**2entFOX**

בניית רשת בייסיאנית שמכילה הסתברות מותנת CPT שמכילה הסתברויות לחולשות מסוימות בהסתמך על מחקרים של נקודות שהתוקף לרוב תוקף

תרחישים נפוצים לדוגמא על ידם חשודים ונבדקו :

1. אם מנסים לבצע שינויים בשירות, שלקורבן אין דרך לשחזר את הנתונים המוצפנים שלה מלבד לשלם כופר.
2. האם ביצעו בקשה להרשאות בספריות רגישות

ברירת המחדל של התוכנה היא לקחת 20 מקרים שונים ולאחר חישוב על ידי שימוש ברשת בייסיאנית נקבל מספר הסתברותי בין 0-1 שיודע הסתברות מאוד גבוהה היא בוצע התקפת כופר או לא

**Detecting crypto‑ransomware in IoT networks based on energy**

המאמר מתבסס על הידע שלנו בצריכה החשמל של כל מכשיר לאחר התקנת אפליקציות פופולאריות על ידי שימוש במכונת למידה.

במאמר נבנה מכונת למידה שעובדת על מאגר גדול של dataset ובכך המודל יודע לפי האנרגיה של המכשיר שאמור להיות לאחר אפליקציות פופולאריות (לפי דגם ) האם האפליקציה זדונית או לא.

**CryptoLock (and Drop It) Stopping Ransomware Attacks on User Data**

תוכנה cryptolock מבוססת על אינדיקטורים (אינדיקטור הוא משתנה מקרי שמציין האם מאורע מסוים התרחש. כאשר המאורע התרחש, הערך שלו הוא 1, וכאשר המאורע לא התרחש ערכו ).

התוכנה מבוססת על 3 אינדיקטורים עיקריים-

1. שינוי סוג הקובץ - חתימות אלה מתארות את הסדר

ומיקום של ערכי בייט ספציפיים הייחודיים לסוג הקובץ,

יש לשקול שינוי של נתונים כאלה כחשודים.

1. העתקת קובץ מקור- כאשר מעתיקים זה אמור להיות דומה בהסתברות 0.
2. - Shannon Entropy – שימוש באינדיקטור שאנון שמעדכן האם יש אי וודאות על הקבצים