22 באפריל 2020
כ"ח בניסן תש"פ
סימוכין: ב-ס-1065

מתווה תקיפה חדש לקבוצת ה-FIN7 APT

תקציר

1. על-פי מידע שהגיע משותפים, קבוצת ה-FIN7 APT החלה לפעול באמצעות מתווה תקיפה חדש.
2. במסגרתו, הקבוצה שולחת לארגונים בדואר התקני USB זדוניים בתור "מתנות", במטרה להשיג גישה לרשתות של הארגונים ולגנוב מהן מידע רגיש.

Modus operandi

1. קבוצת התקיפה FIN7, הפועלת בדרך-כלל נגד ארגונים עסקיים באמצעות הודעות דיוג בדוא"ל, החלה לאחרונה לפעול בדרך נוספת של שליחת התקני USB זדוניים בדואר פיזי. על-פי אזהרה שפרסם ה-FBI, ההתקנים נשלחים לבעלי תפקידים בחברות מטורגטות ובייחוד בהנהלה הבכירה (EM), במחלקת טכנולוגיית המידע (IT) או במחלקת משאבי אנוש (HR), כחלק מחבילות הכוללות לעיתים כרטיסי מתנה (gift cards) או צעצועים.
2. לאחר שהקורבן מחבר את ההתקן למחשבו, מוזרקות פקודות להורדה והרצה של backdoor המכונה GRIFFON. הכונן הזדוני מוגדר כך שיחקה הקשות מקלדת שישגרו פקודת PowerShell לשליפת נוזקה משרת הנשלט על-ידי התוקף. לאחר מכן, התקן ה-USB מתקשר עם שרתי ה-C&C של הנוזקות.
3. התקן ה-USB משתמש במיקרו-בקר ATMEGA32U4 המתוכנן לחקות מקלדת USB. מאחר ומחשבי PC מאשרים מקלדות USB כברירת מחדל, ברגע שהם מתחברים בפעם הראשונה ה-keyboard emulator יכול באופן אוטומטי להזריק פקודות זדוניות. שתי פקודות PowerShell מובילות להצגת תיבת הודעות מזויפת המזהירה מפני שגיאות בהתקן ה-USB.

לאחר מכן, קוד ה-PowerShell מריץ קוד JavaScript נוסף האוסף מידע אודות המערכת ומוריד נוזקות נוספות.

4. לאחר שנאסף המידע אודות היעד, קבוצת התקיפה מבצעת תנועה רוחבית בחיפוש אחר הרשאות מתקדמות. המידע נשלח לשרת ה-C&C.

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.