עדכון חדשות סייבר יומי 25/02/2018

בארץ ובעולם

1. משרד התחבורה במדינת קולורדו בארה״ב דיווח כי למעלה מ-2,000 מחשבים נדבקו בפוגען הכופרה SamSam. דובר מדינת קולורדו אישר כי כובו מחשבים על מנת למנוע התפשטות רחבה יותר של הפוגען וכי אינם מתכוונים לשלם את הכופר לאור העובדה שבוצעו גיבויים (cbslocal ו-cybersecurity-insiders).
2. לקוחות של בנק JP Morgan הצליחו לגשת לחשבונות של לקוחות אחרים של הבנק כאשר ניסו להתחבר לחשבונם האישי. לפי דוברת הבנק, התקלה הייתה בהיקף קטן וטופלה במהירות ועל פי הדיווחים, לא זוהו העברות כספים חשודות (bloomberg).

טכנולוגיה

3. קבוצת התקיפה OilRig משתמשת בסוס טרויאני חדש המכונה Oopsie. על פי הדיווח, כלי זה שימש בתקיפות נגד מוסדות פיננסיים במזרח התיכון. הפוגען שומר על שרידות באמצעות יצירת קובץ VBS. אינדיקטורים רלוונטיים מצורפים בקישור. מערך הסייבר הלאומי יפרסם בהמשך מסמך בנושא זה (paloaltonetworks).
4. הגרסה הבאה של מערכת ההפעלה Android, Android P, תחסום יישומים לא פעילים, שאינם רצים ברקע, המנסים לגשת למצלמה או למיקרופון (bleepingcomputer).
5. חוקר אבטחת מידע גילה פגיעות ב-PayPal המאפשרת חשיפת ארבעת הספרות האחרונות של אמצעי התשלום וכן מידע נוסף על החשבון בשירות התשלומים. על מנת לנצל את הפגיעות, על התוקף לדעת את חשבון הדוא״ל וכן מספר הטלפון המקושר אליו (karansaini).
6. נציבות הסחר הפדרלית (FTC) מזהירה מפני הורדת יישומי VPN מבלי לברר שהללו מאובטחים. אזהרה זו מגיעה בעקבות דו״ח שפורסם על ידי הסוכנות להגנת הצרכן, לפיו כ-300 יישומי VPN אינם משתמשים בהצפנה ואף דורשים גישה למידע רגיש (consumer).

עדכוני אבטחה

7. Drupal פרסמה עדכוני אבטחה למערכת ניהול התוכן שלה בגרסאות 7 ו-8. חלק מן הפגיעויות דורגו כקריטיות ומאפשרות למשתמשים לא מורשים גישה לתוכן רגיש (drupal).