



# מעבדה 1



אבטחת נקודת קצה

עקיפת אפליקציית אנטי-וירוס

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383


## נושאי המעבדה

להבין כיצד להתחמק מאיתור סורקי VirusTotal באמצעות קובצי הפעלת וירוס דחוסים.

## זמן מוערך

40–60 דקות

## סביבת מעבדה

VirtualBox 

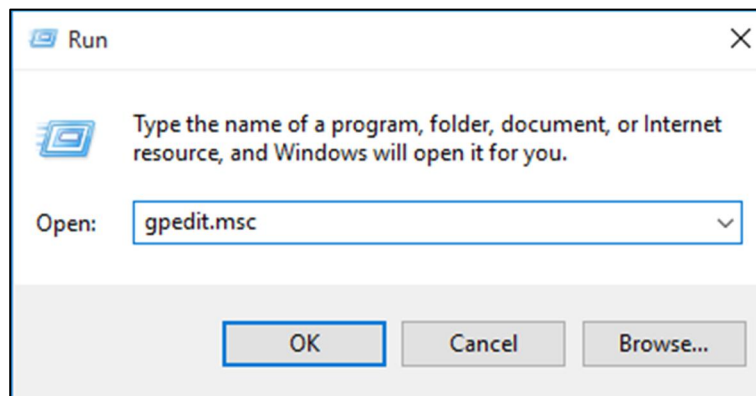
Windows 10 

# משימת מעבדה

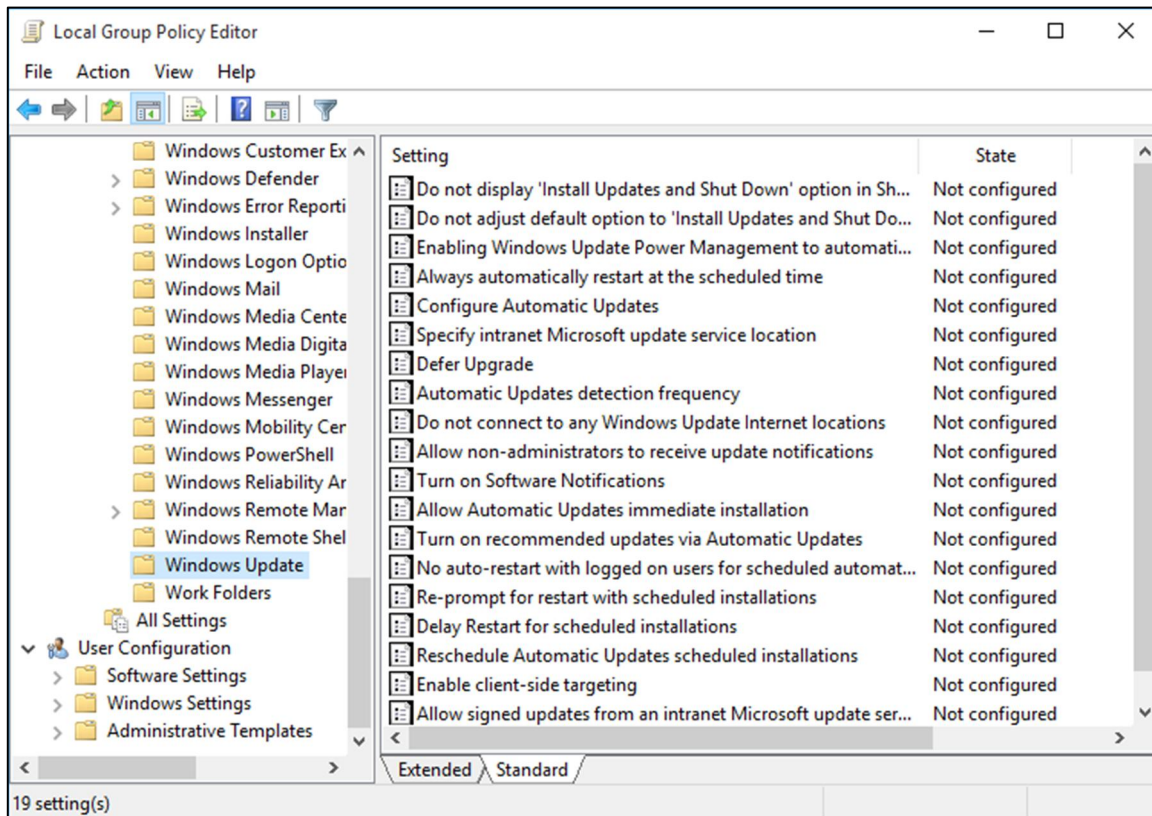
## התקנת Windows

במשימה זו תתקינו מכונה וירטואלית Windows 10 VM ב-VirtualBox, תכינו אותה למעבדה ותשביתו את העדכונים שלה.

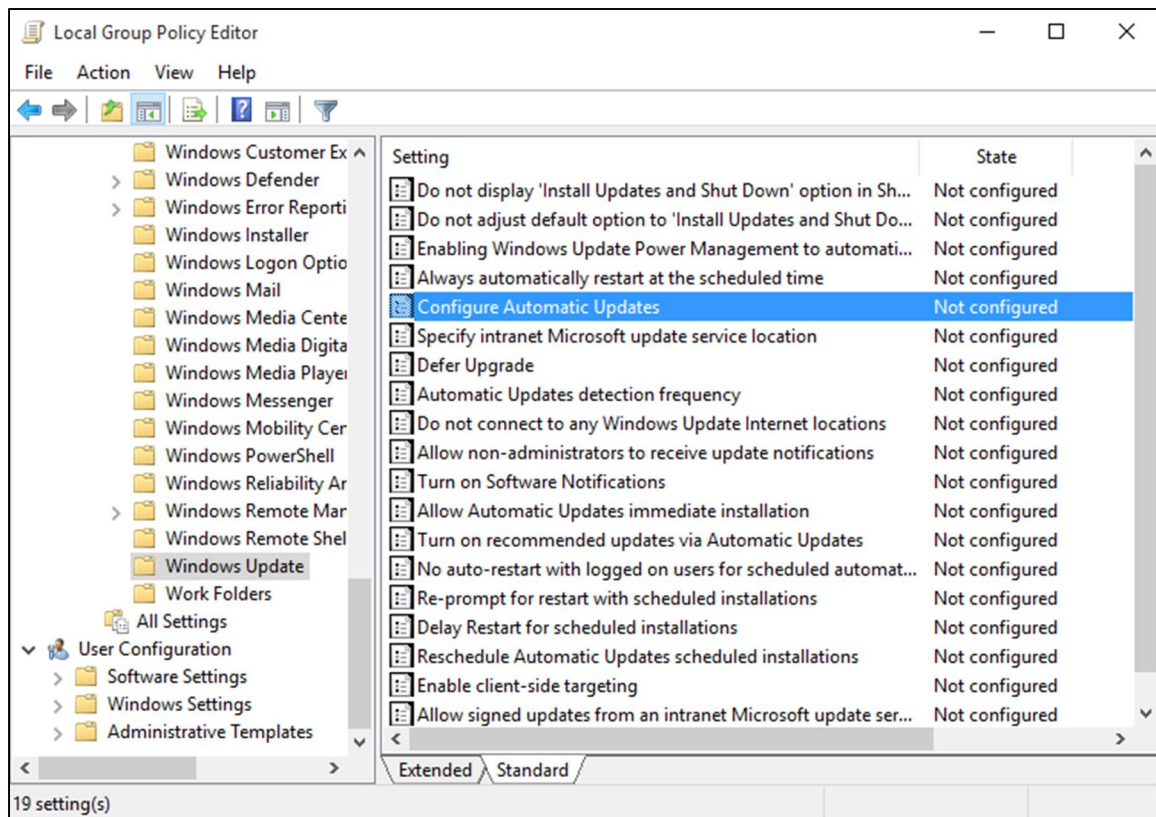
- יש להשתמש במדריך ההתקנה של Windows 10 להתקנת מכונה וירטואלית חדשה של Windows עם תוספות אורח.
- יש ללחוץ על מקש **Windows + R**, להזין **gpedit.msc** וללחוץ על **OK** כדי לפתוח את עורך מדיניות הקבוצות המקומית.



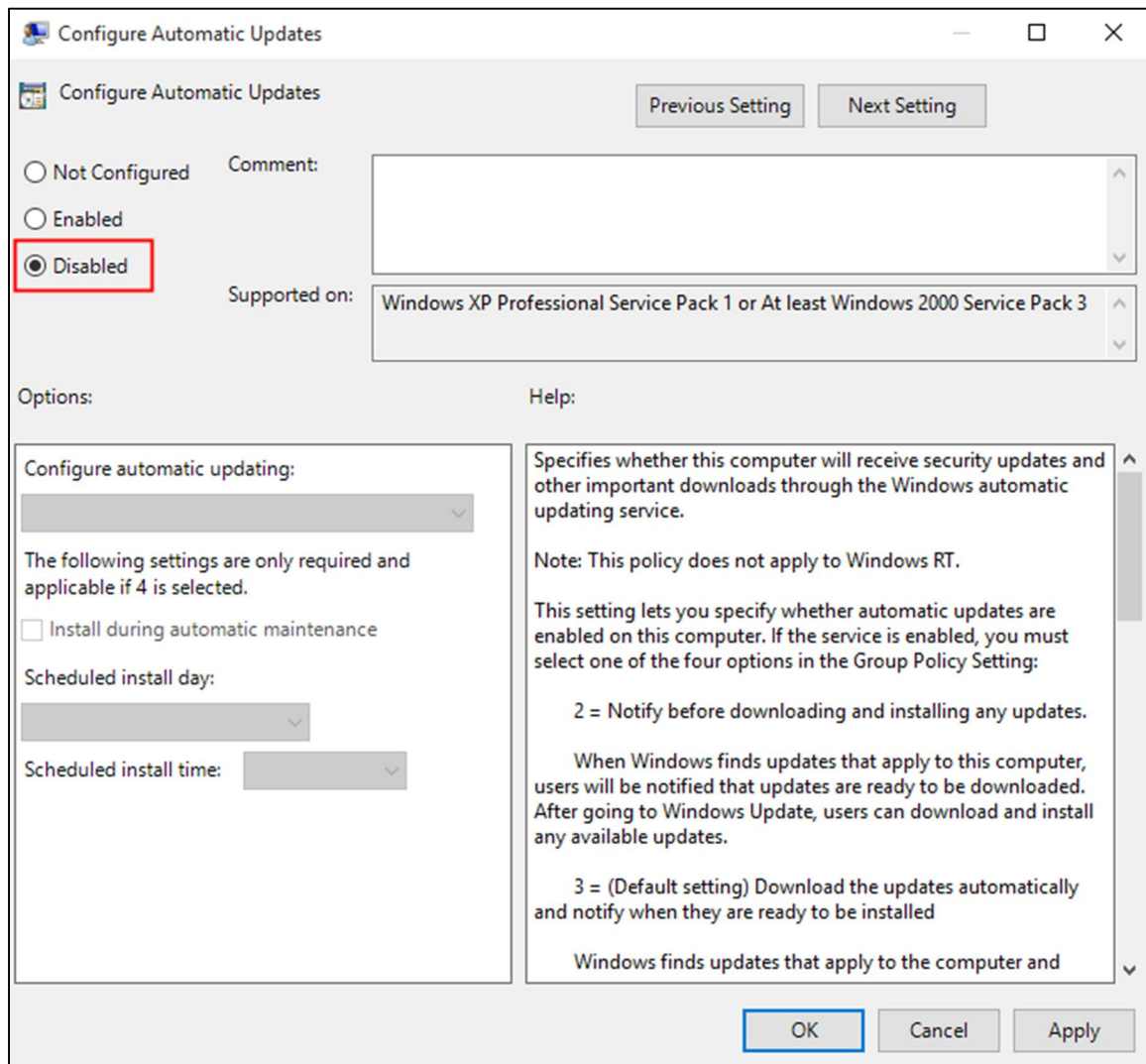
Computer Configuration → Administrative Templates → Windows אל ישי לכוט אל 3  
 Components → Windows Update



#### 4 יש ללחוץ לחיצה כפולה על Configure Automatic Updates (הגדרת עדכונים אוטומטיים).



5 יש להגדיר את האפשרות ל-Disabled, ללחוץ על Apply ולאחר מכן על OK.

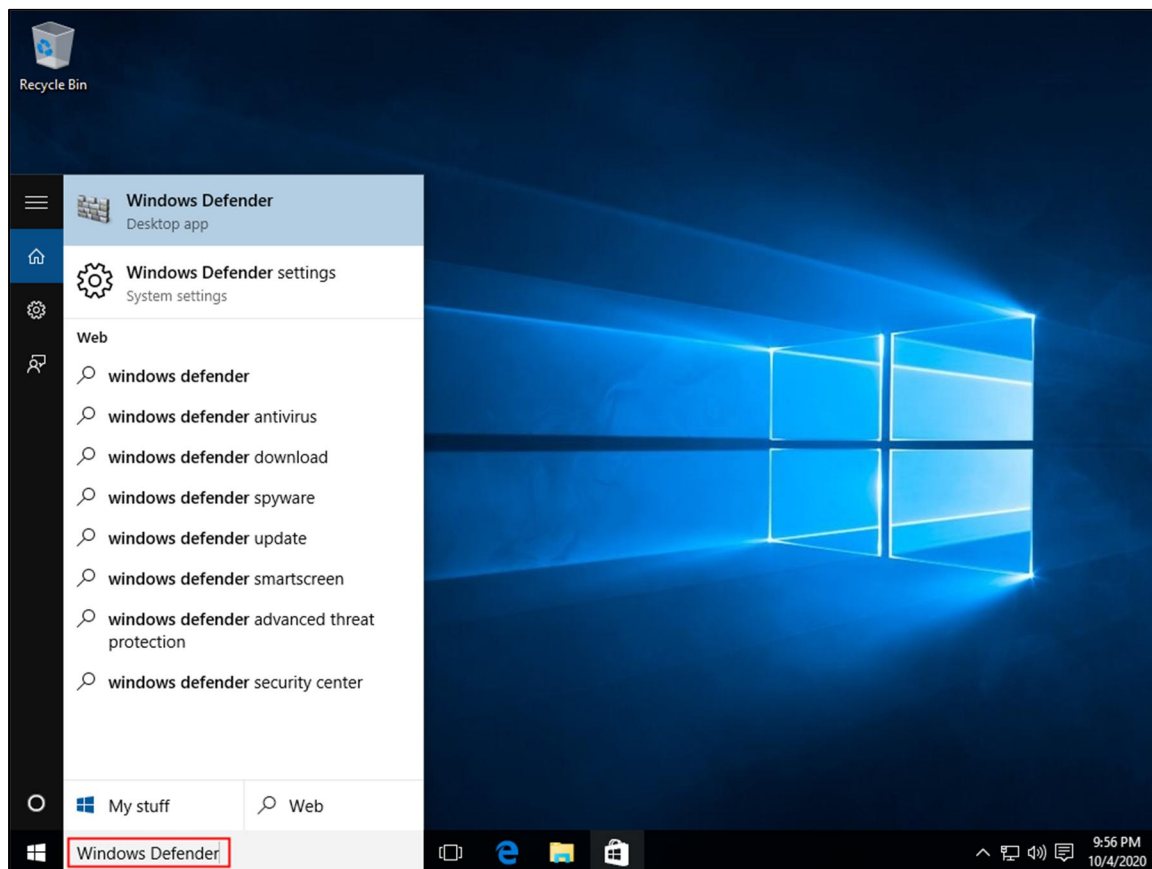


6 יש לסגור את יתר החלונות.

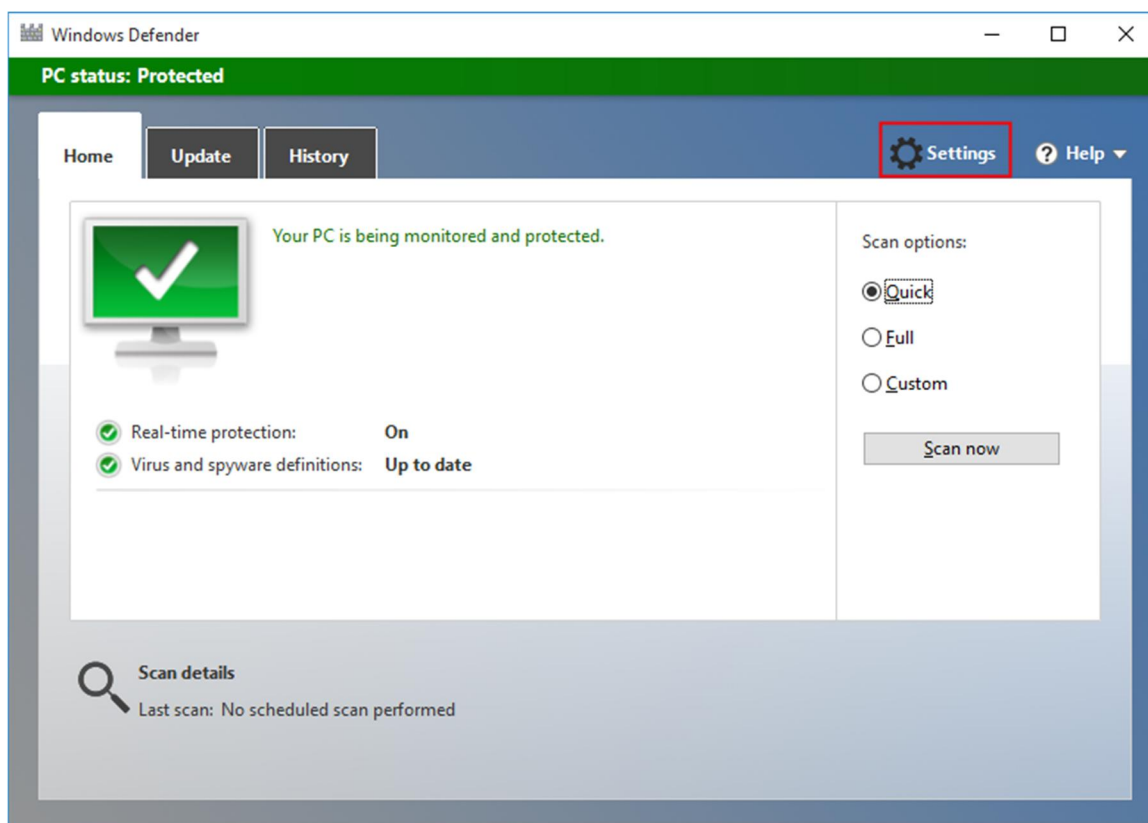
## זיהוי קבצים

במשימה זו, יש לבדוק את זיהוי הקבצים מול מזהה קבצים זדוניים.

1 יש ללחוץ על הסמל של Windows, לחפש את היישום Windows Defender ולפתוח אותו.

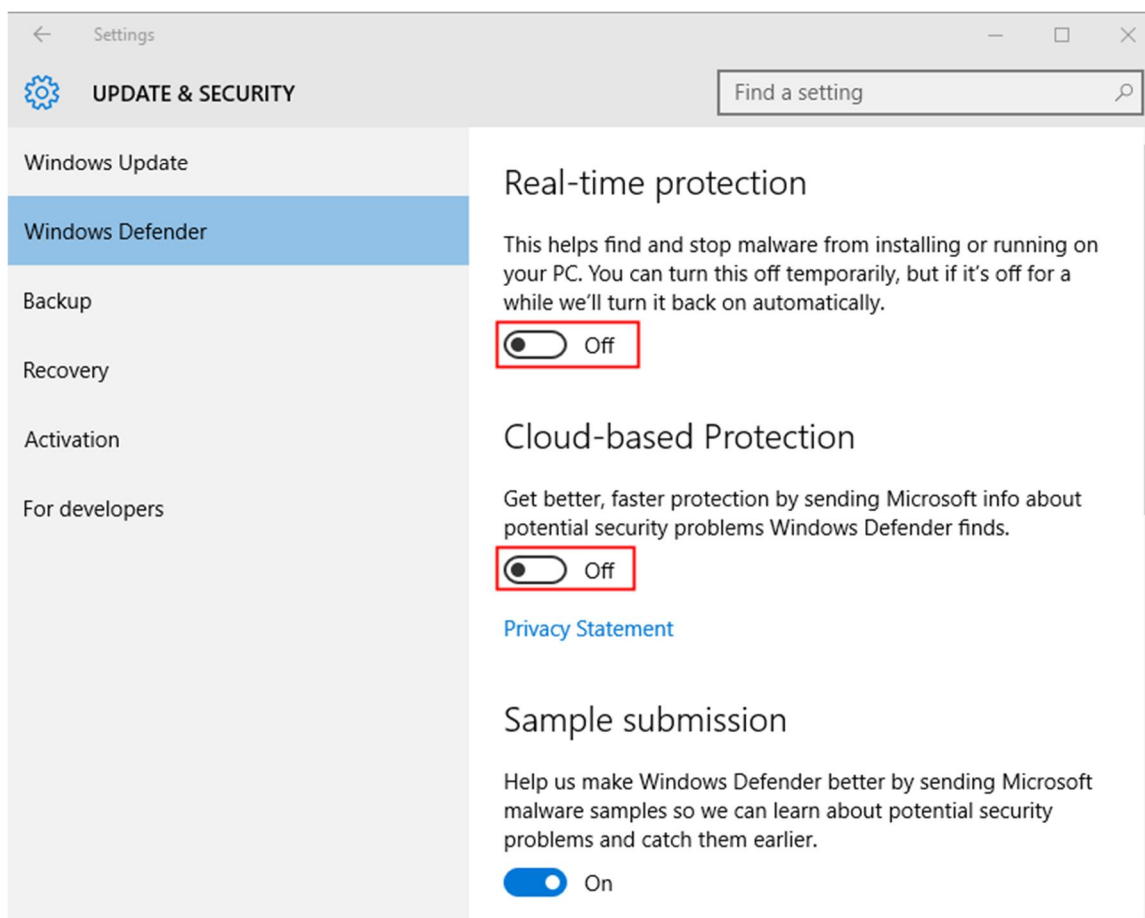




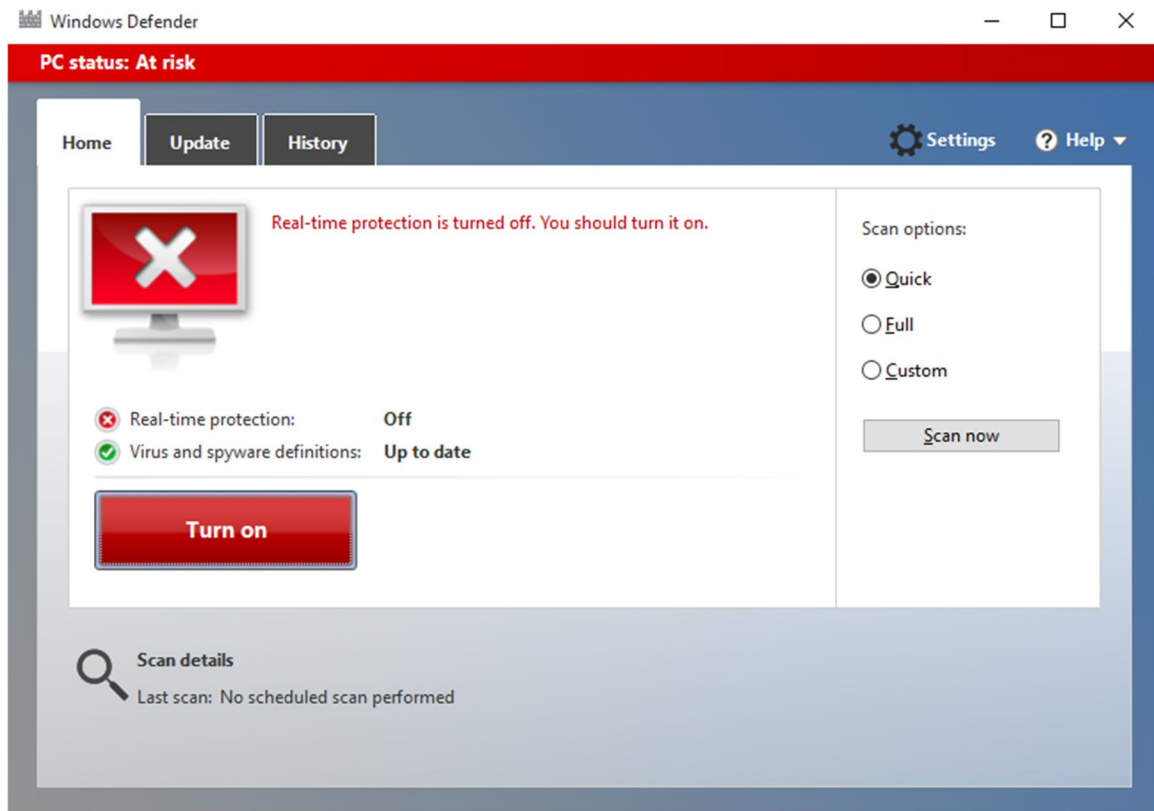




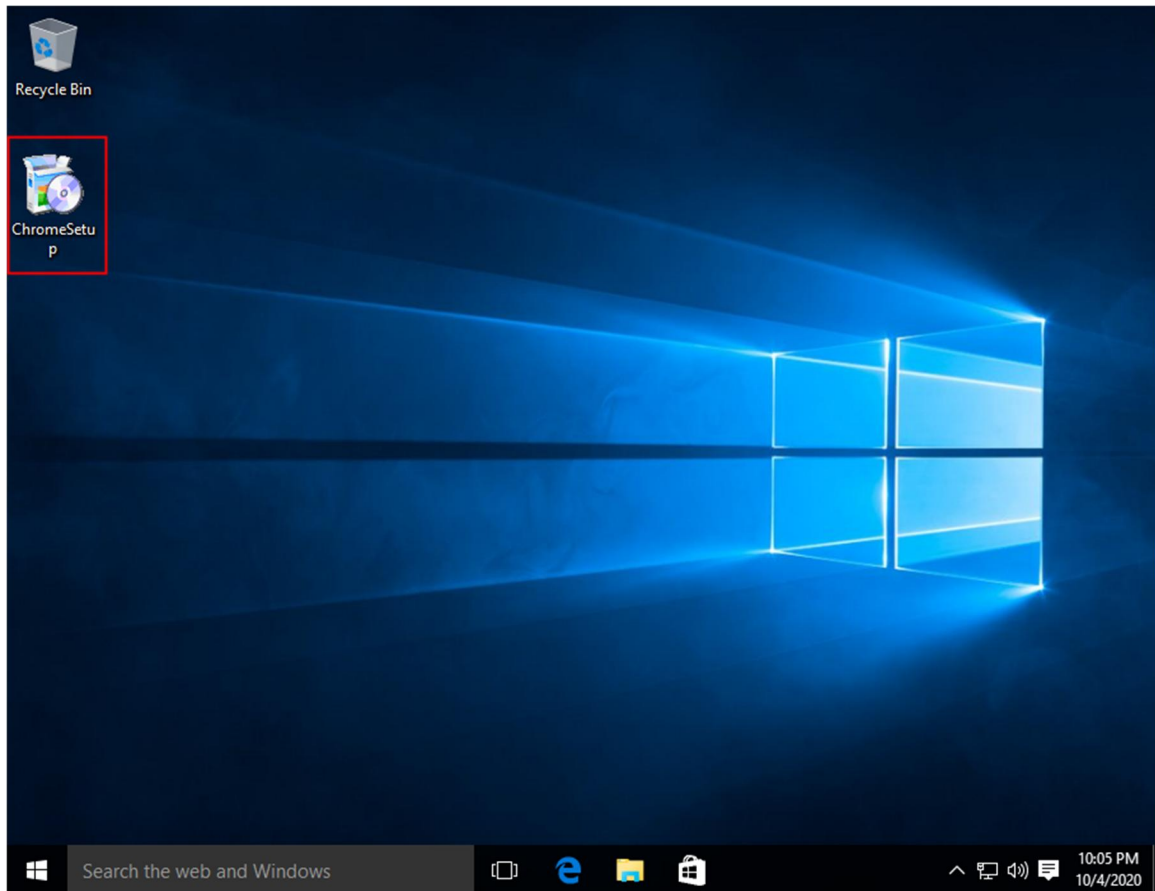
### 3 יש להשבית את Real-Time protection ואת Cloud-based Protection.



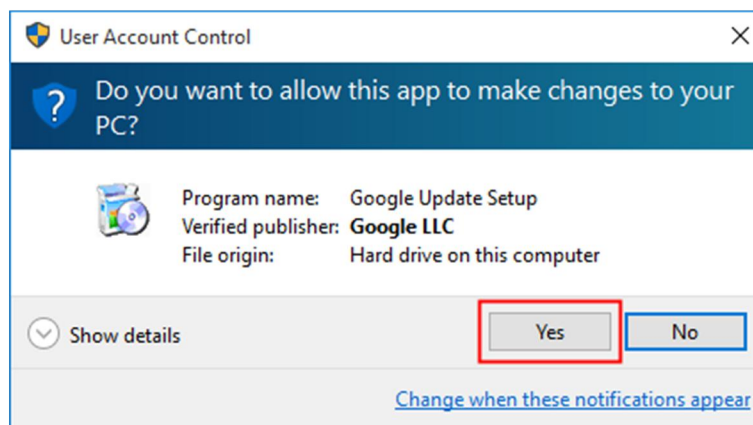
#### 4 יש לסגור את החלון ולוודא ש-Windows Defender כבוי.



5 יש להעתיק את קובץ **ChromeSetup.exe** אל המכונה הווירטואלית Windows 10 וללחוץ לחיצה כפולה על הקובץ כדי להתחיל בהתקנת דפדפן Chrome.



6 יש ללחוץ על **Yes** כדי לאפשר את תחילת ההתקנה.



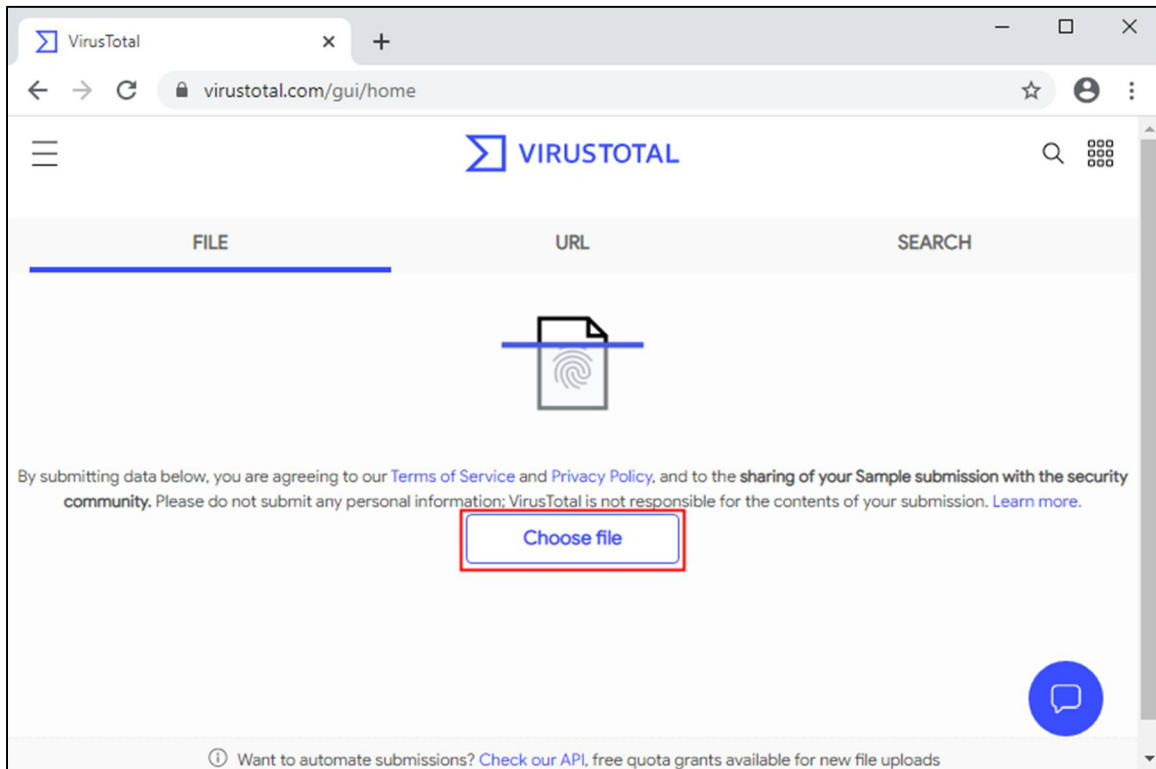
7 כשייפתח חלון הדפדפן, יש לעבור אל:

[https://www.eicar.org/?page\\_id=3950](https://www.eicar.org/?page_id=3950)

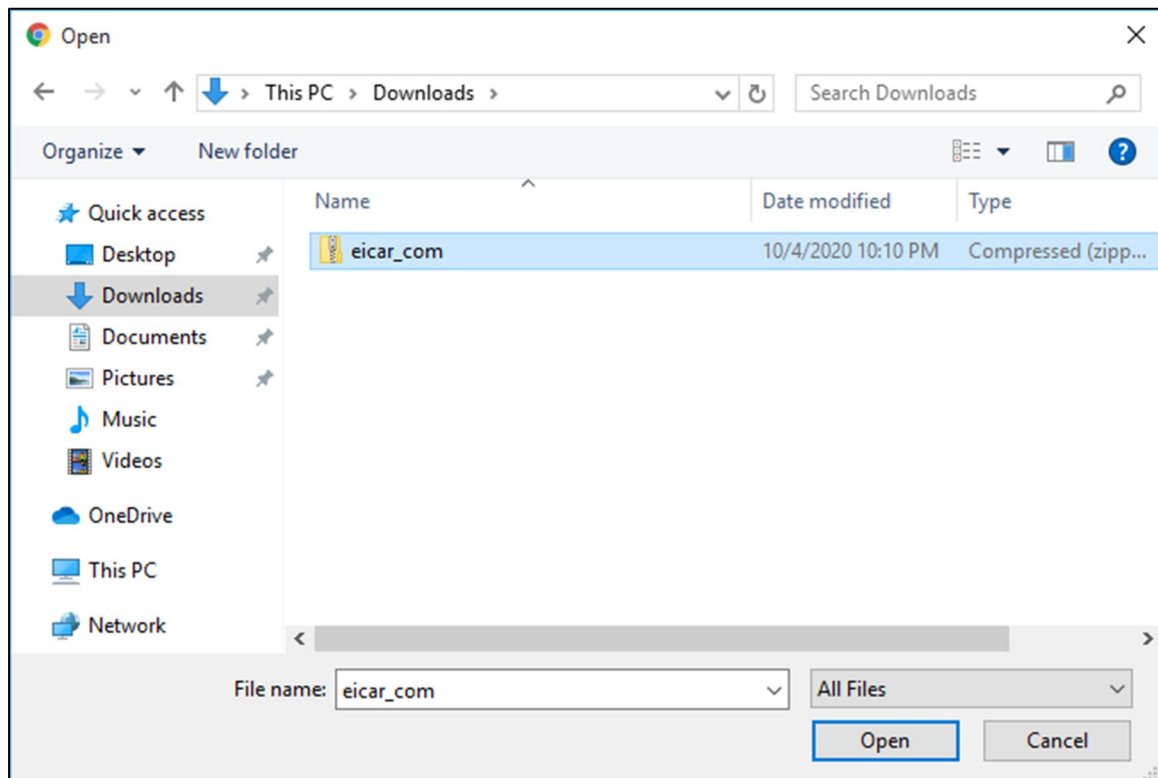
8 יש לגלול מטה ולהוריד את הקובץ **eicar\_com.zip** על ידי לחיצה עליו.

Download area using the standard protocol HTTP			
– Sorry, HTTP download ist temporarily not provided. –			
Download area using the secure, SSL enabled protocol HTTPS			
<a href="#">eicar.com</a> 68 Bytes	<a href="#">eicar.com.txt</a> 68 Bytes	<a href="#">eicar_com.zip</a> 184 Bytes	<a href="#">eicarcom2.zip</a> 308 Bytes

9 יש לגלוש אל <https://www.virustotal.com/gui/home> וללחוץ על **Choose file**.



10 יש לנווט אל **Downloads**, לבחור **eicar\_com.zip**, וללחוץ על **Open**.



11 יש לשים לב שכמעט כל המנועים מסמנים את הקובץ כדדוני.

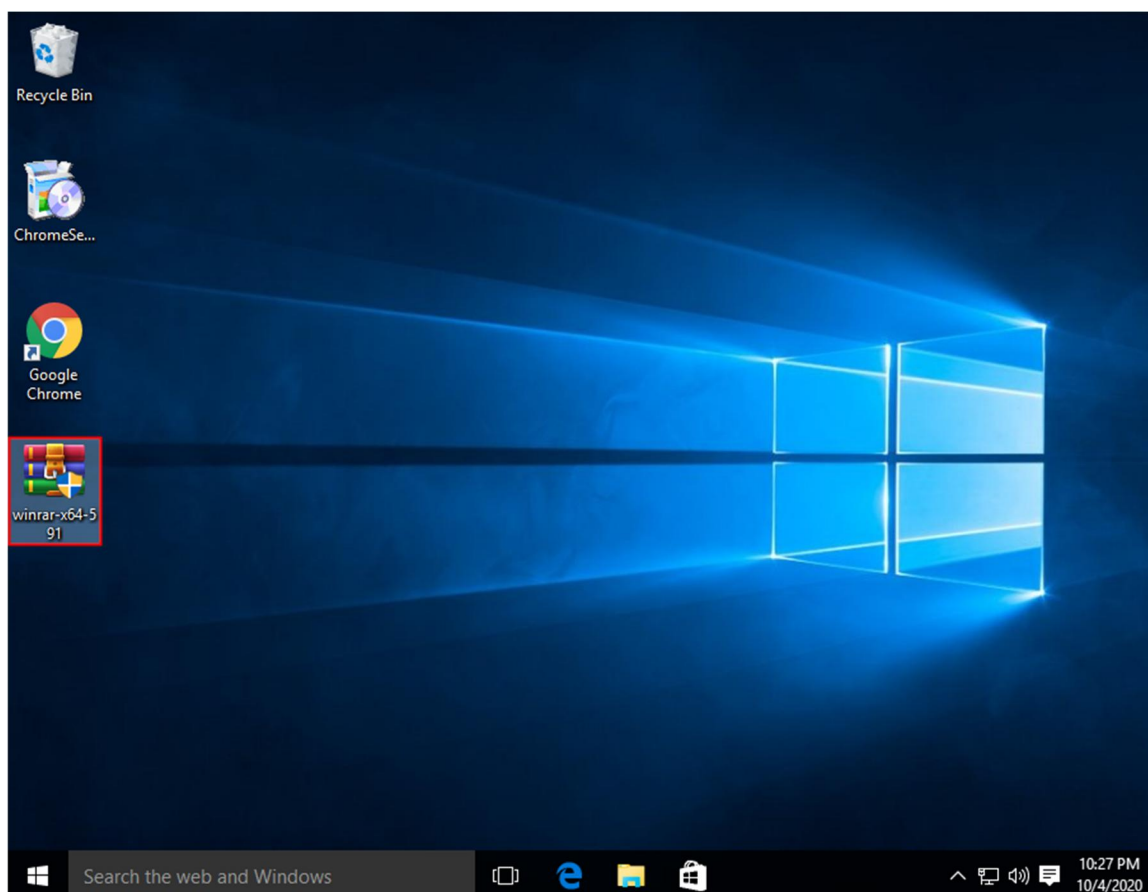
The screenshot shows the VirusTotal interface for a file named 'eicar\_com.zip'. The file's SHA-256 hash is 2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad. The file size is 184.00 B and it was uploaded on 2020-10-04 08:45:29 UTC. The detection score is 57 out of 63 engines. The file is identified as a ZIP attachment via TOR.

Engine	Detection	Engine	Detection
Ad-Aware	EICAR-Test-File (not A Virus)	AegisLab	Test.File.EICAR.00x7
AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Virus:Any/EICAR_Test_File.0211596c
Antiy-AVL	TestFile/Win32.EICAR	Arcabit	EICAR-Test-File (not A Virus)
Avast	EICAR Test -NOT Virus!!!	Avast-Mobile	Eicar
AVG	EICAR Test -NOT Virus!!!	Avira (no cloud)	Eicar-Test-Signature
Baidu	Win32.Test.Eicar.a	BitDefender	EICAR-Test-File (not A Virus)

## התחמקות מגילוי

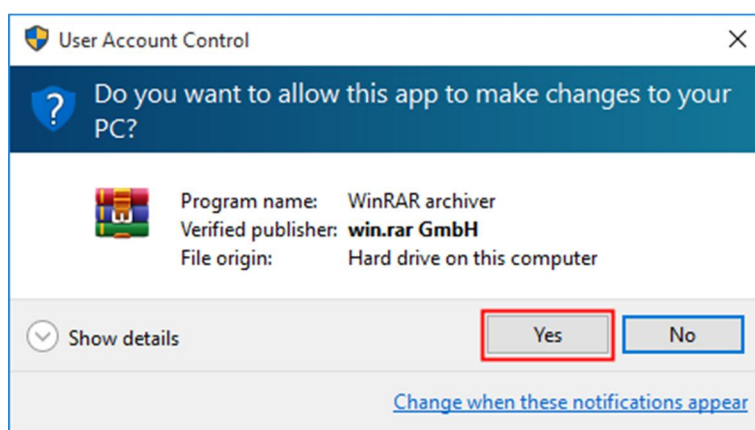
במשימה זו, תטמיעו שיטה שתאפשר לכם לעקוף את זיהוי הקובץ.

- יש להעתיק אל המכונה הווירטואלית Windows 10 VM את קובץ התקנת winrar המסופק **winrar-x64-591.exe** וללחוץ עליו לחיצה כפולה.





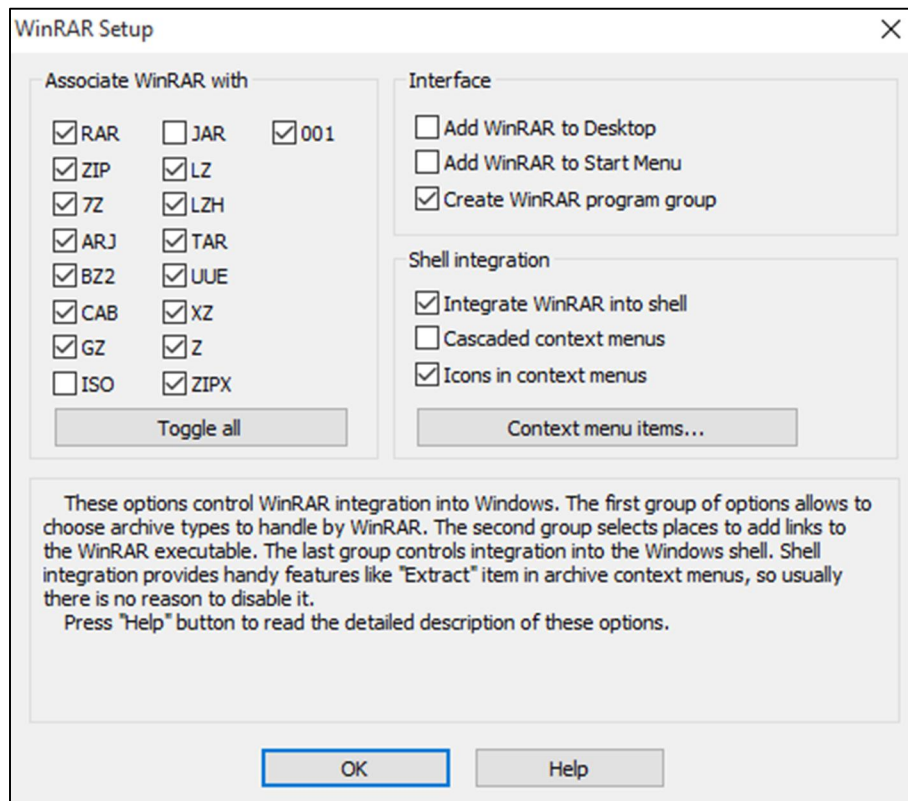
2 יש ללחוץ על Yes כדי לאפשר את תחילת ההתקנה.



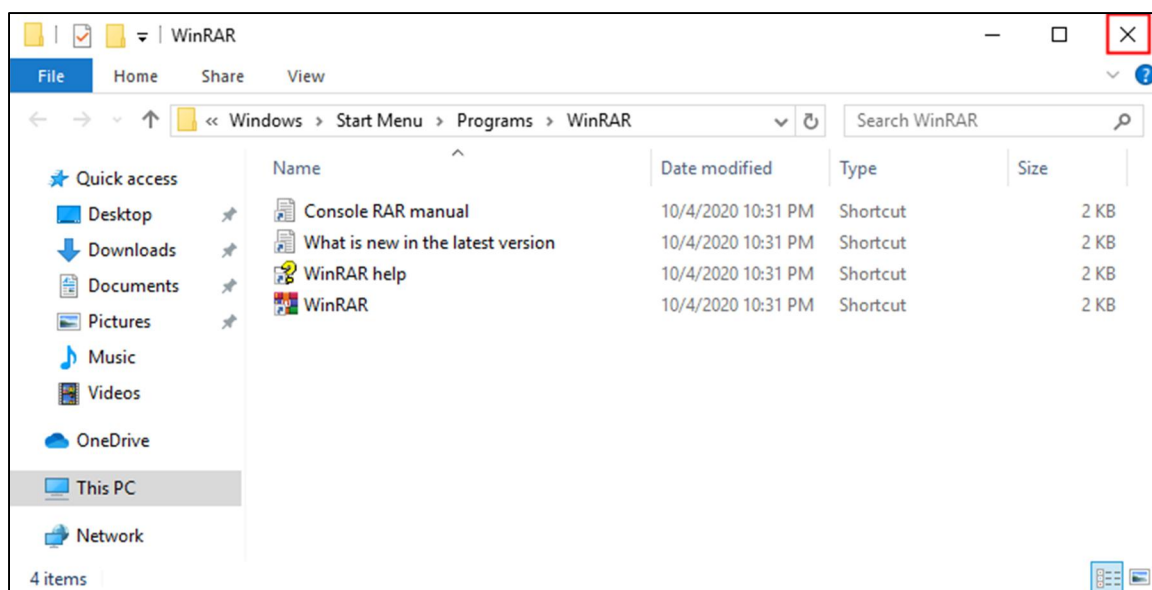
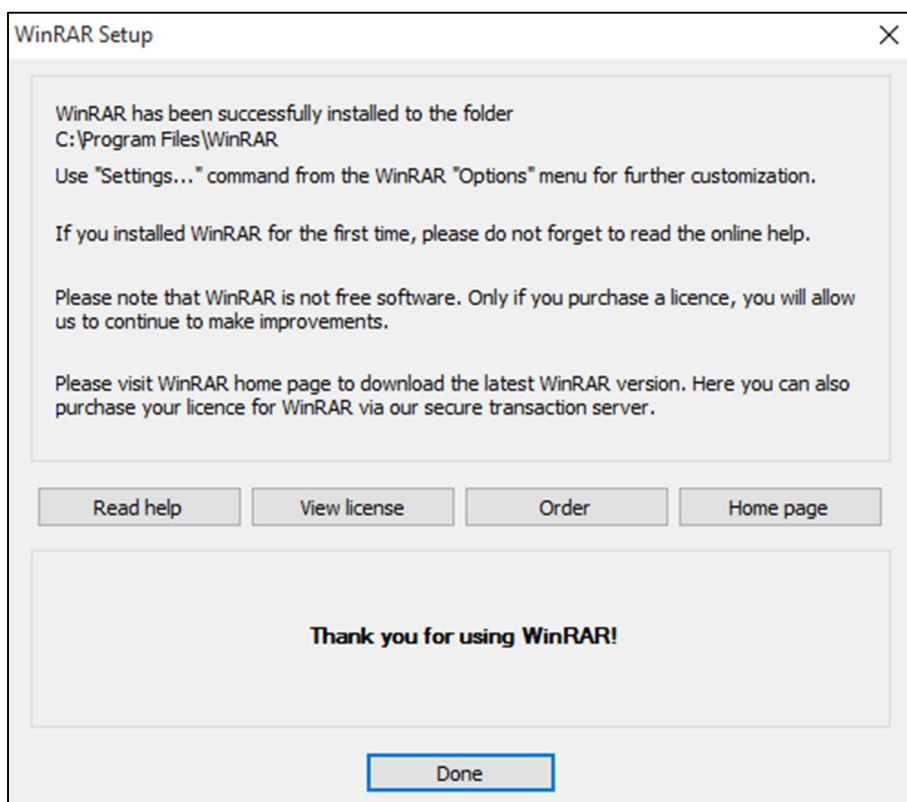
3 יש להשתמש בנתיב ברירת המחדל להתקנה וללחוץ על Install.



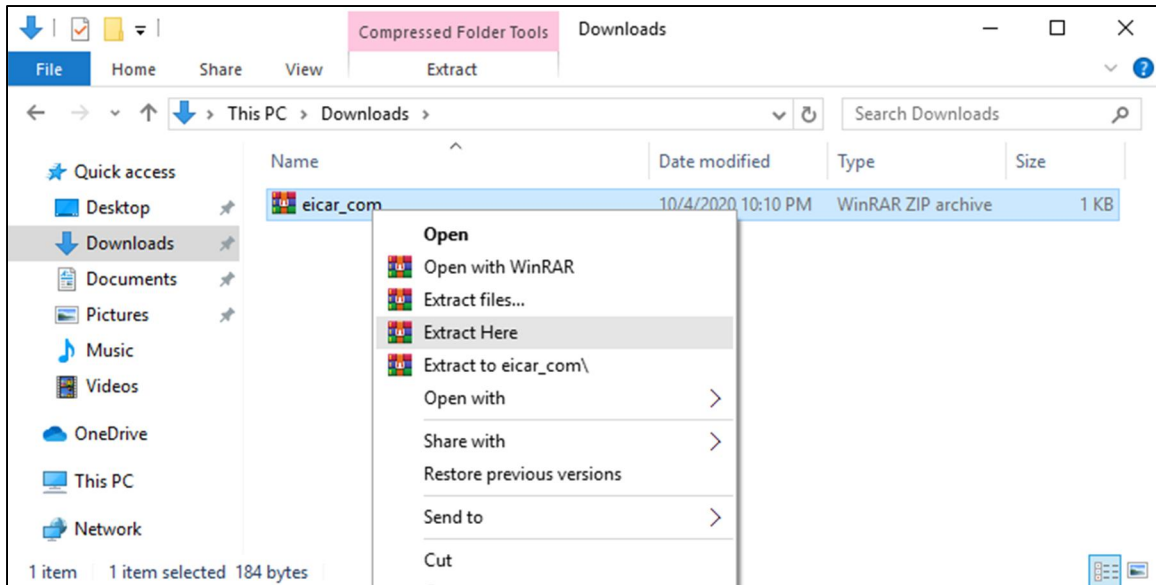
#### 4 יש להשאיר את האפשרויות הנבחרות כפי שהן וללחוץ על OK.



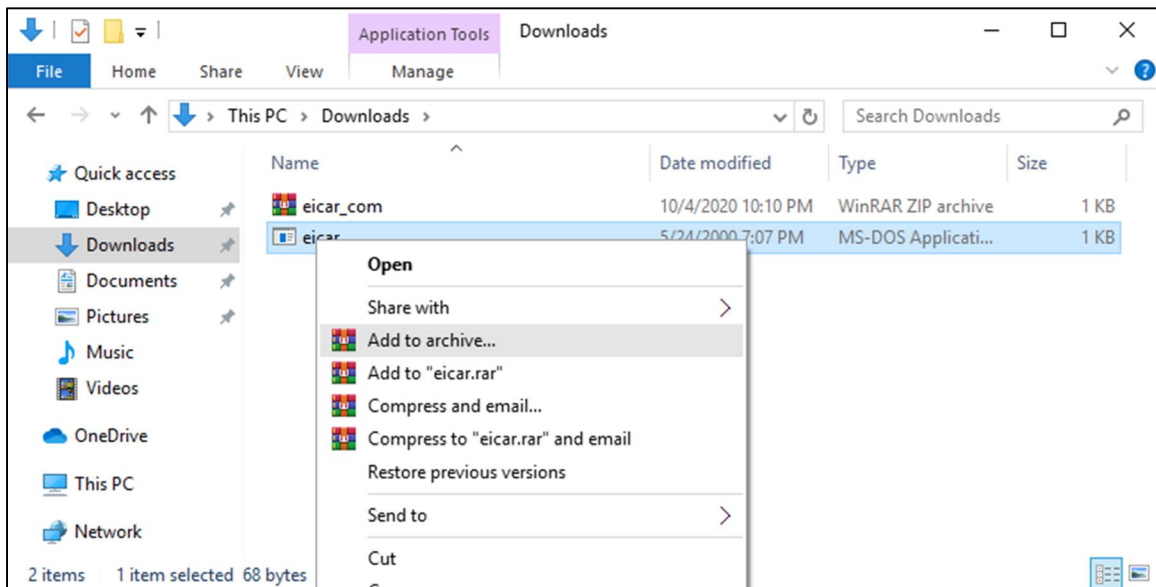
5 יש ללחוץ על **Done** כדי לסיים את ההתקנה, ולסגור את התיקייה שמופיעה.



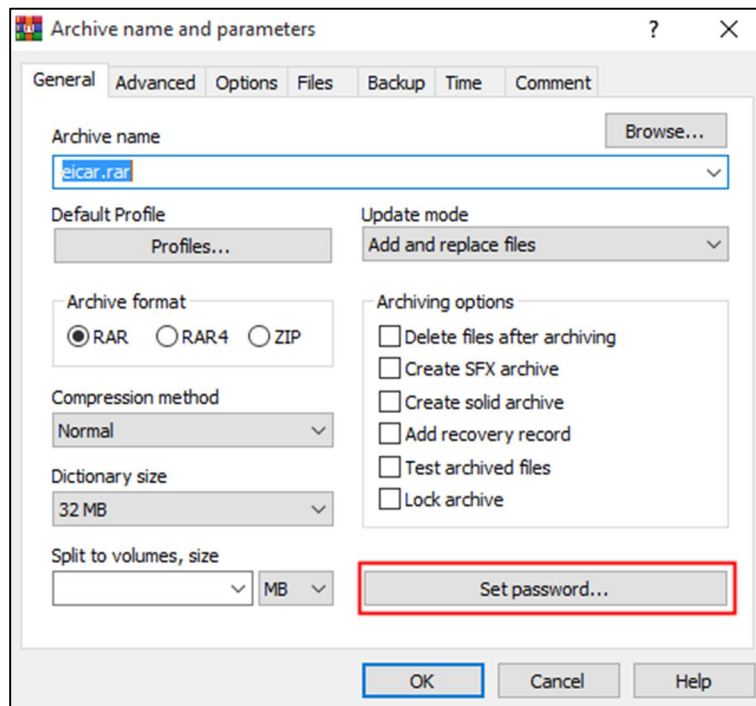
6 יש לפתוח את הספרייה Downloads, ללחוץ לחצן ימני על eicar\_com ולבחור את Extract Here כדי לחלץ אותו.



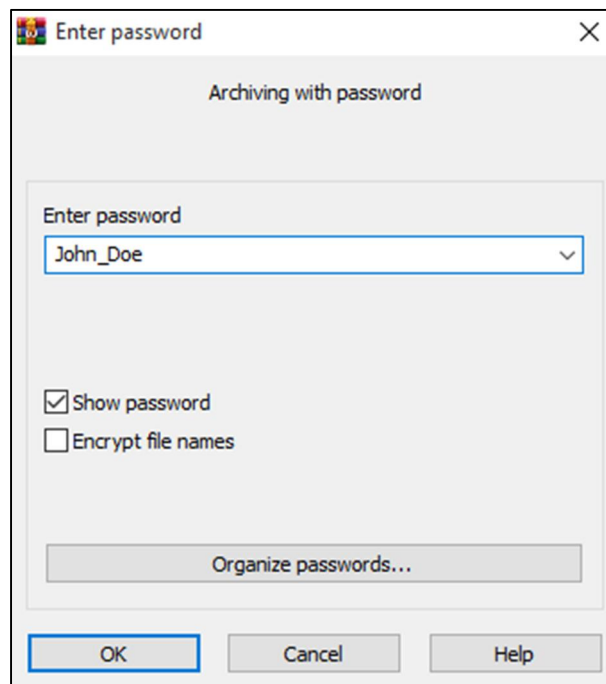
7 יש ללחוץ לחצן ימני על הקובץ eicar ולבחור באפשרות Add to archive...



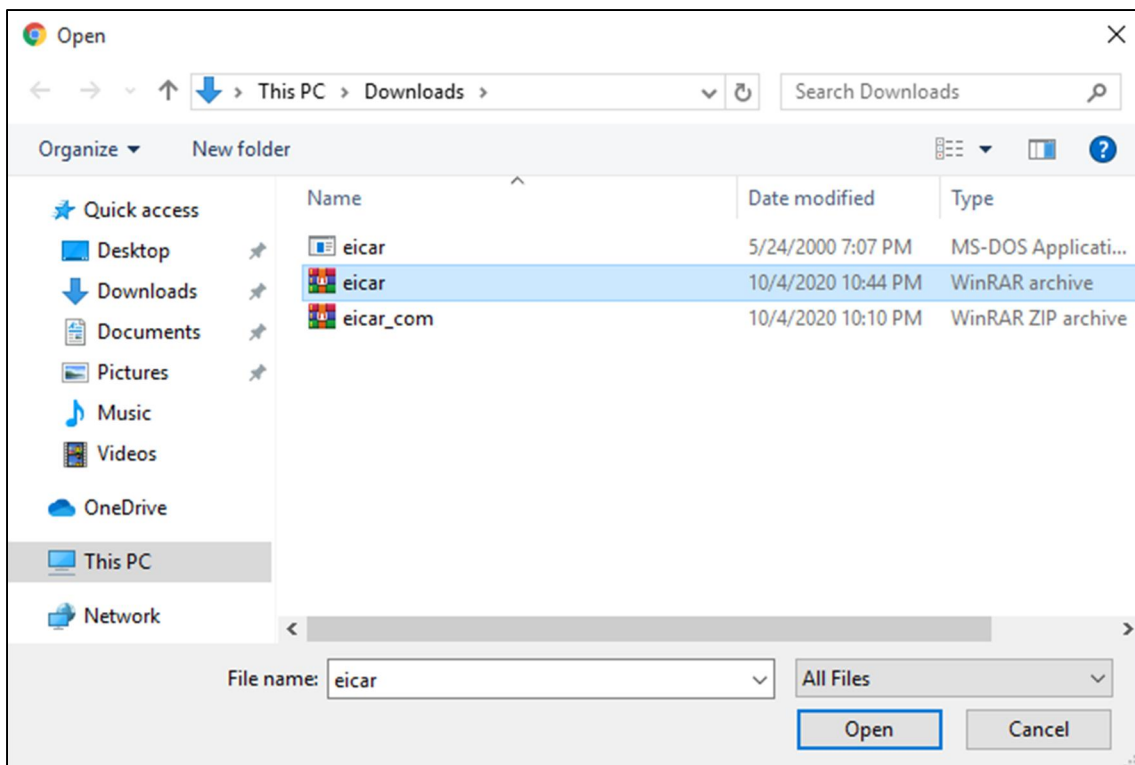
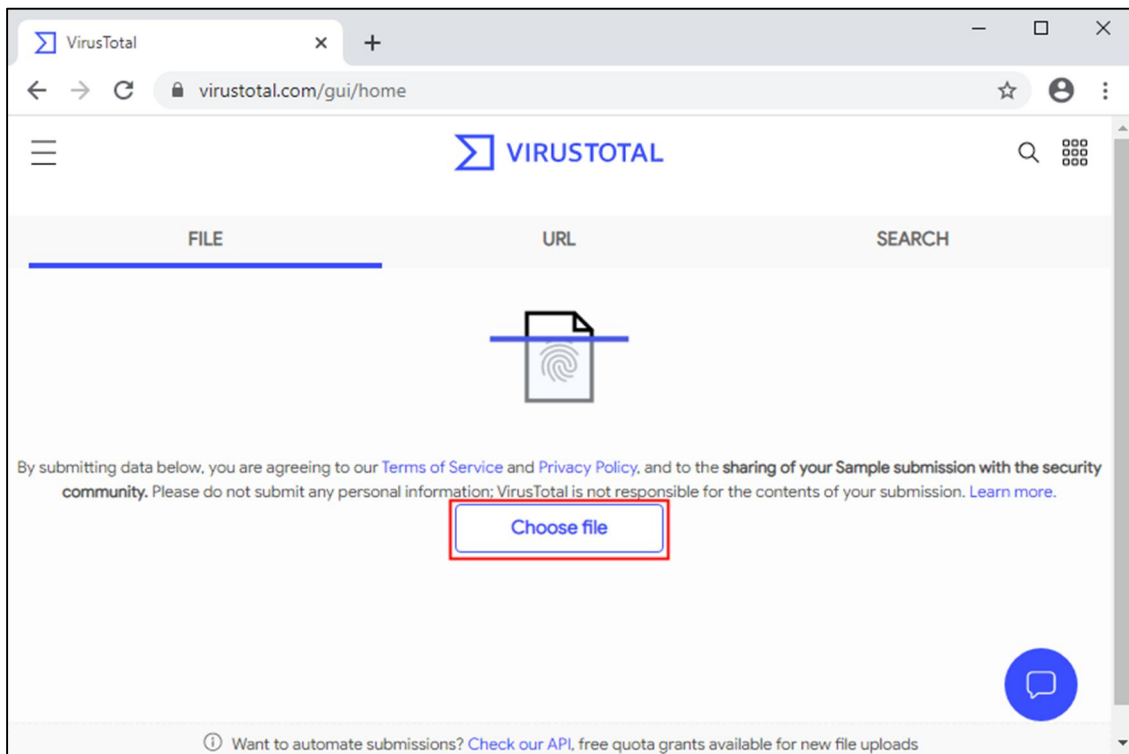
## 8 יש ללחוץ על Set password.



9 יש להשתמש בשם שלך בסיסמה, ללחוץ על OK, ושוב על OK בחלון הקודם כדי להשלים את הדחיסה.



10 יש לגלוש שוב אל <https://www.virustotal.com/gui> ולהעלות את הקובץ החדוס.



11 יש ללחוץ על **Confirm upload** ולשים לב שאף אחד מהמנועים לא סימן את הקובץ כזדוני.

