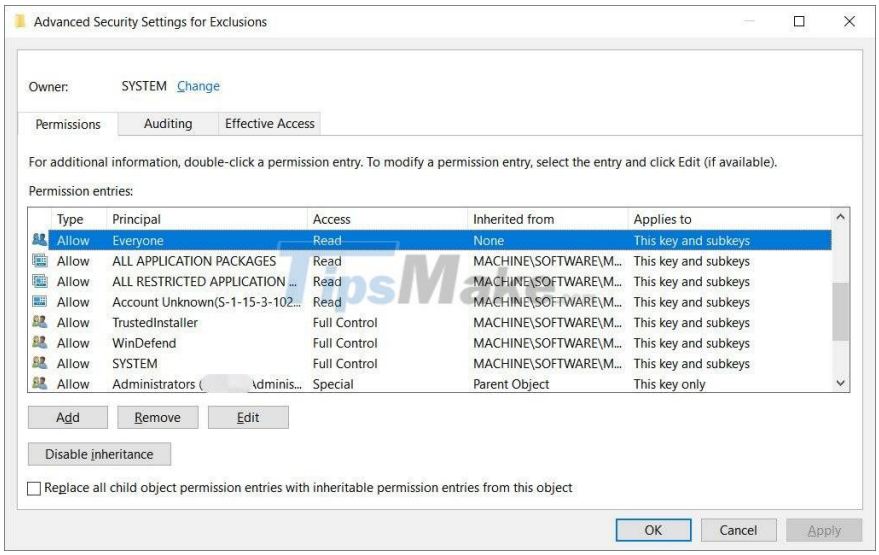
Hackers take advantage of Microsoft Defender's 8-year-old weakness to bypass the virus detection system

Hackers take advantage of the weakness of Microsoft Defender anti-virus software to learn the locations excluded from the scan and plant malware there.

Like any other antivirus, Microsoft Defender allows users to add exclusions (locally or on a network) on their system. When scanning for viruses, Microsoft Defender will ignore these excluded areas and folders.

Often users will create exclusion zones to prevent anti-virus software from affecting the functionality of a genuine application that is mistakenly detected as a virus.

Security researchers discovered that the list of locations excluded from Microsoft Defender's scanning was not protected at all. This results in any local user being able to access this list.



Regardless of permissions, users can access the Registry and find a list of locations excluded from the scan. The hacker will then plant the virus in those excluded locations and execute the malicious code without fear of detection.

Because the directory listings and exclusions are different for each user, there is no universal way to determine this for all computers. This also makes it easier for hackers to hide their behavior.

The news site BleepingComputer has conducted testing to confirm the problem. Testing showed that a ransomware executed from an excluded folder was able to run and encrypt the entire computer without any

hindrance or warning from Microsoft Defender.

A security consultant discovered this problem 8 years ago and realized the advantages it brought to hackers.

Due to the long time of existence, and Microsoft has not taken action to patch the error, users and administrators should actively protect themselves by correctly configuring the exclusion area on the server and local machine via group policies.