עדכון חדשות סייבר יומי 15/01/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

הפרסומים מובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו.

בעולם

1. הרשויות בגרמניה מזהירות מפני עדכוני אבטחה מזויפים לפגיעויות המעבדים Meltdown ו-Spectre. על פי דיווחים שונים, נוצר עמוד דיוג המתחזה לרשות הגרמנית הפדרלית לאבטחת מידע, ומכיל קישור לקובץ ZIP זדוני ובו קובץ הרצה. כאשר הנתקף מריץ את הקובץ, מידע אודותיו עובר לתוקף (blog.malwarebytes).

2. משטרת טייוואן חילקה למנצחי חידון אבטחת מידע התקנים ניידים בהם הותקן פוגען בשם XtbSeDuA.exe. המשטרה קיבלה את ההתקנים מגורם צד ג', אשר בדק אותם על גבי ציוד נגוע ובכך גרם להדבקתם. מאחר והפוגען היה מיושן והשרת אליו הוא אמור לדווח כבר לא קיים, לא נגרם כל נזק. (bleepingcomputer)

טכנולוגי

3. Lenovo הסירה דלת אחורית שנמצאה בקוד הקושחה של חלק מנתביה. מקור הדלת האחורית בתקופה (2004) שבה נתבים אלו היו שייכים לחברת Nortel. החברה פרסמה עדכון קושחה (Lenovo)(Hack Read)

4. האקרים השתלטו על רשומת ה-DNS של BlackWallet.co, אפליקציית ארנק דיגיטלית מבוססת Web עבור המטבע הווירטואלי Stellar Lumen (XLM). ההשתלטות אפשרה לתוקפים הפניית המשתמשים אל אתר מתחזה, וגניבה של מעל 400 אלף דולר (bleepingcomputer).

5. נחשפה אפליקציה בשם Teligram המתחזה ליישום Telegram. לאחר הורדתה למכשיר, האפליקציה המתחזה מתקינה ספריית מודעות ופרסומות במכשיר למטרות רווח (Symantec).

6. חברת Seagate תיקנה פגיעות בקושחה של מוצר מסוג NAS בשם Personal Cloud. הפגיעות הייתה עלולה לאפשר לתוקף גישה בפרוטוקול SSH לציוד, אך דורשת קודם לכן גישה לרשת המקומית (bleepingcomputer).

כתובת לקבלת דואר: משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450811, פקס 03-7450822