עדכון חדשות סייבר יומי 01/02/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

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

בעולם

1. המטבעות הווירטואליים בשווי של למעלה מחצי מיליארד דולר, שנגנבו מבורסת Coincheck, אותרו בחשבון שבעליו אינו מזוהה. ארגון NEM, יוצר המטבעות מסוג XEM שנגנבו מהבורסה הנ"ל, דיווח כי בעלי החשבון מנסים לפצלם ולהעבירם ל- 6 בורסות שונות, בהן ינסו לממש את הרווח מהגניבה. (reuters).

טכנולוגי

2. חוקרי חברות אבטחת מידע זיהו דגימות של פוגענים המנסים לנצל את פגיעויות המעבדים Meltdown ו-Spectre. ככל הנראה מדובר בדגימות בשלבי ניסוי, שמבוססות על קוד להוכחת יכולת (PoC) שפורסם ברשת (bleepingcomputer).

3. חברת AMD דיווחה כי ביצעה שינויים בסדרות שבבים עתידיות, החל מהסדרה Zen 2, כדי להגן עליהן מהאפשרות לניצול פגיעות דוגמת Spectre. מנכ"לית החברה, ליסה סו, סיפרה כי עבור הווריאנט הראשון של הפגיעות, החברה עדיין פועלת עם שותפים לטובת פרסום עדכונים רלוונטיים (zdnet).

4. אותר פוגען כופר חדש בשם GandCrab המופץ באמצעות שני Exploit Kits שונים. אינדיקטורים רלוונטיים מצורפים בקישור (malwarebytes).

5. החל מה-1 למרץ 2018, Windows Defender ומוצרי Microsoft נוספים יחלו להסיר תוכנות המציגות התנהגות חשודה שנועדה לגרום למשתמשים לרכוש את התוכנות הללו. כדי להתכונן לשינוי זה, Microsoft מעדכנת את קריטריוני הערכת התוכנה שלה (csoonline) (Microsoft).

6. פורסם כלי חינמי חדש בשם AutoSploit המבצע סריקה על מנת למצוא האם ציוד המחובר לאינטרנט חשוף לפגיעויות שונות. במידה ומתגלית חשיפה כזו, הכלי תוקף את הציוד הפגיע (motherboard).

7. משפחת פוגענים מסוג Backdoor המכונה Comnie ממשיכה את פעילותה כנגד ארגונים במזרח אסיה. על פי הדיווח, משפחת הפוגענים אותרה בשנת 2013 על ידי חברת אבטחת המידע Sophos. הקמפיין הנוכחי כולל תקיפות נגד מגזרי הביטחון, הממשל, טכנולוגיה ותעשיית החלל. אינדיקטורים רלוונטיים מצורפים בקישור (paloaltonetworks).