
Subject: Installation file is considered malware by browsers and anti-virus software...

Posted by [timritchie](#) on Thu, 05 Feb 2015 09:31:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello,

I downloaded the datawarrior.msi file for Windows. This file is considered malicious by browsers and anti-virus software.

Whilst one can go ahead and make the installation and use Datawarrior, it would be very helpful if the file could be authenticated in some way to prevent such alerts.

Regards,

Tim Ritchie.

Subject: Re: Installation file is considered malware by browsers and anti-virus software...

Posted by [DirkTomandl](#) on Sat, 08 Aug 2015 19:47:17 GMT

[View Forum Message](#) <> [Reply to Message](#)

Same problem at our company:

Today (2015-08-08), Symantec Virus scanner removed the DataWarrior executable from all of our machines!

Messages:

Scan type: Auto-Protect Scan

Event: Security Risk Found!

Security risk detected: Trojan.Gen.2

File: C:\Program Files\DataWarrior\DataWarrior.exe

Location: Deleted or access blocked

User: SYSTEM

Action taken: Delete succeeded : Access denied

Date found: Saturday, August 08, 2015 11:13:23 AM

@Thomas: It is unlikely that your code actually includes a Trojan virus but please check the code to change the libs that may have caused it. Right now we are not able to use DW since it gets automatically removed.

Subject: Re: Installation file is considered malware by browsers and anti-virus software...

Posted by [thomas](#) on Tue, 11 Aug 2015 14:12:39 GMT

[View Forum Message](#) <> [Reply to Message](#)

Dear Dirk,

thank you for the hint. Recently, I received a report from another large pharma company, that Symantec Endpoint Protection had classified DataWarrior on one workstation as potential trojan,

but SEP kept quite on various other client computers with a comparable setup. Thus, I assumed that the one installation may have been infected after the installation.

After calling Symantec it seems that this and your cases are false positive alerts and that DataWarrior.exe needs to be white-listed in the Symantec virus database. I will try to get that done as fast as possible.

Thanks, Thomas

Subject: Re: Installation file is considered malware by browsers and anti-virus software...

Posted by [joetedesco](#) on Sun, 27 Mar 2016 09:12:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

on March 27, 2016 The virus TR/Crypt.XPACK.Gen was detected in the datawarrior.exe file when I tried to install the 32-bit-version msi install file onto my windows 10 system.

I have some screenshots of this event to send you, but I have been blocked by your server from posting links to your messages on the first message (??), so I will send them on the NEXT message.

Joe Tedesco

Subject: Re: Installation file is considered malware by browsers and anti-virus software...

Posted by [joetedesco](#) on Sun, 27 Mar 2016 09:21:29 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hi,

On March 27, 2016 The virus TR/Crypt.XPACK.Gen was detected in the datawarrior.exe file when I tried to install the 32-bit-version msi install file onto my windows 10 system.

I still am blocked by your server from sending http links in this text, so I instead attach 2 pdf files of screenshots (PNG graphics) of my screen to confirm this and to show more details re the 'suspicious' files involved.

I hope this can assist you. I also hope this problem can be rectified soon. I am a new member and look forward to using DataWarrior once this security issue is resolved.

It looks to be a terrific program.

Joe Tedesco

File Attachments

1) [more_info_re_virus_detected_Screenshot_2016-03-27](#)

04.24.18.pdf, downloaded 1485 times

2) virus_detected_Screenshot_2016-03-27_04.24.18.pdf,
downloaded 1500 times

Subject: Re: Installation file is considered malware by browsers and anti-virus software...

Posted by [thomas](#) on Thu, 07 Apr 2016 21:08:21 GMT

[View Forum Message](#) <> [Reply to Message](#)

There were a few single reports about Symantec reporting a virus. However, it is highly unlikely that the executable is infected, because it is now about 9 months old, during this time it was installed and is used by a few thousand people. The executable was build on a Linux computer and the installer was built on a dedicated virtual Windows machine, which is exclusively started and used for building the msi-file and for testing, whether the msi works.

I assume that it is a false alert or that the file got infected after unpacking it from the msi.

For the upcoming version I will publish the MD5 hash codes of the installer files to allowing checking, whether they are still the original ones.

Thomas
