Subject: Trojan in HelloWorld
Posted by andrew7m on Thu, 31 Dec 2015 07:48:06 GMT
View Forum Message <> Reply to Message

I just discovered UPP while searching for cross platform tools.
Looks great. Downloaded it and built the hello world example on Windows 7 no problems.
Uploaded the 3.2MB release build to www.virustotal.com and 7 of 54 virus scanners returned a trojan result (Gen:Trojan.Heur.TP.jFW@b8Z1enf).
False positives no doubt but why. If I make a win32 hello world it doesn't get false positives.
Are all projects built by UPP going to trigger this kind of result?

Subject: Re: Trojan in HelloWorld
Posted by koldo on Fri, 01 Jan 2016 21:39:54 GMT
View Forum Message <> Reply to Message

Hello Andrew

Thank you for you report.

VirusTotal does a good job as it checks uploaded files against 54 anti virus softwares for free.

I have just checked at VirusTotal Hello World example .exe compiled in a Windows 7 64 bits system with:
- Visual Studio 2015 32 and 64 bits
- MinGW TDM 32 ans 64 bits

No virus has been detected.

Could you give us more details about your system as OS and compiler used?

Subject: Re: Trojan in HelloWorld
Posted by andrew7m on Sat, 02 Jan 2016 01:30:57 GMT
View Forum Message <> Reply to Message

I'm using MinGW TDM.
I guess the default build settings were 32-bit. I changed to MINGWx64 and this results in no virus detections, like you observed.
Then I changed back to MINGW (32-bit) and I get 7 detections still.
My OS is Windows 7 Pro 64-bit Service Pack 1.
UPP is Version 9251 (64-bit).

I scanned my PC with five different AV products; MSE, Malwarebytes, eset, f-secure and BitDefender (some were just the online/on-demand scanners). But they didn't find any threats on my machine. I had the 32-bit helloworld.exe running too.
The virus total site says that the scanners they are provided can have stronger heuristics than the

public commercial versions.
I don't know why my 32-bit exe returns detections and yours doesn't, but it seems like nothing to do with UPP itself.
Thanks Koldo for taking the time to experiment though.

Subject: Re: Trojan in HelloWorld
Posted by mirek on Sat, 02 Jan 2016 07:06:27 GMT

View Forum Message <> Reply to Message

koldo wrote on Fri, 01 January 2016 22:39Hello Andrew

Thank you for you report.

VirusTotal does a good job as it checks uploaded files against 54 anti virus softwares for free.

I have just checked at VirusTotal Hello World example .exe compiled in a Windows 7 64 bits system with:
- Visual Studio 2015 32 and 64 bits
- MinGW TDM 32 ans 64 bits

Is this the same version as in U++ release?

Mirek

Subject: Re: Trojan in HelloWorld
Posted by koldo on Sun, 03 Jan 2016 08:16:06 GMT

View Forum Message <> Reply to Message

mirek wrote on Sat, 02 January 2016 08:06koldo wrote on Fri, 01 January 2016 22:39Hello Andrew

Thank you for you report.

VirusTotal does a good job as it checks uploaded files against 54 anti virus softwares for free.

I have just checked at VirusTotal Hello World example .exe compiled in a Windows 7 64 bits system with:
- Visual Studio 2015 32 and 64 bits
- MinGW TDM 32 ans 64 bits

Is this the same version as in U++ release?

Mirek
Sorry Mirek, I do not know what you mean.

Subject: Re: Trojan in HelloWorld
Posted by koldo on Sun, 03 Jan 2016 08:39:57 GMT
View Forum Message <> Reply to Message

andrew7m wrote on Sat, 02 January 2016 02:30I'm using MinGW TDM.
I guess the default build settings were 32-bit. I changed to MINGWx64 and this results in no virus detections, like you observed.
Then I changed back to MINGW (32-bit) and I get 7 detections still.
My OS is Windows 7 Pro 64-bit Service Pack 1.
UPP is Version 9251 (64-bit).

I scanned my PC with five different AV products; MSE, Malwarebytes, eset, f-secure and BitDefender (some were just the online/on-demand scanners). But they didn't find any threats on my machine. I had the 32-bit helloworld.exe running too.
The virus total site says that the scanners they are provided can have stronger heuristics than the public commercial versions.
I don't know why my 32-bit exe returns detections and yours doesn't, but it seems like nothing to do with UPP itself.
Thanks Koldo for taking the time to experiment though.
Sorry Andrew.

I have repeated the check and I think that in previous test I have sent the same file 4 times to VirusTotal :(. Now I have done it right and yes, HelloWorld MinGW TDM 32 bits version raises these errors in VirusTotal:
- ByteHero Trojan.Malware.KillAV.Gen.001
- Fortinet W32/Kryptik.DYEL!tr
I cannot get any additional information about these errors from this page.

Browsing in Internet there are some posts of people complaining about false antivirus errors in MinGW basic "hello world" programs as here or here or here :(.
It seems a work in process... Maybe does it happen because antivirus developers do not check too much their softwares with MinGW?