עדכון חדשות סייבר יומי 08/03/2018

בארץ ובעולם

1. משרד האוצר האמריקני הביע דאגה נוכח הצעת ענקית השבבים Broadcom לרכוש את המתחרה Qualcomm. בעקבות זאת, נדחתה ישיבת בעלי המניות ב-Qualcomm שבה תוכנן לדון בהצעה. יש לציין כי שתי החברות הן אמריקניות, אך על פי ההערכות, החשש של משרד האוצר הוא ממעורבות סינית בתהליך הרכישה (reuters).

טכנולוגיה

2. חוקרי אבטחה זיהו קמפיין תקיפה של הפוגען הפיננסי Gozi ISFB. בקמפיין זה הפוגען מופץ בכמה דרכים: הן בצורה ממוקדת נגד ארגונים ספציפיים והן בצורה רחבה באמצעות הבוטנט Dark Cloud. במסגרת הקמפיין, התוקף משתמש בתשתית רחבה. אינדיקטורים רלוונטיים מצורפים בקישור (talosintelligence).
3. חוקרים מ-Palo Alto מדווחים על פוגען חדש המכונה ComboJack אשר מטרתו גניבת מטבעות וארנקים וירטואליים. הפוגען מחליף את כתובת היעד ובכך מעביר אליו את סכום הכסף. הוא מופץ באמצעות הודעות דוא"ל המכילות צרופה זדונית. אינדיקטורים רלוונטיים מצורפים בקישור (palo alto).
4. הודלפו קודי תקיפה (Exploits) עבור תקיפת מניעת שירות מבוזרת מוגברות. לאחרונה תקיפה מסוג זה הפכה לנפוצה בשימוש בשרתי Memcached. במסגרת אחת התקיפות האחרונות נרשם שיא בהיקף רוחב פס, 1.73Tb. באחד מהקודים שפורסמו צוינו 17 אלף שרתים פגיעים (thehackernews).
5. חברת אבטחת המידע Corero חושפת Kill Switch המיועד לחסום תקיפות מניעת שירות מבוזרות מוגברות המשתמשות בשרתי Memcached. עוד טוענת החברה כי במסגרת המתקפות הללו התוקפים גונבים או משנים מידע בשרתים הפגיעים (corero).

6. פורסם כלי פומבי לניתוח פוגענים מסוג Sandbox בשם Any.Run אשר מסוגל לבצע ניתוח דינמי של קבצים. לדוגמה קבצים אשר דורשים מהנתקף הפעלת פקודות מאקרו (ghacks ו-any.run).

עדכוני אבטחה

7. Cisco פרסמה עדכון אבטחה המטפל ב-22 פגיעויות שונות. חלק מן הפגיעויות מוגדרות כקריטיות ועלולות לאפשר לתוקף להשתלט על המערכת. אחת מהפגיעויות הקריטיות היא במוצר ההזדהות ACS (cisco).