



עדכון חדשות סייבר יומי 16/05/2018

בארץ ובעולם

1. חברת הרכבות RENA הודיעה ללקוחותיה על אירוע דלף מידע שנמשך שלושה חודשים. המשתמשים שפרטיהם דלפו הם אזרחי ארה"ב שרכשו כרטיסים לרכבות באירופה באמצעות החברה. בין המידע האישי שדלף: מספר כרטיס האשראי, מספר cvv (הספרות מאחורי הכרטיס), מספר טלפון ועוד ([scmagazine](#) ו-[securityaffairs](#)).
2. ממשלת הולנד הודיעה כי היא מפסיקה את השימוש במוצרי חברת קספרסקי כאמצעי זהירות והיא ייעצה לחברות במדינה לפעול בהתאם. שר המשפטים ההולנדי הודיע לפרלמנט כי הצעד התקבל בעקבות תוכנית תקיפות הסייבר של ממשלת רוסיה אשר בין יעדיה נמצאים ממשלת הולנד ואזרחיה ([reuters](#)).
3. האקרים גנבו מאות מיליוני פסו (עשרות מיליוני דולרים) מבנקים מקסיקניים. הם שלחו מאות בקשות העברת כספים לחשבונות מזויפים שבשליטתם. החקירה בפרשה נמשכת ([reuters](#)).

טכנולוגיה

4. חוקרים ישראלים מחברת Imperva זיהו דרך לנצל את פרוטוקול UPnP כדי להסוות פקטות לטובת מתקפות מניעת שירות מבוזרות מוגברות. החוקרים פרסמו PoC ([imperva](#)).

עדכוני אבטחה

5. חברת VMware פרסמה עדכוני אבטחה למוצר של חברת הבת VeloCloud. במוצר NSX SD-WAN Edge אותרה פגיעות (CVE-2018-6961) ותוקף יכול לנצלה כדי להריץ קוד זדוני מרחוק ולהשתלט על המכונה ([vmware](#)).
6. חברת Red Hat פרסמה עדכוני אבטחה למגוון מוצרים מתוצרתה בעקבות פגיעות (CVE-2018-1111) המדורגת High (cvss 7.5) ב-DHCP. ככל הנראה, מוצרים של חברות SAP ו-IBM גם כן מושפעים מהפגיעות ([redhat](#)). מערך הסייבר הלאומי יפיץ מסמך בנושא זה בהמשך.