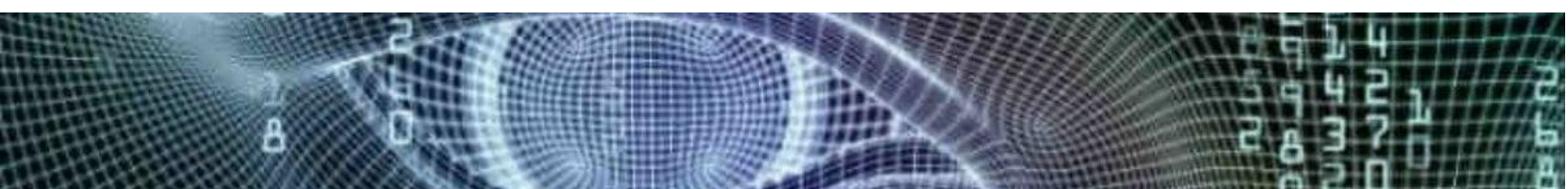
עדכון חדשות סייבר יומי 27/02/2018

בארץ ובעולם

1. שלטונות ארה"ב גזרו על טיילור האדלסטון, תושב ארקנסו, 33 חודשי מאסר בעקבות פיתוח ומכירה של פוגענים. הוא נתפס ע"י ה-FBI והודה באשמה. לפי הדיווח, זהו המקרה הראשון בארה"ב בו נענש אדם על פיתוח פוגענים ולא על השימוש בהם (bleeping computer).
2. פוגען כופר תקף את רשתות משרד מס הכנסה של ניו זילנד והצפין אלפי קבצים. בדיווח לפרלמנט נחשף כי בנובמבר 2017 נשלחה הודעת דיוג, שנפתחה. הפוגען הצפין כ- 3,500 קבצים. לא נמסר באיזה פוגען כופר מדובר ועל פי הדיווח, הקבצים שהוצפנו שוחזרו (reseller).
3. לפי דיווח של אתר "Bad Packets", אתר האינטרנט של העיתון LA Times שימש לכריית מטבעות וירטואליים. התוקפים ניצלו הגדרה לא נכונה כדי לקבל גישה לאתר האינטרנט ולהזריק לתוכן האתר את כורה המטבעות (techrepublic).

טכנולוגיה

4. חוקרי אבטחה של Cisco Talos חשפו פגיעות קריטית ב-Acrobat Reader של חברת Adobe. ניצול של הפגיעות (CVE-2018-4901) מאפשר תקיפה מסוג Buffer Overflow, השתלטות והרצת קוד מרחוק (talosintelligence).
5. דווח כי תוקפים ניצלו שוב פגיעות בשרת WebLogic של חברת Oracle המאפשרת השתלטות מרחוק, על מנת להפעיל כורה מטבע וירטואלי מסוג Monero. מערך הסייבר הלאומי כבר דיווח על תקיפה מסוג זה בעבר. אינדיקטורים רלוונטיים מצורפים בקישור (trendmicro).
6. חברת Visa מדווחת כי זיוף כרטיסי אשראי המבוססים על כרטיס חכם (EMV) ירד ב-70% מאז שהחלו בתי עסק אמריקאים להשתמש במסופים ייעודיים לאמת כרטיס זה במהלך הקניה (visa).
7. חברת אבטחת המידע Trend Micro פרסמה דו"ח המסכם את האיומים על הטלפון החכם לשנת 2017. בדו"ח הוצגו נתונים לפיהם מספר הפוגענים הייחודיים לטלפונים חכמים זינק בלמעלה מ- 400% לעומת שנת 2016 (trendmicro).



8. לאחרונה הועלו מאגרי נתונים חדשים לאתר haveibeenpawned, המאפשר למשתמשים לבדוק האם חשבון משתמש או כתובת דוא"ל שלהם מופיעה במאגרי מידע שדלפו. כמו כן, האתר מאפשר לבדוק האם סיסמה בשימוש המשתמש דלפה בעבר, על מנת למנוע תקיפה מסוג Dictionary Attack, המשתמשת ברשימת הסיסמאות שדלפו כמילון. ניתן למצוא את הכלי בקישור המצורף (troyhunt ו- haveibeenpwned).