CyberGirlz CLUB

חלק ג - Fly High

ברק גונן

START-UP NATION CENTRAL

קרן רש"י RASHI FOUNDATION

המרכז לחינוך סייבר CYBER EDUCATION CENTER

ההאקרים הצליחו להדביק כמה מחשבים בנוזקה עוצמתית. סומכים עליכן שתמצאו איך מסירים אותה!

“Download Sysinternals Suite and master it!”

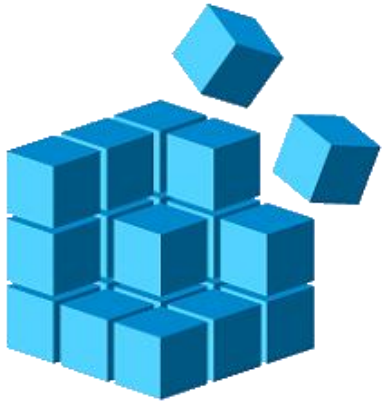
המטרה

- לימוד של כלים שימושיים בסביבת windows, יאפשר:
  - היכרות טובה יותר עם אופן פעולת מערכת ההפעלה
  - יכולת לזהות דברים חריגים
  - הסרת הנוזקה

תוכן העניינים

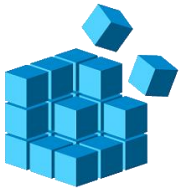
- נלמד להשתמש ב-4 כלים
- ניהול Registry באמצעות Regedit
- כלי Sysinternals:
  - Procmon –
  - Process Explorer –
  - Autoruns –

Regedit



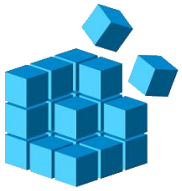
ה- Registry

- מאגר נתונים של מערכת ההפעלה
  - מאורגן בצורה של מפתח Key וערך Value
- הגדרות Settings של אפליקציות ושל מערכת ההפעלה
  - התקני חומרה
  - אבטחה
  - גרפיקה ועוד
- לדוגמה – מה גודל הפונט של ה-Command line?

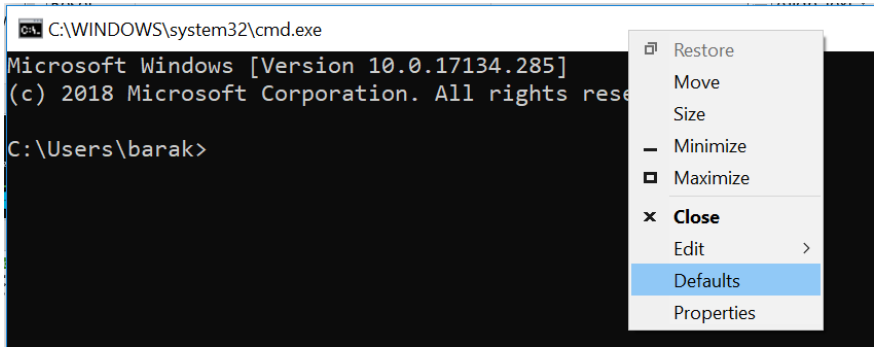


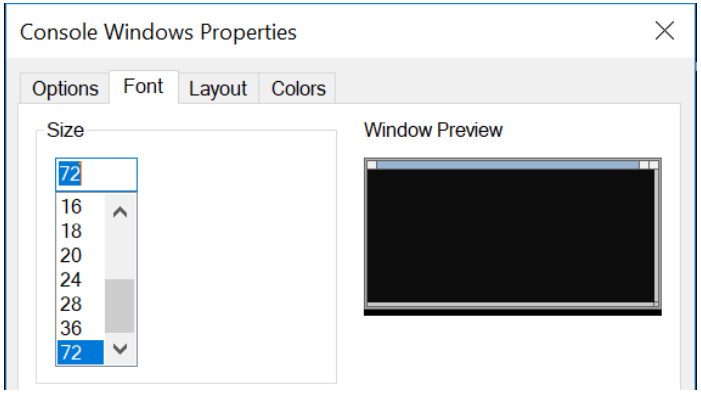
הפעלת Regedit

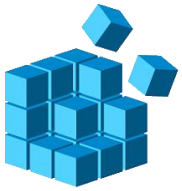
- כלי של מייקרוסופט
  - משמש לצפיה ועריכת ה-registry
  - די מוסתר מהמשתמש (לא מופיע ברשימת התוכניות)
- ליחצו winkey+R וכיתבו regedit
- לפני שינוי ה-registry מומלץ לבצע שמירה (export)



תרגיל

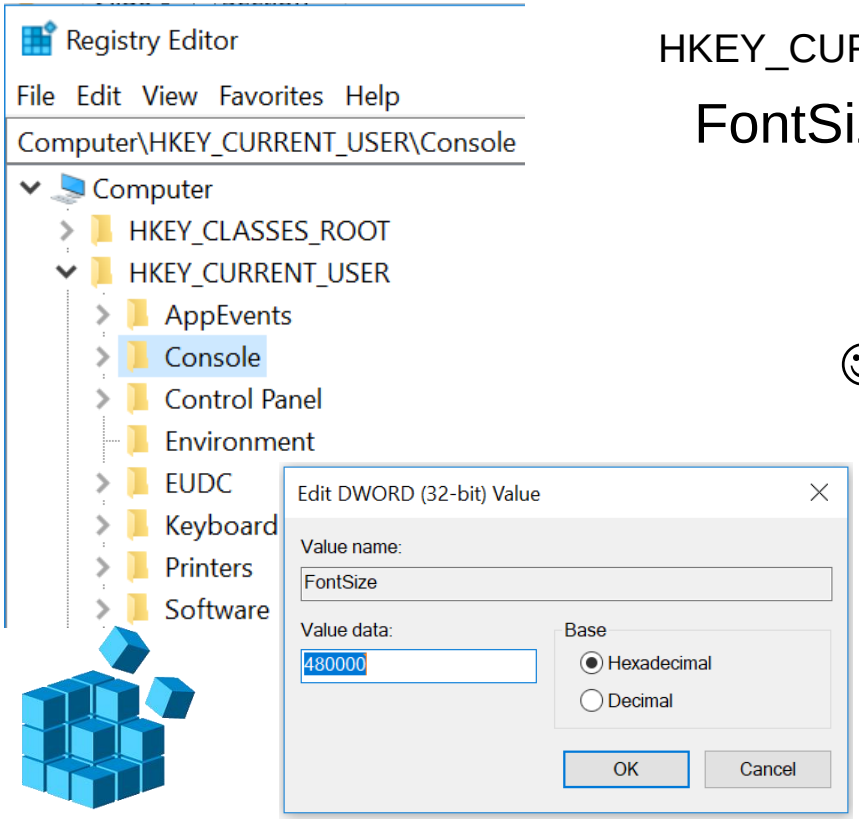






- היכנסו ל-cmd
- קליק ימני באזור הלבן למעלה
- בחרו defaults
- שנו את גודל הפונט ל-76
- סיגרו את cmd ופתחו מחדש
- אבל היכן נשמר השינוי?

Regedit - תרגיל מודרך

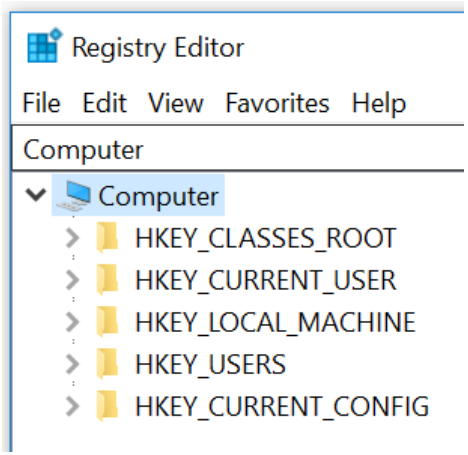


- בצד שמאל, בחרו HKEY_CURRENT_USER\Console
- בצד ימין, מיצאו את ה-key שנקרא FontSize
- הקליקו עליו על מנת לערוך את הערך
- שנו מ-0x48 (==76) ל-0x12 (==18)
- פיתחו cmd ובידקו שהפונט השתנה ☺

- אם אי אפשר לערוך את הרגיסטרי, השתמשו במדריך הבא:

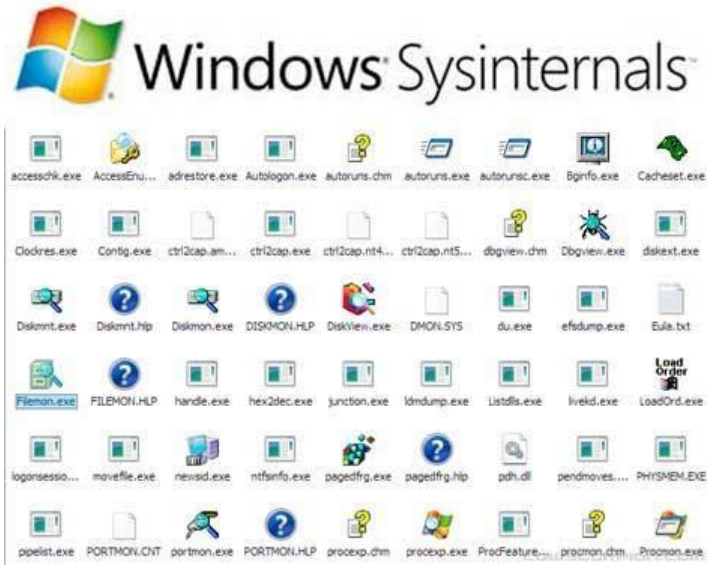
https://www.learningpenguin.net/2017/02/02/regedit-in-windows-10-error-writing-the-values-new-contents/

Registry -ה



- קיימת חלוקה היררכית:
  - HKCU – הגדרות של המשתמש הנוכחי (Current User)
    - שימושי כאשר מספר עובדים חולקים מחשב לאורך היממה
  - HKLM (Local Machine) – הגדרות של המחשב
    - תחת Software כל התוכנות המותקנות במחשב
  - יתר ההגדרות - קריאה עצמית

כלים של SysInternals



- חברת SysInternals פיתחה כלים שמאפשרים למשתמשי Windows לנטר כמעט כל דבר במערכת ההפעלה
- מייקרוסופט שיתפה פעולה, לבסוף רכשה את SysInternals וכיום כל הכלים ניתנים להורדה חופשית חינם
- סרטוני הדרכה טובים ביוטיוב (חפשו Mark russinovich או את שם הכלי המבוקש)
  - https://www.youtube.com/watch?v=7heEYEbFim4
  - https://download.sysinternals.com/files/SysinternalsSuite.zip

Autoruns

Autoruns

- חלק מהערכים ב-registry קובעים למחשב פעולות שהוא צריך לבצע אוטומטית, לדוגמה:
  - אילו תוכנות צריכות לסיים התקנה בפעם הבאה שהמחשב יעלה
  - אילו תוכנות צריכות לרוץ אוטומטית עם עליית המחשב
  - אילו תוספים צריך לטעון עם הדפדפן
  - לבדוק עדכוני תוכנות ביום ושעה מסויימים

Autoruns

- ב-SysInternals מיפו כ-200 מקומות ברגיסטרי בהם מייקרוסופט מאפשרת לתוכנות לקבוע הגדרות של ריצה אוטומטית
  - גם תוכנות זדוניות עלולות לנצל זאת, לדוגמה כדי למנוע מהמשתמש להסיר אותן, קובץ ההתקנה יופעל מחדש בכל עליית מחשב
- תוכנת Autoruns ממפה את כל המקומות הללו ומציגה למשתמש

תרגול Autoruns

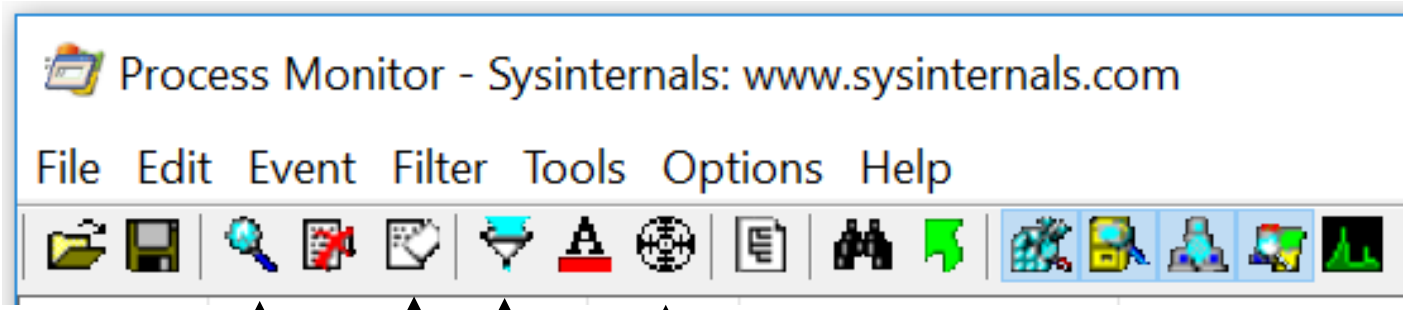
- הריצו את Autoruns כ-Admin (קליק ימני, Run as administrator)
- תרגילים:
  - מיצאו את ה-Scheduled tasks שלכם
  - מיצאו את התוספים של Internet Explorer
  - בטאב Options, הוסיפו:
    - בדיקה באתר Virus Total
    - בדיקה שהקוד חתום כמקורי על ידי היצרן (verified)
  - עיברו לטאב Everything- חפשו התרעות של Virus Total (יותר מ-0 בודקי וירוסים חושדים בקובץ)
    - בצעו קליק ימני- Search online ובידקו מהו הקובץ החשוד

Procmon

Procmon

- Process Monitor – הכרנו בשיעור שעבר
- Event- כל מה שעובר פילטר של Procmon
- מאפשרת לנטר את פעולת כל התוכנות הרצות על המחשב
  - רשימה של Eventים
  - מי ביצע Event מסויים?
  - מה אוסף כל ה-Eventים שביצעה תוכנה ספציפית?
  - אוסף פילטרים מסייע למקד את המחקר

Procmon



התחל הקלטה חדשה

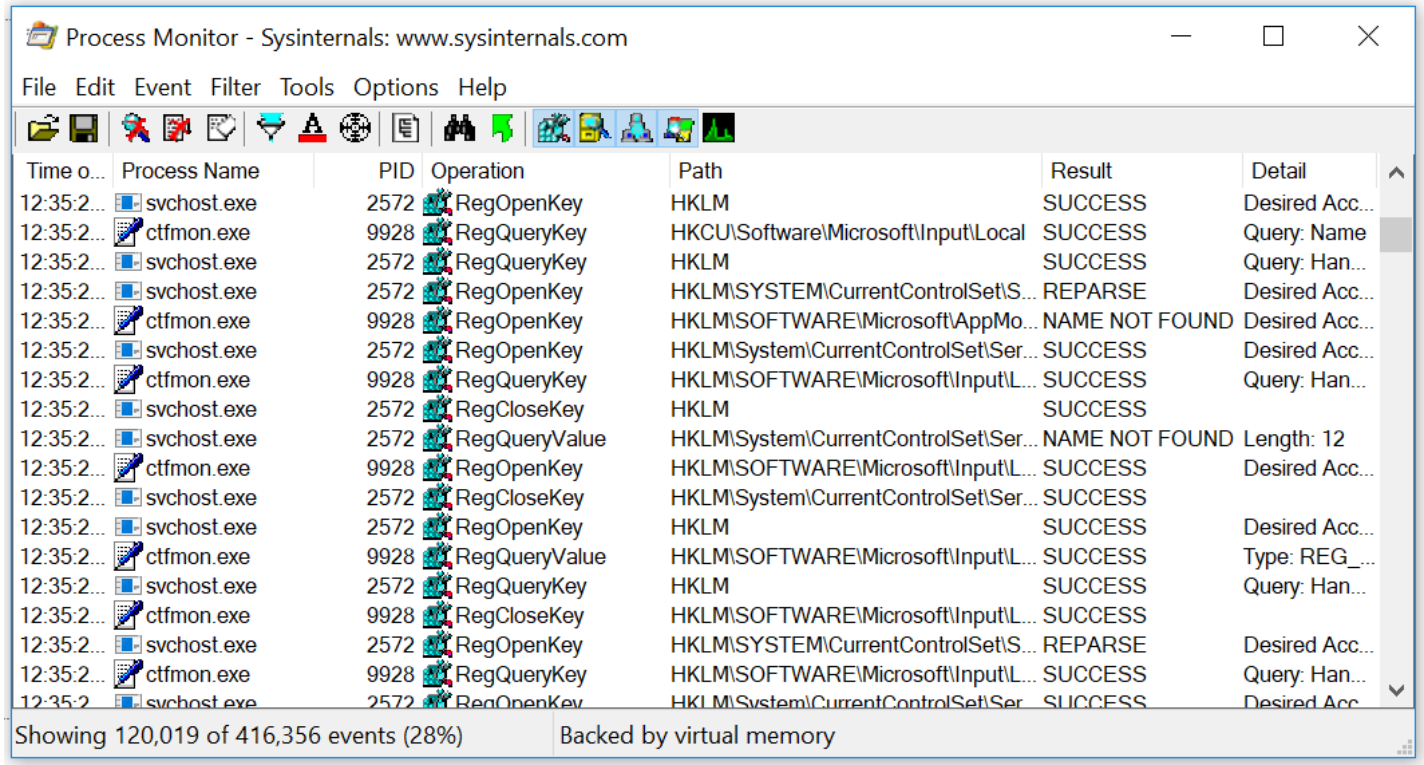
מחק מידע קודם

ערוך פילטר

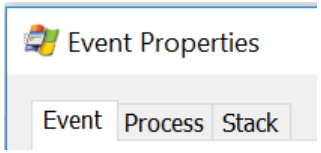
אסוף את כל המידע על תוכנה
שהמשתמש מצביע עליה

Procmon

- כל מה שעובר את הפילטר יופיע כ-Event ברשימה



Procmon



- הקלקה על Event תעניק מידע נוסף:
  - תחת Process יופיעו Modules – מאפשר לבדוק האם ה-Process קורא לקוד חשוד
    - שם ה-Module לא מוכר / חשוד
    - היצרן לא מוכר / חשוד

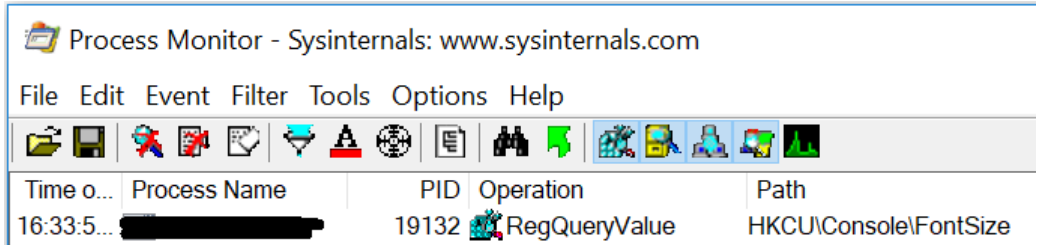
Modules:

Module	Address	Size	Path	Company
SHCore.dll	0x7ff8aab00000	0xa9000	C:\Windows\System32\SHCore.dll	Microsoft Corpor...
user32.dll	0x7ff8aaca0000	0x190000	C:\Windows\System32\user32.dll	Microsoft Corpor...
combase.dll	0x7ff8aae40000	0x323000	C:\Windows\System32\combase.dll	Microsoft Corpor...
ntdll.dll	0x7ff8ac820000	0x1e1000	C:\Windows\System32\ntdll.dll	Microsoft Corpor...

  - תחת Stack תופיע שרשרת הקריאות לפונקציות

Procmon - תרגילים

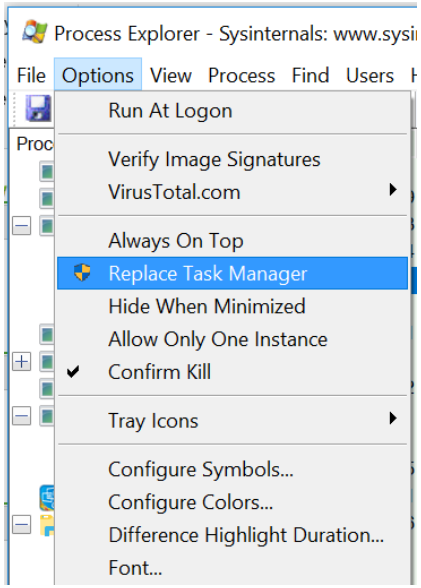
1. הציגו את כל מה שמבצע chrome.exe
2. הציגו את כל מי שמבצע WriteFile
3. הציגו את כל מי שמבצע RegQueryValue
   - איך נקראת הפונקציה של ntdll ש-RegQueryValue קוראת לה?
4. הציגו את כל מי שקורא את הרגיסטרי במיקום HKCU\Console\FontSize ופיתחו cmd – מה שם ה-Process?



Process Explorer

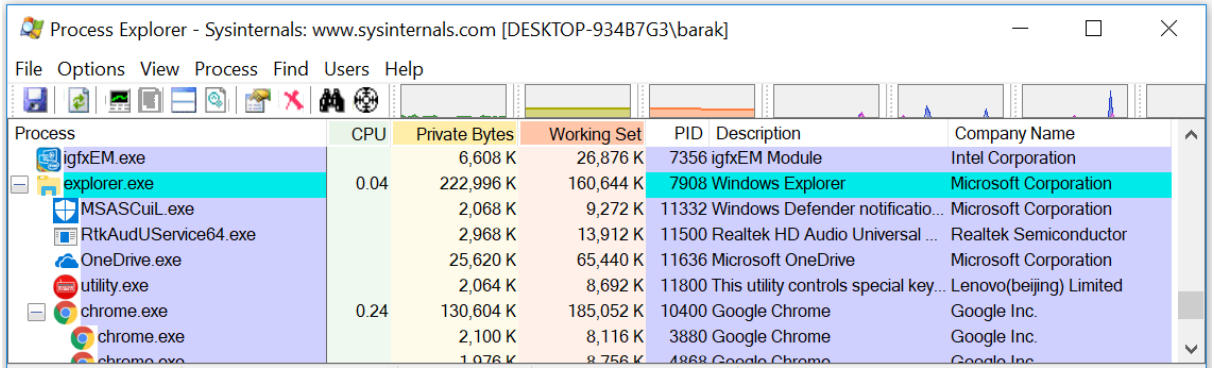
Process Explorer

- "Task Manager על סטרואידים"
- מומלץ לבחור באפשרות ההחלפה



Process Explorer

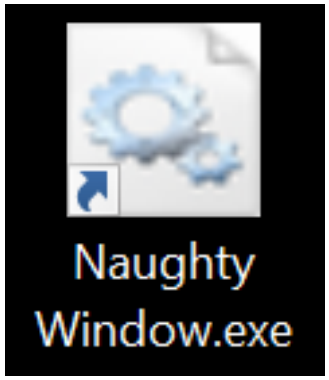
- יכולות (בין היתר):
  - תצוגת כל ה-Processים, מי יצר את מי
  - בדיקה האם יש Process שמוכר כתוכנה זדונית
  - בדיקה האם Process חתום (אם לא- יתכן שזדוני)
  - בדיקה כל ה-Processים שמשתמשים בקוד מסוים (שיתכן שתקול / זדוני)

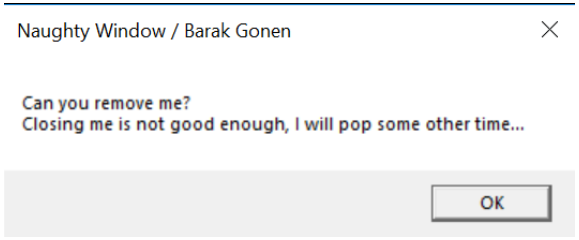


Process Explorer - תרגילי לימוד עצמי

1. הפעילו את chrome. איזה Process הוא האבא שלו?
2. בצעו "verify" ל-chrome. מי חתום עליו?
3. הגישו את chrome ל-Virus Total. מה הציון שלו?
4. מיצאו בזיכרון את המחרוזת שמתחילה ב- try-chrome. כיצד היא מסתיימת?
5. מהו אחוז ה-cpu שצורך system idle process?
6. כמה proecssים משתמשים כרגע ב-user32.dll?
7. הוסיפו לטבלת ה-Processים עמודות של Verified Signer ושל Virus Total. האם יש Processים שאינם חתומים ויש לגביהם ציון שאינו 0?

תרגול SysInternals





- בתרגיל זה תצטרכו להסיר נוזקה חביבה, שפותחה על ידינו לצרכי לימוד
  - הקליקו על חבילת ההתקנה והתקינו אותה
  - לחצו לחיצה ימנית על ה-icon על ה-desktop ובחרו **run as administrator**
- כעת הנוזקה מותקנת אצלכם. האם תוכלו להסיר אותה לחלוטין?
  - דגש: כדי לוודא שהתוכנה הוסרה לחלוטין, הפעילו את המחשב מחדש

https://data.cyber.org.il/CyberGirlzClub/NaughtyWindow.msi