


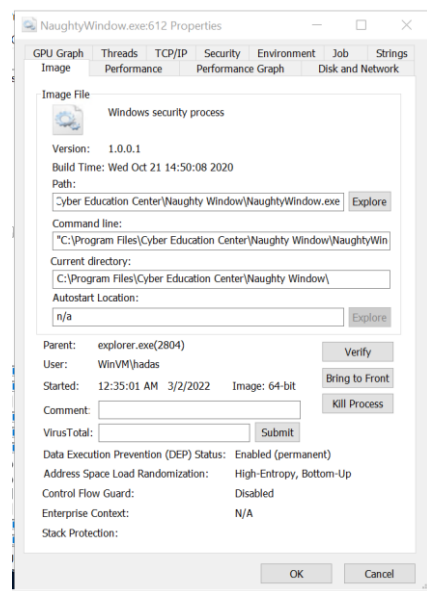
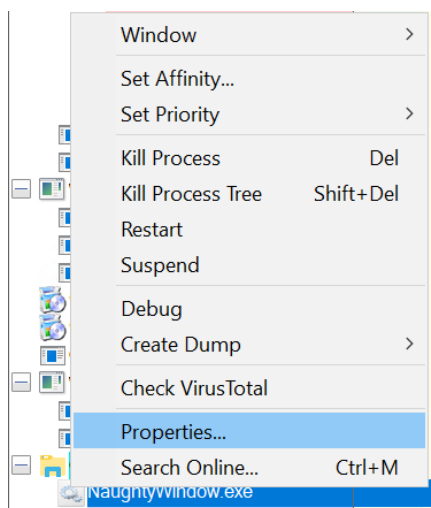
## מהו הפרוסס שהחלונות הקופצים שייכים אליו?

כדי לענות על שאלה זו היה צורך לפתוח process explorer ולהשתמש ב- . גררתי את המטרה מעל לחלון הקופץ כדי לסמן שזה התהליך שאני מחפשת לדעת מי הוא. והמטרה סימנה לי בכחול את התהליך שמריץ את הקובץ NaughtyWindow.exe (שזה גם השם שמופיע על החלון הקופץ)

explorer.exe	< 0.01	30,620 K	101,432 K	2804 Windows Explorer	Microsoft Corporation
NaughtyWindow.exe		1,504 K	7,620 K	612 Windows security process	Microsoft Corporation

## מהו קובץ ההרצה (exe) שהפרוסס מריץ והיכן הוא מותקן?

פתחתי את המאפיינים של התהליך וכתוב ב-Path את המיקום של הקובץ  
C:\Program Files\Cyber Education Center\Naughty Window\NaughtyWindow.exe



## כיצד התוכנה מצליחה להיות מופעלת גם אחרי ריסטרט, ומהו / מהם הפרוססים שהיא מפעילה? מה המיקום של קבצי ה-exe שמורצים?

בעצם מה שהנוזקה עשתה היא יצרה לעצמה עוד 2 עותקים של עצמה במקומות אחרים בזיכרון:

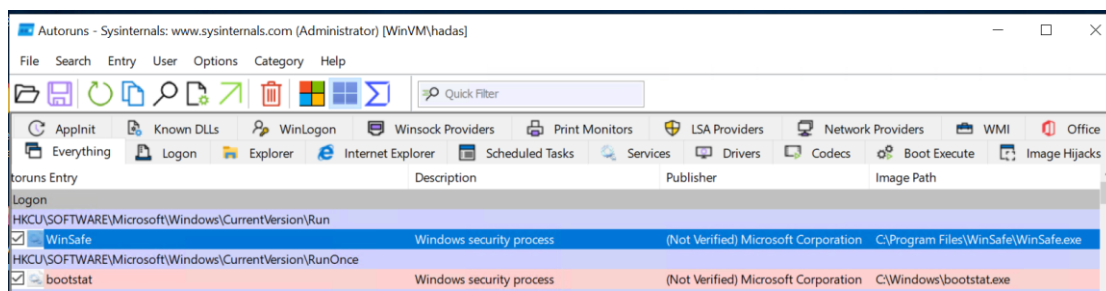
- winsafe.exe במיקום C:\program files\winSafe\winsafe.exe
- bootstat.exe במיקום C:\program files\windows\bootstat.exe

כך שגם אם אני יהרוג את התהליך שלה וימחק אותה מהזיכרון עדיין לא נהרסו את העותקים שלה (שאלם הם רצים הם גם דואגים לייצר עותק חדש לנוזקה מאיפה שהסרנו אותה). זה קצת כמו חבורה של בריונים שכל אחד מגן על השני.

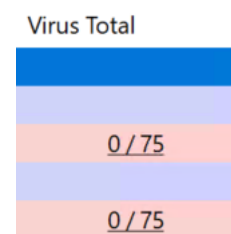
מה שגורם לתהליכים האלו לרוץ זה בעצם שהם רשמו את מיקום הקובץ שלהם ב-Registry במקום שבו מאחסנת מערכת ההפעלה מהם התהליכים שהיא צריכה להריץ אחרי ה-BOOT

תהליך הזיהוי:

פתחתי AutoRuns וראיתי שיש 2 קבצי הרצה ששמורים ב-Registry במיקום שבזמן ריסטרט וטעינה מחדש של מערכת ההפעלה (BOOT) תוכנות אלו צריכות שיפעילו אותם.



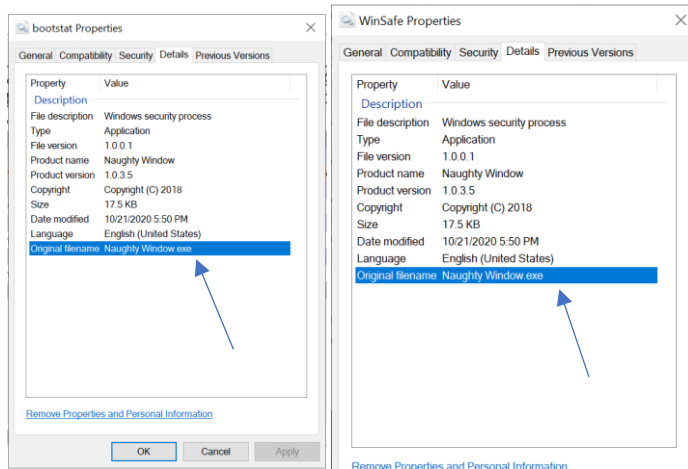
אומנם Totulvirus לא חושב שמדובר בנוזקה:



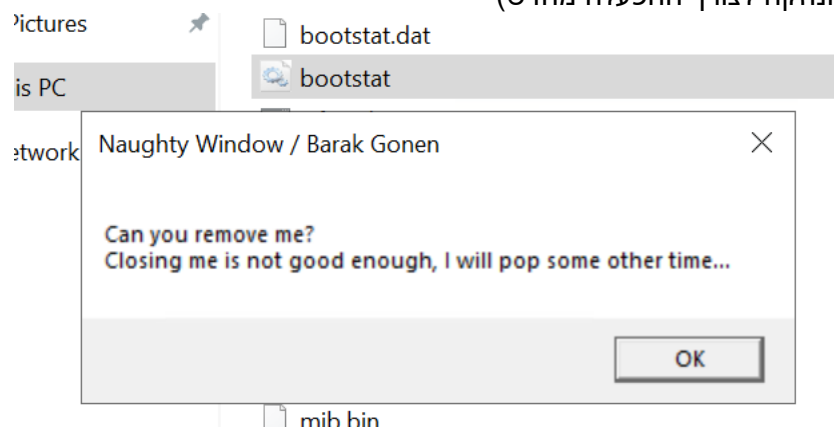
**אבל:**

1. יוצרי נזקות אוהבים להפחיד משתמשים מלהרוס תהליכים שנראים חשובים כמו "Windows security process" או לגרום להם להראות אמינות בכך שהם אומרים שמי שיצר אותם זה חברה מוכרת כמו Microsoft. וגם המיקום שבהם הם שמרו את עצמם נראה מקום שמשתמש מפחד לגעת בו כי יושבות שם תוכנות חשובות (C:\program files\windows\bootstat.exe , C:\program files\winSafe\winsafe.exe) אך תוכנות אלו לא חתומה ואפליקציות של חברות גדולות לרוב חתומות במיוחד אם היה מדובר בתהליך שקשור לאבטחה.

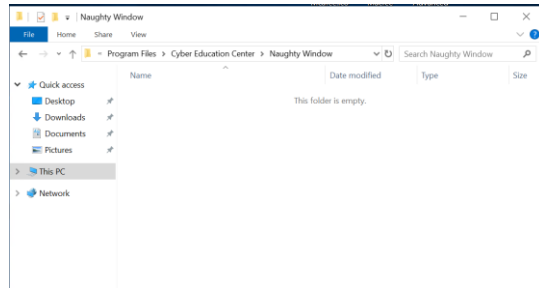
2. פתחתי לראות יותר פרטים: השם המקורי של הקובץ הוא בדיוק אותו השם של הנוזקה שראינו process explorer



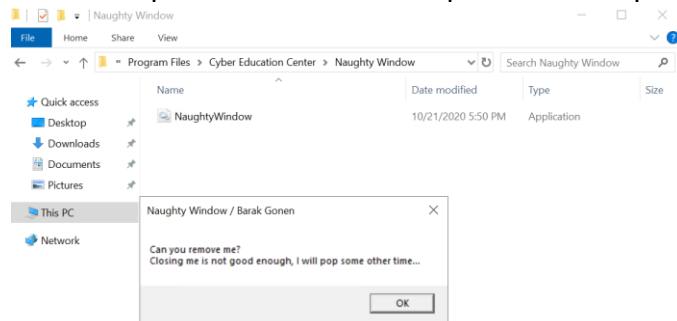
3. כדי לוודא שבאמת הם אלו שמפעילות את הנוזקה בזמן ההפעלה מחדש- פשוט הרצתי אותם וראיתי שהרצה שלהם גרמה לאותם התופעות שהנוזקה גרמה ושהם פועלות בדיוק באותו אופן שהנוזקה עובדת (כולל כתיבה ל-Registry המיקום של שתי העותקים של הנוזקה לצורך ההפעלה מחדש)



4. ובנוסף אם נמחק עכשיו את אחד מהעותקים למשל את העותק המקורי שנמצא ב-  
C:\Program Files\Cyber Education Center\Naughty Window\NaughtyWindow.exe

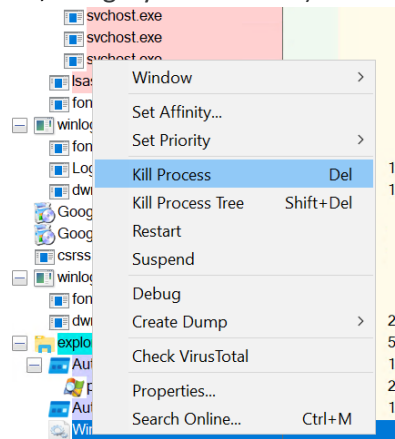


ונריץ את אחד העותקים האחרים נראה שהעותק הזה נוצר שוב:

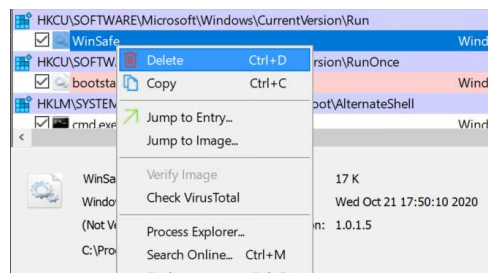


### תהליך המחיקה:

1. הריגת התהליכים שרצים: (בכל אחד מהשמות שהם יכולים להופיע: (winsafe.exe, bootsts.exe, NaughtyWindow.exe)



2. מחיקה של כל העותקים מ-Registry ואפשר באמצעות AutoRuns או ישירות מ-Registry.



3. ללכת למיקום בזיכרון של כל אחד מהנוזקות ולמחוק את הקובץ EXE שלהם.