עדכון חדשות סייבר יומי 06/02/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

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

בארץ ובעולם

1. משטרת בריטניה בשיתוף פעולה עם ה-Europol וחברות נוספות השביתה את הכלי "Luminosity Link". הכלי, שנמכר ב-78 מדינות שונות, אפשר לתוקפים להשתלט על מחשבי הקורבנות מרחוק, להפעיל מצלמה, להקליט הקשות, לשחזר סיסמאות ועוד (NCA,europol).

2. מאז אוגוסט 2015, המשרד הממונה על אבטחת מידע בבריטניה קנס 104 חברות בסך 8.7 מיליון לישי"ט בעקבות הפרת תקנות הנוגעות לאבטחת מידע (helpnetsecurity).

טכנולוגי

3. חוקר אבטחת מידע פרסם כי שינה שלוש תקיפות שפורסמו ע"י קבוצת ה-Shadow Brokers באפריל 2017 והתאים אותם לביצוע תקיפות אמינות נגד כל גרסאות Windows החל מגרסת Windows 2000. הפגיעויות ניתנות להפעלה כמודולים של Metasploit. מי שהתקין את עדכוני האבטחה הרלוונטיים, MS-17-010, אשר פורסמו במרץ 2017 ו/או את גרסאותיהם עבור מערכות הפעלה שאינן נתמכות, מוגן מפני תקיפות. המערך יפרסם בהמשך מסמך בנושא (github, bleepingcomputer).

4. חוקרי חברת אבטחת המידע Qihoo דיווחו כי איתרו בוטנט חדש שהחל בימים האחרונים לתקוף מכשירים בעלי מערכת הפעלה Android. על פי הדיווח, בשלב זה מטרת הבוטנט היא לכרות מטבעות וירטואליים מסוג Monero (bleepingcomputer).

5. נחשף עדכון תוכנה מזויף ל-Flash Player אשר ברגע הכניסה של המשתמש לאתר העדכון, מורד קובץ הרצה אשר מנצל את כוח המעבד על מנת לכרות מטבע וירטואלי (bleepingcomputer).

6. חברת האנליטיקה Mixpanel הודיעה ללקוחותיה כי אחד מכלי החברה אסף בטעות נתונים שהוזנו בשדה הסיסמא בעקבות כשל שנמצא בערכת פיתוח התוכנה (SDK). החברה הודיעה כי הכשל תוקן וכל הפרטים שנאספו נמחקו (reddit, bleepingcomputer).

עדכוני אבטחה

7. חברת סיסקו עדכנה כי קיימים מוצרים נוספים החשופים לפגיעות הקריטית שאותרה ב- Adaptive Security Appliance שעליה פורסם בסוף ינואר האחרון. עוד עדכנה החברה כי קיימים וקטורי תקיפה נוספים היכולים לנצל את פגיעות זו. עדכון למסמך שהוציא המערך יתפרסם בהמשך (cisco).

8. התוסף Grammarly הבודק שגיאות איות ודקדוק בזמן שימוש בדפדפני Chrome ו- Firefox היה חשוף לפגיעות אשר אפשרה לתוקפים לקבל מידע על היסטוריית הגלישה של המשתמש, מסמכים ועוד. על פי הדיווח, העדכון האחרון של הדפדפנים מטפל בפגיעות זו (nakedsecurity).