

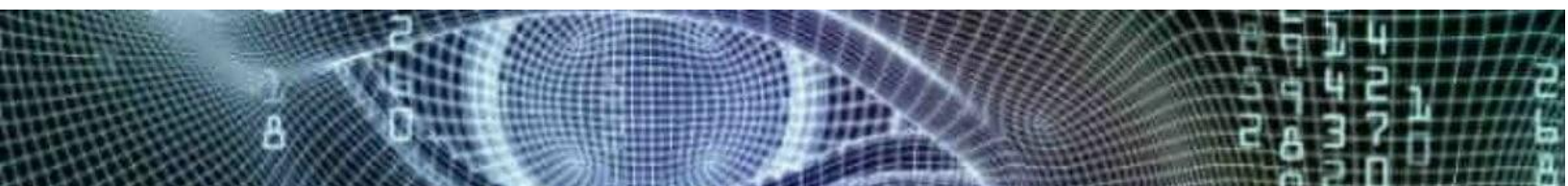
עדכון חדשות סייבר יומי 13/03/2018

בארץ ובעולם

1. נשיא ארה"ב דונלד טראמפ, החליט לעצור את עסקת הרכישה של חברת Qualcomm בידי Broadcom מסיבות של ביטחון לאומי. חברת Broadcom בתגובה מסרה כי איננה מסכימה עם טענה זו של הבית הלבן. Qualcomm טרם הגיבה להחלטה ([cnbc](#)).

טכנולוגיה

2. חוקרי אבטחה מ-McAfee מדווחים על פגיעויות רבות במערכת pacs אשר נפוצה בשימוש של בתי חולים. המערכת מקבלת מידע ממגוון מכשירי דימות ושומרת אותו במאגר נתונים. למערכת יש גרסאות בתשלום וגם גרסאות חינמיות ובשתיהן נמצאו פגיעויות רבות כחלק מרשימת OWASP. החברה דיווחה ליצרנים על הפגיעויות ([mcafee](#)).
3. קבוצת התקיפה APT 15 השתמשה בפוגענים מסוג Backdoor כחלק ממתקפה רחבת היקף נגד הממשל הבריטי וארגונים צבאיים בבריטניה. חוקרי אבטחה מקבוצת NCC מדווחים כי קבוצת התקיפה השתמשה בין היתר בכלי RemoteExec על מנת להתפשט ברשת הארגונית. אינדיקטורים רלוונטיים מצורפים בקישור ([nccgroup](#)).
4. חוקרי אבטחה מ-TrendMicro מדווחים על קמפיין תקיפה בעל מאפיינים דומים לקמפיין שכונה MuddyWater וממוקד לארגונים במזרח התיכון ובמרכז אסיה. טרם אותרה זהותם של התוקפים, אך נחשף כי חלק מן מטרת הקמפיין הינה איסוף מידע למטרות ריגול. אינדיקטורים רלוונטיים מצורפים בקישור ([trendmicro](#)).
5. זוהה קמפיין ספאם חדש המתחזה לאתר Craigslist, אתר המכיל לוח מודעות מקוון, על מנת להפיץ את פוגען הכופרה Sigma. הודעת הדוא"ל שנשלחות בקמפיין מכילות צרופה אשר מורידה סקריפט זדוני ומצפינה קבצים בעמדה המותקפת. אינדיקטורים רלוונטיים מצורפים בקישור ([bleepingcomputer](#)).





6. הגרסה החדשה של דפדפן Mozilla, Firefox 60, אשר תפורסם במאי הקרוב תשבית גישה לשני API כברירת מחדל. ממשקים אלו אפשרו שימוש בחיישני המכשיר על מנת לקבל גישה לנתוני מיקום המשתמש ועוד ([lukaszolejnik](#) ו-[bleepingcomputer](#)).

