Emulator - Emulator Issues #11871

Since 5.0-10918 there's a threat detected by Windows 10 as Trojan:Win32/Azden.A!cl in the updater.exe

10/01/2019 03:51 PM - markwest76

Status:	Fixed	**% Done:**	0%
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Operating system:	Windows	**Relates to performance:**	No
Issue type:	Other	**Easy:**	No
Milestone:	Current	**Relates to maintainability:**	No
Regression:	No	**Regression start:**	
Relates to usability:	No	**Fixed in:**	

Description

Game Name?

-

Game ID? (right click the game in the game list, Properties, Info tab)

-

MD5 Hash? (right click the game in the game list, Properties, Verify tab, Verify Integrity button)

-

What's the problem? Describe what went wrong.

Since 5.0-10918 downloading Dolphin is impossible because Windows 10 (Windows defender) detects a virus and eliminates the dowloaded file (threat detected Trojan:Win32/Azden.A!cl in the updater.exe)

What steps will reproduce the problem?

download Dolphin or use auto updater (virus seems to be locxated in the updater.exe)

Is the issue present in the latest development version? For future reference, please also write down the version number of the latest development version.

Yes, 5.0-10938

Is the issue present in the latest stable version?

No

If the issue isn't present in the latest stable version, which is the first broken version? (You can find the first broken version by bisecting. Windows users can use the tool https://forums.dolphin-emu.org/Thread-green-notice-development-thread-unofficial-dolphin-bisection-tool-for-finding-broken-builds and anyone who is building Dolphin on their own can use git bisect.)

5.0-10918

If your issue is a graphical issue, please attach screenshots and record a three frame fifolog of the issue if possible. Screenshots showing what it is supposed to look like from either console or older builds of Dolphin will help too. For more information on how to use the fifoplayer, please check here: https://wiki.dolphin-emu.org/index.php?title=FifoPlayer

[Attach any fifologs if possible, write a description of fifologs and screenshots here to assist people unfamiliar with the game.]

What are your PC specifications? (CPU, GPU, Operating System, more)

Win10
gtx1060
i7700

Is there anything else that can help developers narrow down the issue? (e.g. logs, screenshots, configuration files, savefiles, savestates)

Threat detected: Trojan:Win32/Azden.A!cl in the updater.exe

History

#1 - 10/01/2019 03:59 PM - JosJuice

The bisect seems invalid. I get the alert with Windows Defender's malware definition that was created 3.5 hours ago, but not one that was created 19 hours ago.

#2 - 10/01/2019 04:04 PM - JosJuice

I will try to see if we can ask Microsoft to check whether this is a false positive.

#3 - 10/01/2019 04:06 PM - markwest76

I don't think I'm wrong: Windows 10 allows me to download 5.0-10916 (no thret detected by Windows Defender), but not 5.0-10918 (Trojan detected in the updater.exe)

#4 - 10/01/2019 04:11 PM - JosJuice

Yes, you're actually right. I suppose there are two conditions for this happening, then: 5.0-10918 or later, and the newest definitions.

#5 - 10/01/2019 11:46 PM - delroth

- Status changed from New to Fixed

- Operating system Windows added

- Operating system deleted (N/A)

I fwded that to Microsoft via some contacts and reported through their Security Intelligence portal. Definitions v1.303.648.0 and later should be fixed. If you still encounter this issue, please report back on the bug with: 1. Dolphin version; 2. Defender definitions version.

#6 - 10/02/2019 03:28 PM - markwest76

unfortunately the problem is still there: Dolphin 5.0-10943 - Defender version 1.303.701.0

#7 - 10/06/2019 10:48 AM - markwest76

Today same problem: Dolphin 5.0-10956 - Defender version 1.303.1004.0

#8 - 10/06/2019 11:03 AM - JosJuice

- Milestone set to Current

- Status changed from Fixed to New

Re-opening for now.

#9 - 10/16/2019 05:00 PM - mbc07

I posted this on the forums and was instructed to report here too:

> Windows Defender now flags the updater binary of every new Windows build of Dolphin as malware (I haven't tried PR builds but they're

probably affected too). The detection name is always **Trojan:Win32/Azden.A!cl** and, as indicated by the **!cl** at the end of the detection name, it's always caused by their cloud definitions (which AFAIK are based on machine learning), so the version of the local definitions doesn't matter at all.

I noticed this happened with all builds from 5.0-10960 to the current (at time of this post) 5.0-10979. I submitted the updater of every affected build for analysis but all Microsoft seems to do is whitelist the updater of that specific build some hours after receiving the submission instead of fixing whatever is causing the false detection, so it's just a matter of a new Dolphin build being released for the whole loop repeating itself again.

I don't know if there's another way or channel to contact them about this situation other than the file submission portal, but manually uploading the updater of every new build is a tedious process and at this pace it's just a matter of time before complaining users start appearing on our forums and other social media. Perhaps I was lucky to be online at the time those builds were released and the manual analysis was finished before others had time to download the affected builds and get Windows Defender yelling at them, but that won't always be the case.

To be honest, I'm officially giving up after manually filling up 10 file analysis submissions just in the past week and simply configured Windows Defender to always ignore files identified with Trojan:Win32/Azden.A!cl, but I think it's important bringing attention to this issue to our staff and be ready when the complains start appearing again...

#10 - 10/16/2019 05:28 PM - BhaaL

It would be interresting to know what part of the updater is detected as such; to at least give us a chance on actually changing the offending code. Even more so when it is part of the libraries we use; since we're not the only ones that do.

#11 - 10/17/2019 03:04 AM - mbc07

Assuming that Microsoft whitelist the updater binary of that particular false positive report after receiving the file for analysis and considering our updater code hasn't changed for a long while, couldn't we do something to make the updater binary generated by our buildbot always have exactly the same hash? As of now, every build of Dolphin has a unique hash for the updater binary, even through the source code used to generate that updater binary is the same.

If we could get the binary to get a different hash only when its source code really changed, we could theoretically report that binary for Microsoft and be done with the false alarms for as long as the updater doesn't receive any source code change...

#12 - 10/20/2019 02:08 AM - Roadhog360-2

I recently started experiencing this, too. Glad I am not the only one! It seems like all I had to do was go to the Defender settings and add the updater.exe to the exceptions, although this just a temporary workaround, I'm hoping Windows fixes this soon.

#13 - 11/17/2019 12:14 PM - markwest76

On my end I think this problem has been solved, I mean now it's been some weeks that I haven't experienced this problem anymore...so what do you think?

#14 - 11/17/2019 12:19 PM - JosJuice

- Issue type changed from Bug to Other

- Status changed from New to Fixed

I have heard no reports about it in the forums or anywhere else, so I guess we can assume it's solved. We can reopen the issue if someone still is having problems.