עדכון חדשות סייבר יומי 27/03/2018

בארץ ובעולם

1. קבוצת האקרים הרוויחה כ-75 אלף דולר באמצעות ניצול פגיעות הקיימת בשרתי Linux (CVE-2013-2618) מעל ל-5 שנים. ההאקרים ניצלו פגיעות זו על מנת להתקין כורה מטבעות וירטואליים מסוג Monero. למידע נוסף אודות החולשה. (nvd, bleepingcomputer)

2. הנציבות הפדרלית לאנרגיה בארצות הברית הגישה כתבי אישום נגד תשעה אזרחים וחברה איראנית בטענה כי ניסו לפרוץ לאלפי אוניברסיטאות ברחבי העולם, לחברות שונות ולמשרדים בממשל האמריקאי. לטענתה, מתקפה זאת החלה משנת 2013. (Washington examiner)

3. מנהיג קבוצת התקיפה העומדת מאחורי הפוגענים Carbanak ו-Cobalt נעצר בספרד. הקבוצה אחראית למתקפות על כ-100 מוסדות פיננסים וגניבת סכום העומד על מיליארד אירו. עיקר תקיפותיה התבססו על שליחת דוא"ל ובו צרופה זדונית. (scmagazineuk)

4. Google הסירה מחנות היישומים שלה כ-22 אפליקציות אשר דווחו כנגועות בפרסומות זדוניות מסוג Guerilla ו-HiddnAd. על פי הדיווחים, מספר ההורדות ליישומים אלו עומד על כ-50,000 הורדות. אינדיקטורים רלוונטיים בקישור. (bleepingcomputer)

טכנולוגיה

5. נחשפה פגיעות במערכת MacOS בגרסה 10.31.1. הפגיעות מאפשרת לתוקף להשיג סיסמאות בכתב טקסט ברור. ניתן לנצל חולשה זו באמצעות פקודות טרמינל. (mac4n6)

6. חוקרים של חברת FireEye מדווחים על קמפיין פישינג חדש המתמקד בגופים ממשלתיים. הקמפיין מופץ באמצעות הודעת דוא"ל אליה מצורף קובץ Word עם פקודת מאקרו אשר מורידה את הפוגען "Sanny". אינדיקטורים רלוונטיים בקישור. (fireeye)