MALWARE ANALYSIS

סדנה 4 – הנדסה לאחור – חורף תשפ"א

היום בסדנה

- נחקור payload של malware בסיסי (אך מגניב).
- הpayload מסופק לכם בשתי דרכים –
  - כרצף ערכי hex בקובץ shellcode.txt
  - כמחרוזת בינארית בקובץ shellcode.bin

- מטרתכם לענות על השאלה - מה בדיוק מבצע ה shellcode?
- הוכיחו באמצעות דוגמה!

איך מתחילים?

- איך נחקור את ה malware? ובכן ישנן המון דרכים, אתם יכולים לבחור באיזו דרך שאתם רוצים.

- ניתן לחקור את ה payload בצורה סטטית:
  - ע״י הכנסת הבתים ל disassembler (בפרט, IDA).
  - על מנת ליצור ממנו executable ניתן לכתוב עבור מעטפת ב C.
  - ניתן גם לכתוב קובץ PE של ממש! (היזכרו בתרגול 2).

- ניתן לחקור את ה payload בצורה דינאמית:
  - ניתן להכניס אותו כקלט לתכנית פגיעה ולעבוד עם ה debugger.
  - ניתן גם להזריק אותו! (צריך לכתוב injector)

מספר הכוונות

- על מנת לוודא שהבנתם נכון את דרך הפעולה של ה shellcode, בדקו שאתם יודעים לענות על השאלות הבאות.

- איך ה malware מוצא כתובות פונקציות ששייכות ל DLLs?
  - רמז, תרגול 2 + סוף תרגול 5.
- איך ה malware מבצע קריאות לפונקציות? נסו לשער מדוע.
- מה ה side effects של הרצת ה malware? נסו ליצור דוגמה המוכיחה זאת.

בהצלחה!