



## עדכון חדשות סייבר יומי 25/03/2018

### בארץ ובעולם

1. מספר ימים לאחר פרסום מצד ממשלת ארה"ב אודות התרעה לניסיונות תקיפה רוסיים כנגד תשתיות מדינה קריטיות, רשות החשמל של מדינת פורטו ריקו דיווחה כי היא חוותה פריצה בסוף השבוע האחרון. לטענתם, לתוקפים לא הייתה גישה למערכת פרטי הלקוחות. ([reuters](#))
2. ראש עיירת אטלנטה, ג'ורג'יה דיווח במסגרת מסיבת עיתונאים כי מערכות העירייה חוו מתקפת כופרה מסוג SamSam, במסגרתה חלקן הוצפנו. לדבריו, מערכות קריטיות בארגון לא הוצפנו וטרם הוחלט האם לשלם את דמי הכופר. ([foxnews](#))
3. לאחר שפורסם בחודש ינואר האחרון כי מאגר הנתונים הלאומי של ממשלת הודו חווה דלף מידע, ארגון IDA המאחסן פרטי זהות ומידע ביומטרי על תושבי הודו נפרץ בשנית. הפגיעות מאפשרת לכל אזרח לקבל מידע על כל תושב הרשום לשירות זה. ([zdnet](#))

### טכנולוגיה

4. לפי דיווחים של MalwareHunterTeam, פוגען הכופרה "AVCrypt" מנסה להסיר את תוכנות האבטחה הקיימות במחשב הנתקף וכן את Windows Update. לאחר מכן הפוגען מצפין את קבצי המשתמש. אינדיקטורים רלוונטים בקישור. ([bleepingcomputer](#))
5. צוות אבטחת המידע של חברת Drupal דיווח על חולשה המוגדרת כקריטית. הפגיעות משפיעה בגרסאות 7 ו-8 של המערכת. על פי הדיווחים, עדכון אבטחה עתיד לצאת החודש גם לגרסאות שאינן נתמכות. ([drupal](#))
6. חודשיים לאחר הפצתו, פוגען הכפרה Rapid שב בגרסה חדשה. בשונה מהגרסה הקודמת, הפוגען יזהה את הגדרות המחשב של הקורבן ובמידה והוא יזהה כי אזור ההגדרות משויך לרוסיה, הפוגען לא יצפין את קבצי המשתמש. אינדיקטורים רלוונטים בקישור. ([bleepingcomputer](#))

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

