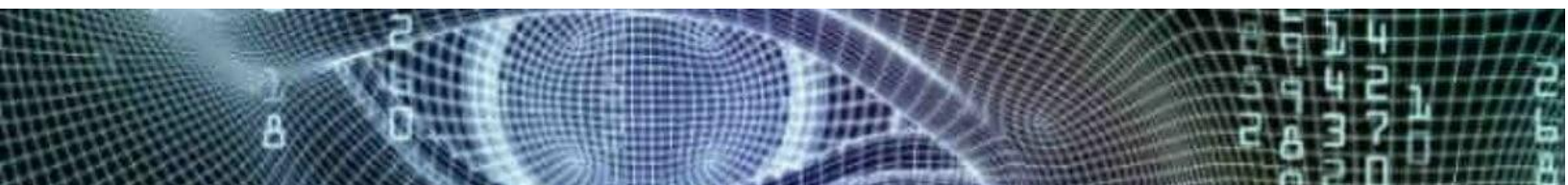
עדכון חדשות סייבר יומי 14/03/2018

טכנולוגיה

1. חוקרים מחברת Palo Alto מדווחים על קבוצת פוגעים למכשירי Android המכונה HenBox. הפוגענים מתחזים ליישומים לגיטימיים ולעיתים אף מורידים יישום לגיטימי על מנת להסוות עצמם. הפוגענים גונבים מידע אישי על המשתמש ועל המכשיר, מפעילים אפשרות של מעקב אחר המכשיר ועוד. אינדיקטורים רלוונטיים מצורפים בקישור (paloaltonetworks).
2. FireEye מדווחים על קמפיין תקיפה נגד גופים ממשלתיים באסיה ובמזרח התיכון. קמפיין זה החל בחודש ינואר 2018 ומיוחס לקבוצה איראנית המכונה Zegros. וקטור התקיפה הראשוני של התוקף הוא דוא"ל המכיל צרופה זדונית. כאשר הנתקף פותח את הצרופה, מופעלת פקודת מאקרו שמורידה פוגען מסוג Backdoor לעמדה הנגועה. אינדיקטורים רלוונטיים מצורפים בקישור (fireeye).
3. פוגענים לכריית מטבעות וירטואליים תקפו 42% מהארגונים ברחבי העולם. כך קובע הדו"ח החודשי של Check Point לחודש פברואר 2018. השירות הנפוץ ביותר שבו השתמשו למטרות אלו הוא CoinHive (checkpoint).
4. מיקרוסופט הודתה כי בשבוע שעבר ביצעה עדכונים שונים למערכת Windows 10 ללקוחות אשר ביקשו להשהות את תהליך העדכונים למערכותיהם. בתגובה לכך, הודיעה החברה כי ניתן להחזיר את מערכת ההפעלה לגרסתה הקודמת (bleepingcomputer).

עדכוני אבטחה

5. פורסם עדכון אבטחה לשרתי Samba המטפל בשתי פגיעויות אשר אפשרו לתוקפים לבצע מתקפת DDoS ולהחליף את סיסמאות המשתמשים, כולל את סיסמת ה-Admin. הפגיעויות רלוונטיות לגרסאות 4.0.0 ומעלה (samba).
6. מיקרוסופט שחררה את עדכון האבטחה החודשי שלה הכולל עדכוני אבטחה ל-75 פגיעויות שונות ש-15 מתוכן מוגדרות כקריטיות. מערך הסייבר הלאומי יפרסם בהמשך מסמך בנושא



(microsoft).

7. Adobe שחררה עדכון אבטחה קריטי לשתי פגיעויות שנחשפו ב– Adobe Flash Player בגרסה 28.0.0.161 למערכות Windows, Mac ,Linux ו-Chrome os (adobe).