משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

TLP: לבן

13/05/2017

י"ג אדר תשע"ז

סימוכין: ב-ס-161

ארוע "חץ וקשת" - הנחיות התמודדות עם כופרת WannaCry - עבור משקי הבית

תקציר

ביום שישי ה-12 במאי זוהה גל התקפות כופרה מאסיבי כנגד עשרות אלפי מחשבים בארגונים רבים ובעשרות מדינות ברחבי העולם, ביניהם Telefonica בספרד, שירות הבריאות הלאומי בבריטניה ו-FedEx בארה"ב. התקיפה מנצלת חולשת אבטחה אשר פורסמה בהדלפות Shadow Broker במהלך חודש שעבר.

פרטים

ביממה האחרונה זוהו מתקפות כופרה מאסיביות במספר מדינות באירופה בהן ספרד, בריטניה ופורטוגל באמצעות פוגען כופר ממשפחת WannaCry. נראה כי התקיפה מנצלת מספר חולשות אבטחה ידועות, אחת מהן פורסמה בהדלפה של Shadow Broker במהלך אפריל (מדובר על פגיעות מוכרת של חברת מיקרוסופט, MS17-010, שתוקנה במרץ 2017 וכולל פגיעות בפרוטוקול SMB V1[1]).

דיווחים רבים אודות המתקפה והשפעותיה התקבלו ממספר בתי חולים ברחבי בריטניה. תקיפות אלו גרמו, בין השאר, להשבתת הפעילות באותם בתי חולים ולהפרעה בטיפול בחולים. בנוסף, מתקפת הכופרה בספרד הובילה לפגיעה משמעותית בחברת התקשרות הענקית "Telefónica" .

תוכנת הכופר מגיעה למחשבי המשתמשים באמצעות הודעת דוא"ל עם קובץ מצורף. פתיחת הקובץ על ידי המשתמש, מפעילה את תהליך ההתקנה וההתפשטות של תוכנת הכופר. בעת ההפעלה, מבצעת תוכנת הכופר סריקה של כתובות בתוך הרשת הפנימית של הארגון וגם בטווח כתובות רנדומאלי באינטרנט לטובת חיפוש אחר מחשבים פגיעים לחולשת שירות שיתוף הקבצים של מיקרוסופט בגרסה 1 (SMBv1).

תוכנת הכופר סורקת את תיקיות המחשב ומצפינה את רוב סוגי הקבצים השימושיים. לאחר ההצפנה, התוכנה מציגה הודעה הדורשת מהמשתמש לשלם עבור פתיחת ההצפנה סכום של בין 300-600 דולרים. תרשים א' מציג מסך לדוגמא בו נדרש מהמשתמש תשלום הכופר. פרטים נוספים נמצאים עדיין בחקירה,

[1] https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html

בלמ"ס

TLP: **לבן**

ויתעדכנו עם המשך החקירה. רשימת מערכות ההפעלה הפגיעות לסוג זה של תוכנת כופרה מפורטת בנספח א'.

תרשים א': צילום מסך של הודעת הכופרה לאחר הצפנת הקבצים

להלן אוסף פעולות לביצוע:

1. גיבויים - גבו את הקבצים החשובים ביותר – גיבוי על כונן חיצוני ועל הענן. עצה זו מגנה לא רק מנוזקת הכופר אלא גם מפוגענים אחרים.

שימו לב – הכונן החיצוני נדרש לטובת גיבוי בלבד, חשוב לנתקו באופן מסודר עם סיום הגיבוי מהמחשב.

2. חשוב לוודא כי מערכת ההפעלה והתוכנות המותקנות במחשב הן בגרסתן האחרונה ומעודכנות בעדכוני האבטחה האחרונים. מומלץ לוודא כי מצב העדכון האוטומטי במערכת מופעל.
3. התקנת תוכנות אנטי וירוס הכוללות מנגנונים של מוניטין, הגנה על דפדפנים ובדיקות מקיפות (רוב תוכנות אנטי וירוס מכילות רכיבים אלו).
4. הגדרת הדפדפן לחסימת חלונות קופצים תצמצם באופן ניכר את קפיצתן של פרסומות שעשויות לשמש כהדבקה בפוגענים בעת גלישה באתרים. יש לזכור כי הפעלת קוד מאקרו בקבצי אופיס עשויה להתקין פוגען על המחשב.
5. מיקרוסופט שילבה בדפדפן Internet Explorer בגרסה 11 ואילך את אופציית Smart-Screen שיכולה לסייע בצמצום המקרים הבאים:
   - Anti – Phishing.
   - Application Reputation.
   - Anti-Malware Protection.

להלן הקישור לדף ההסבר על התוכנה https://support.microsoft.com/he-il/kb/930168

רשימת כלים להתמודדות עם כופרות

RasnsomFree

Mcaffe free tools

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: 072-3990800

team@cert.gov.il

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

TLP: **לבן**