עדכון חדשות סייבר יומי 06/05/2018

בארץ ובעולם

1. תקיפת מניעת שירות מבוזרת הפילה ככל הנראה את אתר האינטרנט המרכזי של הבחירות במחוז בארה"ב. על פי הדיווח, האתר שהציג את תוצאות ההצבעות למחוז Knox בטנסי הופל למשך כשעה ולאחר מכן שוחזר. לפי מקורות המעורבים בנושא, הדבר לא השפיע על תוצאות הבחירות משום שהמכונות שספרו את הקולות לא היו מחוברות לרשת (cnet).

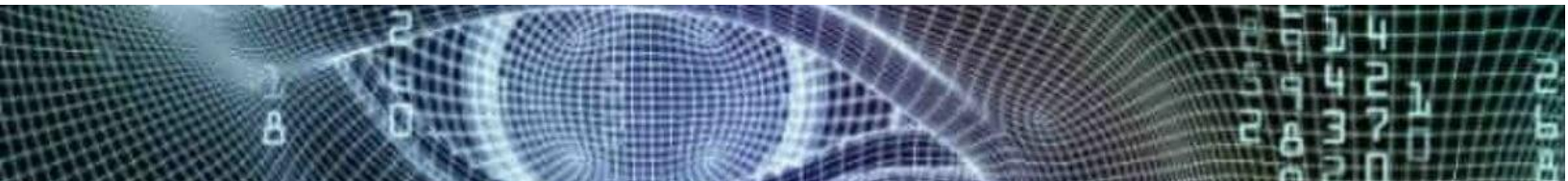
טכנולוגיה

2. מגזין גרמני דיווח על שמונה וריאנטים חדשים של פגיעות Spectre. לפי הדיווח, אינטל הגדירה ארבעה מהם כקריטיים והיא פועלת כדי לתקן זאת. ככל הנראה גם מעבדי ARM חשופים לוריאנטים הללו (techspot).

3. טוויטר הודיעה כי מצאה תקלה באופן שבה סיסמאות נשמרות בלוגים הפנימיים שלה. לפי דיווח החברה, לא נמצאה אינדיקציה לפרצה או לשימוש לרעה בעקבות התקלה. מומלץ לכל המשתמשים, כאמצעי זהירות, לשנות את הסיסמאות (twitter).

4. מאז הפלת אתר WebStresser, תקיפות ה-DDoS באירופה צנחו ב-60%. כך לפי דיווח של חברת Link11. האתר סיפק שירות של תקיפות מסוג זה בתשלום והורד בשבוע שעבר (bleepingcomputer).

5. נחשף קמפיין ריגול שתקף יעדים במזרח התיכון ב-3 שנים האחרונות. הקמפיין המכונה ZooPark, התמקד במכשירי אנדרואיד. וקטור התקיפה הראשונה היה באמצעות ערוצים (channels) בטלגרם וכן באמצעות תקיפות מסוג Watering Hole. אינדיקטורים רלוונטיים מצורפים בדו"ח המלא בקישור (securelist).



6. נחשפו שלוש פגיעויות, אחת מהן קריטית, במכשירי CT מסוג Brilliance של חברת פיליפס. הפגיעות הקריטית (CVE-2018-8857) היא כתוצאה מסיסמאות Hard-Coded בציוד. החברה פרסמה דרכי התמודדות (us-cert).

7. חוקרים מ-Alien Vault זיהו קמפיין חדש לכריית מטבעות וירטואליים שתוקף שרתים באמצעות ניצול פגיעויות. הקמפיין המכונה MassMiner משתמש בפגיעויות ב-SMB, בשרתי אורקל ובשרתי Apache (bleepingcomputer).