G Data press release 2016

Pokemon Go: Backdoor descoperit intr-o aplicatie de Android

Sfaturile specialistilor de la G Data va vor mentine in siguranta la vanatoare de Pidgey si alti Pokemoni.

Bucuresti (Romania) 14.07.2016

Adorabilele creaturi Pokemon din anii '90, s-au intors. Aceste mici animale japoneze au revenit sub forma unui joc virtual-realitate pentru smartphone-uri. Infractorii incearca sa profite de pe urma popularitatii acestui joc nou-nout si ii jefuiesc pe jucatorii nerabdatori care nu mai vor sa astepte ca jocul sa fie lansat oficial: a fost descoperita cel putin o versiune malware a aplicatiei. Intr-o retea de partajare de fisiere, a fost descoperita o versiune a programului de instalare al aplicatiei, ce contine un un modul control de la distanta pentru dispozitivele cu Android. Se pare ca aplicatia legitima a fost reambalata impreuna cu componente malware folosind un instrument numit "DroidJack". Instrumentul in sine pare legitim pentru dezvoltatori, dar in acest caz, a fost folosit pentru a adauga un fragment de malware numit "AndroRAT". Utilizatorii G DATA sunt protejati de aplicatia malware ce este detectata ca "Android.Trojan.Kasandra.B".

Analiza efectuata de expertii G Data si sfaturile acestora pot fi gasite pe blogul G Data Software: https://blog.gdatasoftware.com/2016/07/28734-pokemon-go-catch-em-all-but-not-at-any-cost

Sfaturi pentru a ramane in conditii de siguranta in timpul jocului:

- Instalati aplicatii numai din surse de incredere! Aplicatia malware a fost distribuita in afara magazinului oficial Google Play Store. Acest lucru inseamna ca aplicatia poate fi instalata numai in cazul in care este permisa, in mod explicit, instalarea de aplicatii din surse necunoscute.
- Protejati-va dispozitivul mobil cu o solutie de securitate! Un dispozitiv mobil, la fel ca si calculatorul de acasa, trebuie sa fie echipat cu o solutie completa de securitate pentru a contracara atacurile digitale.
- Verificati permisiunile solicitate de catre o aplicatie in timpul instalarii! Aplicatiile nelegitime vor incerca sa asigure permisiuni suplimentare. Aplicatiile care solicita permisiunea de a utiliza serviciile care pot costa bani sau care solicita accesul la înregistrare audio trebuie sa fie intotdeauna examinate cu atentie. Versiunile curente de Android va vor cere confirmarea permisiunilor si atunci cand aplicatia ruleaza pentru prima data.
- Fiti atenti atunci cand sunteti la vanatoare de Pokemoni, atat online cat si offline! Lumea reala poate fi un loc periculos - mai ales daca sunteti in urmarirea unui exemplar rar de Pokemon aflat in mijlocul unei strazi circulate.

- Ganditi mai intai, apoi mergeti la vanatoare! Nici un joc nu este perfect si poate contine erori minore. In cazul in care un Pokemon se afla in apropierea unei zone abrupte, este mai bine sa renuntati decat sa va expuneti la riscuri. De asemenea, evitati vanatoarea de Pokemoni in "zone dubioase" , niciodata sa nu excludeti faptul ca poate exista un hot in viata reala, care intentionează sa va fure telefonul.
- Ganditi-va la intimitatea voastra! Jocul are nevoie de coordonatele GPS ale telefonului sau tabletei pentru a functiona. Datele culese in acest proces sunt disponibile pentru dezvoltatori. Fotografiile din joc, surprinse de ecranul telefonului si postate pe Internet, pot divulga locatia curenta.
- Evitati cheltuielile nedorite! In multe jocuri puteti cumpara obiecte din joc cu bani reali, iar acestea va pot crea un avantaj in interiorul jocului. Astfel de achizitii pot scapa de sub control, daca sunt neverificate. Va recomandam sa dezactivati in totalitate achizitiile din aplicatii sau cel putin sa le monitorizati cu atentie si sa verificati facturile la sfarsit de luna.