עדכון חדשות סייבר יומי 05/02/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

הפרסומים מובאים בשם אומרם ואינם משקפים את עמדת המערך ו/או פעולותיו.

בארץ ובעולם

1. משרד המשפטים האמריקני הודיע כי הגיש כתב אישום נגד פיטר לבשוב, אשר תפעל את הבוטנט Kelihos שהדביק למעלה מ-100 אלף מכשירים כדי להפיץ פוגענים. הוא יעמוד לדין ביום שישי הקרוב בעקבות מימוש הסכם הסגרה בין ספרד לארה"ב (reuters).

2. צעיר יפני בן 17 נעצר לאחר שפיתח פוגען אשר גונב סיסמאות של משתמשים בעת העברת מטבעות וירטואליים מתוכנת ארנק בשם MonaCoin. על פי צו המעצר, הצעיר פיתח אפליקציה שמתחזה לשירות חיפוש מטבעות וירטואליים בזמן אמת, אך בפועל היא שימשה כאמור למטרות זדוניות (hackread).

טכנולוגי

3. הבוטנט Smominru משתמש בפגיעות EternalBlue שפורסמה על ידי קבוצת Shadow Brokers ובה השתמשו בין השאר במתקפת WannaCry. על פי דיווחים שונים, הבוטנט כבר השתלט על למעלה מחצי מיליון מכשירים כדי לכרות מטבע וירטואלי מסוג Monero (proofpoint).

4. משרד התקשורת פרסם לאחרונה שימוע לציבור לפיו ספקיות סלולר יחוייבו לבצע ניוד מספרים באמצעות אימות דו שלבי בהודעת SMS. זאת בתגובה לפניות שהגיעו למשרד לפיהן "קיימים גורמים המזייפים התקשרות למספר הטלפון הייעודי ומשתלטים על מספר טלפון לא להם" (gov.il).

5. לאחרונה אותר בוטנט חדש המחפש פגיעויות בציוד IoT . באחת הפגיעויות , CVE-2017–17215, נעשה שימוש בעבר בבוטנט Satori. אחד הדומיינים שאותרו בתשתית זו, משויך לשרת של המשחק הפופולרי GTA San Andreas, ועלול לשמש לפגיעה במשתמשים רבים (radware).

6. חוקרי חברת McAfee חושפים פרטים חדשים אודות קמפיין תקיפה סביב אולימפיאדת החורף בפיונגצ'אנג, שתחל ביום שישי הקרוב. אחת הדגימות שאותרה היא של פוגען המכונה Gold Dragon ומסוגל לגנוב מידע מהגורם הנתקף, הכולל תצורת רשת ופרטי תקשורת נוספים. אינדיקטורים רלוונטיים מצורפים בקישור (mcaffe).