עדכון חדשות סייבר יומי 08/02/18

עדכון זה ניתן כשירות ומבוסס על לקט פרסומים גלויים.

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

בעולם

1. בספטמבר האחרון דיווח מנהל מחלקת ביטחון המולדת (DHS) בארה"ב כי רוסיה ניסתה לחדור למערכות מחשוב של 21 מדינות בארה"ב כדי להשפיע על תוצאות מערכת הבחירות האחרונות. היום אישרה מנהלת מחלקת אבטחת הסייבר ב-DHS כי אכן אירע ניסיון תקיפה מסוג זה, אך הוא צלח רק במספר קטן של מדינות (nbc).

2. פושעי סייבר גנבו מטבעות וירטואליים מסוג Ethereum בשווי של 5,000 דולר באמצעות התחזות לבכירים בתחום הסייבר ואבטחת המידע. ההתחזות בוצעה באמצעות קריאה למשתמשים ברשת טוויטר לתרום לקהילת Ethereum (bleepingcomputer).

טכנולוגי

3. חברות אבטחת המידע Bitglass ו-Cylance זיהו זן חדש של פוגען כופר בשם Gojdue הנמכר ב-Darknet. על פי הדיווח, פוגען זה מסוגל לחמוק מרוב מנועי האנטי וירוס, ביניהם גם מנגנוני ההגנה לשירותי הענן הפופולריים Google Drive ו- Microsoft Office 365. מתוך 67 מנועי אנטי וירוס הנמצאים בשירות Virus Total, רק בודדים זיהו את הפוגען כזדוני (globenewswire).

4. חוקר אבטחת מידע מדווח כי שירות ה-VPN הפופולרי Hotspot Shield אשר אמור לאפשר אנונימיות ברשת האינטרנט, עלול להדליף את כתובת ה-IP המקורית של המשתמש, ואף פרטים רגישים נוספים (paulosyibelo ו-zdnet).

5. לאחרונה אותרה גרסה חדשה של פוגען הכורה מטבע וירטואלי מסוג Monero, אשר תוקף מחשבי Mac. הפוגען הופץ באמצעות הדבקה של אתר MacUpdate. אינדיקטורים רלוונטיים מצורפים בקישור (malwarebytes).

6. קוד המקור עבור רכיב מרכזי במערכת ההפעלה iOS עבור מכשירי אייפון פורסם ב-GitHub. לפי הדיווחים, הקוד לרכיב "iBoot" אחראי על אתחול מערכת ההפעלה באופן מהימן. הקוד שפורסם הוא עבור גרסה ישנה של המערכת, אך ייתכן כי ניתן לנצל חלקים ממנו לתקיפת גרסאות חדישות יותר (motherboard).

עדכוני אבטחה

7. עדכון האבטחה האוטומטי האחרון של WordPress (4.9.3) גורם לשגיאות. בשל כך פרסמה החברה עדכון אבטחה חדש (4.9.4) אותו יש לעדכן בצורה ידנית. כמו כן, על מנת שהמשתמש יוכל בעתיד לקבל עדכוני אבטחה, עליו להיות מעודכן לגרסה האחרונה של הפלטפורמה (wordpress).