עדכון חדשות סייבר יומי 07/01/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

הפרסומים מובאים בשם אומריהם ואינם משקפים את עמדת המערך ו/או פעולותיה.

בעולם

1. פרשיית המעבדים: חברות טכנולוגיה רבות נוספות דוגמת Cisco ו-IBM הודיעו כי חלק ממוצריהן חשופים לתקיפות. עדכוני אבטחה ופרטים נוספים בקישורים. מערך הסייבר הלאומי יפרסם מסמך מעודכן אודות הפרשייה (cisco ו-IBM).

טכנולוגי

2. בוטנט חדש מפיץ פוגען כרייה בשם PyCryptoMiner המשתמש ב- pastebin כדי לקבל עדכון לגבי כתובת שרת ה - C&C של התוקף, כאשר השרת המקורי איננו זמין. הבוטנט תוקף מערכות לינוקס והוא מתפשט דרך פרוטוקול SSH. הבוטנט יכול לנצל בנוסף פגיעות מסוימת בשרתי JBoss (F5).

3. חברת Quick Heal זיהתה פוגען פיננסי שתוקף 232 אפליקציות בנקאיות. הפוגען מופץ באמצעות אפליקציה מזויפת של Flash Player ומסוגל לגנוב נתוני הזדהות, מידע מהודעות SMS ועוד (quickheal).

4. זוהה קמפיין תקיפה נגד ארגונים המשתתפים באולימפיאדת החורף בפיונצ'אנג שבדרום קוריאה אשר צפויה להתקיים בפברואר הקרוב. במסגרת הקמפיין נשלח קובץ Word זדוני. מזהים רלוונטיים בקישור (mcafee).

5. 22 אפליקציות של פנס וציוד אחר מפיצות פוגענים דרך חנות האפליקציות הרשמית של גוגל. כך חשפה חברת צ'ק פוינט. לדברי החברה, היקף ההורדות של אפליקציות אלו נע בין 1.5 ל-7.5 מיליון הורדות. צ'ק פוינט הודיעה לגוגל שהסירה את האפליקציות מהחנות הרשמית (checkpoint).

6. חברת טרנד מיקרו איתרה 36 אפליקציות בחנות האפליקציות הרשמית של גוגל שמסוות עצמן כשירותים שונים כולל אבטחת מידע, אך בפועל מעבירות מידע רב לתוקף. גוגל הסירה אפליקציות אלו מהחנות (trend micro).

7. סקר שערכה חברת קספרסקי בשיתוף עם B2B International שכלל כ-1,000 חברות תעשייתיות גילה כי כ-30% מהן חוו התקפת סייבר בשנה האחרונה. 20% מהחברות גילו את התקיפות לאחר מספר שבועות (kaspersky).

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