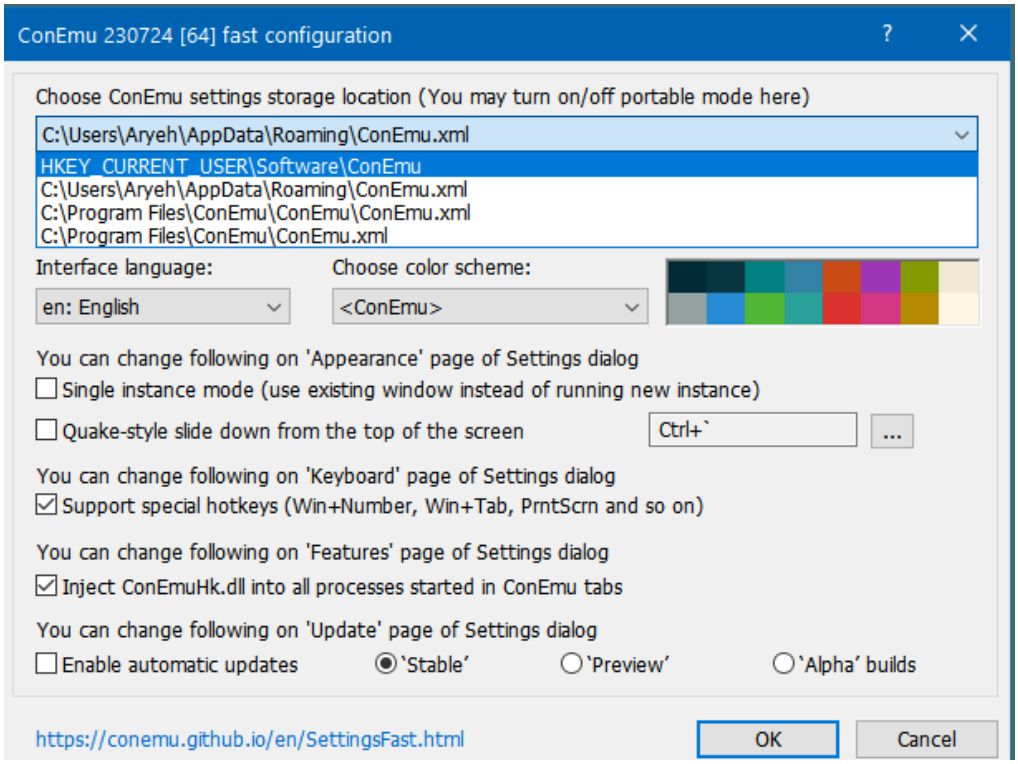
בס"ד

תרגיל כיתה 1 – מערכות הפעלה, תשפ"ג

מבוסס על **הרעיון** מהספר: מערכות הפעלה, Operating Systems / Barak Gonen, פרק 1

<u>תוכנת Regedit</u>

1. התקינו את טרמינל חלופי מהקישור(קובץ התקנה עם סיומת EXE , אשרו הכל):
https://github.com/Maximus5/ConEmu/releases
2. הריצו, **בהרצה ראשונה** יופיע:



תבחרו את המיקום המוצע ב REGISTRY כמקום שמירת ההגדרות.

3. הפעילו את תוכנת registry editor ע"י כתיבת regedit

שימו לב!

שינויים ב regedit משפיעים על המערכת כולה. מומלץ לבצע export (שמירה של המידע הנוכחי) לפני השימוש, ובכל מקרה – להשתמש בזהירות ובהבנה מה אתם עושים.

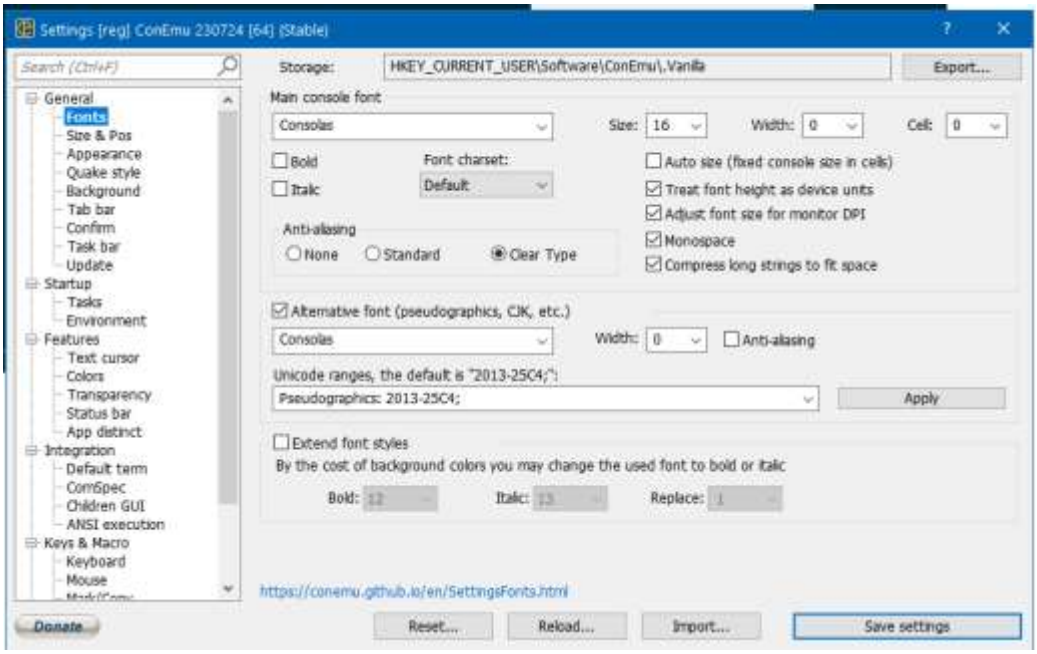
ביצוע Export:

- בחרו בלשונית File ובחרו Export... . שמרו את כל הערכים ב Registry שלכם לקוב
- טעינה בהמשך תתבצע באמצעות Import, ותבטל כל שינוי שאולי תעשו.

אם אי אפשר לערוך את הרגיסטרי, (בגלל שאין לכם הרשאה):

- קליק ימני על הענף Console, ובחרו Permission (ראו צילום מסך : ---------- >
- בחרו הרשאות משתמש של Full Control.
- להלן קישור להסבר כיצד לבצע זאת:
https://www.learningpenguin.net/2017/02/02/regeditin-windows-10-error-writing-the- :

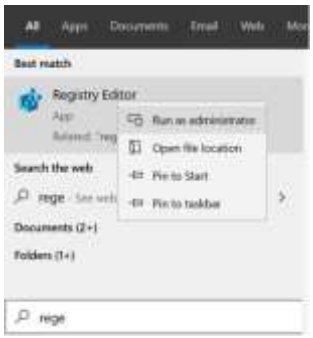
4. ב CONEMU, לחצו על כותרת החלון ע"י קליק ימני. בחרו: SETTINGS , ושנו את גודל הפונט ל-36.



5. סגרו את ה CONEMU , ופתחו מחדש. ודאו שהשינוי בוצע, סגרו עוד פעם.

כעת נעבור לבדוק היכן נשמרו השינויים.

(הערה: ניתן לפתוח את regedit גם דרך חלון החיפוש של windows, ובחירה בקליק ימני – הפעל כ administrator):



6. בתכנת Registery Editor בחרו בצד שמאל ב HKEY_CURRENT_USER\SOFTWARE\ConEmu\.Vanilla (המיקום שבחרתם בהרצה הראשונה)
7. מצאו בצד ימין את המפתח של FontSize.
8. הקליקו על המפתח על מנת לערוך את הערך והחליפו ל 16(הערך המקורי).
9. פיתחו CONEMU ובדקו שהפונט השתנה☺

בצעו צילום מסך:

1. של תכנת regedit בשלבי העריכה של המפתח
2. 2 מסכי של ה CONEMU לפני ואחרי השינוי

פרטו את החסרונות בשמירת ההגדרות ב REGISRTY

להגשה

עבור כלים אלו קיימים סרטוני הדרכה טובים ביוטיוב.

- חפשו: sysinternals tutorial video
- חפשו: Mark Russinovich sysinternals
- חפשו את שם הכלי המבוקש
- דוגמא לסרטון של מיקרוסופט:
https://www.youtube.com/watch?v=7heEYEbFim4

את חבילת התוכנות של Sysinternals ניתן להוריד מהקישור:
https://download.sysinternals.com/files/SysinternalsSuite.zip

כלי Sysinternals

תוכנת Autoruns

1. הריצו את Autoruns בתור מנהל מערכת. (אין זה משנה אם אתם מפעילים את Autoruns או Autoruns64)
2. מצאו את ה Scheduled Tasks שלכם.
3. בדקו - מהם התוספים של Internet Explorer?
4. בלשונית Option – תחת Scan Option, הוסיפו בדיקה של כל התוכנות באתר Virus Total.

אתר Virus Total, הוא אתר שמרכז מידע על נוזקות, ע"פ מידע שנאסף מאנטי-וירוסים שונים. ניתן להגיש לאתר קובץ, ולקבל בחזרה מידע האם הקובץ מזוהה כנוזקה על ידי האנטי-וירוסים השונים. אתר זה הוא שימושי ביותר אם אתם חושדים שקובץ כלשהו שיש לכם על המחשב עלול להיות נוזקה.

5. כעת המתינו עד שכל המידע בחלונית Everything נשלח ומתקבל. האם זוהו אצלכם תוכנות זדוניות? (שימו לב, שעלולים להיות פספוסים. אם רק אנטי-וירוס אחד או שניים מזהים קובץ כנוזקה, ייתכן שזו טעות. אם הרבה אנטי-וירוסים מזהים קובץ כנוזקה, סביר שנדבקתם)
6. אם מצאתם תוכנה שחשודה כתוכנה זדונית, הקליקו קליק ימני על השורה בה היא כתובה ובחרו באפשרות Search Online.תקבלו מידע על התוכנה ומה רמת הסיכון שלה. אין אצלכם תוכנה חשודה? בחרו את החיפוש על תוכנה אחרת כלשהי.
7. כדי לראות למי יש חתימה דיגיטלית, בלשונית Options, תחת Scan Option, הוסיפו בדיקה חתימות.

בצעו צילום מסך:

3. של ה Scheduled Tasks שלכם
4. של התוספים של Internet Explorer
5. המידע על הנוזקות שהתגלו אצלכם
6. קישור למידע באינטרנט על הנוזקה / תוכנה אחרת

להגשה

את התוכנה ניתן להוריד גם מהקישור
https://learn.microsoft.com/he-il/sysinternals/downloads/process-explorer

תוכנת Process Explorer

1. פתחו את תוכנת process explorer.
2. לחצו Ctrl+I (או דרך התפריט) כדי לפתוח את System Information.
3. ענו על השאלות הבאות:
   א. מה אחוז ה CPU-שהמחשב שלכם מנצל?
   ב. כמה מעבדים (או ליבות) יש לכם במחשב? (תחת הערך Topology)
   ג. מהי כמות ה Physical Memory -שאתם מנצלים כרגע?
   ד. כמה זיכרון RAM יש לכם בסך הכל במחשב? (תחת הערך Total)

4. הפעילו את דפדפן chrome ומצאו אותו בתוכנה.
5. ענו על השאלות הבאות:
   א. בצעו verify לדפדפן. מי חתום עליו?
   ב. מה הציון של הדפדפן ב virus total?
   ג. מצאו בזיכרון את המחרוזת try-chrome. כיצד היא מסתיימת?
   ד. מהו אחוז ה CPU שצורך system idle process?
   ה. כמה תהליכים משתמשים כרגע ב user32.dll?
   ו. הוסיפו לטבלת התהליכים, את העמודות Verified Singer, virus Total. האם יש תהלכים שאינם חתומים ויש לגביהם ציון שאינו 0?

6. הכלי Process Explorer מאפשר לבדוק איזה תוכנות עושות שימוש במשאב מסוים. המשאב יכול להיות DLL או קובץ.
לשם כך, פתחו קובץ כלשהו בתוכנת word. שימו לב לשם הקובץ.
7. חפשו בתוך procexp ע"י Ctrl+F או בלשונית Find. חפשו חלק משם הקובץ, ומצאו את התהליך שקשור אליו. מהו?

כתבו את התשובות לשאלות מהסעיפים הקודמים:

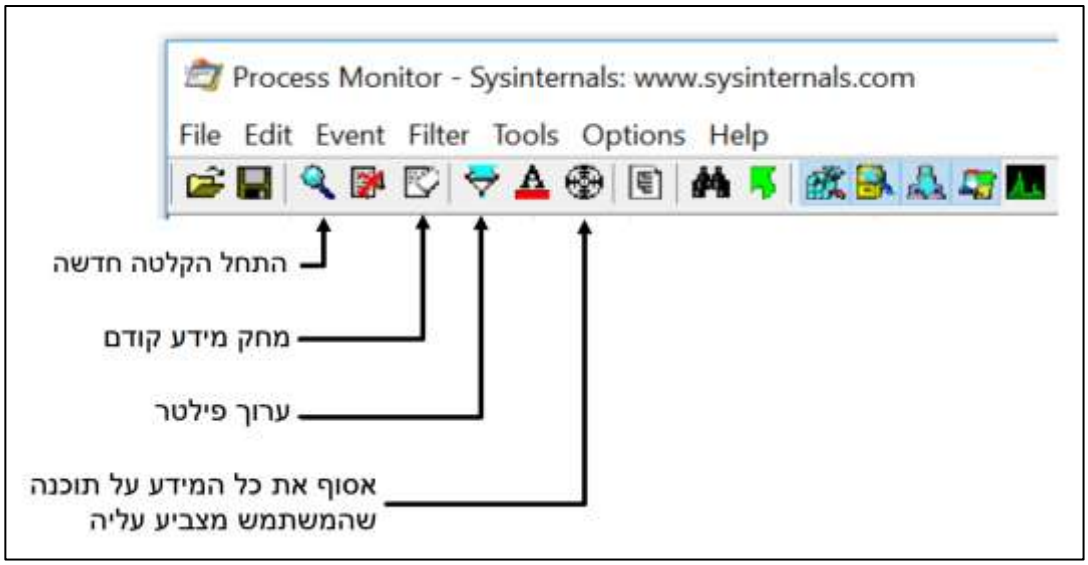
7. שאלה 3, סעיפים א עד ד.
8. שאלה 5, סעיפים א עד ו.
9. שאלה 7

להגשה

תוכנת Procmon

(מבוסס על המדריך הבא מתוך אתר MSDN -
https://docs.microsoft.com/en-us/archive/blogs/appv/process-monitor-hands-onlabs-and-examples)

1. כהכנה לתרגיל, פיתחו את Procmon והתחילו הקלטה חדשה.



שימו לב!!

בדקו שאתם אכן מקליטים אירועים ומפעילים עליהם פילטר (סינון) באופן מוצלח.

Showing 265 of 404,955 events (0.065%)

- הביטו בפינה השמאלית התחתונה כמה אירועים נקלטים וכמה מתוכם מסוננים
- אם אף אירוע לא מוקלט, סימן שלא התחלתם הקלטה.
- אם אף אירוע לא מוצג, סימן שהפילטר שלכם לא תפס שום אירוע, וייתכן ששגיתם במשהו. (למשל: שם ה Process עם שגיאת כתיב)

2. כעת פיתחו את תוכנת Autoruns64, ושנו את גודל הפונט וסוג הפונט. (בלשונית Options, תחת Font). סגרו את Autoruns64 ועצרו את ההקלטה.
3. כדי למצוא את ההגדרות נצמצם את החיפוש ככל האפשר:
   א. ראשית, נסיר את כל הProcessים שאינם Autoruns:
   שתי שיטות אפשריות –
   * נמצא שורה כלשהי ששייכת ל Process autoruns64, קליק ימני, לבחור Include ואז לבחור Process Name.
   * לחיצה על Ctrl+L, יפתח עורך הפילטרים – ובו נוסיף את הפילטר "Process name autoruns64.exe"
   ב. נוסיף פילטר נוסף – צפיה באירועים שקשורים לכתיבה לרגיסטרי . בשורת האייקונים העליונה ישנם מספר לחצנים שכל אחד מהם מבטל או מאפשר סוג מסוים של אירועים . השאירו לחוץ רק את לחצן אירועי הרגיסטרי.

   ג. כעת נתחיל לבטל ארועי רגיסטרי שאינם קשורים. עמדו על אירועים כגון RegOpenKey RegEnumKey, RegCloseKey, ובאמצעות קליק ימני ואז

Exclude Operation צרפו אותם לפילטר. נותרנו עם אירועים מסוג RegSetValue. כל האירועים הללו נמצאים בנתיב:
HKCU\SOFTWARE\Sysinternals\AutoRuns

ד. כעת, בין האירועים שנותרו מצאו על פי התיאור את האירוע בו שיניתם את הפונט (שם הפונט החדש יופיע בתוך התיאור)
ה. הקליקו על האירוע כדי לקבל מידע מפורט יותר. בצעו צילום מסך.
ו. חזרו לרשימת האירועים, ולחצו קליק ימני על האירוע הנ"ל, ובחרו Jump To. תגיעו אל ערך הרגיסטרי בתוך RegEdit. בצעו צילום מסך.

4. הציגו כל מה שמבצע התהליך chrom.exe.
5. הציגו את כל האירועים שמבצעים WriteFile
6. הציגו את כל מי שמבצע RegQueryValue
7. איך נקראת הפונקציה של ntdll ש RegQueryValue קורא לה? (בדקו בתוך הstack)

8. הציגו את כל מי שקורא את הרגיסטרי במיקום:
HKCU\SOFTWARE\ConEmu\.Vanilla \FontSize
9. תוך כדי ביצוע סעיף 8, פתחו ConEmu ומצאו מהו שם התהליך (בצעו include ל path ב Filter).

תרגיל סיכום:

רקע: בתרגיל זה תתקינו תוכנה לימודית שובבה, שפותחה במיוחד לצורך התרגיל. התוכנה

צרפו צילומי מסך:

10. שאלה 3, תת-סעיפים ה,ו.
11. שאלה 4.
12. שאלה 5.
13. שאלה 6
14. שאלה 8

וכתבו את התשובות לשאלות מהסעיפים הקודמים:

15. שאלה 7
16. שאלה 9

להגש

טורדנית מעט, אך היא אינה עושה נזק למחשב. מטרתכם היא להסיר אותה. מיד תראו שמי שמתקין את התוכנה הם אתם, ויכול להיות שתשאלו את עצמכם האם זה משקף את המציאות? כלומר, מדוע שמישהו יתקין תוכנה בעייתית במחשב שלו בעצמו? למעשה זה נפוץ מאד. נוזקות רבות מציגות את עצמן כתוכנות שמבצעות דברים טובים ומשכנעות אותנו להוריד ולהתקין אותן. לאחר שהתקנו אותן צריך להתמודד איתן ולמצוא דרך להסיר אותן.

התקנת התוכנה הלימודית – והסרתה:

1. הורידו את התוכנה הלימודית מהלינק הבא:
https://data.cyber.org.il/os/NaughtyWindow.msi
2. הקליקו על חבילת ההתקנה Naughty Window. כעת נוצר קיצור דרך על שולחן העבודה שלכם.

3. הפעילו את ההתקנה באמצעות לחיצה ימנית Run as administrator (חשוב מאד! בלי הרשאה מתאימה ההתקנה לא תעבוד כמו שצריך)
4. כעת התוכנה מותקנת. צלמו מסך כדי להראות את פעולתה.
5. נסו להסיר אותה. השתמשו בכלים שנלמדו בשיעור.
6. הדליקו את המחשב מחדש ובדקו שהתוכנה כבר לא מקפיצה הודעות למסך.
7. כתבו מדריך להסרת התוכנה לאחר שהותקנה, בדרך הקצרה והיעילה ביותר (היכן ללחוץ, מה לשנות)

צרפו צילומי מסך:

17. שאלה 4.

וכתבו את התשובות לשאלות מהסעיפים הקודמים:

18. שאלה 7

להגשה

<u>למתקדמים</u>

כתבו את התוכנה בעצמכם.

לשם כך עיינו בספר ובצעו שם את עמוד 17, סעיף 1.4.1

בהצלחה רבה!