


קבצים להפעלת התוכנה:

1. Test - קובץ וורד פשוט שיהיה להצפנה, קובץ זה צריך להיות ממוקם בשולחן העבודה (desktop) אחרת הקוד של ההצפנה לא ימצא אותו.
2. procMon.py – קובץ להפעלת הסקריפט של הפאורשל בתור אדמין.
3. encryptTest.py – סקריפט בפייטון להצפין קובץ מסוים לבדיקה של התוכנה, התהליך ימשיך לרוץ לעוד 60 שניות מהרגע שהצפין כדי שנוכל לבדוק האם באמת אפשר לסגור את התהליך.
4. start_procmon.ps1 – סקריפט פאורשל להפעלת תוכנת Procmon וקבל ממנה את המידע הנחוץ.
5. ProcmonConfiguration.pmc – קובץ הגדרות עבור הProcmon.
6. Dist (folder) – תיקייה המכילה את קובץ ProcessMonitorApp.exe, זאת התוכנה שמוצאת תהליכים זדוניים (תהליכים מצפינים)

ProcessMonitorApp.exe 

תמונה של הקובץ

7. Procmon.exe – התוכנה שמביאה מידע על תהליכים וממירה את זה לקובץ pml*. וגם *.csv.
8. Process_monitor.py הקוד של התוכנה ProcessMonitorApp.exe.

צעדים להפעלת התוכנה:

1. מפעילים את קובץ procMon.py ולאחר מכן יש 10 שניות להפעיל את ההצפנה על קובץ הוורד כדי שProcmon יתפוס את התהליך, הסקריפט מפעיל את Procmon ל10 ואחר מכן לוקח את המידע וסוגר אותו.
2. לאחר השלב הראשון יופיעו בתיקייה שני קבצים חדשים שהם txt.csv. לאחר הופעת הקבצים הללו אפשר להפעיל את ProcessMonitorApp.exe שימצא את התהליך שמצפין.
3. לאחר קפיצת חלון עם מס' התהליך שנחשב לחשוד יש ללחוץ על הכפתור ותהליך ההרצה של ההצפנה אמור להסתיים.