העדכון שלפניכם לוקט ועובד במסגרת פעילות ה-CERT הלאומי על בסיס מגוון מקורות רחב, כדי לרכז מידע רלוונטי ואקטואלי לעוסקים בתחום הגנת הסייבר. כפועל יוצא, ה-CERT הלאומי אינו יכול לערוב לחלוטין למידע המובא בעדכון או למסקנות המשתמעות ממנו, ואין באמור בעדכון משום המלצה לנקיטת פעולות כלשהן או לשינוי מדיניות אבטחה קיימת. אין באזכור חברות אבטחה או גורמים מסחריים אחרים משום הבעת עמדה או המלצה ביחס אליהם או לשירותים או המוצרים המוצעים על ידם.

16 פברואר 2016

ז' אדר א תשע"ו

סימוכין: ל-ס-169

הנדון: עדכון מזהים - התרעה על פוגעני TeslaCrypt

רקע:

בשבועות האחרונים מזוהה גל תקיפות נרחב נגד אתרים ויעדים ישראליים באמצעות פוגען כופר (Ransomware) מסוג TeslaCrypt.

מטרת מסמך זה לפרט בקצרה את תהליך ואופן פעולת הפוגען וכן לספק דרכי התמודדות. כמו כן, המסמך כולל מזהים אפשריים מוכרים.

בהמשך להתרעה בסימוכין CERT-IL-ALERT-G-C-167, מצורף בזאת מזהים עדכניים נוספים על אודות הפוגען.

דרכי הדבקה

1. גלישה: הדבקה באמצעות גלישה לאתרים המכילים את הפוגענים ו/או מבצעים ניתוב מחדש לאתרים זדוניים אשר מדביקים את המחשבים ע"י הורדת הפוגען למחשב.
2. פתיחת קבצים: הדבקה באמצעות שליחת דוא"ל עם צרופה נגועה (כגון קבצי Word ו-Pdf) וניצול חולשות מוכרות בצרופות.

להלן שני מערכים העושים שימוש באוסף של כלי תקיפה אשר מנצלים חולשות להתקנת הנוזקה:

1. Angler Exploit Kit- משפחת פוגענים המוכרת מזה כשנתיים ומנצלת חולשות של Java, Acrobat Reader, Flash ו-Silverlight. רוב השרתים המארחים את הפוגענים אותרו באוקראינה.
2. Nuclear Exploit Kit – משפחת פוגענים המנצלת חולשות של Java, Acrobat Reader, Flash ו-Silverlight.

שלבי התקיפה

1. הדבקת המחשב והתקנת הפוגען באמצעות יצירת קובץ מסוג EXE. בתיקיית %AppData%.
2. הורדת מפתח ההצפנה מהאינטרנט
3. חיפוש קבצי נתונים והצפנה עם מפתח AES-256 ביט
4. מתן סיומת חדשה לקבצים המוצפנים (משתנה בין הגרסאות). להלן מספר סיומות מוכרות: **.micro, **.abc, **.ecc.
5. יצירת קובץ הנחיות לנתקף בפורמט txt ,html לשחזור הקבצים המוצפנים. קובץ ההנחיות מכיל קישור לאתר ייעודי בו, לכאורה, ניתן לפענח את ההצפנה. כמו כן, באתר זה יופיע גם סכום הכופר הנדרש.

מסמך זה מופץ כ TLP: לבן. מקבלי מידע TLP לבן יכולים לשתף מידע המסווג "לבן" ללא הגבלה ובערוצים פומביים דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים. כל זאת בכפוף לזכויות יוצרים.

<u>דרכי מניעה</u>

1. עדכון שוטף של טלאי אבטחה למערכות ההפעלה ולתוכנות המותקנות במחשב, בדגש על טלאי האבטחה המופיעים מטה.
2. עדכון חתימות Antivirus וחתימות IDS ייעודיות לגרסת הפוגען הנוכחי באמצעות פניה יזומה לספק האנטי וירוס לבקשת קבלת חתימות מעודכנות.
3. סינון תוכן הגלישה באמצעות Proxy ומימוש URL Filtering מחמיר.
4. סינון תעבורת דוא"ל ארגוני באמצעות Mail Filtering / Mail Relay.
5. הגברת תדירות ביצוע עדכונים וגיבויים למידע הארגוני ושמירה של מספר גרסאות גיבויים לאחור.

<u>דרכי תגובה והכלה מיידיות</u>

כאשר מזהים תחנה החשודה כנגועה בפוגען כופר יש לפעול ע"פ ההנחיות הבאות:

1. ניתוק פיזי / התקשורת של המחשב מהרשת הארגונית.
2. שמירת "תמונת זכרון" (memory dump) באמצעות תוכנה ייעודית ושמירה על Disk on Key ייעודי בגודל של 16gb לפחות.

   (DumpIt - http://www.toolwar.com/2014/01/dumpit-memory-dump-tools.html)
3. כיבוי אלים של המחשב **רק** לאחר שמירת תמונת הזיכרון.

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

מסמך זה מופץ כ TLP: לבן. מקבלי מידע TLP לבן יכולים לשתף מידע המסווג "לבן" ללא הגבלה ובערוצים פומביים דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים. כל זאת בכפוף לזכויות יוצרים.