 2.0

(Nov 18, 2016 11:27 AM)Blezzedd Wrote: [\[CITE\]](#) when it comes to windows XP its best to have non-dependant malware since its pre-installed with no .net frameworks.

It actually comes with the very first .NET framework (1.0) but your point is valid, it's always best to use native apps to target WinXP and below.

(Nov 18, 2016 11:27 AM)Blezzedd Wrote: [\[CITE\]](#) Ok then, what OS'es come pre-installed with these?

windows XP - nothing

windows vista - (dont bother, nothing)

windows 7 - .net 2.0

windows 8 / 8.1 - .net 3.0

windows 10 - .net 4.5 (or 4.0 I really cannot remember)
some linux distros - java (pls no java malware)
Windows XP - .NET 1.0
Windows vista - .NET 2.0
Windows 7 - .NET 3.5 (which includes 2.0)
Windows 8 / 8.1 - .NET 4.0+
Windows 10 - .NET 4.5+

Slavoj Žižek - November 19, 2016, 1:08 am

(Nov 18, 2016 05:10 PM)QU?CKSILVER Wrote: [\[CITE\]](#) It's actually the other way around. 3.5 includes 2.0

It actually comes with the very first .NET framework (1.0) but your point is valid, it's always best to use native apps to target WinXP and below.

Windows XP - .NET 1.0
Windows vista - .NET 2.0
Windows 7 - .NET 3.5 (which includes 2.0)
Windows 8 / 8.1 - .NET 4.0+
Windows 10 - .NET 4.5+
thanks for the correction man, updated thread ?

TheHolyTrinity - November 19, 2016, 4:10 am

The whole Java thing is fair but spreading to Minecrafters with Java malware is actually really powerful as Java stays FUD for large periods of time. I've written my own malware in Java over 2 years ago and still has 0/35 detections, I haven't had to change anything and I get large executions rates across all platforms.

I understand that the average person trying to spread doesn't always use Minecraft but if you have that option it is extremely effective because of Java's ability to practically bypass all antiviruses. Plus if the Java malware is written effectively it should work on most installations no matter what operating system is running.

CichyCichoCiemny - November 19, 2016, 9:27 am

Epic :) it's really nice to see posta like this onse in this section ;)

Armada - November 19, 2016, 9:40 am

We really need more informative posts like this OP.
Thank you.

So often am I asked what is compatible to what, and even at times I get confused. Further its very nice to see others contributing to help make the thread the most updated and informative possible.

Kudos.

Codefuser - November 30, 2016, 7:58 am

Go lang has a pretty large file size too last I checked, don't discriminate autoit :p

Slavoj Žižek - November 30, 2016, 8:22 am

(Nov 30, 2016 08:58 AM)Codefuser Wrote: [\[CITE\]](#) Go lang has a pretty large file size too last I checked, don't discriminate autoit :p

AutoIT is great, its just the file size and how easy some code is to get into is a slight issue. ?

Codefuser - November 30, 2016, 8:29 am

(Nov 30, 2016 09:22 AM)Blezzedd Wrote: [\[CITE\]](#) AutoIT is great, its just the file size and how easy some code is to get into is a slight issue. ?

Golang is like 3mb bruh

autoit is 800kb

gua - November 30, 2016, 9:06 am

Here is some stupid question, if you have java crypter can you successfully crypt for example net based rat?

Shanonnn - November 30, 2016, 10:47 am

awesome thread blezz, im sure this will help a LOT of people out...

Slavoj Žižek - November 30, 2016, 1:16 pm

(Nov 30, 2016 10:06 AM)gua Wrote: [\[CITE\]](#) Here is some stupid question, if you have java crypter can you successfully crypt for example net based rat?

I seriously don't see why you would want to. But as long as you can write RunPE (I'm pretty sure its been done) in java it can be done (by injecting into another .net process)

EDIT : <https://hackforums.net/showthread.php?tid=3320638> - It can be done, but its pretty stupid to do so.

GordonJones - November 30, 2016, 3:03 pm

You wrote very useful thread for most users on HF, appreciate you effort. Threads like this make this place better.

iLogic™ - December 9, 2016, 8:27 am

Glad you updated OP with my suggestion. ?

LanMan - December 10, 2016, 2:37 pm

More information:

- Windows 10 Anniversary Update include .net 4.6.2 by default
- Windows 8.1 include .net 4.5.1
- Windows 8 include .net 4.5

- C++ and C can have microsoft VCRuntime dependencies (if they are not statically compiled)
- .net 4.0 is backward compatible with 2.0, but the PE CLR headers has changed.

#Skyline - December 10, 2016, 6:53 pm

Good to see a useful thread within this section.

Thanks for sharing !

ken0man - January 3, 2017, 2:10 am

good information.

what language is pony malware coded in and what type of crypter is best for it?

Slavoj Žižek - January 4, 2017, 8:48 am

(Jan 3, 2017 03:10 AM)ken0man Wrote: [\[CITE\]](#) good information.

what language is pony malware coded in and what type of crypter is best for it?

I have already sent you a PM answering the list of questions you had.

Pony was coded in MASM ?

purest21 - January 7, 2017, 4:49 pm

Thanks. Quality thread down here mate

The One Who Knocks - January 7, 2017, 8:00 pm

Thanks! Short read that clears up a few misconceptions I had.

Mr 4rs4l4ne - January 7, 2017, 8:26 pm

Thanks a lot for this precious informative article .

IKSector - April 3, 2017, 9:31 am

Great tutorial, thanks OP.

Armada - April 3, 2017, 9:42 am

Actually missed this thread, but it is a great accurate write up.

Thanks for sharing OP.

Slavoj Žižek - September 14, 2017, 6:35 pm

It's been a while since I was last on HF so I thought I would bump this thread to give it more attention.

presto.enterprize - October 4, 2017, 3:24 pm

Nice one. Keep it up Blezzedd!

TheWarOwl - October 4, 2017, 7:20 pm

I'm aware this is an old post but it's been bumped, so I'd like to leave my 2 cents here as well.

In regards to how many computers have .net installed, almost every version of windows has some form installed, see data here:

<https://blogs.msdn.microsoft.com/astebner/2007/03/14/mailbag-what-version-of-the-net-framework-is-included-in-what-version-of-the-os/>

Around 7% of the population uses windows xp or lower, which you might as well say it doesn't have .net because of huge compatibility issues that garbo gives lol. That leaves a large amount of the population at .net 3.4 and up. I feel linux based and other OS users are irrelevant, they have no reason to download an .exe unless you're targeting whine users for whatever your .exe is doing. You're still completely right though, if we're talking malware .net isn't optimal nor is it necessary. I'd think 85% - 90% of computers downloading are going to work fine, which is acceptable as a novice, however I think anyone planning to go big should have native languages as a standard.

I also feel I should mention that I believe it's possible to have .net capabilities in a c++ server (assuming we're talking about a rat) but void the .net dependencies within the client, since the server isn't what's being sent. There's a lot of complications with stuff like this, when I get asked questions it's tempting to slap people with the "learn to program first" card.

Good on you for making a post somewhat summarizing these things :blackhat might send people to read here first to save time.