# עדכון חדשות סייבר יומי 24/04/2018

## בארץ ובעולם

1. מאגר מידע של חברת הבריאות האמריקאית Health Stream שהכיל פרטים אודות 10,000 חובשים ורופאים היה חשוף ברשת. המידע הוסר מאתר אינטרנט, אך נשמר בארכיון והכיל כתובות דוא"ל, תעודות זהות ועוד(theregister ו-securityaffairs).
2. בנק SunTrust מדווח כי עובד לשעבר ניסה להעתיק מידע אודות 1.5 מיליון לקוחות ולמכור אותו לגורם צד ג'. לדברי הבנק, המידע כלל כתובות מגורים, יתרת החשבון ומספרי טלפון בלבד ולא פרטים אישיים רגישים יותר כמו רישיון נהיגה, מספרי חשבון בנק ועוד (reuters).

## טכנולוגיה

3. חברת Symantec זיהתה קמפיין של קבוצת תקיפה המכונה Orangeworm במסגרתו במגוון רחב של ארגוני בריאות בינלאומיים הפועלים בארה"ב, אירופה ואסיה. לפי הדיווח, פוגען הותקן במערכות הדמיה ואפשר השתלטות על המערכת הנגועה. אינדיקטורים מצורפים בקישור (symantec).
4. חוקרי חברת אבטחת מידע netlab360 חשפו בוטנט המכונה Muhstik ומשתמש בפגיעות קריטית של Drupal. הבוטנט פעיל מזה שבועיים וסורק כתובות בחיפוש אחר רשתות וציוד שבהן טרם הותקן עדכון האבטחה הרלוונטי לפגיעות CVE-2018-7600 (netlab360). מערך הסייבר הלאומי יוציא בהמשך עדכון למסמך על השימוש בפגיעות זה לתקיפות.
5. גוגל השיקה שירות העברת הודעות חדש עבור משתמשי Android בשם Allo. לפי דיווחים של הארגון למען זכויות אדם, אמנסטי, שירות זה לא יכלול הצפנה מקצה לקצה ובכך יחשוף את המשתמשים להאזנות מצד תוקפים אופציונליים (amnesty).
6. נחשפה פגיעות חדשה בפונקציית השלמה אוטומטית AutoFill של LinkedIn. הפגיעות מאפשרת העברת פרטי המשתמשים לגורמים צד שלישי ללא אישור המשתמשים. עד כה, פונקציה זו הייתה אפשרית עבור אתרים אשר הוגדרו מראש, אך חוקר אבטחה חשף כי ניתן לנצל פונקציה זו בכל האתרים. החברה דיווחה כי היא טיפלה בפגיעות (lightningsecurity).

*** עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים המובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו. ***

7. חוקרי אבטחה חשפו פגיעות Zero Day בקוד ה-Kernel של Internet Explorer המכונה Double Kill. קבוצת APT השתמשה בפגיעות זו וניצלה אותה בתוך מסמכי Office (bleepingcomputer).

*** עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים המובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו. ***