עדכון חדשות סייבר יומי 21/05/2018

בארץ ובעולם

1. לפי דוח של חברת FireEye, האקר סיני נחשד בחשד למכירת נתונים אודות 200 מיליון משתמשים יפנים ב-DarkNet. לפי דיווחים, התוקף פרץ ל-50 אתרים ומשם אסף את המידע. הנתונים כוללים שמות, כתובות דוא"ל, מספרי טלפון ועוד (securitybrief).

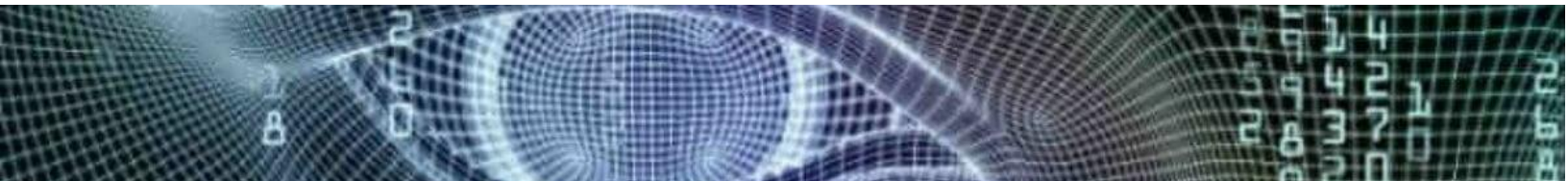
2. סקר שנערך על ידי חברת איפסוס ב-25 מדינות מגלה כי מעל למחצית (52%) מהמשתתפים מודאגים ממצב הפרטיות ברשת, וכי רמת האמון של הגולשים בחברות האינטרנט הינה אפסית. כמו כן, הגולשים מדווחים כי מנועי החיפוש משפיעים יותר מדי על בחירות המשתמשים (calcalist)

3. תושב מקסיקו נידון ל-15 שנות מאסר ותשלומי פיצויים בעקבות ביצוע מתקפות DDoS על מגוון רחב של ארגונים, בינהם רשויות אכיפת חוק, בתי משפט, בנקים, מתחרים עסקיים ועוד. הוא השתמש בשירותי מתקפות מבוזרות בתשלום, ובזמן המתקפה שלח דוא"ל המציע עזרה מטעמו (securityaffairs).

טכנולוגיה

4. חוקרי אבטחת מידע מחברת Eclypsium פרסמו דרך חדשה לניצול פגיעות Spectre. הפגיעות מאפשרת לתוקפים לשחזר נתונים הנמצאים באזור מאובטח במעבד (System Management Mode). Intel בתגובה הודיעה כי העדכון האחרון מגן מפגיעות זו (eclypsium).

5. חברת הנתבים הטיוואנית DrayTek מדווחת כי הם סובלים ממתקפת Zero Day המאפשרת לתוקפים לשנות את הגדרות הDNS במכשיר. החברה אישרה כי אכן נראו ניסיונות לניצול פגיעות זו, בעיקר על מנת לבצע מתקפת Man-in-the-middle ולגנוב פרטים אישיים אודות משתמשים. (draytek)



6. לפי דיווחים של חוקרים מחברת Fortinet, נחשפה גרסה חדשה של הבוטנט Mirai אשר זוהתה לראשונה בשנת 2016. לדבריהם, "Wicked Mirai" סורק פורטים פתוחים ומנצל exploit-ים חדשים על מנת להשתלט על ההתקן הפגיע. אינדיקטורים רלוונטיים מצורפים בקישור (fortinet)

עדכוני אבטחה

7. ארגון Mozilla פרסם עדכון אבטחה קריטי המטפל בפגיעות בThunderbird- תוכנת דואר אלקטרוני המבוססת קוד פתוח. פגיעות זו מאפשרת לתוקף להשתלט על מערכת פגיעה (mozilla).