**זיהוי תוכנות זדוניות על פי הצגה בינארית**

מגיש: אסף הראל

מורה: גד לידרור

בית הספר: תיכונט

# הבעיה

במשך השנים אנו הופכים ליותר ויותר תלויים בטכנולוגיה ודבר זה פותח חלון לאנשים בעלי כוונות זדוניות לנצל זאת וליצור וירוסים שיפגעו במחשבים שלנו/יגנבו מאיתנו מידע.

כיום יש הרבה תוכנות אנטי וירוס שמטרתן לזהות תוכנות זדוניות שהוחדרו למחשב אך גם אותן האקרים מצליחים לעקוף.

# הפתרון

בעזרת רשת נוירונים שבנו שלושה חוקרים מאוניברסיטת פלימאות׳ באנגליה ניתן להגיע ל-94.1% הצלחה בזיהוי תוכנות זדוניות מסוג ransomware ([קישור למאמר](https://arxiv.org/pdf/1904.00859.pdf)).

המידע שהרשת מקבלת הוא ייצוג בינארי של קבצים – ייצוג בינארי הופך את התוכן הבינארי של הקובץ למידע שניתן להציג בתמונה, הנה למשל ייצוג בינארי של התוכנה VMware player ושל תוכנה זדונית של סוס טרויאני:

A picture containing text

Description automatically generatedA picture containing background pattern

Description automatically generated

VMware player

סוס טרויאני

# תוצר סופי

התוכנה הסופית תסרוק את כל הקבצים במחשב (כמו אנטי וירוס רגיל) ותכניס את הייצוג הבינארי שלהם למכונה והמכונה תחזיר סיווג פשוט – האם הקובץ הוא קובץ חשוד ומאיזה סוג הוא.

# איסוף נתונים

המאגר שבו החוקרים השתמשו אינו מצויין במאמר אז השתמש בחלק קטן יחסית ממאגר וירוסים שפורסם על ידי מייקרוסופט באתר kaggle ששוקל מעל 500GB – [קישור למאגר](https://www.kaggle.com/c/malware-classification/data).

המאגר מכיל 9 סוגים שונים של תוכנות זדוניות