**הסבר מפרוט על מה הפרוץ עושה ומה הקורבן :**

הרעיון של הצפנת קבצי הצפנת קבצים הומצא ויושם על ידי יאנג ויונג באוניברסיטת קולומביה והוצג בכנס IEEE Security & Privacy ב -1996. זה נקרא סחיטה cryptoviral וזה היה בהשראת פצפוצי הבדיוני בסרט Alien. [13] סחיטה קריפטוביראלית היא הפרוטוקול הבא בן השלושה עגולים שבוצע בין התוקף לקורבן. [1]

[תוקף → קורבן] התוקף מייצר צמד מפתחות ומניח את המפתח הציבורי המקביל בתוכנה זדונית. התוכנה הזדונית משוחררת.

[קורבן → תוקף] כדי לבצע את התקפת הסחיטה הקריפטו-ויראלית, התוכנה הזדונית יוצרת מפתח סימטרי אקראי ומצפינה את נתוני הקורבן איתו. הוא משתמש במפתח הציבורי בתוכנה זדונית כדי להצפין את המפתח הסימטרי. זה ידוע כצפנה היברידית וזה מביא להצפנה א-סימטרית קטנה כמו גם להצפנה סימטרית של נתוני הקורבן. זה מאפס את המפתח הסימטרי ואת נתוני הפלאסט המקוריים כדי למנוע התאוששות. זה מעלה הודעה למשתמש שכולל את הצופן הצבע הא-סימטרי וכיצד לשלם את הכופר. הקורבן שולח את התצפית והכסף האלקטרוני הא-סימטרי לתוקף.

[תוקף → קורבן] התוקף מקבל את התשלום, מפענח את הצופן הצבע הא-סימטרי עם המפתח הפרטי של התוקף ושולח את המפתח הסימטרי לקורבן. הקורבן מפענח את הנתונים המוצפנים באמצעות המפתח הסימטרי הדרוש ובכך השלים את ההתקפה הקריפטובירולוגית.

המפתח הסימטרי נוצר באופן אקראי ולא יסייע לקורבנות אחרים. בשום שלב לא נחשף המפתח הפרטי של התוקף לקורבנות והקורבן צריך רק לשלוח תוקף קטן מאוד (מפתח הצופן הצפוני המוצפן) לתוקף.

התקפות Ransomware מתבצעות בדרך כלל באמצעות טרויאני, נכנסות למערכת דרך, למשל, קובץ מצורף זדוני, קישור משובץ בהודעת דיוג או פגיעות בשירות רשת. לאחר מכן התוכנית מריצה מטען, אשר נועל את המערכת בצורה מסוימת, או טוענת שהיא נועלת את המערכת אך אינה עושה זאת (למשל, תוכנית תוכנת צלקת). עומסי מטען עשויים להציג אזהרה מזויפת כביכול על ידי גורם כמו סוכנות אכיפת חוק, בטענה כוזבת שהמערכת שימשה לפעילות בלתי חוקית, מכילה תוכן כמו פורנוגרפיה ומדיה "פיראטית". [14] [15] [16]

עומסים מסוימים מורכבים פשוט מאפליקציה שנועדה לנעול או להגביל את המערכת עד לתשלום, בדרך כלל על ידי הגדרת מעטפת Windows לעצמה, [17] או אפילו שינוי רשומת האתחול הראשית ו / או טבלת המחיצות כדי למנוע הפעלה למערכת. מאתחול עד לתיקונו. [18] העומסים המשוכללים ביותר מצפינים קבצים, כאשר רבים משתמשים בהצפנה חזקה בכדי להצפין את קבצי הקורבן בצורה כזו שרק למחבר התוכנה הזדונית יש את מפתח הפענוח הדרוש. [1] [19] [20]

התשלום הוא כמעט תמיד המטרה, והקורבן נאלץ לשלם עבור הסרת תוכנת הכופר באמצעות אספקת תוכנית שיכולה לפענח את הקבצים, או על ידי שליחת קוד נעילה המבטל את שינויי המטען. אמנם התוקף יכול פשוט לקחת את הכסף מבלי להחזיר את תיקי הקורבן, אך לטובתו של התוקף לבצע את הפענוח כמוסכם, שכן הקורבנות יפסיקו לשלוח תשלומים אם נודע שהם לא משרתים שום מטרה. אלמנט מרכזי ביצירת עבודת ransomware עבור התוקף הוא מערכת תשלום נוחה שקשה לעקוב אחריה. נעשה שימוש במגוון של אמצעי תשלום כאלה, כולל העברות בנקאיות, הודעות טקסט בשיעור פרמיה, [21] שירותי שובר בתשלום מראש כמו paysafecard, [6] [22] [23] והמטבע הדיגיטלי bitcoin. [24] [25] [26]