עדכון חדשות סייבר יומי 17/06/2018

בארץ ובעולם

1. ספרנית מארה"ב החליטה לתבוע את חברת Equifax לאור אירוע דלף המידע האחרון ב-2017. הספרנית הגישה את התביעה על סך 5,000 דולר כמה ימים לאחר שנודע על הפריצה. לאחרונה בית המשפט קיבל את תביעתה, אך הסכים להעניק לה 690 דולר (krebsonsecurity).

2. קספרסקי החליטה על השהייה של שיתוף הפעולה עם היורופול כחלק מפרויקט NoMoreRansom, זאת לאחר החלטת האיחוד האירופי לבחון את ההסכמים עליהם הגופים חתומים מול חברות אבטחת מידע. בהחלטה נאמר כי מוצר של החברה נחשב כזדוני וניתנה המלצה להחרימו (bleepingcomputer).

3. היורופול בשיתוף גורמים מצרפת, בריטניה ותאילנד עצרו שמונה חשודים שהיו מעורבים בקבוצת התקיפה Rex Mundi שהייתה פעילה החל מ-2012. הקבוצה נהגה לפרוץ לחברות ולבקש כופר (bleepingcomputer).

4. 23 אלף חשבונות נפרצו באירוע דלף מידע של חברת HealthEquity, זאת לאחר שעובד החברה פתח הודעת דוא"ל זדונית (scmagazine).

טכנולוגיה

5. נחשפה פגיעות חדשה במעבדי אינטל. בדומה לפגיעויות הקודמות, גם פגיעות זו (CVE-2018-3665), המכונה Lazy State, היא מסוג Speculative Execution ומאפשרת קריאת מידע רגיש. ישנן מערכות הפעלה שכבר חסינות לפגיעות זו (intel ו-zdnet).

6. חברת ThreatFabric חשפה פוגען חדש שתוקף מערכות Android 7 ו-8. פוגען זה שנמצא עדיין בשלבי פיתוח וטרם הצליח להתפשט בצורה רחבה, הוא בעל מאפיינים דומים ל-LokiBot והוא מכיל אלמנטים של כופר ו-Keylogger (threatfabric).

7. חברת Trend Micro חשפה קמפיין חדש של קבוצת התקיפה האיראנית MuddyWater. לפי הדגימה שמצאה החברה, בדומה לקמפיין האחרון, במקרה זה נשלחות הודעות דוא"ל עם צרופות של Office המכילות מאקרו זדוני שמריץ פקודות PowerShell. אלו בתורן מורידות פוגען מסוג Backdoor. אינדיקטורים רלוונטיים בקישור (trendmicro).