מעבדה 1

CYBER SCHOOL

אבטחת נקודת קצה

עקיפת אפליקציית אנטי-וירוס

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

נושאי המעבדה

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

זמן מוערך

40–60 דקות

סביבת מעבדה

- VirtualBox
- Windows 10

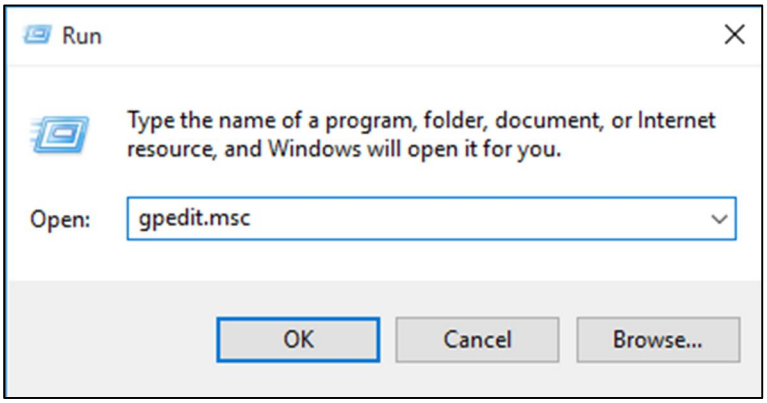
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

משימת מעבדה

התקנת Windows

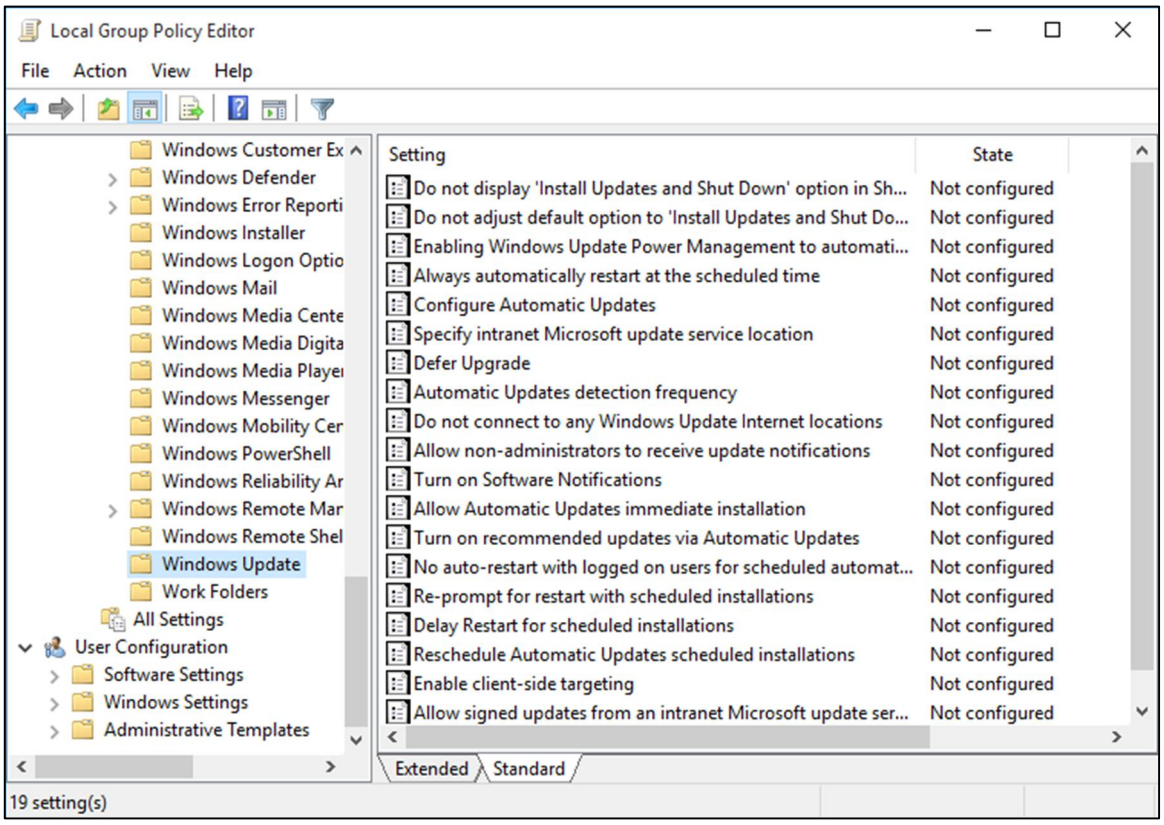
במשימה זו תתקינו מכונה וירטואלית Windows 10 VM ב-VirtualBox, תכינו אותה למעבדה ותשביתו את העדכונים שלה.

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



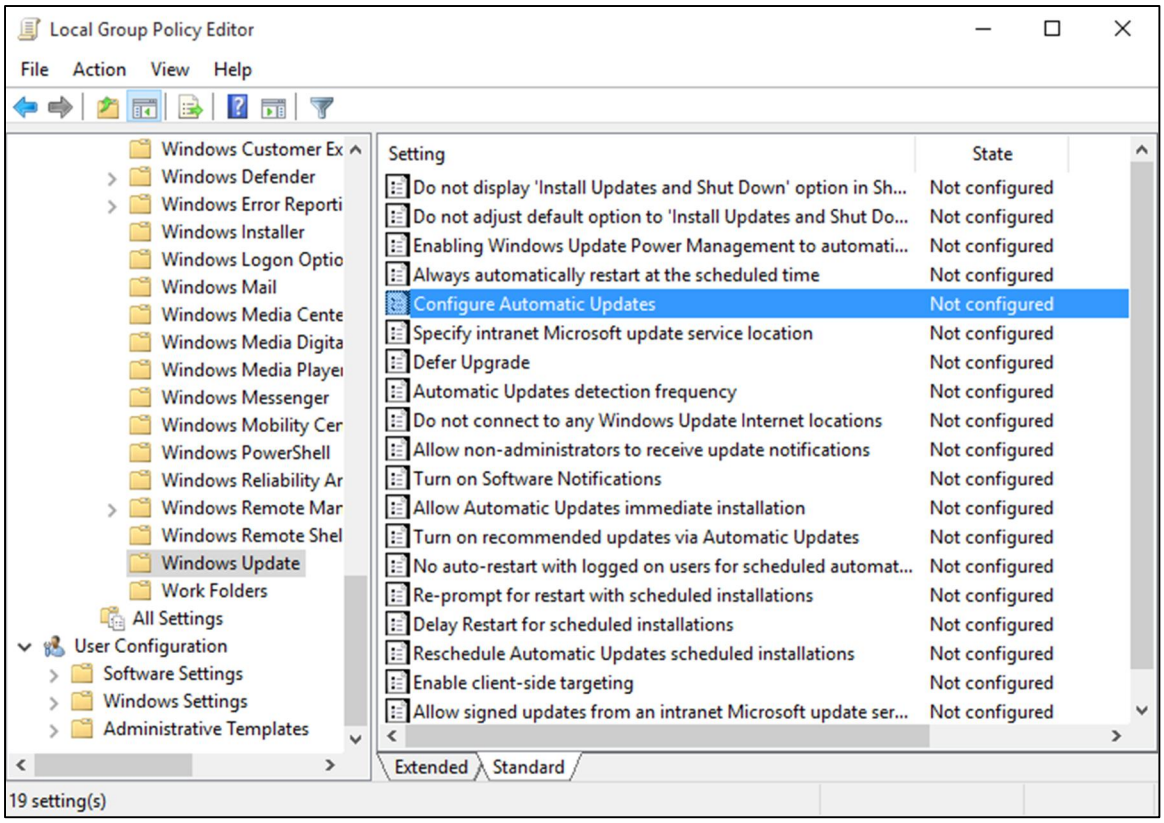
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

3 יש לנווט אל Windows → Administrative Templates → Computer Configuration
Components → Windows Update



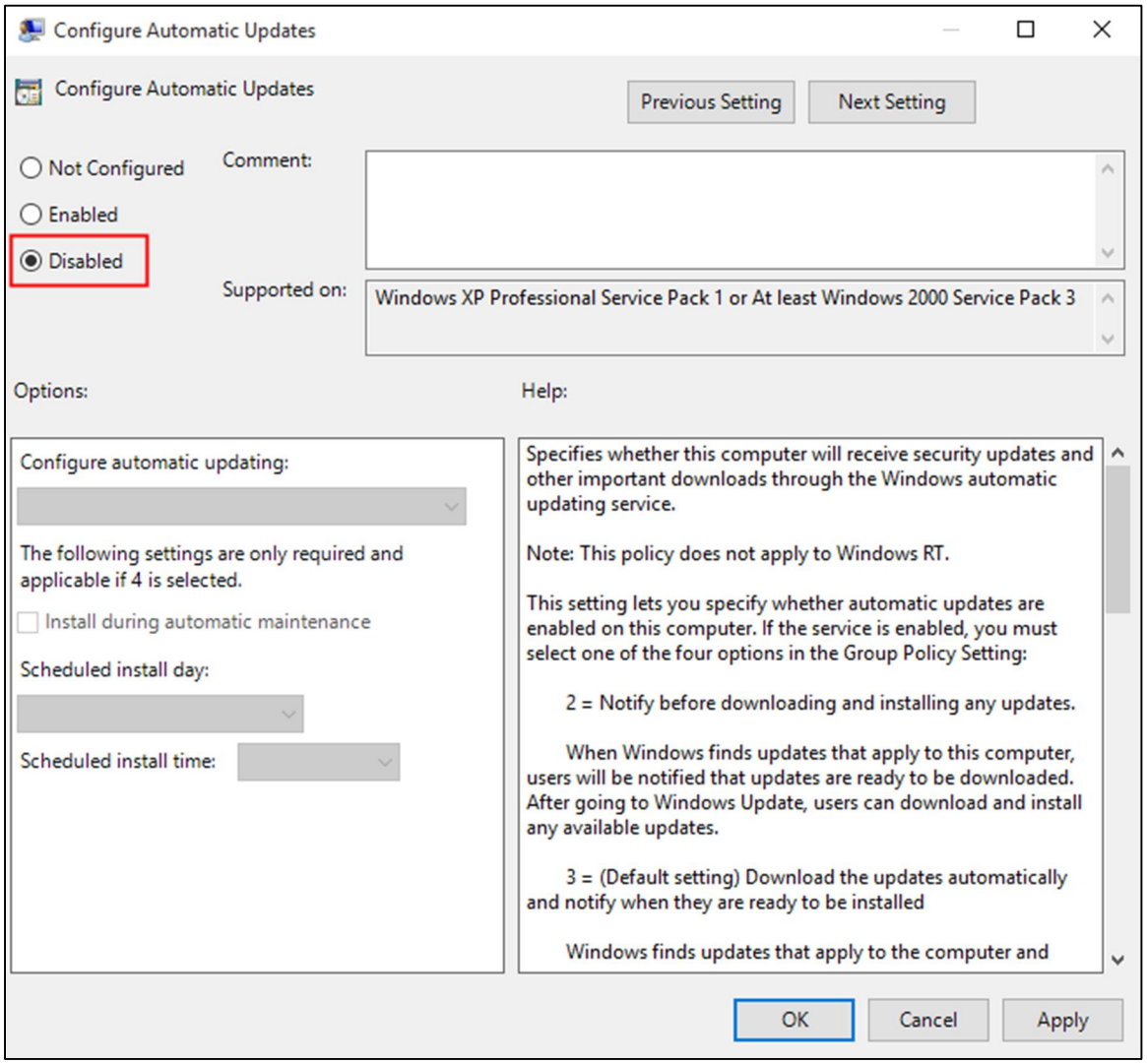
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383
CYBER SCHOOL

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



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

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



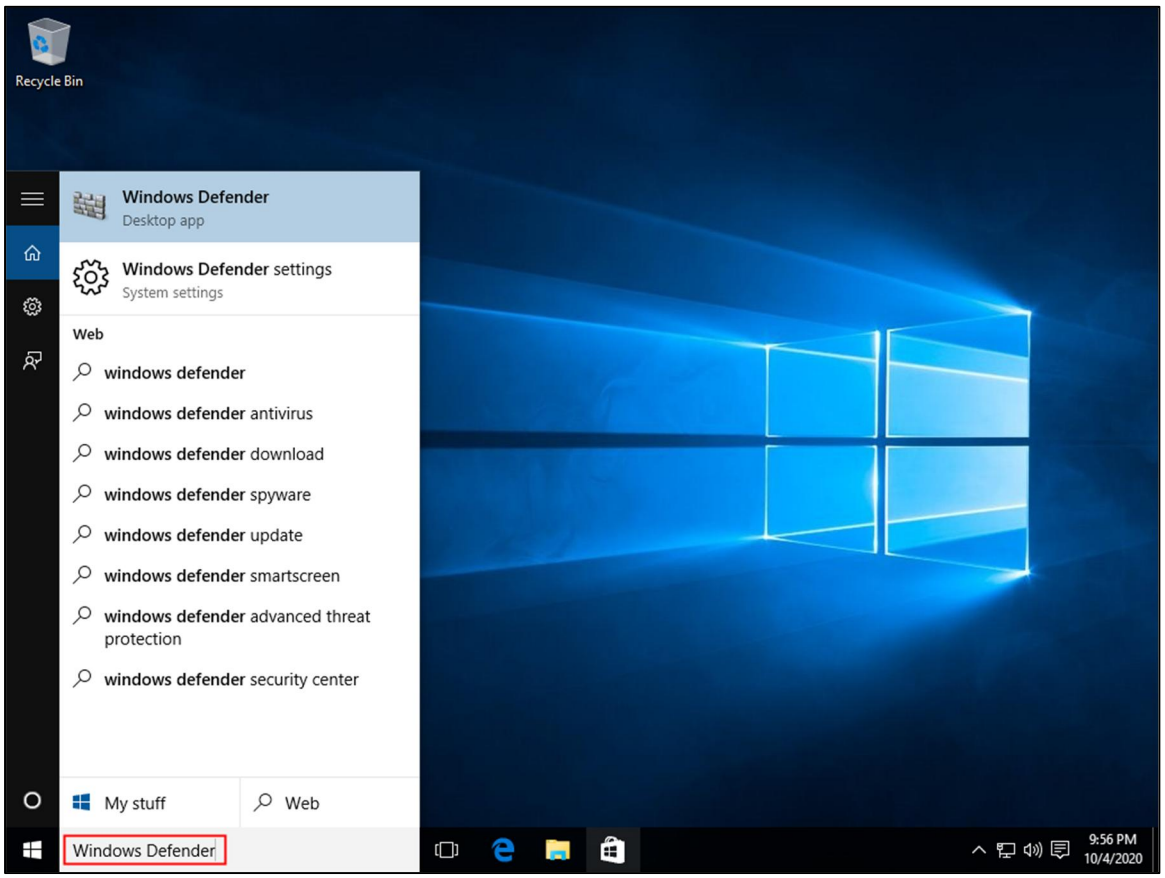
6 יש לסגור את יתר החלונות.

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

זיהוי קבצים

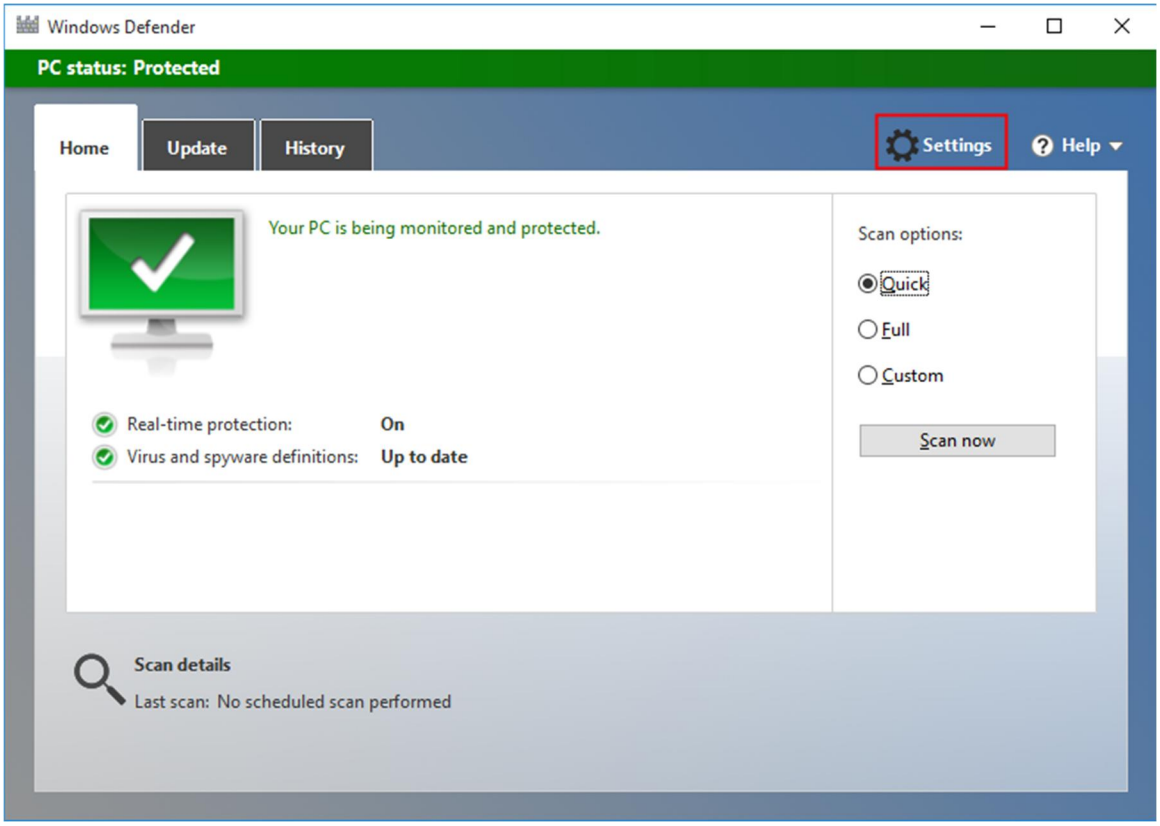
במשימה זו, יש לבדוק את זיהוי הקבצים מול מזהה קבצים זדוניים.

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



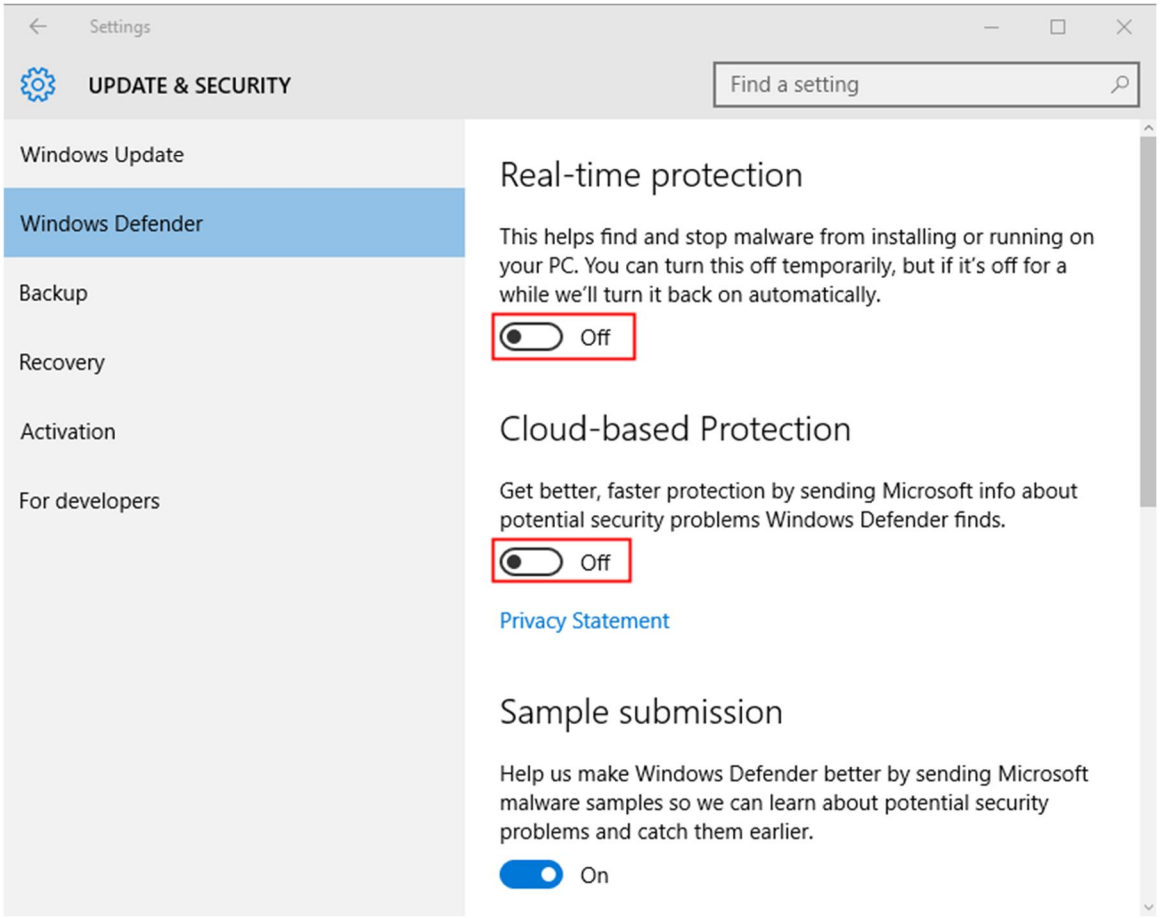
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

2 יש ללחוץ על Settings.



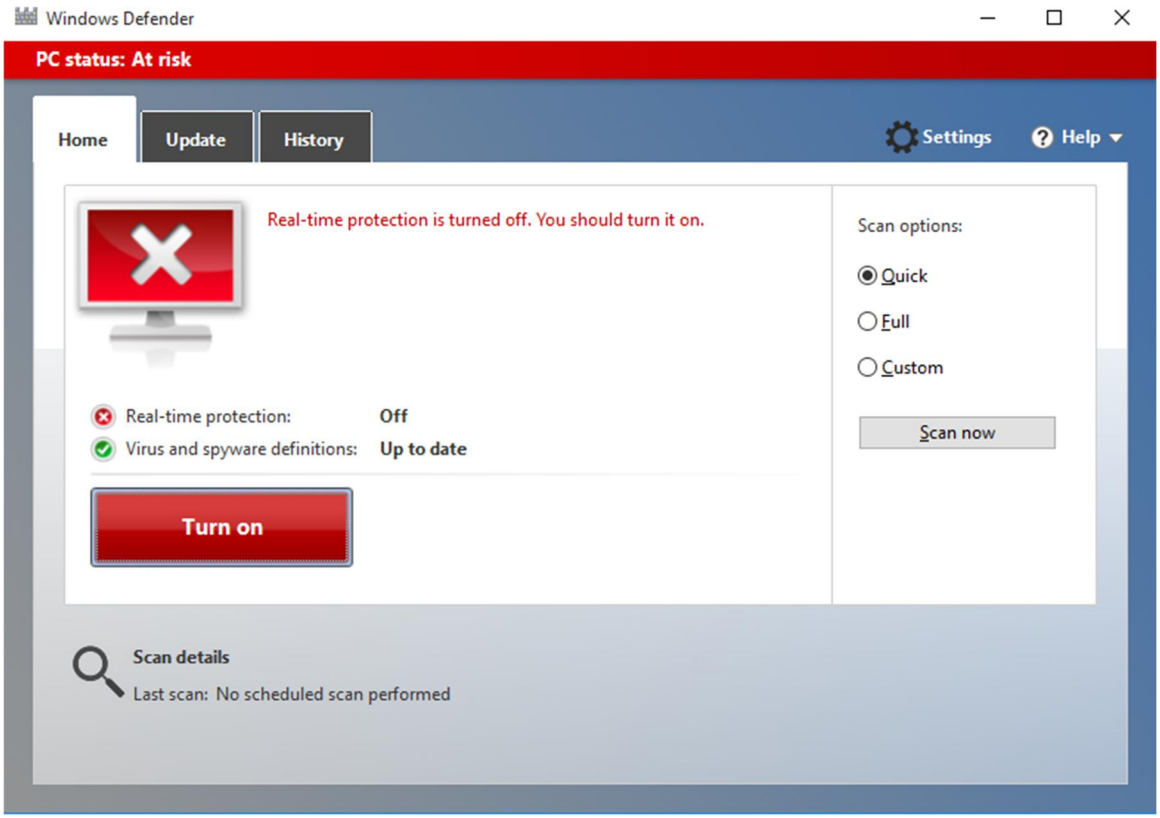
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

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



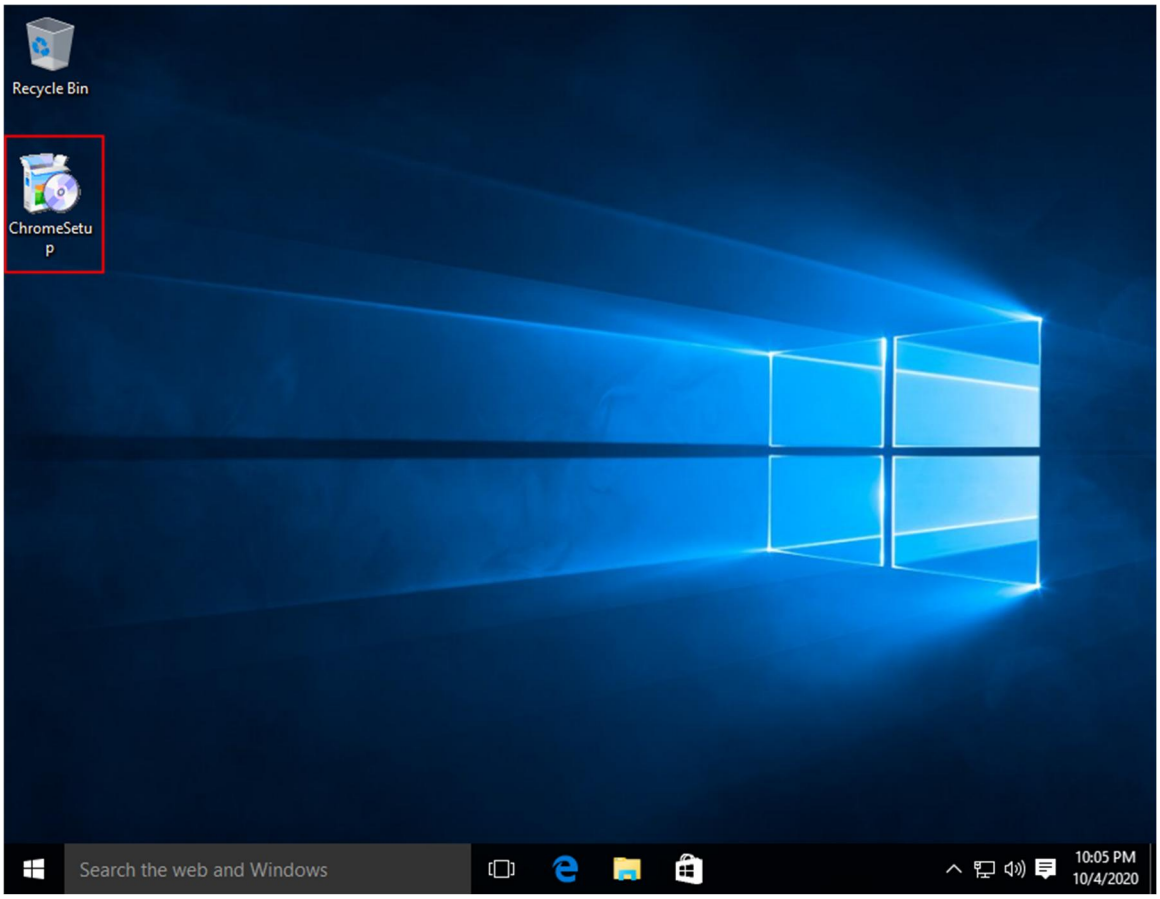
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

4 יש לסגור את החלון ולוודא ש-Windows Defender בבוי.

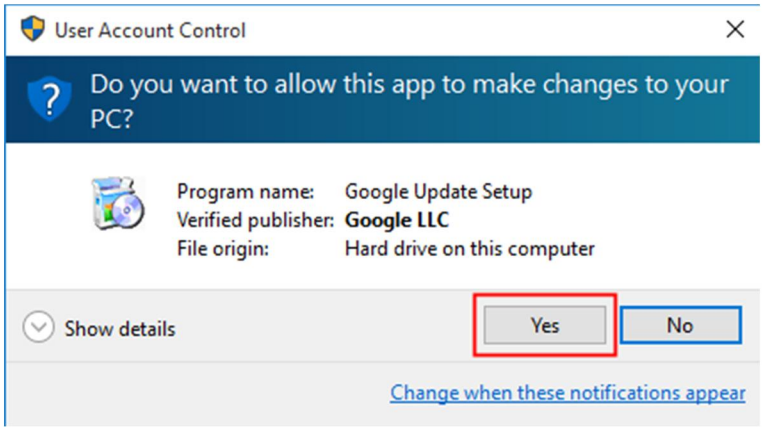


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

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



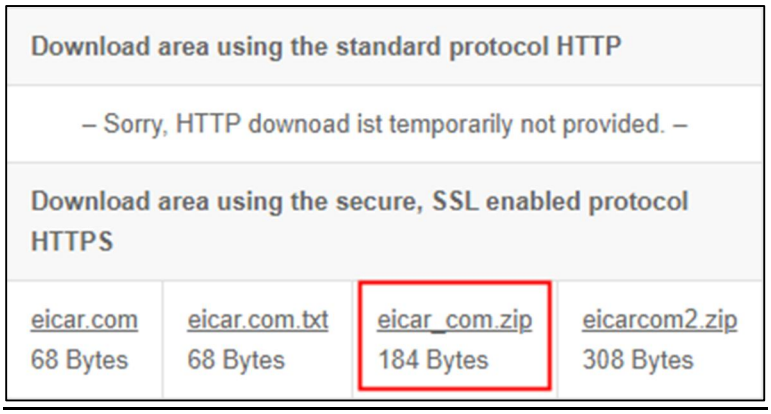
6 יש ללחוץ על **Yes** כדי לאפשר את תחילת ההתקנה.



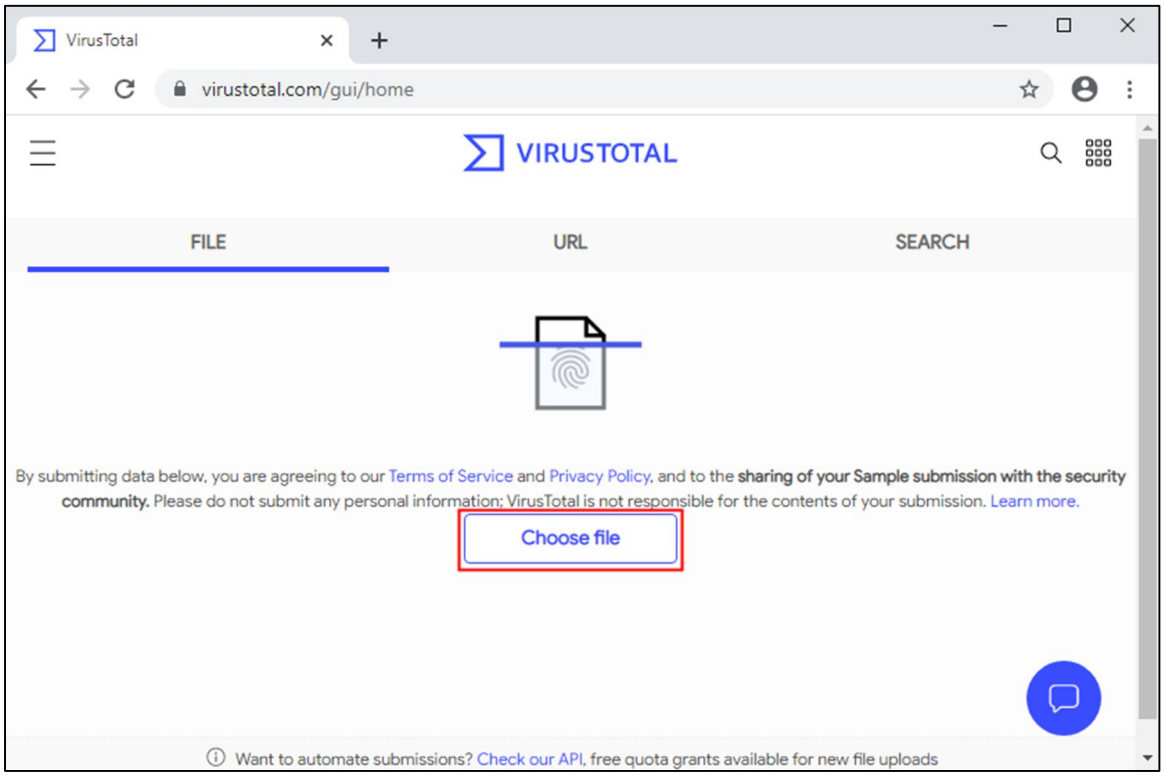
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

7 בשייפתח חלון הדפדפן, יש לעבור אל: https://www.eicar.org/?page_id=3950

8 יש לגלול מטה ולהוריד את הקובץ **eicar_com.zip** על ידי לחיצה עליו.

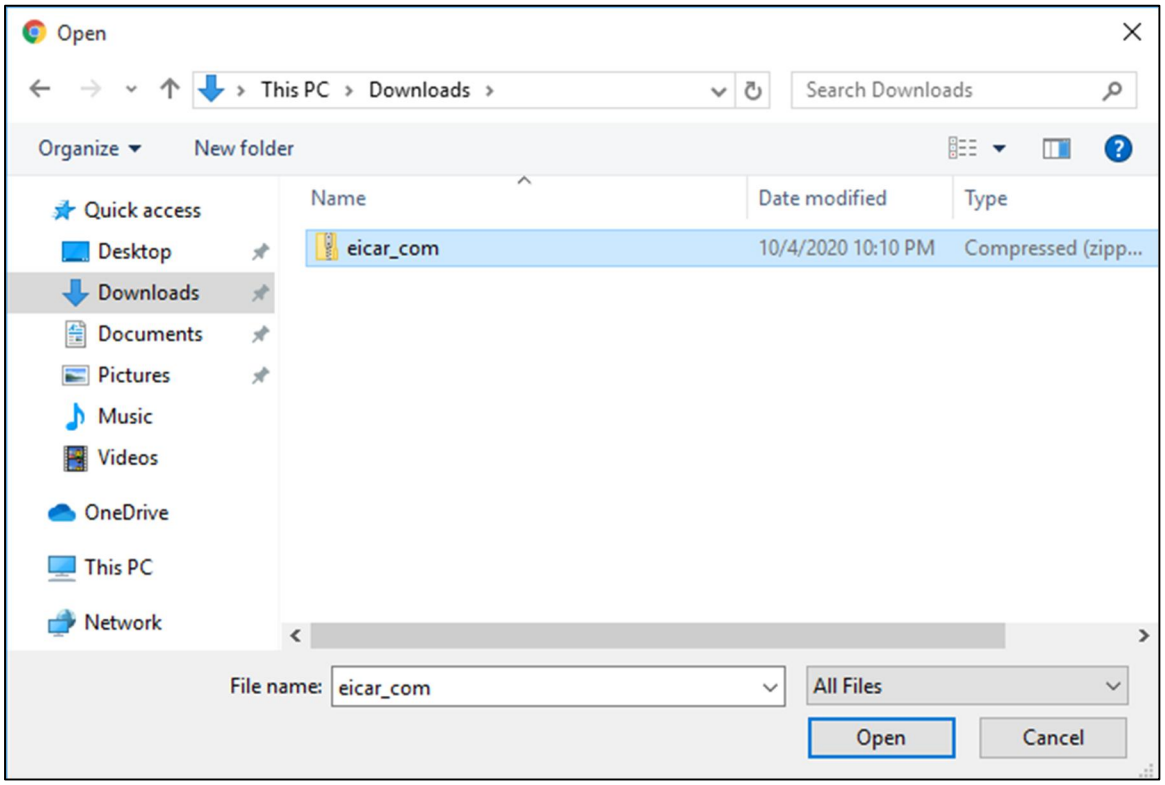


9 יש לגלוש אל https://www.virustotal.com/gui/home וללחוץ על **Choose file**.



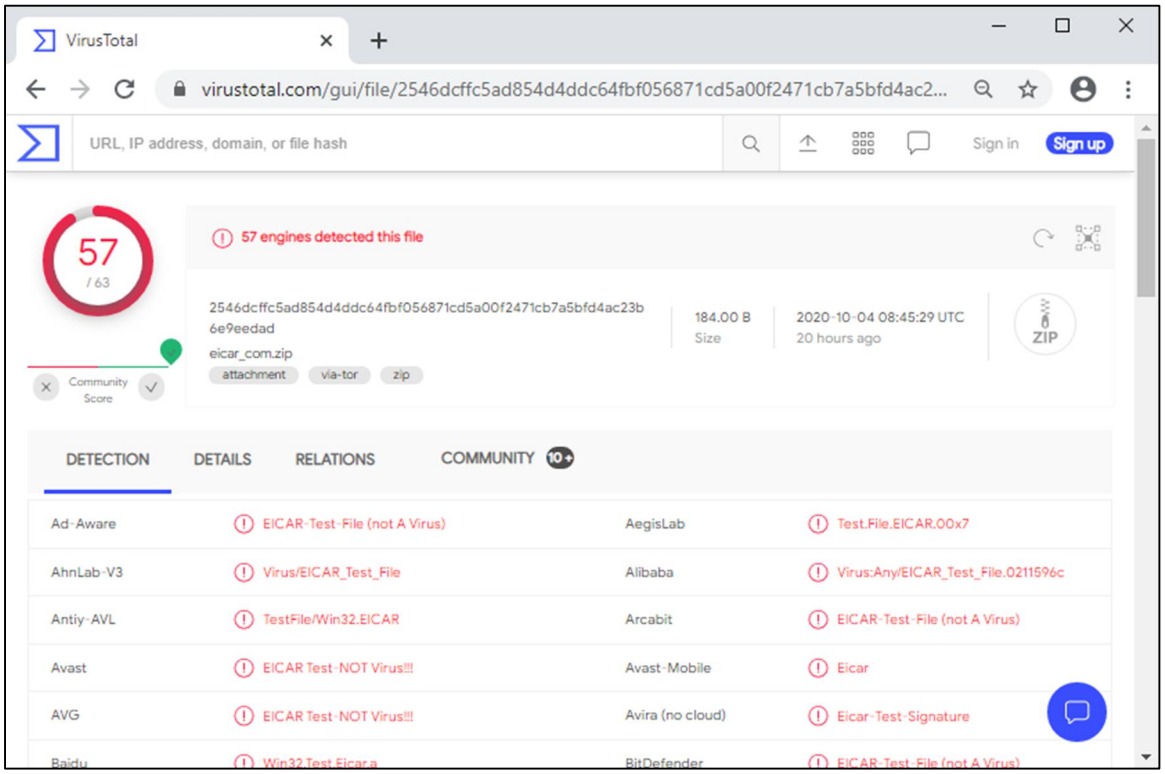
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

10 יש לנווט אל **Downloads**, לבחור **eicar_com.zip**, וללחוץ על **Open**.



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

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

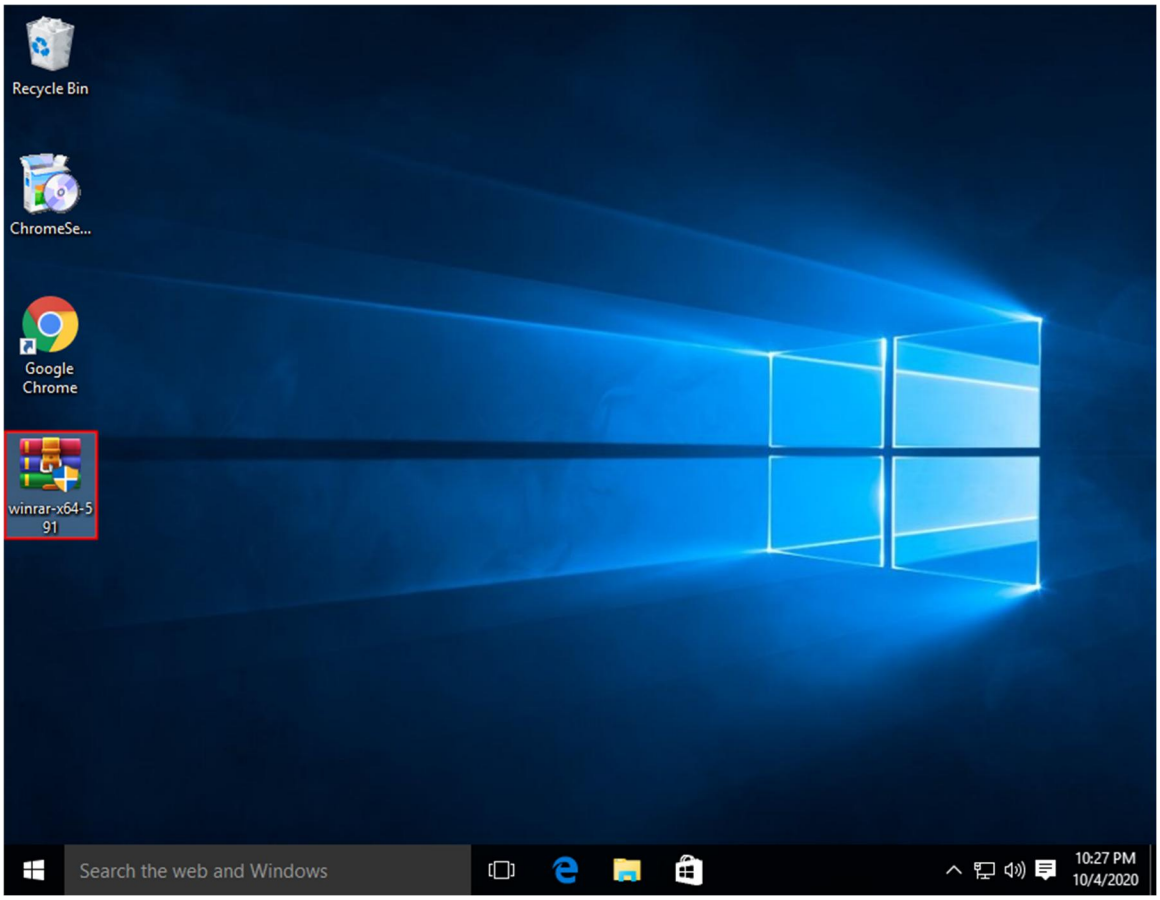


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

התחמקות מגילוי

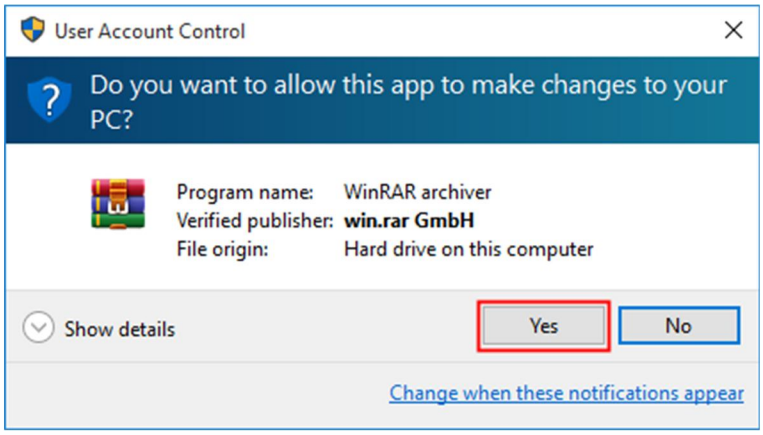
במשימה זו, תטמיעו שיטה שתאפשר לכם לעקוף את זיהוי הקובץ.

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



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

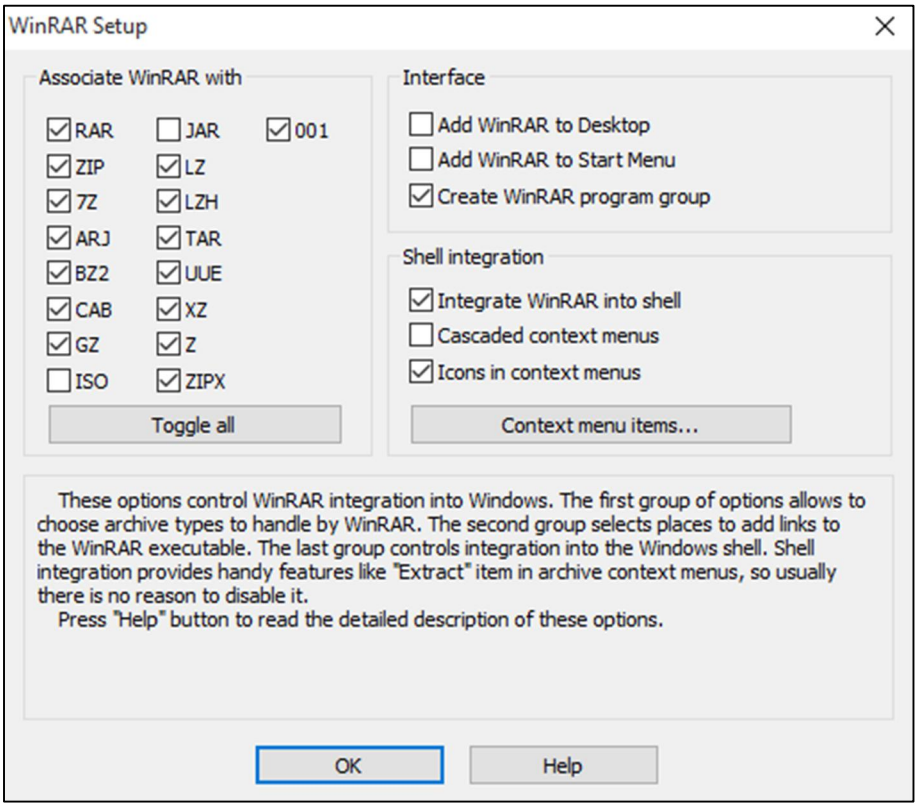
2 יש ללחוץ על **Yes** בדי לאפשר את תחילת ההתקנה.



3 יש להשתמש בנתיב ברירת המחדל להתקנה וללחוץ על **Install**.

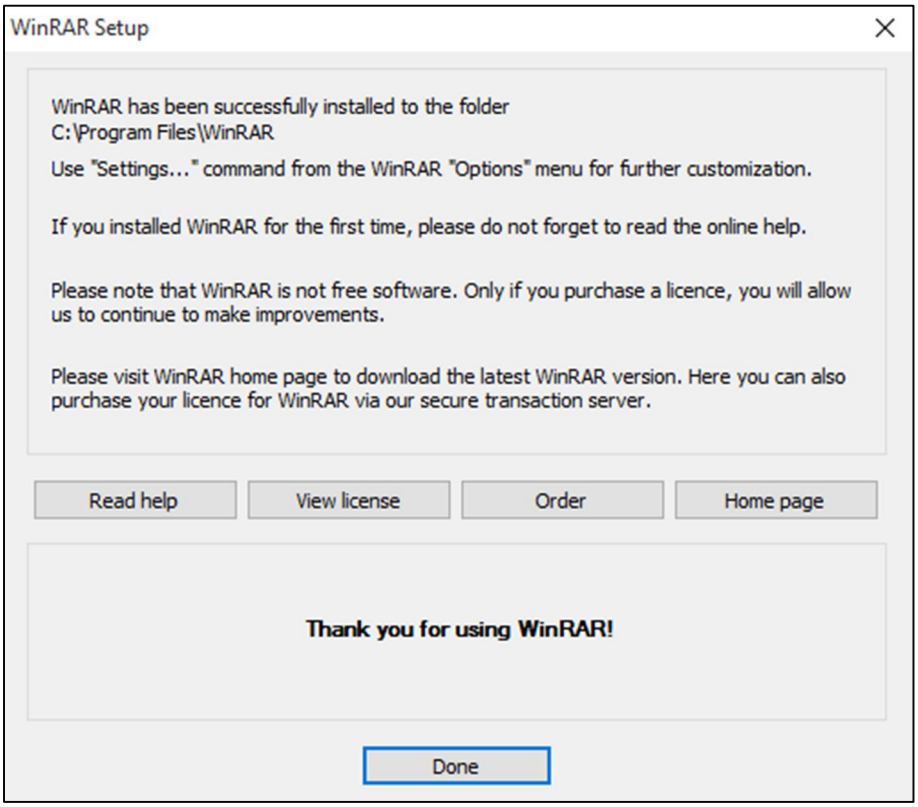
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

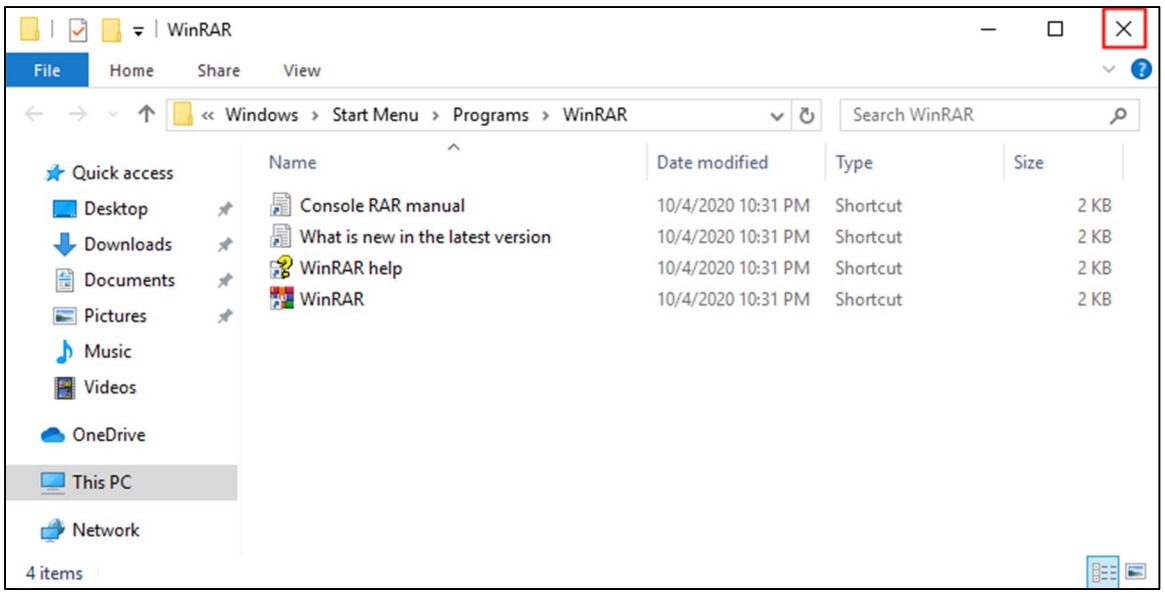
4 יש להשאיר את האפשרויות הנבחרות כפי שהן וללחוץ על **OK**.



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

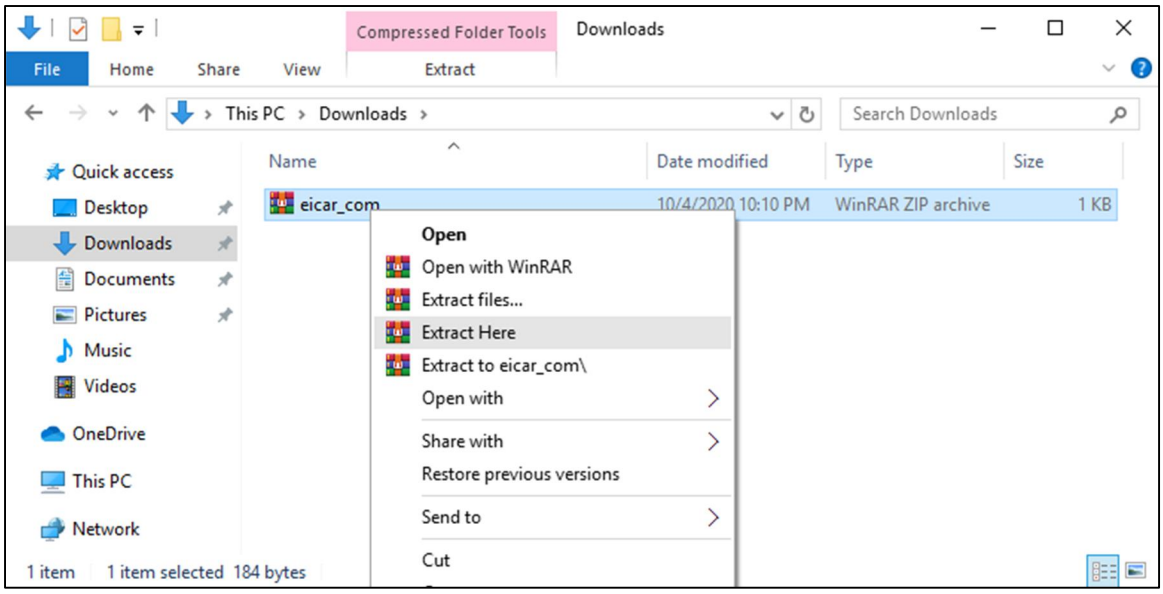
5 יש ללחוץ על **Done** בדי לסיים את ההתקנה, ולסגור את התיקייה שמופיעה.



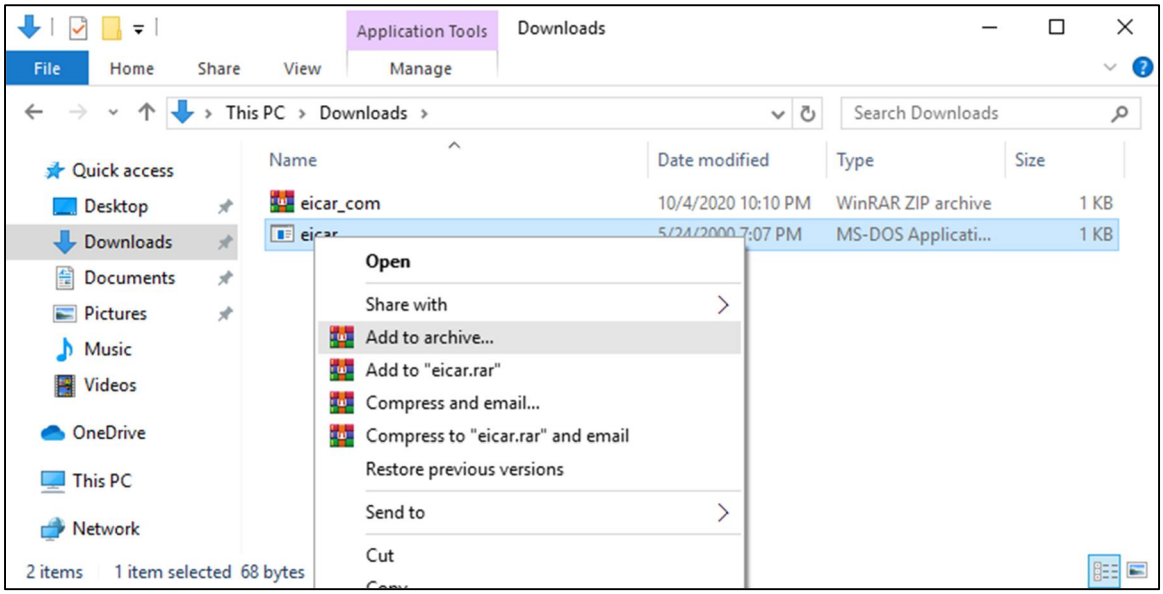


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

6 יש לפתוח את הספרייה Downloads, ללחוץ לחצן ימני על **eicar_com** ולבחור את **Extract Here** בדי לחלץ אותו.

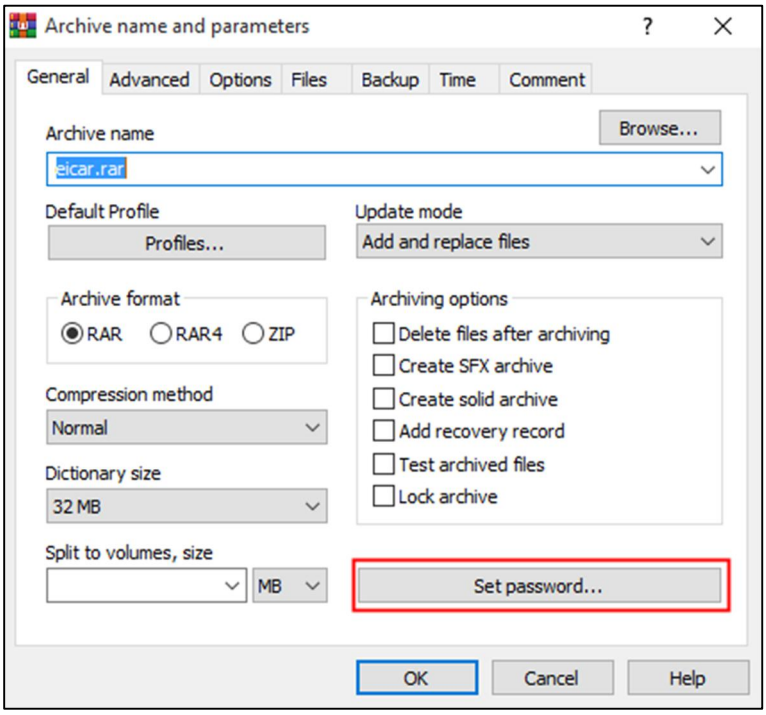


7 יש ללחוץ לחצן ימני על הקובץ **eicar** ולבחור באפשרות **Add to archive...**

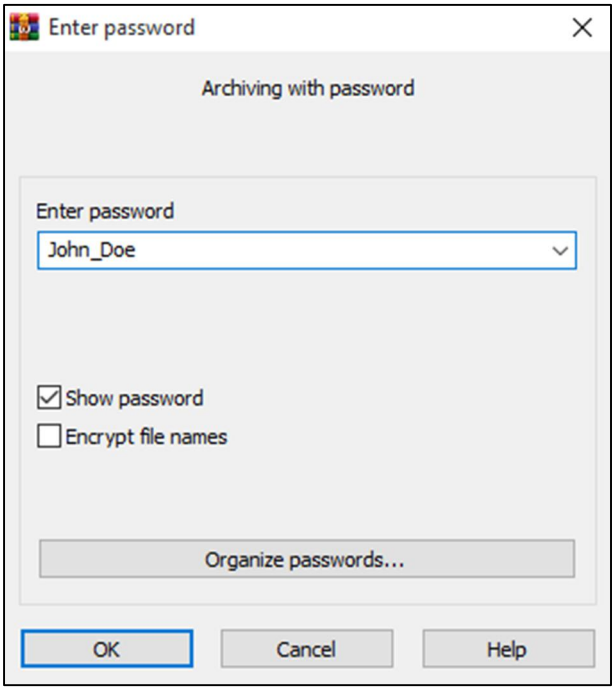


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

8 יש ללחוץ על **Set password**.

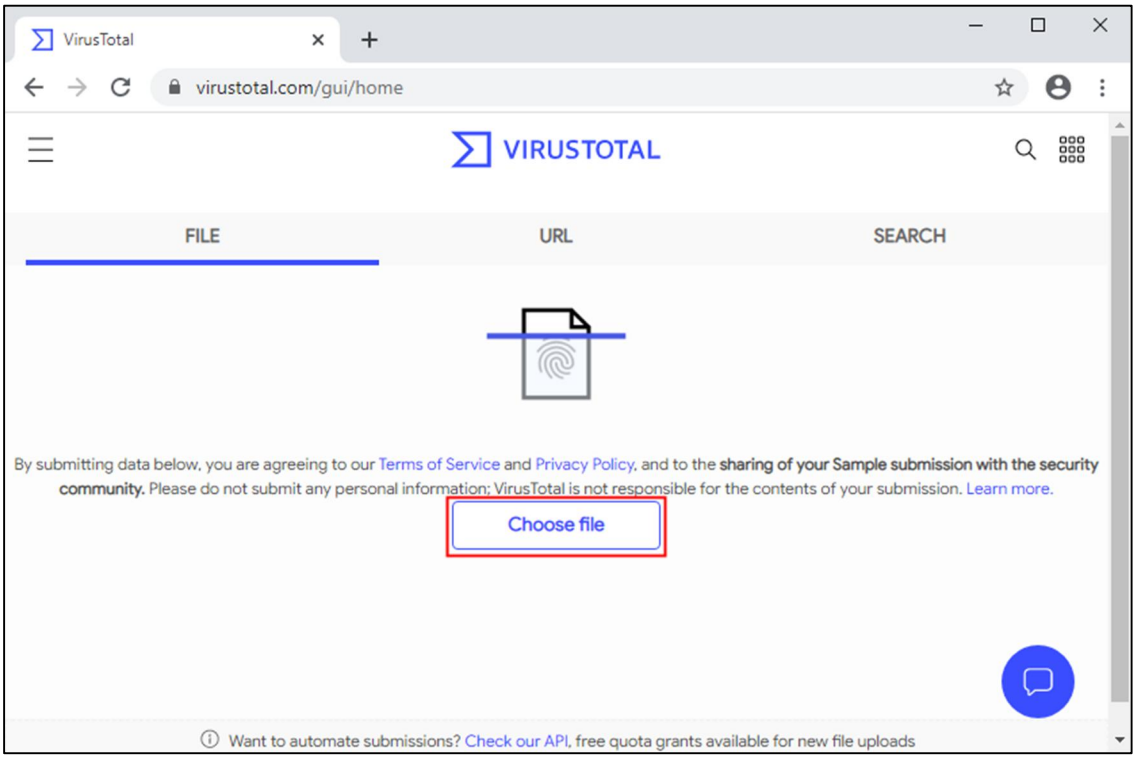


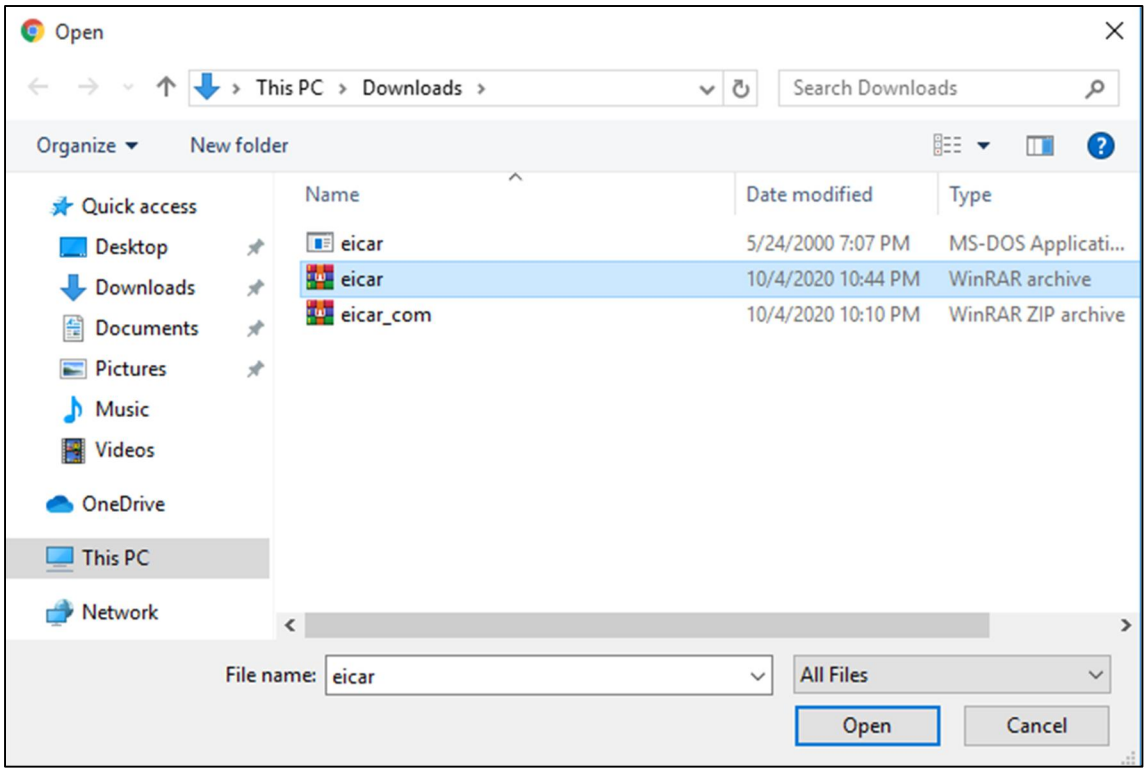
9 יש להשתמש בשם שלך בסיסמה, ללחוץ על **OK**, ושוב על **OK** בחלון הקודם בדי להשלים את הדחיסה.



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

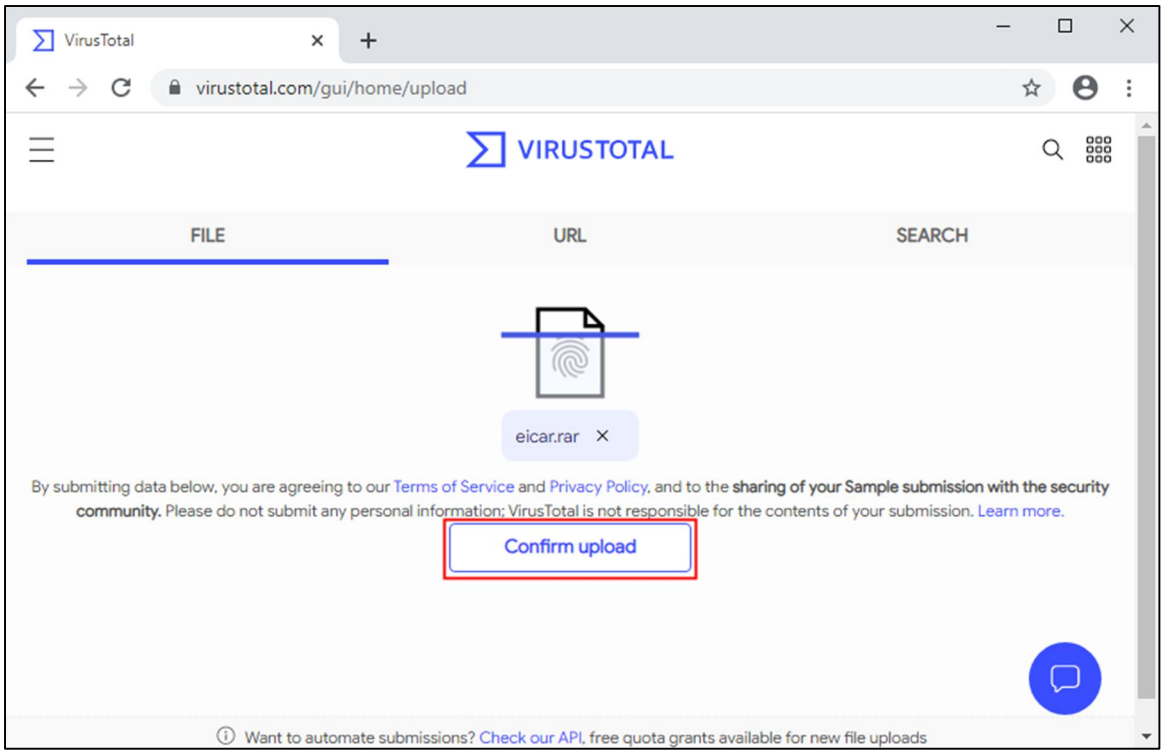
10 יש לגלוש שוב אל https://www.virustotal.com/gui ולהעלות את הקובץ הדחוס.

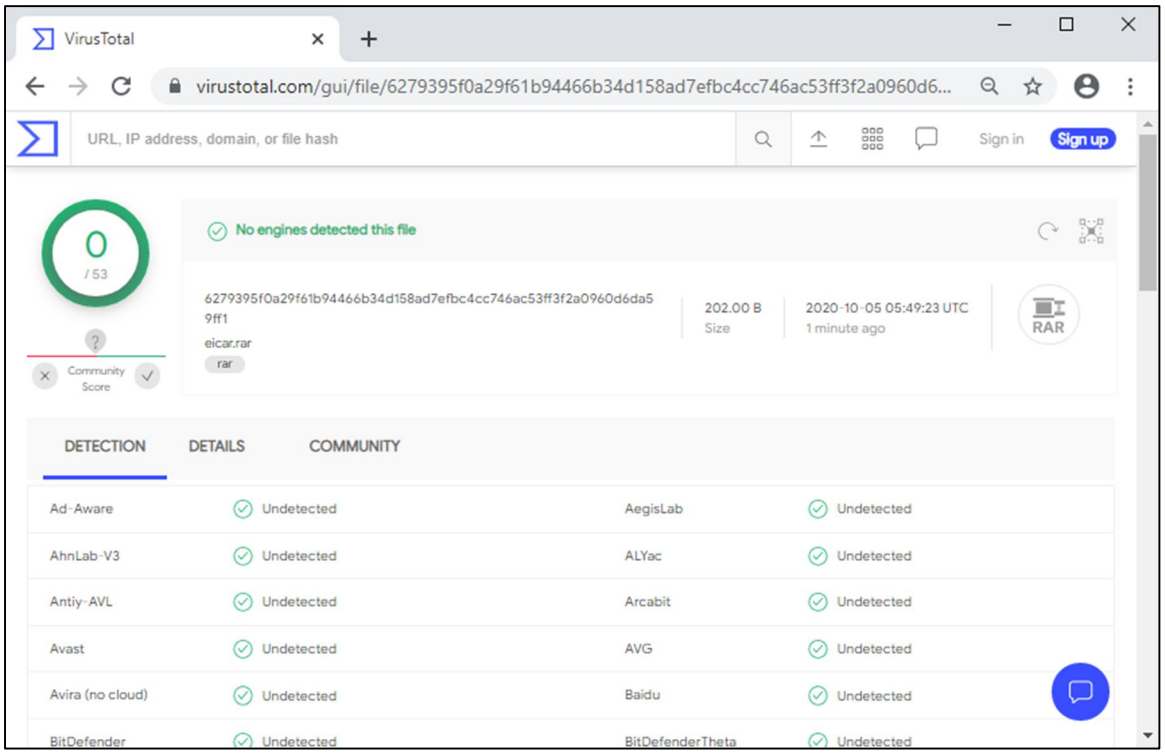




כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

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





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