



CyberGirlz

☆ CLUB ☆

חלק ג - Fly High



ברק גובן





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



“Download Sysinternals Suite and master it!”

המטרה

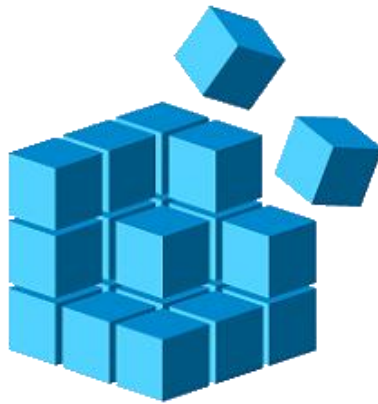
- לימוד של כלים שימושיים בסביבת windows, יאפשר:
 - היכרות טובה יותר עם אופן פעולת מערכת ההפעלה
 - יכולת לזהות דברים חריגים
 - הסרת הנוזקה

תוכן העניינים



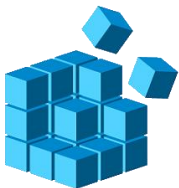
- נלמד להשתמש ב-4 כלים
- ניהול Registry באמצעות Regedit
- כלי Sysinternals:
 - Procmon
 - Process Explorer
 - Autoruns

Regedit



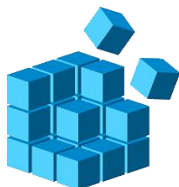
ה-Registry

- 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?

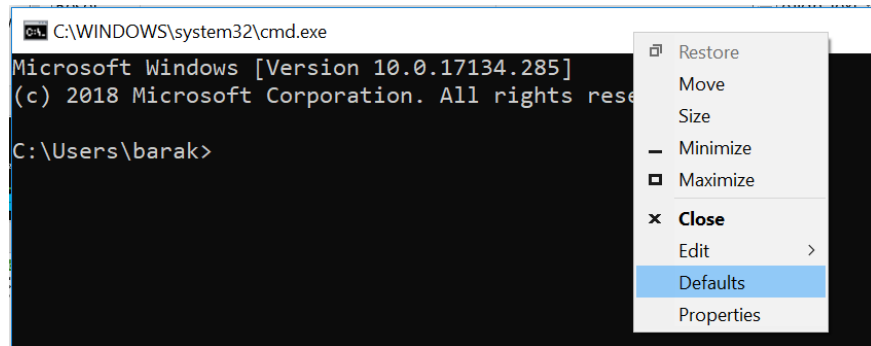


הפעלת Regedit

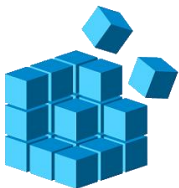
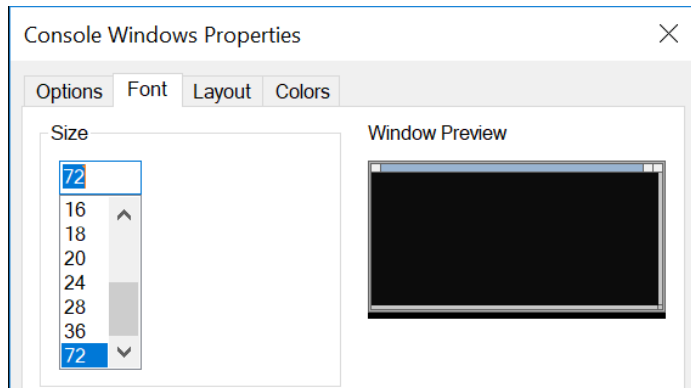
- כלי של מייקרוסופט
 - משמש לצפיה ועריכת ה-registry
 - די מוסתר מהמשתמש (לא מופיע ברשימת התוכניות)
- ליחצו winkey+R וכיתבו regedit
- לפני שינוי ה-registry מומלץ לבצע שמירה (export)



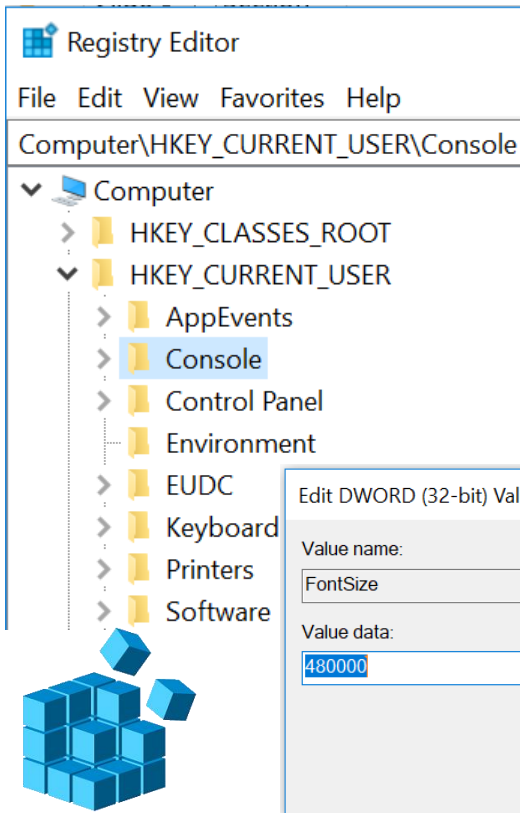
תרגיל



- 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?



תרגיל מודרך - Regedit



- 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/>

ה-Registry

- קיימת חלוקה היררכית:

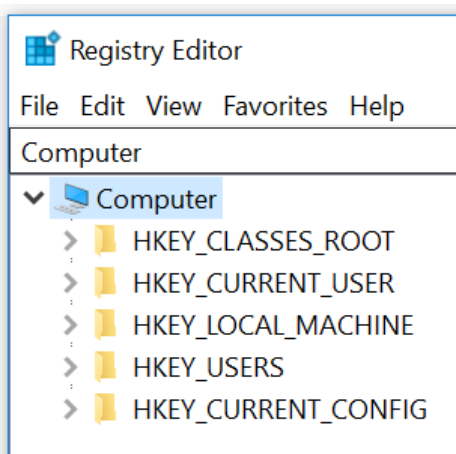
– הגדרות של המשתמש הנוכחי – HKCU
(Current User)

- שימושי כאשר מספר עובדים חולקים מחשב
לאורך היממה

– הגדרות של המחשב – HKLM (Local
Machine)

- 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



Autoruns תרגול

- 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

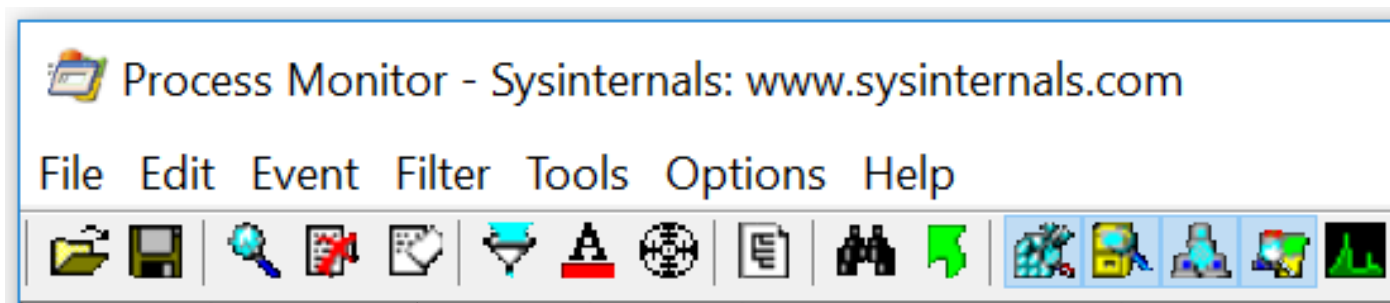


Procmon

- Process Monitor – הכרנו בשיעור שעבר
- Event- כל מה שעובר פילטר של Procmon
- מאפשרת לנטר את פעולת כל התוכנות הרצות על המחשב
 - רשימה של Event'ים
 - מי ביצע Event מסויים?
 - מה אוסף כל ה-Event'ים 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



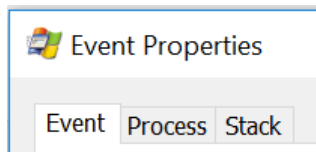
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
12:35:2...	svchost.exe	2572	RegOpenKey	HKLM	SUCCESS	Desired Acc...
12:35:2...	ctfmon.exe	9928	RegQueryKey	HKCU\Software\Microsoft\Input\Local	SUCCESS	Query: Name
12:35:2...	svchost.exe	2572	RegQueryKey	HKLM	SUCCESS	Query: Han...
12:35:2...	svchost.exe	2572	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\S...	REPARSE	Desired Acc...
12:35:2...	ctfmon.exe	9928	RegOpenKey	HKLM\SOFTWARE\Microsoft\AppMo...	NAME NOT FOUND	Desired Acc...
12:35:2...	svchost.exe	2572	RegOpenKey	HKLM\System\CurrentControlSet\Ser...	SUCCESS	Desired Acc...
12:35:2...	ctfmon.exe	9928	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\L...	SUCCESS	Query: Han...
12:35:2...	svchost.exe	2572	RegCloseKey	HKLM	SUCCESS	
12:35:2...	svchost.exe	2572	RegQueryValue	HKLM\System\CurrentControlSet\Ser...	NAME NOT FOUND	Length: 12
12:35:2...	ctfmon.exe	9928	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\L...	SUCCESS	Desired Acc...
12:35:2...	svchost.exe	2572	RegCloseKey	HKLM\System\CurrentControlSet\Ser...	SUCCESS	
12:35:2...	svchost.exe	2572	RegOpenKey	HKLM	SUCCESS	Desired Acc...
12:35:2...	ctfmon.exe	9928	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\L...	SUCCESS	Type: REG_...
12:35:2...	svchost.exe	2572	RegQueryKey	HKLM	SUCCESS	Query: Han...
12:35:2...	ctfmon.exe	9928	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\L...	SUCCESS	
12:35:2...	svchost.exe	2572	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\S...	REPARSE	Desired Acc...
12:35:2...	ctfmon.exe	9928	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\L...	SUCCESS	Query: Han...
12:35:2...	svchost.exe	2572	RegOpenKey	HKLM\System\CurrentControlSet\Ser...	SUCCESS	Desired Acc...

Showing 120,019 of 416,356 events (28%) Backed by virtual memory

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:

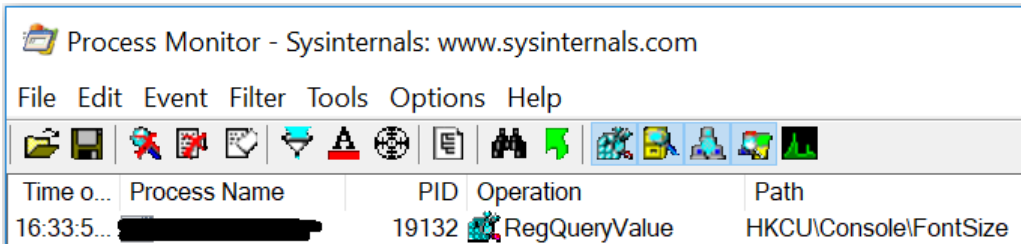
Module	Address	Size	Path	Company
SHCore.dll	0x7ff8aab00000	0xa9000	C:\Windows\System32\SHCore.dll	Microsoft Corpor...
user32.dll	0x7ff8aaca0000	0x190000	C:\Windows\System32\user32.dll	Microsoft Corpor...
combase.dll	0x7ff8aae40000	0x323000	C:\Windows\System32\combase.dll	Microsoft Corpor...
ntdll.dll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

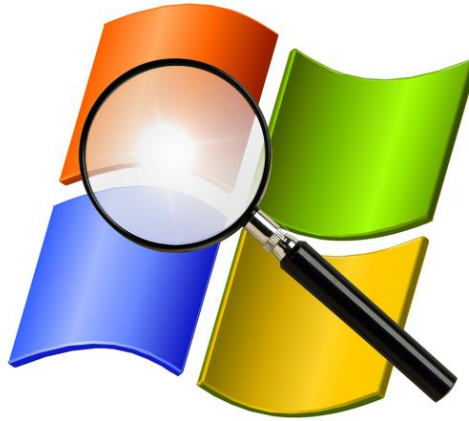


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

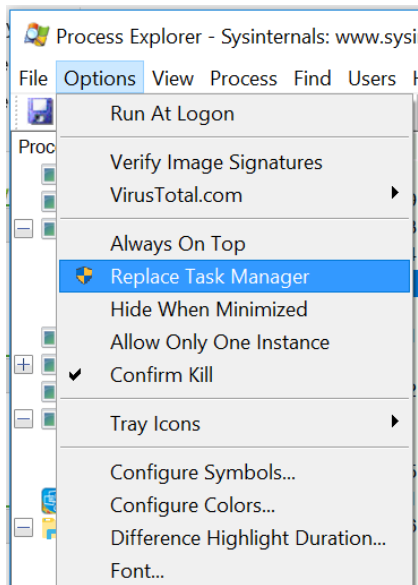
Time o...	Process Name	PID	Operation	Path
16:33:5...	[REDACTED]	19132	RegQueryValue	HKCU\Console\FontSize

Process Explorer



Process Explorer

- "Task Manager על סטרואידיים"
- 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 - Sysinternals: www.sysinternals.com [DESKTOP-934B7G3\barak]

File Options View Process Find Users Help

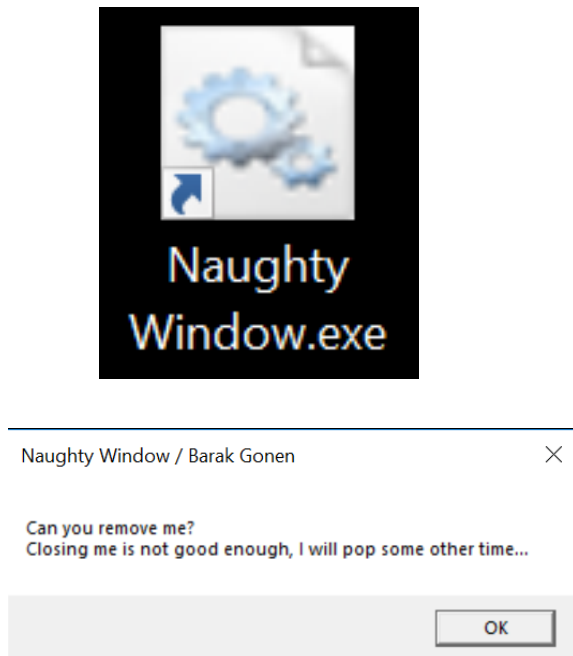
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
igfxEM.exe		6,608 K	26,876 K	7356	igfxEM Module	Intel Corporation
explorer.exe	0.04	222,996 K	160,644 K	7908	Windows Explorer	Microsoft Corporation
MSASCuiL.exe		2,068 K	9,272 K	11332	Windows Defender notificatio...	Microsoft Corporation
RtkAudUService64.exe		2,968 K	13,912 K	11500	Realtek HD Audio Universal ...	Realtek Semiconductor
OneDrive.exe		25,620 K	65,440 K	11636	Microsoft OneDrive	Microsoft Corporation
utility.exe		2,064 K	8,692 K	11800	This utility controls special key...	Lenovo(beijing) Limited
chrome.exe	0.24	130,604 K	185,052 K	10400	Google Chrome	Google Inc.
chrome.exe		2,100 K	8,116 K	3880	Google Chrome	Google Inc.
chrome.exe		1,076 K	8,756 K	4868	Google Chrome	Google Inc.

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 proecss משתמשים כרגע ב-user32.dll?
7. הוסיפו לטבלת ה-Process עמודות של Verified Signer ושל Virus Total. האם יש Process 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>