



עדכון חדשות סייבר יומי 17/05/2018

בארץ ובעולם

1. המשרד להגנת הסביבה יחייב השנה 60 מפעלים בעלי סיכון גבוה להטמיע מערכות ואמצעים לגילוי ונטרול מתקפות סייבר בזמן אמת. על פי הערכות, מדובר במפעלים ביטחוניים, בתי זיקוק, תעשיות כימיות ועוד ([globes](#)).

טכנולוגיה

2. מיקרוסופט עצרה את פריסת עדכוני האבטחה של אפריל האחרון למערכות הפעלה Windows 10 עבור מחשבים שמשתמשים ב-SSD של חברות אינטל וטושיבה. זאת לאחר דיווחים על תקלות שונות כתוצאה מהעדכוני. החברה ממליצה למשתמשים לחזור לגרסה הקודמת של מערכת ההפעלה. לא צוין מתי תתוקן התקלה, על פי הערכות היא תתוקן ביוני ([microsoft](#), [bleepingcomputer](#)) בתוך כך, פרסמה החברה Build חדש ל-Windows 10 שכלל תיקונים של פיצורים אבטחתיים וכן דרישה להתאמות נוספות מיצרני אנטי-וירוס ([microsoft](#)).

3. נחשף פוגען חדש של תוקף רוסי, ככל הנראה, אשר אוסף מידע רב מגרסת שולחן העבודה של Telegram. וריאנט של הפוגען אוסף נתוני הזדהות מאתר Steam, פלטפורמה המספקת מגוון שירותים, ביניהם משחקים אונליין וניהל זכויות יוצרים. אינדיקטורים רלוונטיים בקישור ([talos](#)).

4. חוקרים מחברת Pangu Lab איתרו פגיעות שלטענתם משפיעה על 10% מכל אפליקציות iOS. הפגיעות המכונה ZipperDown היא טעות בתכנות שעלולה להוביל במקרים מסוימים להרצת קוד ([zipperdown](#)).

5. גוגל פרסמה כלי של Project Sheild שמספק בחינם הגנה מפני מתקפות מניעת שירות מבזרות (DDoS). הכלי היה זמין עד כה לעיתונאים, ארגוני זכויות אדם וגורמים אחרים ועתה פורסם לציבור הרחב. לפי הדיווח, הכלי מגן כיום על 700 אתרים והצליח להדוף בין היתר את תקיפת בוטנט Mirai על האתר של העיתונאי Brian Krebs העוסק באבטחת מידע ([cnet](#)).





עדכוני אבטחה

6. חברת Cisco פרסמה עדכון אבטחה למגוון מוצרים, הכולל 3 עדכונים קריטיים (cvss 10) עבור Digital Network Architecture (cisco). מערך הסייבר הלאומי יפרסם מסמך בנושא זה בהמשך.

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

