ISRAELDEFENSE
יום ראשון, י"א תמוז התשע"ו
17.07.2016

הורדתם Pokemon Go? ייתכן ומדובר בכלי ריגול מתחזה

דו"ח מחקר של חברת White-Hat חושף פרטים על כלי ריגול שמשתמשים בכסות מזוייפת למשחק הפופולרי Pokemon GO

עמי רוחקס דומבה | 13/07/2016

youtube.com

Pokemon GO היא אפליקציית משחקים העובדת על "מציאות רבודה" למציאת פוקימונים על פי מיקומו הגיאוגרפי של המשתמש וסביבת הטבע שלו. לדוגמה, אם המשתמש נמצא בסביבת מים כמו נחל אז הוא יקבל פוקימוני מים, אם הוא יהיה בסביבת פארק, אז הוא יקבל פוקימוני יער וכו'.

הרעיון של משחק זה הוא תפיסתם של פוקימונים שונים, כאשר נמצא פוקימון אז מכשיר הטלפון ירטט להודיע כי אותר פוקימון בסביבה. האפליקציה נמצאת גם בחנות האפליקציות של Apple וגם של Google , אך אינה זמינה להורדה לכלל המשתמשים אלא לחנויות הוירטואלית במדינות: ארה"ב, אוסטרליה וניו זילנד כרגע.

"בעקבות ההתלהבות הגדולה שנוצרה סביב האפליקציה בימים האחרונים נצפו אפליקציות אשר מתחזות לאפליקציה המדוברת אשר מהוות "סוס טרויאני" על המכשיר", נכתב בדו"ח של חברת White-Hat שמספקת שירות סייבר למגזר העיסקי, הביטחוני והממשלתי. "ה-APK של האפליקציה הזדונית מכיל DroidJack RAT אשר מאפשר שליטה מלאה על המכשירים הסלולריים של אותם אנשים שמורידים את האפליקציה. כרגע נצפו רק זיופים למערכת ההפעלה אנדרואיד."

קצת על DroidJack

DroidJack RAT – תוכנת "שליטה מרחוק" למחשבים וסמארטפונים כמו כל RAT אחר המיועד למכשירים בעלי מערכת הפעלה אנדרואיד.

ה – RAT מאפשר לתוקף להשתלט על מכשירו של הקורבן, לראות את הודעות ה -SMS שלו, קבצים בסמארטפון וגם שליטה על GPS. היישום מאפשר גם גישה לתיבת הדוא"ל של הקורבן (בין היתר הארגונית), כולל אפשרות לציטוט שיחות ואפשרות להתחבר למצלמת מכשיר הקורבן מרחוק.

איך ניתן להתגונן מפני האפליקציה הזדונית?

1. לא להתקין אפליקציות ממקורות חיצוניים, אלא רק מתוך "Google Play Store" :

1.1. נכנסים להגדרות המכשיר, לוחצים על לשונית "אבטחה" ומורידים את הסימון ב "מקורות לא ידועים":

1.2. לחסום פופ-אפ בהגדרות הדפדפן, דרך הגדרות הדפדפן > הגדרות מתקדמות > חסום פופאפ.

ניתן גם להתשמש בתוכנת Clueful שבודקת כל אפליקציה ואת ההרשאות שנתתם לה. לאחר ההתקנה, כאשר המשחק החדש מבקש גישה לכל רשימת אנשי הקשר, המיילים והתעבורה, Clueful תסמן את האפליקציות שבהן יש חשד מבחינת אישורי השימוש ותזהיר את המשתמש. תוכלו גם לדרג אפליקציות בעצמכם, ולהזהיר משתמשים אחרים מאפליקציות מזיקות.
[לינק להורדה]

READ NE

פרויקט ת'