**2entFOX**

בניית רשת בייסיאנית שמכילה הסתברות מותנת CPT שמכילה הסתברויות לחולשות מסוימות בהסתמך על מחקרים של נקודות שהתוקף לרוב תוקף (כמו למשל מנסים לבטל את המנגנון החשוב ביותר של חלונות לאחסון קבצי הגיבוי החמים של המשתמשים, לבצע שינויים בשירות, שלקורבן אין דרך לשחזר את הנתונים המוצפנים שלה מלבד לשלם כופר. אחת ההתנהגויות בהן נתקלנו בניתוח רכיבי כופר הייתה קבלת גישה לספריות מיוחדות.) במחקר ביצעו 6 תרחישים שונים אך במאמר עצמו מדברים רק על התרחיש הראשון :

אחרי חילוץ כל אחת מהתכונות באופן עצמאי ושלב אחר שלב.

ברירת המחדל של התוכנה היא לקחת 20 מקרים שבמידה וקרו מספר מהמקרים המערכת מתריעה שזה התקפת כופר (מעל 85% הסתברות)

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

במאמר זה מתבססים על מכונת למידה כך שידוע שלכל אפליקציה יש צריכה מסוימת , לאחר המון ניסויים בנו מודל כך שמריצים על המון dataset ובכך המודל יודע לפי האנרגיה של המכשיר שאמור להיות לאחר אפליקציות פופולאריות (לפי דגם ) האם האפליקציה זדונית או לי

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

קישור להורדה :   
<https://cryptolocker-ransomware.en.uptodown.com/windows/download>

היו מספר רשויות שנפלו למתקפת כופר !.

תוכנה cryptolock מבוססת על אינדיקטורים, יש לה 3 אינדיקטורים עיקריים-

1. שינוי סוג הקובץ - חתימות אלה מתארות את הסדר

ומיקום של ערכי בייט ספציפיים הייחודיים לסוג הקובץ, ולא

פשוט את פרטי הכותרת. מכיוון שקבצים בדרך כלל שומרים על שלהם

סוג הקובץ והעיצוב במהלך קיומם, בתפזורת

יש לשקול שינוי של נתונים כאלה כחשודים.

1. העתקת קובץ מקור- כאשר מעתיקים זה אמור להיות דומה בהסתברות 0.
2. שנאנון אח יקר –

אינדיקטור משניים-

1. מחיקה של קבצי מערכת
2. לא הבנתי