



עדכון חדשות סייבר יומי 24/06/2018

בארץ ובעולם

1. מערך הסייבר הלאומי וחברת אבטחת המידע מקאפי הודיעו על תחילת שיתוף פעולה המבוסס על ממשק שיתוף המידע הפתוח של החברה – OpenDXL. הממשק מקשר בין מוצרי אבטחה שונים, כולל מוצרים בפיתוח מקומי וקוד פתוח ([ynet](#)).
2. הבנק המרכזי של הודו הורה לבנקים לשדרג את מערכת ההפעלה XP שרצה על כספומטים במדינה. על פי ההודעה, התהליך יהיה מדורג וכלל הבנקים צריכים לסיים את השדרוג בכל הכספומטים עד יוני 2019 ([documentcloud](#)).
3. אינטל הכריזה על שיתוף פעולה עם שתי חברות סטארט-אפ ישראליות בתחום הסייבר: Duality ו-Enigma. סגן נשיא בקבוצת התוכנה והשירותים ומנהל כללי של חטיבת אבטחת הפלטפורמות באינטל העולמית, שמבקר בישראל לרגל שבוע הסייבר אמר כי הגיע לארץ כי ישראל היא מרכז סייבר משמעותי וחשוב לחברה ([calcalist](#)).

טכנולוגיה

4. חוקר אבטחה דיווח לאפל על פריצה באייפון המאפשרת פריצה למכשיר במצב נעילה. הפריצה התאפשרה, בין היתר, בעקבות הסרת אופציה בטלפון של מחיקתו לאחר 10 ניסיונות כושלים של הקשת סיסמאות. החוקר פרסם PoC ([fortune](#)).
5. חוקרים מאוניברסיטה באמסטרדם הצליחו לחלץ את מפתחות ההצפנה מכמה מעבדים של חברת אינטל. הפגיעות הזו מכונה TLBleed ואיננה משתמשת בטכניקה קשורה לפגיעויות Meltdown ו-Spectre ([theregister](#)).
6. חברת Palo Alto חשפה קמפיין חדש של קבוצת תקיפה המכונה Tick. הקבוצה החליטה לתקוף התקן נייד ספציפי שמיוצר על ידי חברה ביטחונית בדרום קוריאה. התקיפה מנסה להדביק רק מערכות XP ו-Server 2003, וזוהי אינדיקציה לכך שיעדי הקבוצה הן מערכות קריטיות סגורות. אינדיקטורים רלוונטיים מצורפים בקישור ([paloaltonetworks](#)).



עדכוני אבטחה

7. חברת Rockwell פרסמה עדכוני אבטחה לשני בקרים מתוצרתה: CompactLogix ו-Compact GuardLogix. העדכונים מטפלים בפגיעות אותה ניתן לנצל מרחוק ומאפשרת תקיפת מניעת שירות ([ics-cert](#)).

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

