

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Trend Micro antivirus modified Windows registry by mistake — How to fix

32

Trend Micro antivirus modified Windows registry by mistake — How to fix

By **Sergiu Gatlan** (<https://www.bleepingcomputer.com/author/sergiu-gatlan/>)
May 7, 2022 10:03 AM 0

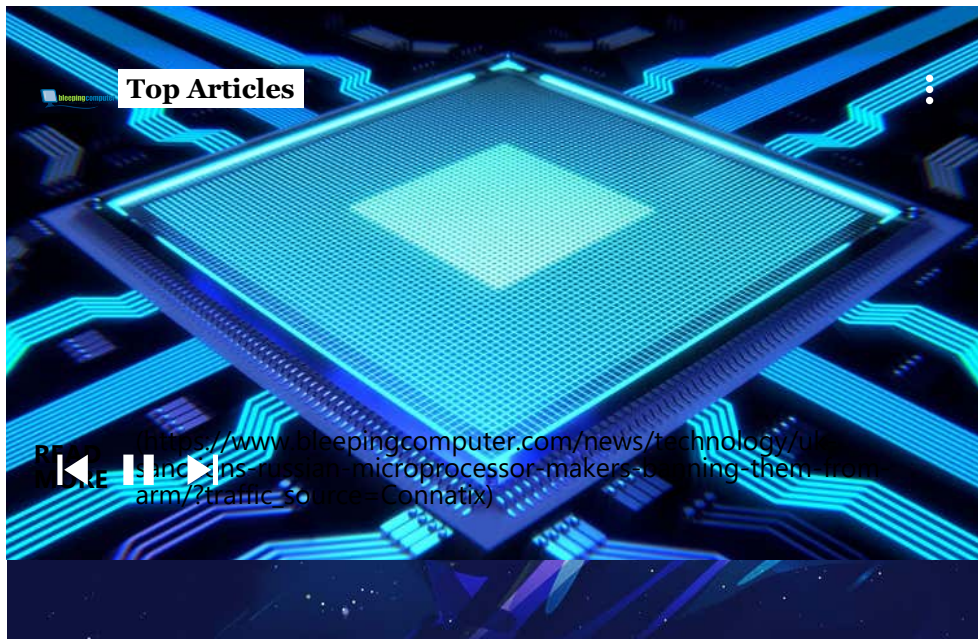


Trend Micro antivirus has fixed a false positive affecting its Apex One endpoint security solution that caused Microsoft Edge updates to be tagged as malware and the Windows registry to be incorrectly modified.



According to hundreds of customer reports that started streaming in earlier this week on the company's forum (<https://success.trendmicro.com/forum/s/question/0D54T00001QDqzgsAD/we-are-getting-this-message-from-every-client-since-several-minutes-it-a-false-positiv-error-or-do-we-have-a-real-trojaner-problem->) and on social networks (https://www.reddit.com/r/sysadmin/comments/uhd002/trend_apexone_flagging_false_positive_on_latest/), the false positive affected update packages stored in the Microsoft Edge installation folder.

As users further revealed, the Trend Micro Apex One flagged the browser updates as Virus/Malware: TROJ_FRS.VSNTTE222 and Virus/Malware: TSC_GENCLEAN.



Fix and workaround available

The cybersecurity software maker addressed the issue and published an advisory urging customers to update their products and ensure that the Smart Scan Agent Pattern and Smart Scan Pattern are updated to the latest version.

"Trend Micro is aware of a detection issue that was reported earlier today regarding a potential false positive with Microsoft Edge and a Trend Micro Smart Scan pattern," the company said (https://success.trendmicro.com/dcx/s/solution/000290966?language=en_US).

"The pattern has been updated to remove the detection in question and we are doing an investigation on the root cause of the issue. More information can be provided after the investigation is complete.

"Please confirm that both the Smart Scan Agent Pattern is 17.541.00 or later AND Smart Scan Pattern is 21474.139.09 or later which resolves the issue."



Trend Micro also shared a temporary workaround if the pattern update didn't fix the issue which requires adding multiple Microsoft Edge folders to Apex One's exclusion list.

Restoring registry changes

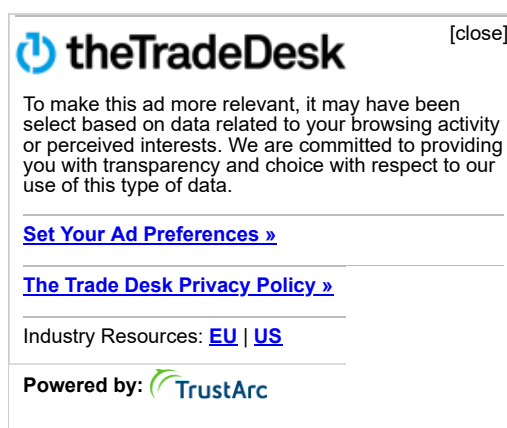
While the fix provided by Trend Micro for the false positive can easily be applied by updating Apex One, some customers also reported that this issue also led to Windows registry entries being altered after the agent's Damage Cleanup tool was executed.

"It was reported that some customers observed some registry changes as a result of the detection depending on their endpoint cleaning configuration settings," Trend Micro added.



Windows Registry changes seen by Trend Micro customer

This requires affected users to restore backups made by the Apex One agent through a procedure that will help revert the changes made by Damage Cleanup.



The company also shared a script
 (https://success.trendmicro.com/dcx/s/solution/000290966?
 language=en_US#:~:text=Reference%20Script%20For%20Restoration)



that would help system admins to automate the registry restoration procedure with the help of group policies or other enterprise scripting tools.

However, you should first test this automation tool before running it across the entire environment.

"Please note that administrators looking to utilize this script as a batch file or via other method should first carefully review the script and test in their environment before any widespread development," Trend Micro explained.

"Customers who are continuing to have issues are advised to contact their authorized Trend Micro representative for further assistance."

Related Articles:

New Raspberry Robin worm uses Windows Installer to drop malware
(<https://www.bleepingcomputer.com/news/security/new-raspberry-robin-worm-uses-windows-installer-to-drop-malware/>)

Microsoft: Windows 11 KB5012643 update will break some apps
(<https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-11-kb5012643-update-will-break-some-apps/>)

Microsoft PowerShell lets you track Windows Registry changes
(<https://www.bleepingcomputer.com/news/microsoft/microsoft-powershell-lets-you-track-windows-registry-changes/>)

Windows 'RemotePotatoo' zero-day gets an unofficial patch
(<https://www.bleepingcomputer.com/news/security/windows-remotepotatoo-zero-day-gets-an-unofficial-patch/>)

Windows 11 gets new group policies to tweak the Start Menu
(<https://www.bleepingcomputer.com/news/microsoft/windows-11-gets-new-group-policies-to-tweak-the-start-menu/>)

