עדכון חדשות סייבר יומי 11/02/2018

בארץ ובעולם

1. דיווחים שונים ברוסיה מעידים על כך שבמתקן למחקר גרעיני בעיר סרוב ביצעו כרייה של מטבעות וירטואליים. הרשויות המקומיות פתחו בחקירה ועצרו כמה מדענים שהשתמשו במחשב-על כדי לכרות מטבעות ביטקוין (wccftech ו-bloomberg).
2. דליפת המידע מחברת Equifax הייתה ככל הנראה גדולה יותר ממה שהחברה דיווחה בתחילת החשיפה. על פי בכירה בוועדה בסנאט האמריקני, רשומות נוספות נגנבו, כגון רישיון נהיגה ומספר הזיהוי לצורכי מס, אך לדברי החברה מספר הקורבנות נותר בעינו (wsj, cnn ו-zdnet).
3. תקלה טכנית ב-FW של עיתון מקומי בקליפורניה השאירה 19 מיליון רשומות אודות בוחרים חשופות במשך שבועיים. על פי הדיווח, האקרים הצליחו לאתר את המאגר, הצפינו את המידע ודרשו מהעיתון כופר. העיתון סירב לשלם ומחק את המאגר (ibtimes).

טכנולוגיה

4. לראשונה נחשף פוגען לכריית מטבעות וירטואליים התוקף מערכות ICS. לפי חברת Radiflow, הפוגען תקף את רשת ה-OT של מתקן לטיהור מים באירופה והשרתים שנפגעו היו בעלי מערכת הפעלה Windows XP והריצו תוכנה של GE Digital בשם CIMPLICITY SCADA (securityweek).
5. חברת PhishMe מדווחת כי לאחרונה אותרו קמפיינים של דיוג מבוססי מיקום. הקמפיינים הקימו עמודי דיוג שונים שהבחינו בין צפון אמריקה ואוסטרליה לבין אירופה (helpnetsecurity).
6. חוקרי חברת Imperva זיהו התקפות שהשתמשו בפגיעות DoS באתרי WordPress. הפגיעות פורסמה באתר המערך (bleepingcomputer).
7. מפתח הצפנה לפוגען הכופר Cryakal הועלה לאתר No More Ransom בזכות מאמץ משותף של הרשויות בבלגיה וחברת Kaspersky. הפוגען נפוץ בעיקר ברוסיה, אך ככל הנראה גם תוקף יעדים נוספים באירופה (zdnet).

עדכוני אבטחה

8. אינטל פרסמה גרסה חדשה לעדכוני אבטחה מעודכנים שייתנו מענה לפגיעות Spectre. בשלב זה העדכונים הם למעבדי Skylake בלבד. ככל הנראה, עדכונים נוספים צפויים לצאת בקרוב (intel).
9. שתי פגיעויות קריטיות אותרו בשבבי ה-Wi-fi תוצרת Broadcom המצויים במחשבים ניידים מסדרת ThinkPad של Lenovo. החברה פרסמה עדכון אבטחה (lenovo).