עדכון חדשות סייבר יומי 11/06/2018

בארץ ובעולם

1. מנכ"ל ה-GCHQ לשעבר אמר למשתתפי הכנס InfoSec Europe כי רוסיה מהווה איום גדול על עולם אבטחת המידע וכי היא מבצעת "הדגמות חיות" של יכולותיה המגוונות. בנוסף ציין כי איראן החלה לתקוף בנקים (theregister).

2. פרטיהם של אלפי ישראלים המשתמשים בשירותי ההסעדה סודקסו דלפו לרשת, כך עולה מדיווחים בטוויטר. שם מדליף המידע דיווח כי הוא השיג גישה לשרתי החברה בתור מנהל המערכת. חברת סודקסו מסרה בתגובה כי היא טיפלה בפרצות, וכי מידע אודות כרטיסי אשראי של משתמשים לא הודלף (mako).

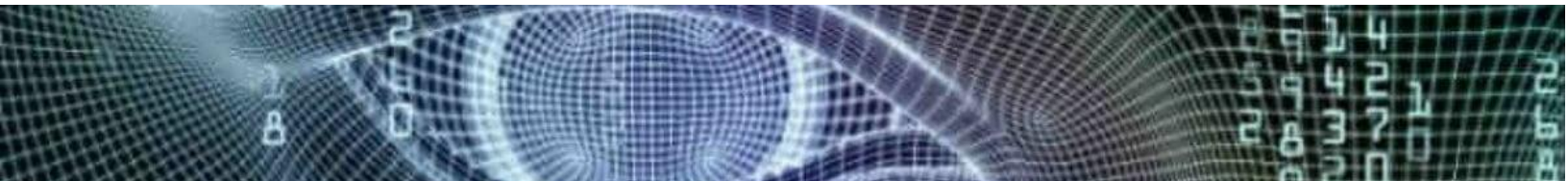
3. בעקבות פריצה לבורסת Cryptocurrency בדרום קוריאה, ערך הביטקוין צנח בכ-10%. מתחילת שנת 2018, צנח המטבע בכ-50%. כמו כן, יתר המטבעות הוירטואליים גם כן איבדו מערכם (cnbc).

טכנולוגיה

4. באירוע המפתחים השנתי של חברת אפל WWDC 2018 , חשפה החברה בין השאר את העדכונים לדפדפן ספארי של החברה. הגרסה החדשה של הדפדפן תחסום ותקפיץ התרעה במידה ואחת התוכנות ברשת תנסה לעקוב אחר הרגלי הגלישה של המשתמשים (cnet).

5. לפי דו"ח של חברת ProofPoint אשר מסכם את הרבעון הראשון של שנת 2018, כ-59% מן המתקפות היו באמצעות סוסים טרויאנים, בשונה משנה שעברה שבה בלטו בעיקר פוגעני הכופר. כמו כן, היקף התקפות באמצעות הודעות דוא"ל עלה ב-20% מהרבעון האחרון של שנת 2017 (proofpoint).

6. חברת Trend Micro מדווחת כי האקרים השתמשו בגרסה חדשה של הפוגען KillDisk אשר פגע באלפי מחשבים הנמצאים בבנק המרכזי בצ'ילה וגרם להסחת דעתם של העובדים על מנת שהם יוכלו להעביר את כספי הבנק באמצעות מערכת העברת הכספים Swift. לפי דיווחים שונים, עיקר מטרתם הייתה שימוש במערכת ה-Swift המקומית של הבנק. כ-9000 מחשבים ו-500



שרתים נהרסו במתקפה זו. אינדיקטורים רלוונטיים בקישור(trendmicro).

7. לפי דיווחים שונים, תוקפים החלו לעשות שימוש בקבצי iqy אשר נפתחים כברירת מחדל ב-Excel ומשמשים להורדת נתונים מהרשת. שיטה זו מצליחה לעקוף את מנועי האנטי וירוס ועלולה לאפשר לתוקף להתקין תוכנות זדוניות על מחשב הקורבן. על מנת להפעיל תוכנה זו, יש לאפשר ל-Excel לבצע פקודת מאקרו (barkly).

עדכוני אבטחה

8. חברת F-secure פרסמה עדכוני אבטחה קריטיים אשר מטפלים בפגיעות במנועי האנטי וירוס הביתיים והארגוניים אשר אפשרה לתוקפים להריץ קוד זדוני מרחוק. הפגיעות היא בתוכנה zip-7 אשר החברה עושה בה שימוש. משתמשים שברירת המחדל היא הגדרת עדכונים אוטומטיים, לא נדרשים לעשות דבר. אחרת, יש להתקין את העדכון באופן ידני מאתר החברה (f-secure ו-bleepingcomputer).