עדכון חדשות סייבר יומי 09/04/2018

בארץ ובעולם

1. לפי סקר עולמי מקיף שערכה חברת PwC, 36% מהמשתתפים הישראלים בסקר דיווחו כי ארגונם חווה מתקפת סייבר בשנתיים האחרונות. שיטת התקיפה הנפוצה ביותר בארגונים בישראל היא דיוג (Phishing). בנוסף, 42% מהארגונים בישראל מדווחים כי ישנה נכונות גדולה לדווח על התקפות סייבר לרשויות המדינה, לעומת 28% מבין משיבי הסקר העולמי (themarker).
2. פרטים אישיים על כ-130,000 אזרחים פינים הודלפו. המידע הודלף בעקבות פריצה לאתר של ארגון המספק עצות עסקיות ליזמים. מדובר באירוע דלף המידע הגדול ביותר בהיסטוריה של המדינה (securityaffairs ו- viestintavirasto).

טכנולוגיה

3. חוקרים מדווחים כי נחשף דף המתחזה לתהליך הורדת הדפדפן Google Chrome. לדבריהם, בעת לחיצה על כפתור ההורדה יורד קובץ ChromeSetup.exe והרצתו פותחת תוכנה זדונית בשם InstallCore (bleepingcomputer).
4. חוקר אבטחה מדווח כי ניתן לבצע מניפולציה על Gmail. לפי בדיקה שערך, התגלה כי Gmail מתעלמת מסימנים כגון נקודה (״.״) בכתובות משתמשיה. בעקבות זאת, משתמשים בעלי שם משתמש דומה מקבלים הודעות אשר אינן שייכות להם ועלולים להיחשף למידע אישי אודות משתמשים אחרים (jameshfisher).
5. לפי דיווחים של חברת Netskope, נחשף פוגען חדש התוקף כספומטים בשם ATMJackpot. פוגען זה אותר בהונג קונג בסוף מרץ 2018 ונראה כי הוא עדיין בשלבי פיתוח (netskope).
6. נחשף וריאנט חדש של פוגען Agent Tesla אשר מופץ באמצעות מסמכי Word המכילים פקודת מאקרו זדונית. הפוגען מסוגל לבצע צילומי מסך, להקליט הקשות מקלדת וכן לגנוב נתוני הזדהות. אינדיקטורים רלוונטיים מצורפים בקישור (fortinet).

7. חוקרים מחברת Malwarebytes מדווחים כי מצאו פגיעות בתוכנת ההצפנה בה משתמש פוגען הכופר LockCrypt. באמצעות פגיעות זו יוכלו הנפגעים מפוגען זה לשחזר את קבציהם מבלי לשלם את סכום הכופר (malwarebytes).

עדכוני אבטחה

8. נחשפה פגיעות קריטית בפלטפורמת Auth0 אשר משמשת אלפי ארגונים כאמצעי זיהוי והתחברות של המשתמשים לחשבונם האישי באתרים ובאפליקציות. החולשה מאפשרת לתוקף לעקוף את אימות הכניסה באמצעות כתובת הדוא"ל או אמצעי הזיהוי של המשתמש. מומלץ להתקין את הגרסאות החדשות של ה-SDK (auth0.js 9 and Lock 11) (auth0).