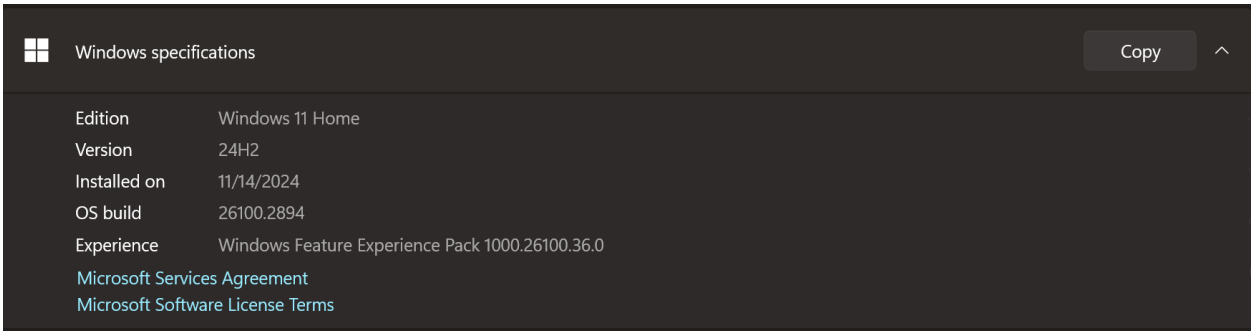
Malware Protection Test – (36 points)

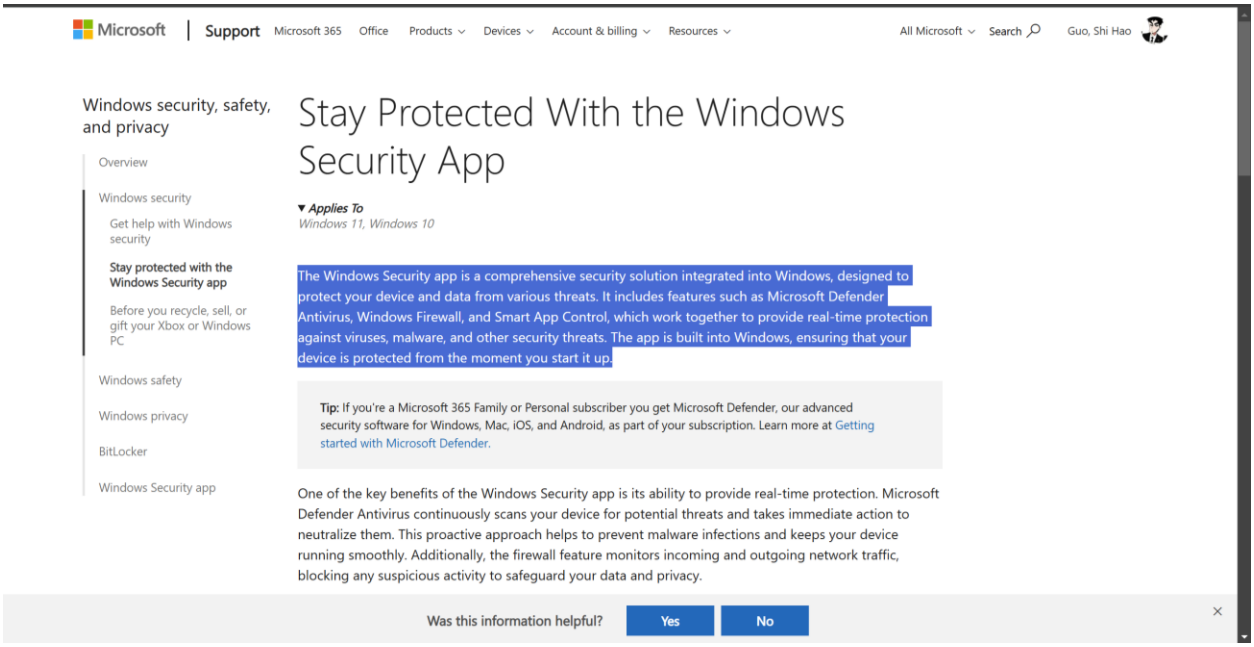
The purpose of this assignment is for you to test two malware / end-point protections of your choice using a test file known as "eicar". The "eicar" file is harmless to your computer, but malware protections know to flag the file as malicious for testing purposes.

Download the "eicar-test-smb.zip" from Canvas and answer the following questions. Provide screenshots to support your answers.

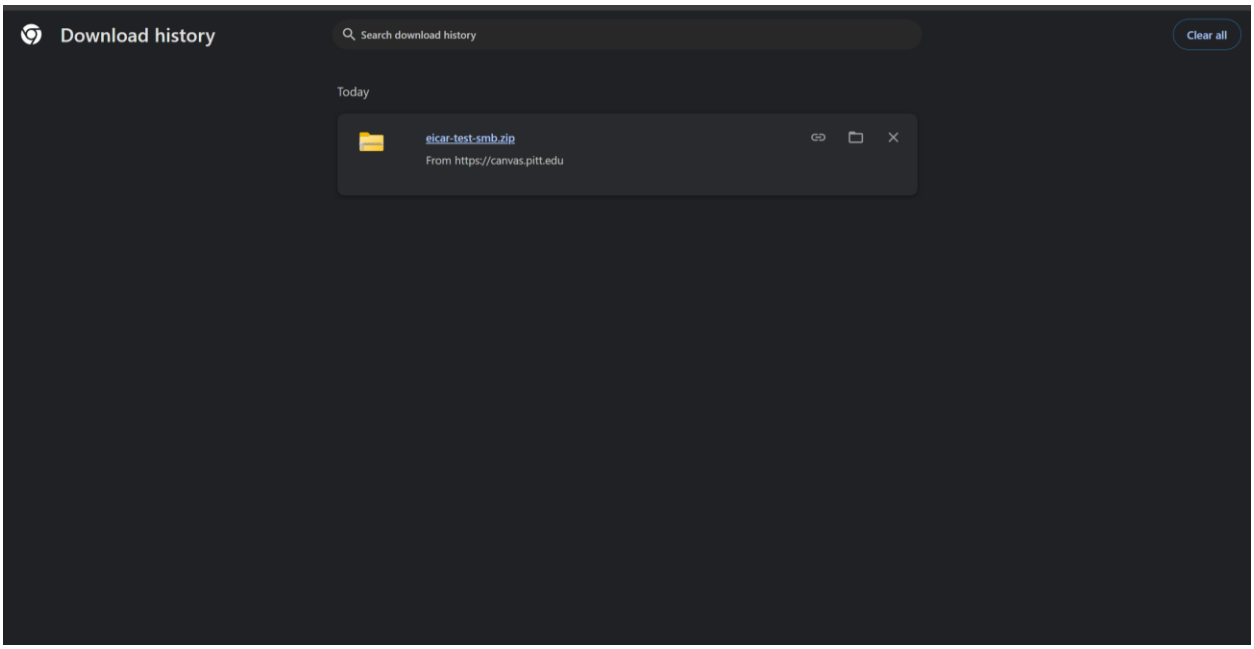
1. **What type / OS version are you running?** Microsoft Windows 11 Home (24H2).



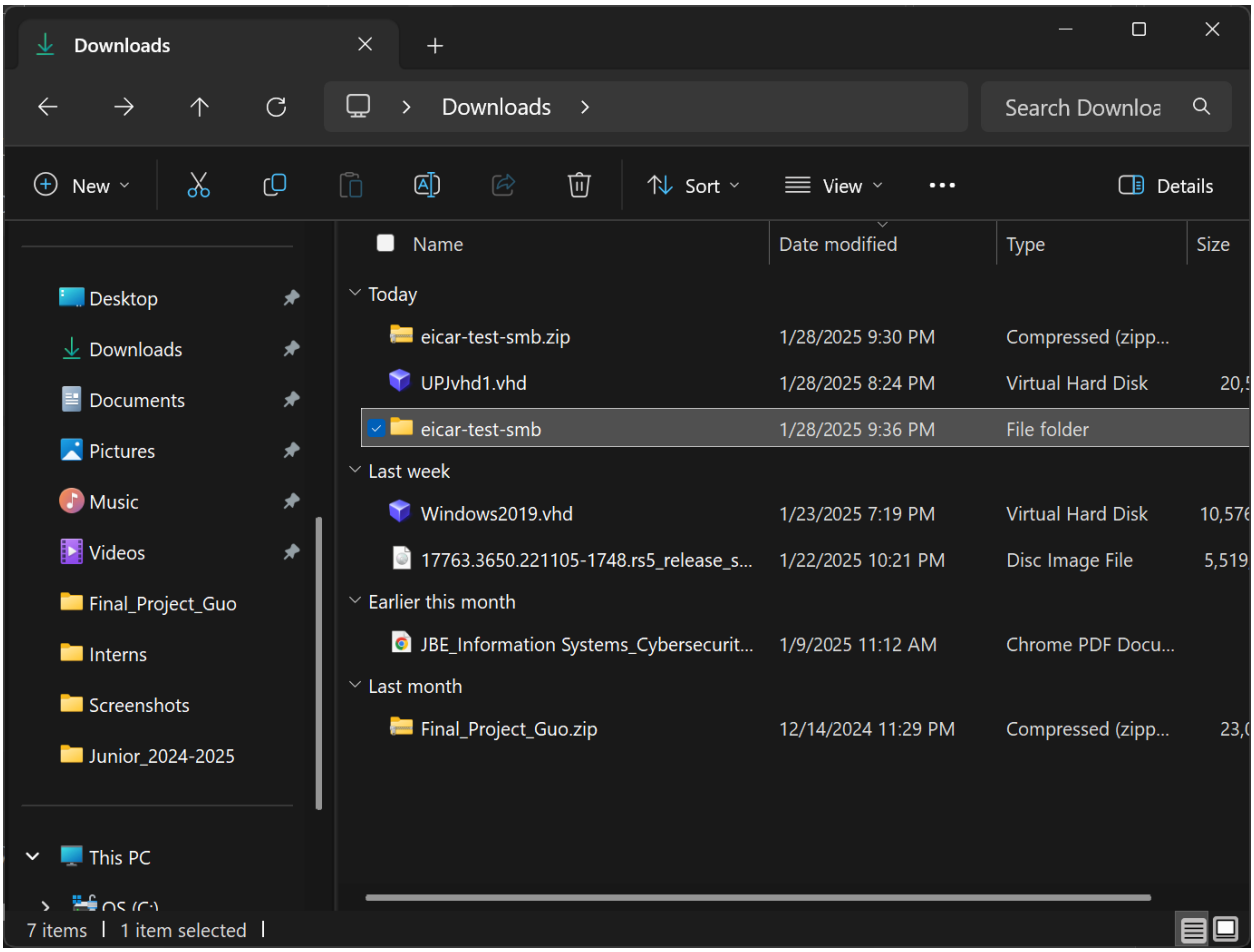
2. **What malware / end-point protection are you running for your test?** Microsoft Windows Security App (Microsoft Defender Antivirus).



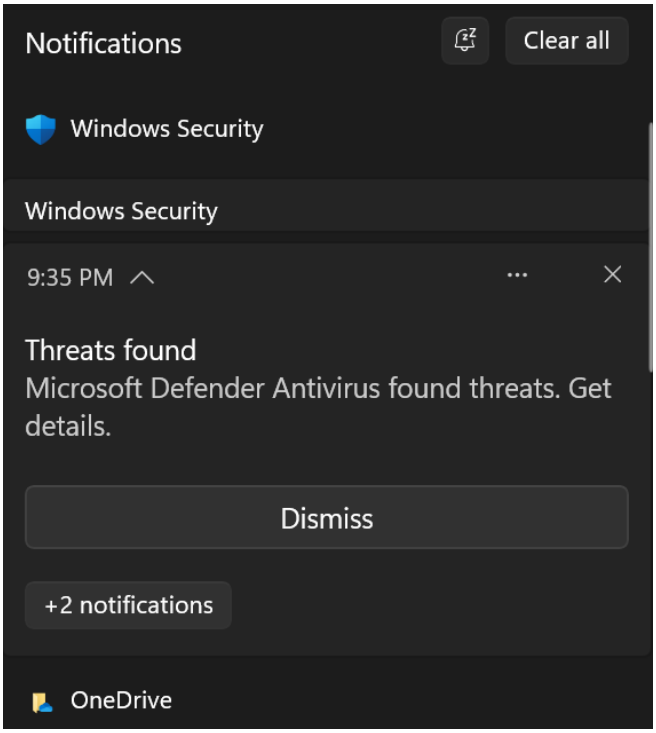
3. **Download the "eicar-test-smb.zip" to your computer. Did your malware protection detect a malicious file as soon as you downloaded the file to your computer?** No, my malware protection does not detect the file as malicious when I downloaded it.



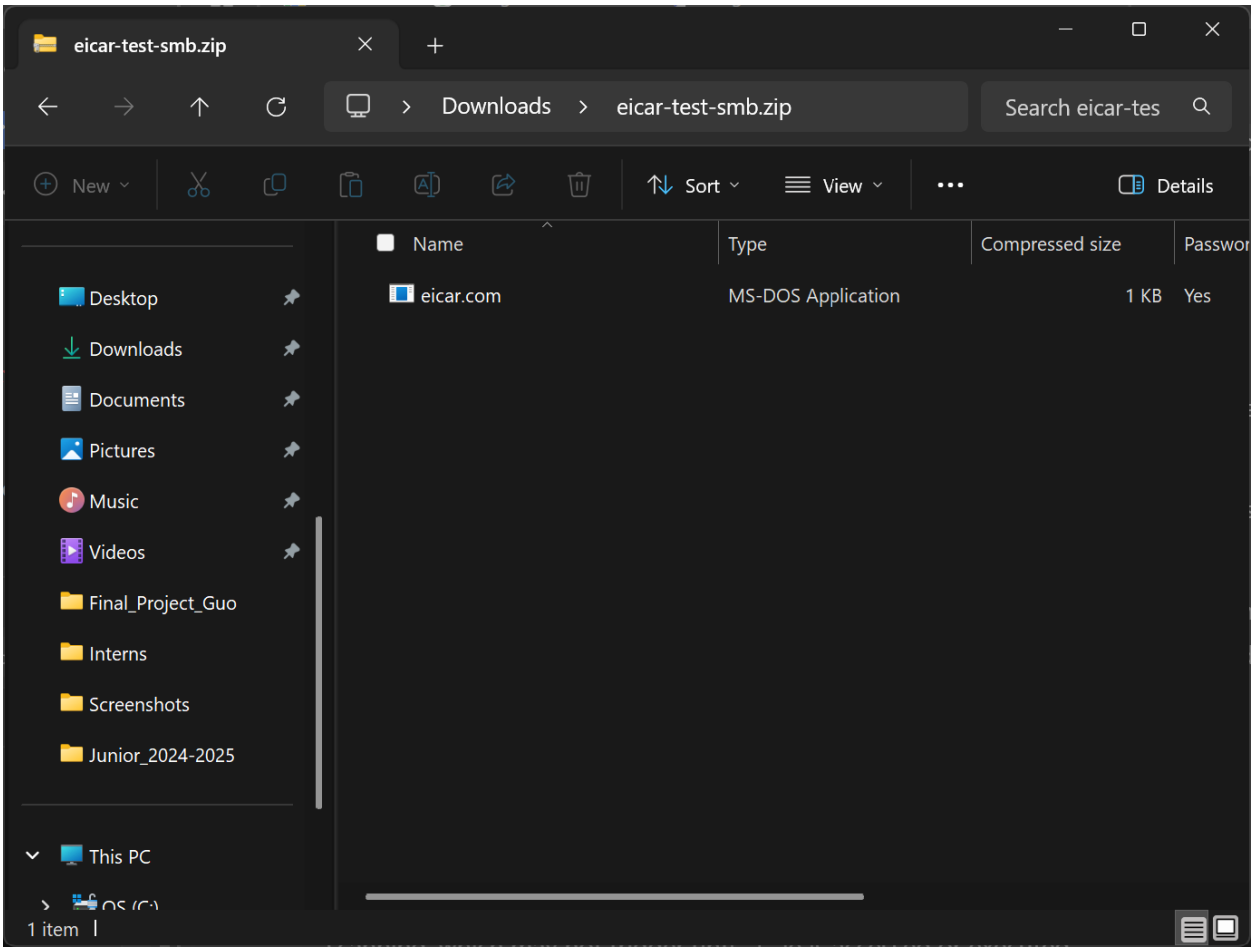
4. **Unzip the "eicar-test-smb.zip" using the password "f11-11"**

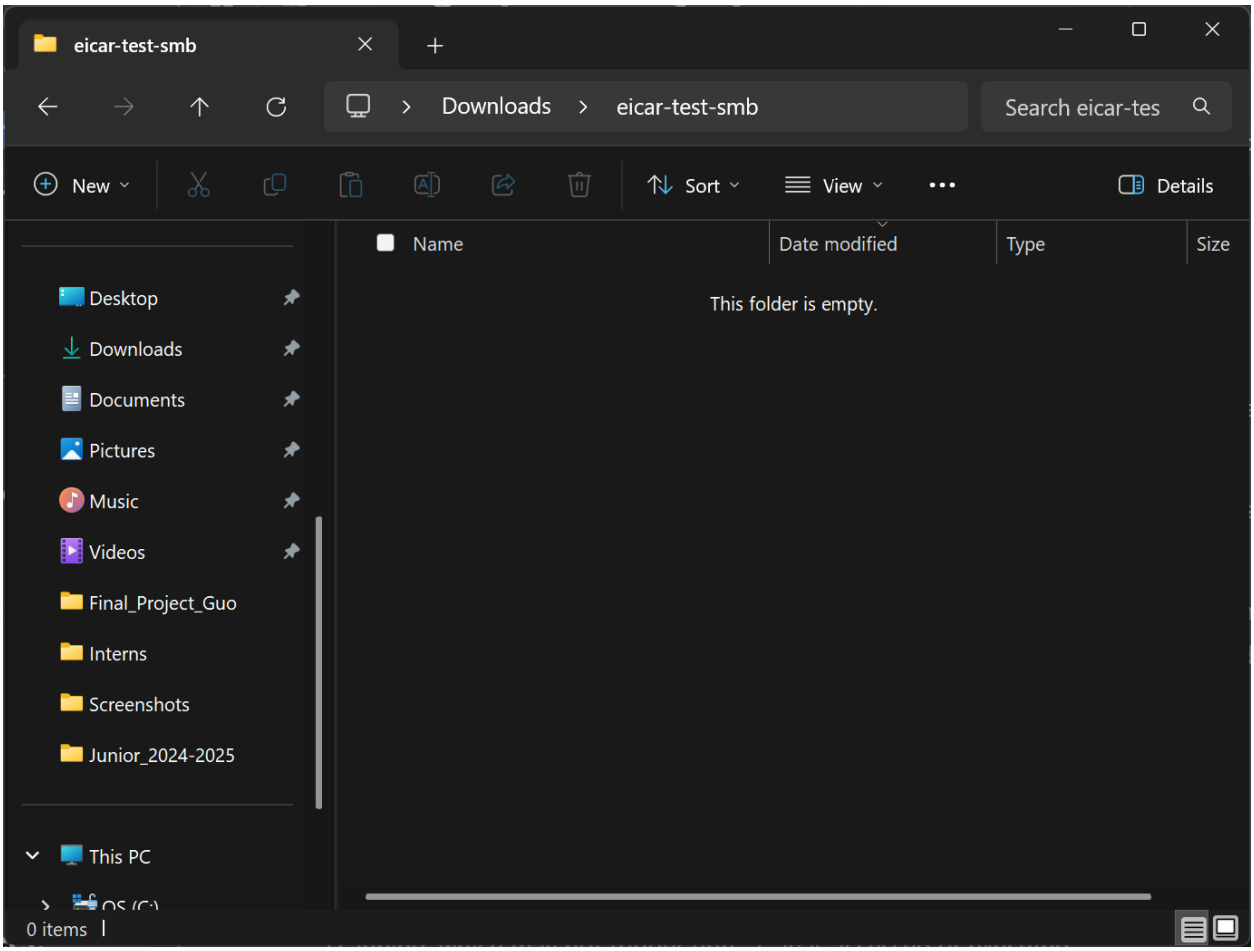


5. **Did your malware / end-point protection detect "eicar" file as malware?** Yes, it did.

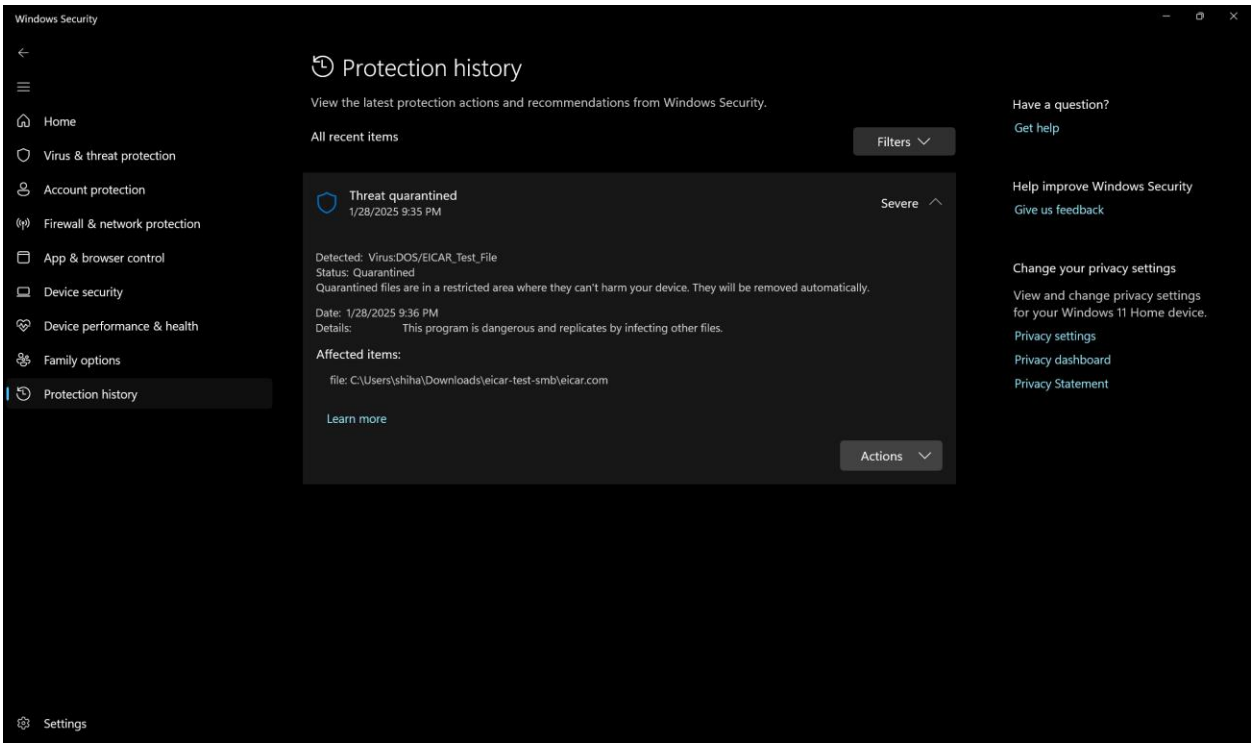


6. **Why did your malware / end-point protection not detect the file as malware for step 3, but did after you unzipped the file?** The most likely reason is because this specific ZIP file is password-protected, the antivirus cannot inspect its content until password is entered and file is extracted.
7. **Did your malware automatically delete or quarantine the eicar file once it was detected? If so, which one?** Yes, it automatically deleted the “eicar.com” application after I extracted the file.


eicar-test-smb.zip
Downloads
eicar-test-smb.zip
Search eicar-tes
New
Sort
View
Details
Name
Type
Compressed size
Passwor
eicar.com
MS-DOS Application
1 KB
Yes
Desktop
Downloads
Documents
Pictures
Music
Videos
Final_Project_Guo
Interns
Screenshots
Junior_2024-2025
This PC
1 item

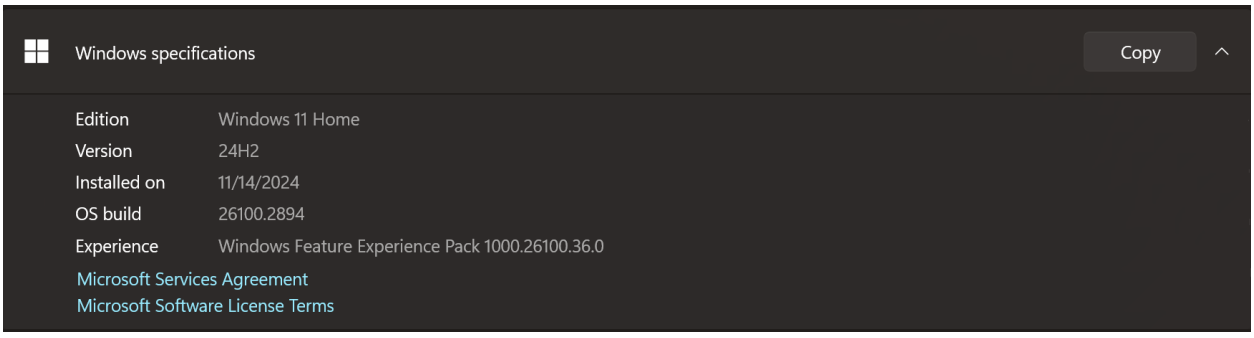


8. **Were you given a choice on what type of action your malware protection would perform to the file?** Nope, it did not prompt me with any choice, it just notified me that the file is malicious and deleted the file.
9. **Does your malware protection show a history of detection / actions taken?** Yes, it does show me a history of detection and operation.

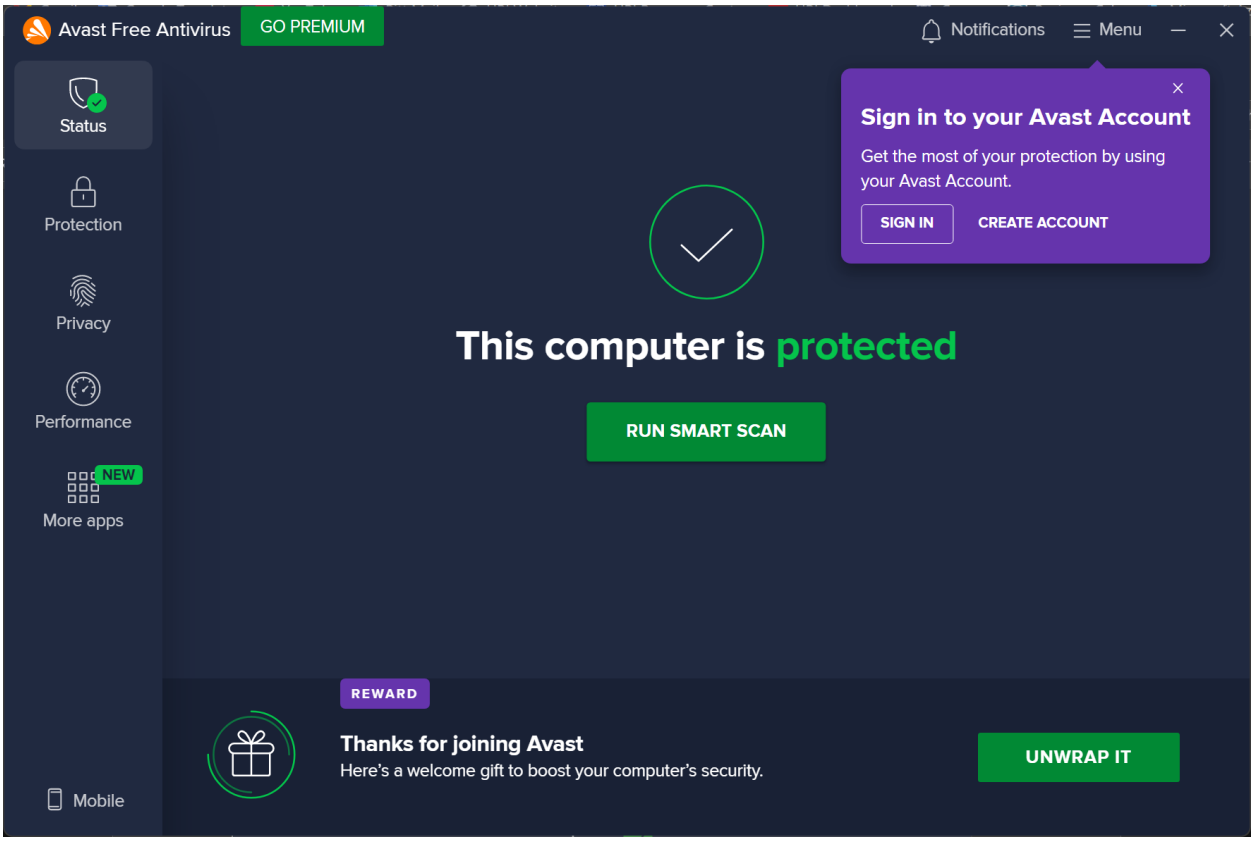


10. **Repeat steps 1-9 again testing with a second malware / end-point protection.** ***Note: You can test within a VM using a hypervisor or the cloud and/or just use a different computer.***

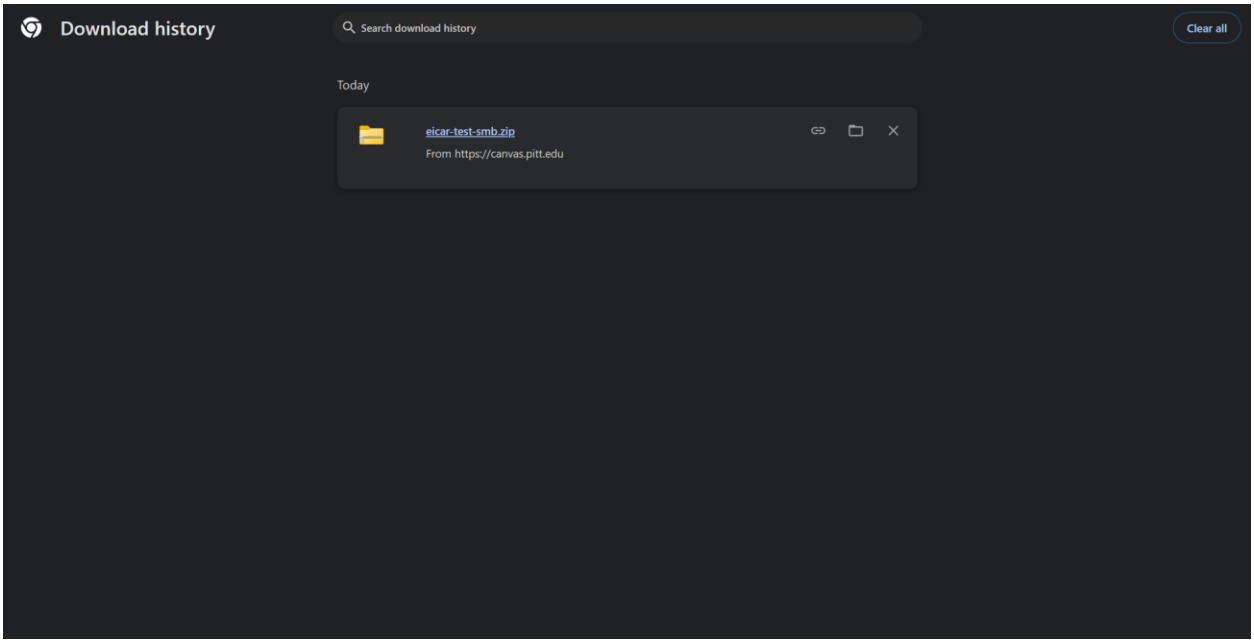
11. **What type / OS version are you running?** Microsoft Windows 11 Home (24H2).



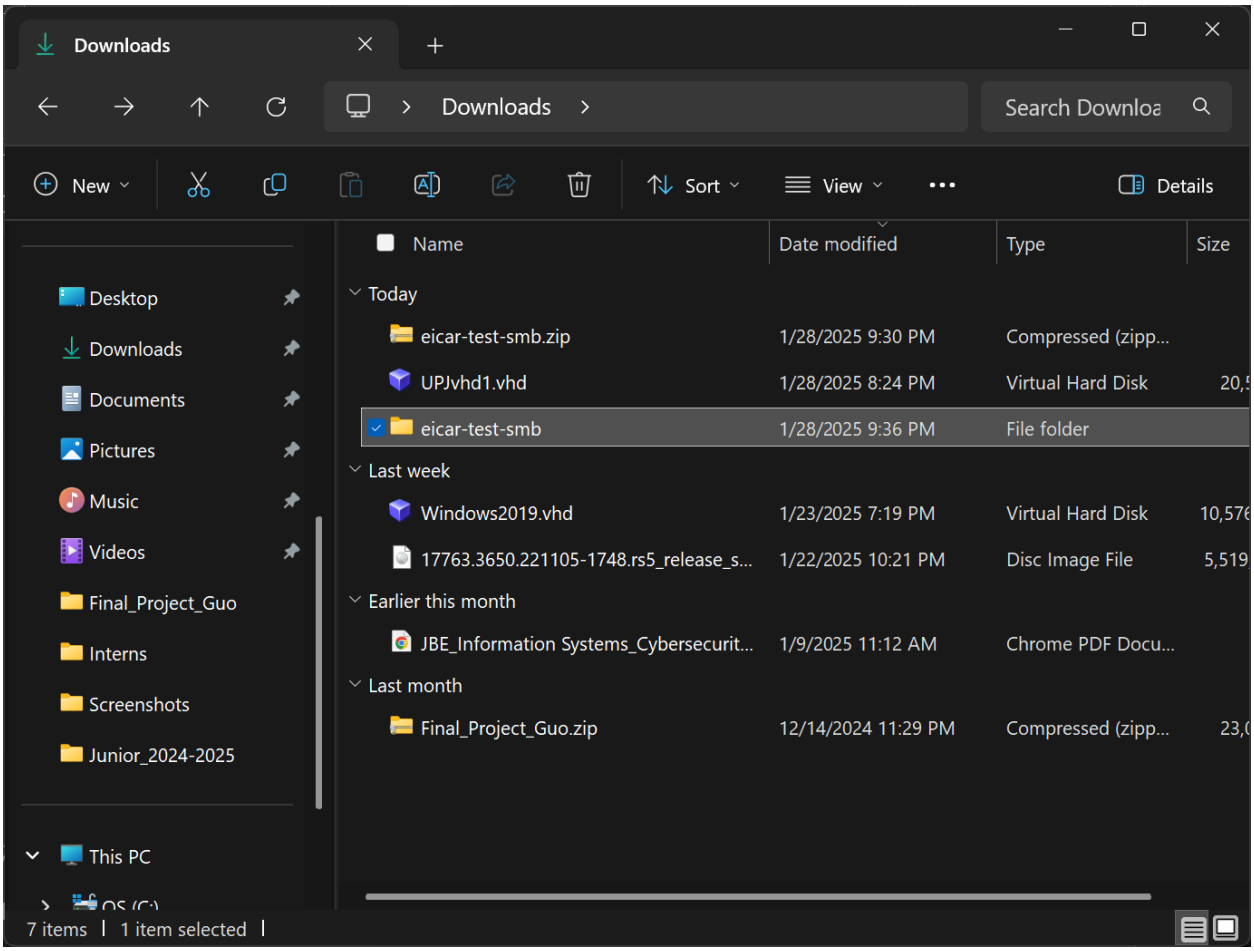
12. **What malware / end-point protection are you running for your test?** Avast Free Antivirus



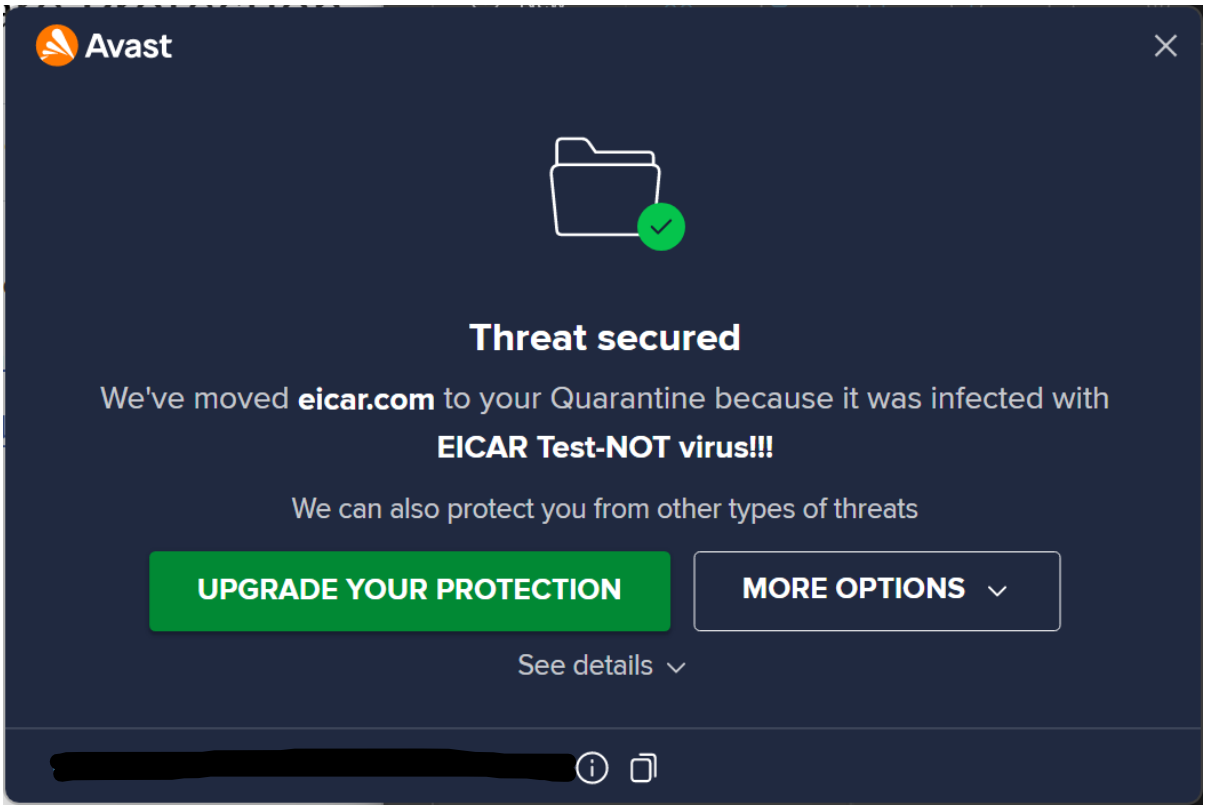
13. **Download the "eicar-test-smb.zip" to your computer. Did your malware protection detect a malicious file as soon as you downloaded the file to your computer?** No, my malware protection does not detect the file as malicious when I downloaded it.



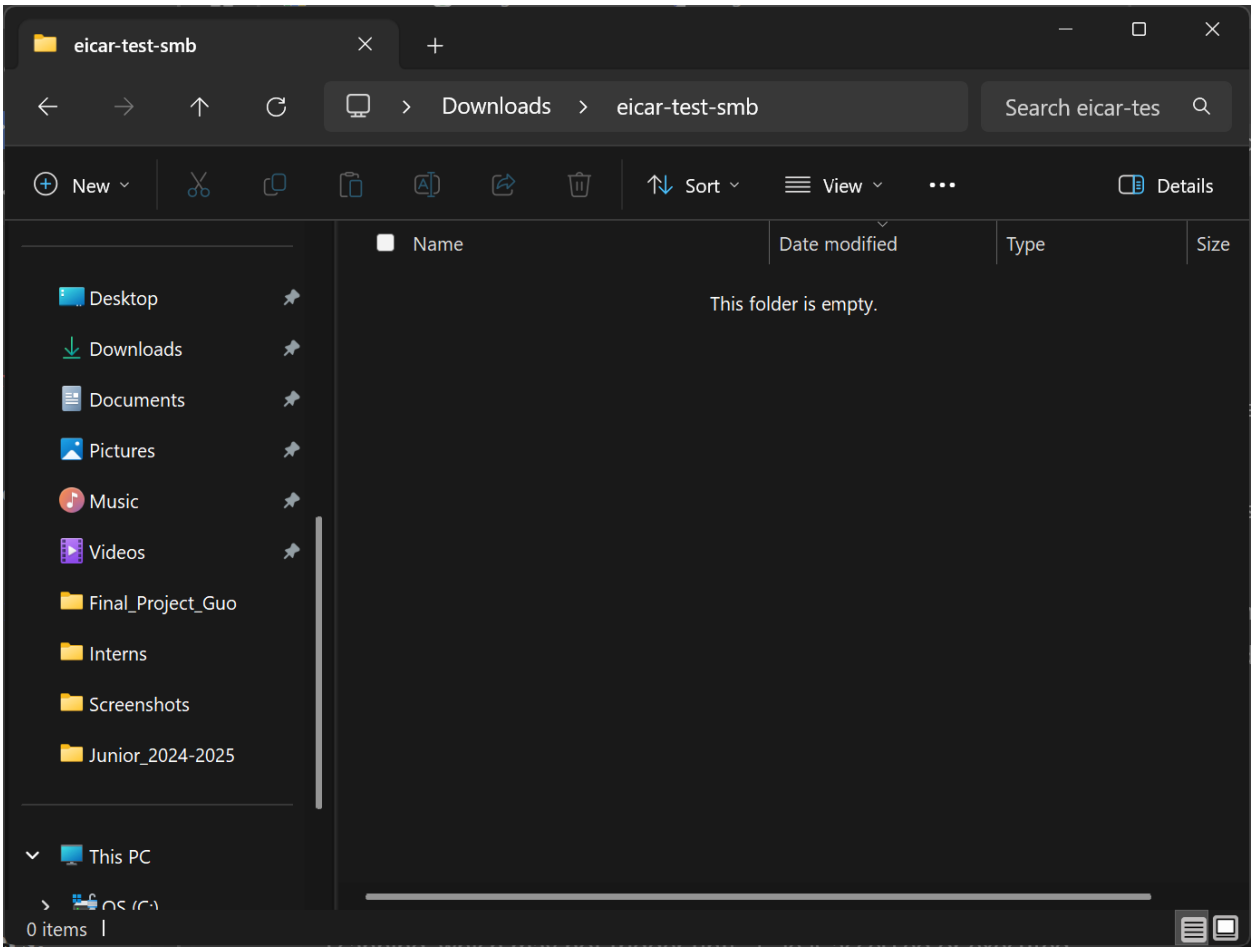
14. **Unzip the "eicar-test-smb.zip" using the password "f11-11"**



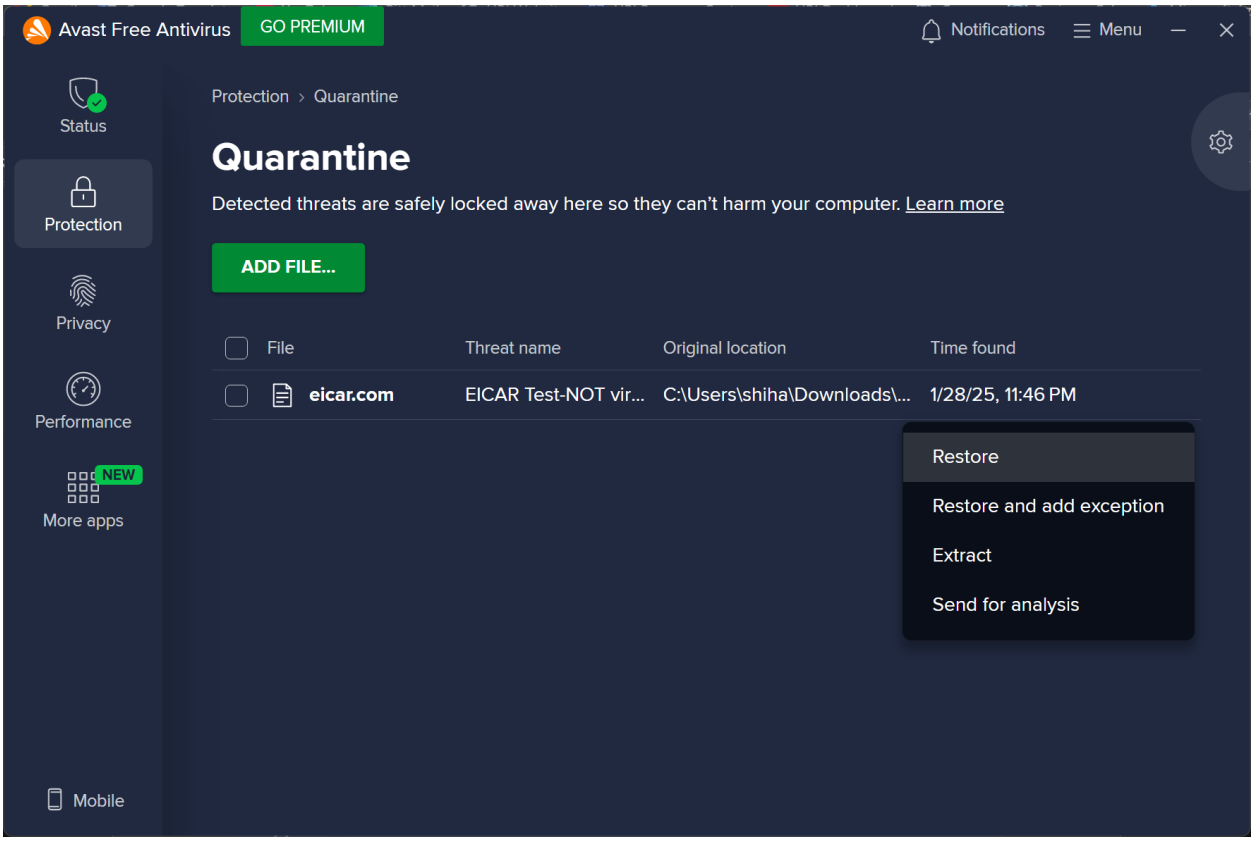
15. **Did your malware / end-point protection detect "eicar" file as malware?** Yes, it did.



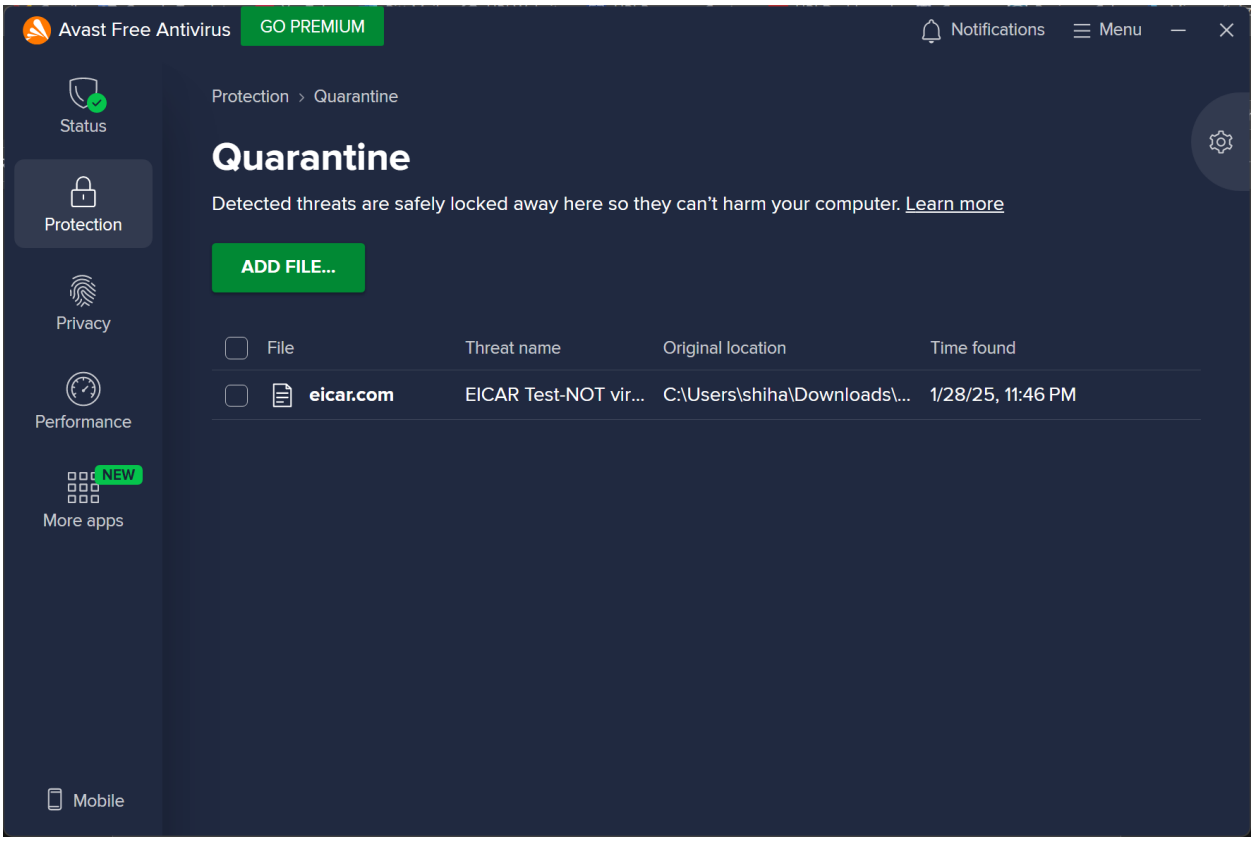
16. **Why did your malware / end-point protection not detect the file as malware for step 3, but did after you unzipped the file?** The most likely reason is because this specific ZIP file is password-protected, the antivirus cannot inspect its content until password is entered and file is extracted.
17. **Did your malware automatically delete or quarantine the eicar file once it was detected? If so, which one?** Yes, it automatically quarantines the “eicar.com” application after I extracted the file.



18. **Were you given a choice on what type of action your malware protection would perform to the file?** Nope, it did not prompt me with any choice, it just notified me, just like Microsoft Defender, that the file is malicious and deleted the file. But I can go into quarantine and restore the file or operate other actions.



19. **Does your malware protection show a history of detection / actions taken?** Yes, it does show me a history of detection and operation.



Be sure to include screenshots to support each of your answers!