עדכון חדשות סייבר יומי 18/02/2018

בארץ ובעולם

1. האקרים גנבו 340 מיליון רובל (6 מיליון דולר) מבנק רוסי באמצעות מערכת SWIFT. כך נחשף בדו"ח שנתי של הבנק המרכזי של רוסיה. טרם נמסרו פרטים נוספים (reuters).
2. תוכנית איתור פגיעויות של חיל האוויר האמריקני שילמה 12,500 דולר לחוקר שמצא פגיעות בודדת. מדובר בסכום הגבוה ביותר ששילם הממשל האמריקני עבור מציאת פגיעות, אשר נמצאה באתר חיל האוויר ואפשרה וקטור כניסה לרשת מסווגת של משרד ההגנה (eweek).

טכנולוגיה

3. פגיעות במערכת הפעלה iOS מאפשרת מניעת שירות. הפגיעות מנוצלת על ידי שליחת תו בשפה ההודית לאפליקציות מסרים מיידים שונות כולל וואטסאפ, פייסבוק וכן אפליקציות נוספות. הפגיעות רלוונטית לגרסאות רבות ובמקרים מסוימים גם למערכת ההפעלה macOS. על פי הדיווח, אפל תתקן אותה לפני הפצת גרסת מערכת ההפעלה הבאה iOS 11.3 (theverge ו-bleepingcomputer).
4. חוקרים איתרו פוגען אשר מפעיל פקודות מאקרו זדוניות ללא אישור מצד הנתקף. הפוגען מנצל את פגיעות CVE-2017-11882, ברכיב Equation Editor הנמצאת בתוכנת Office, שכבר נוצלה מספר פעמים בעבר על ידי תוקפים. (trustwave ו-threatpost).
5. קבוצת תקיפה המכונה Gold Lowell הצליחה תוך חודש וחצי לסחוט למעלה מ-350 אלף דולר מנתקפים לאחר שהצפינה להם את הקבצים באמצעות וריאנט של פוגען הכופר SamSam. לפי הדיווח, הקבוצה פעילה משנת 2015. אינדיקטורים רלוונטיים מצורפים בקישור (secureworks).

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

עדכון אבטחה

6. אותרה פגיעות קריטית (cvss 9.8) בממסר הגנה של חברת GE בשם D60 Line Distance Relay. תוקף המנצל את הפגיעות, מסוג Buffer Overflow, יכול להריץ קוד זדוני מרחוק. החברה פרסמה עדכון קושחה (gegridsolutions ו-ics-cert).

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