04 נובמבר 2015

כ״ב חשון תשע״ו

סימוכין : י-ס-158

הנדון: התרעה על פוגען Fareit

תיאור : לאחרונה התקבל ב-CERT הלאומי דיווח על מערך תקיפה המבצע שימוש בגרסה חדשה של פוגען בשם Fareit. ככל הנראה, המערך עובד בשיטת "Pay For Infection", במסגרתה תוקף המערך יעדים לבקשת לקוחותיו תמורת תשלום.

הפוגען משמש כראש גשר להורדת פוגענים נוספים, וכן עבור גניבת נתוני הזדהות ממחשב הקורבן. גרסת הפוגען החדשה מכילה רכיב מיוחד המשנה את קובץ הפוגען עבור כל מחשב שבו הוא מופעל. רכיב זה נועד לשנות את תוצאת חישוב פונקציית הגיבוב על הקובץ ובכך למנוע את זיהוי הפוגען מתוך רשימה שחורה.

אינדיקטורים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חדירה או פגיעה במערכות מחשב.

כלל המזהים שנצפו מצורפים כדבוקה.

(יתכן וחתימות מסוימות לא יופיעו כלל עקב אי הפעלת שלב מסוים , או עקב שינוי בשמות הקבצים, יתכן אף כי גם כתובות ה IP של שרתי ה- C&C משתנות ואינן הכתובות שנצפו בתקיפות שהתגלו)

קישורים ומידע נוסף:

- http://blogs.cisco.com/security/talos/fareit-analysis

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר.
לכל מידע נוסף ניתן לפנות אלינו .

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,

CERT-IL

טל: 03-7450801

team@cert.gov.il