מגישים: רון עמר ואילונה גרנד מנחה: ד"ר גיא לשם

MALCLASS

רקע

מה הבעיה? כיום, קיימים אנטי וירוסים אשר מזהים נוזקות (malware) אך לא יודעים להגדיר מהו סוג הנוזקה (ransomware, adware….), לא ניתן לדעת מה היא סוג הנוזקה, מה רמת הנזק שלה. ובנוסף, לא מבצע סיווג עפ"י הפעולות שלה.

הפתרון שלנו- מערכת המבצעת סיווג לנוזקות בעזרת רשת נוירונים. תחילה, יבוצע סיווג נוזקות על פי סט הפעולות של כל תוכנה. נעשה זאת בעזרת מאגר נוזקות, ונריץ על פלטפורמה ייחודית המנתחת את הנוזקות ופעולותיהן. ננתח את המידע, נעביר למסווג ונדע לבסוף מה הוא סוג הקובץ.

תיאור המערכת

- ✓ עמוד בית – הכנסת הקובץ עליו ירצה המשתמש לדעת האם הוא נוזקה או לא, ואם כן אז מה סוגו.
- ✓ Sandbox – Cuckoo + VM שמבצע את הניתוח של הנוזקה, מייצר פלט של כלל הפעולות שהיא מבצעת – כקובץ JSON.
- ✓ Mongo DB – בסיס הנתונים בו קובץ ה-JSON נשמר, ומומר לקובץ CSV.
- ✓ מערכת הלומדת – חילוץ קובץ ה-CSV אל האלגוריתם שיודע לפענח האם הקובץ נוזקה ומה סוגו. בסוף הרצתו יוצג למשתמש את ניתוח הקובץ.

אמצעים טכנולוגיים

שפה: Python | Sandbox: Cuckoo | VM: Ubuntu 18 | בסיס נתונים: MongoDB | Deep learning: Pytorch |