Ransomware Software

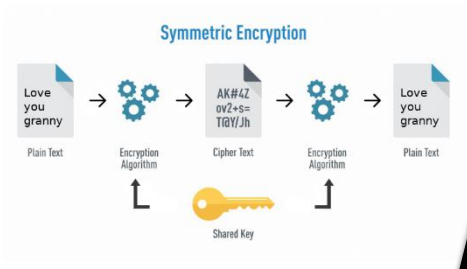
מכון טכנולוגי חולון
Holon Institute of Technology
הפקולטה למדעים
מערך פרויקטים ושיתוף פעולה עם התעשייה

מגישים : מנור שערבי, עדי לנגשטד , דוד אלישיב
מנחה : רועי זימון
המחלקה למדעי המחשב , תשפ"ג

מטרת הפרויקט:

הרחבת הידע לגבי התקפות סייבר והפרט התקפות כופרה , כיצד הן עובדות וכיצד ניתן להתגונן מפניהן.

מטרתנו היא לספק מידע לציבור הנרחב את הקלות הביצוע של מתקפת הכופרה וכמה צעדים



קוד QR לאתר GitHub בו נמצא הקוד שלנו:

תהליך ופיתוח:

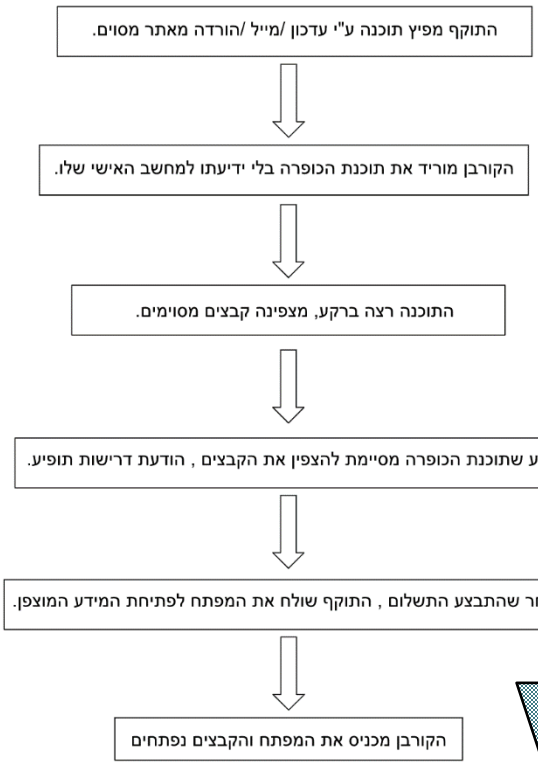
תוכנת הכופרה שלנו מורכבת משני סוגי הצפנה, הצפנה סימטרית והצפנה א-סימטרית.

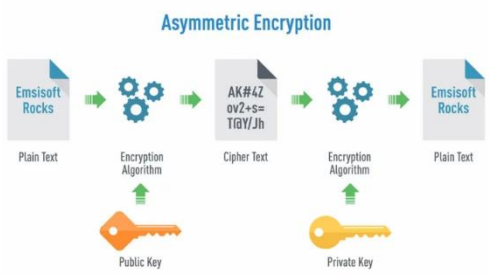
לכל קורבן ניצור מפתחות הצפנה ייחודיות משלו על מנת שלא יקרה מצב כי קיימים מפתחות זהים.

לאחר שהתוכנה תחפש את הקבצים במערכת , אותם היא צריכה להצפין באמצעות המפתח הסימטרי AES. היא תשנה את סיומת הקובץ לסיומת ייחודית, MAD_HIT.

לאחר מכן , על מנת שתוכנת הכופר תהיה חזקה ויעילה יותר , המערכת מצפינה את המפתח ה-AES באמצעות המפתח הציבורי שנוצר דרך האלגוריתם RSA.

אם הקורבן שילם את הכופר, מפתח AES יפוענח באמצעות המפתח הפרטי של התוקף אשר נשלח לנתקף לאחר ביצוע התשלום ואז הקבצים יפוענחו באמצעות המפתח ה-AES המחוזר.





מסקנות:

תוכנת כופרה היא אחת מהדוגמאות הפופולריות בשימוש לרעה של קריפטוגרפיה .

ההשלכות המסוכנות של תוכנות כופרה כגון מניעת שירותים של מחשב הארגון או הפרט יכולה להשפיע על תחומים רבים , כגון מערכת ממשלתית , מערכת חינוך ואפילו מערכת בריאות , אשר יכול להוביל לאובדן חייהם של אנשים.

פרויקט זה כולל יצירת תוכנת כופה באמצעות השפה python , ספר הפרויקט בו מוסבר יותר בהרחבה על תוכנת הכופרה ועל הרכיבים הקריפטוגרפים שהשתמשנו .