**2entFOX A Framework for High Survivable**

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)

**A behavioural-based approach**

עגכ

**A Comprehensive Survey on Ransomware Attack\_ A Growing Havoc Cyberthreat**

עכג

**A Survey on Detection Techniques for Cryptographic Ransomware**

עגכ

**AN EXPERIMENTAL STUDY TO EVALUATE THE PERFORMANCE OF MACHINE LEARNING ALGORITHMS IN RANSOMWARE DETECTION**

עג

**Automated Analysis Approach for the Detection of High Survivable Ransomware**

גכעגדשגשדג

**Automated detection and remediation of ransomware attacks involving a storage device of a computer network**

גדש

**Critical Evaluation of Current Methods Aimed at Improving Ransomware Detection**

שדג

**Cryptocurrency Based Malware and Ransomware Detection Systems and Methods**

שדג

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

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 –

**Cutting the Gordian Knot A Look Under the Hood of Ransmoware Attack**

עכגעגכ

**Deep Learning for Ransomware Detection**

גדשגשד

**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

**Detecting Ransomware using Support Vector Machines**

גדשגשד

**Detecting Ransomware with Honeypot techniques**

עכג

**Machine Learning and Cryptographic Algorithms±Analysis and Design in Ransomware and Vulnerabilities Detection**

גדש

**Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems**

כשדגשד

**Machine LearningandCryptographicAlgorithms**

גדשגשדג

**Machine Learning-Based Detection of Ransomware Using SDN**

גדש

**PayBreak Defense Against Cryptographic Ransomware**

גדש

**Ransomware, Threat and Detection Techniques**

גדשג

**Ransomware, Threat and Detection Techniques\_ A Review**

גדש

**RansomwareEvolutionGrowthandRecommendationforDetectionpublished**

גד

**Software-Defined Networking-based Crypto Ransomware Detection Using HTTP**

דשג

**זיהוי התקפה באמצעות אינפוט אאוטפוט**

גשד

ג