Domoljubni radio

Portal domoljubnog radija

Instalirali ste ove aplikacije? Odmah ih brišite jer kradu podatke i upadaju u vaše Facebook i Google račune

Mario Strinavić · Friday, February 7th, 2020

Aplikacije za pametne telefone mogu biti izuzetno korisne, ali mogu i izazvati velike probleme za korisnike. Tvrtka za računalnu sigurnost VPNpro, objavila je izvještaj u kojem ističe kako su pronašli cijeli niz aplikacija za Android, kojima je jedina zadaća prevariti korisnike i ukrasti im vrijedne podatke.

Iako su aplikacije u međuvremenu uklonjene s Google Play Storea, već su bile prikupile više od 382 milijuna preuzimanja.

Stručnjaci za sigurnost otkrili su da su 24 aplikacije koje su identificirali (od prognoze vremena do kalendara i kamere), od korisnika tražile širok pristup različitim podacima, što može biti opasno jer ugrožava korisnikovu sigurnost i privatne podatke. Tako su aplikacije mogle uspostavljati pozive, fotografirati pa čak i snimati video i audio bez ikakvog znanja korisnika.

Aplikacije koje bi svakako trebalo prestati koristiti i obrisati sa svog pametnog telefona (ako ih imate) su:

Sound Recorder
Super Cleaner
Virus Cleaner 2019
File Manager
Joy Launcher
Turbo Browser
Weather Forecast
Candy Selfie Camera
Hi VPN, Free VPN
Candy Gallery
Calendar Lite
Super Battery

Hi Security 2019
Net Master
Puzzle Box
Private Browser
Hi VPN Pro
World Zoo
Word Crossy!
Soccer Pinball
Dig it
Laser Break
Music Roam
Word Crush

Naime, stručnjaci su primijetili da, osim što neovlašteno špijuniraju svoje korisnike, sve te podatke šalju u Kinu. Tko točno stoji iza njih, nije jasno jer se radi o aplikacijama različitih autora.

No, to nije sve

Stručnjaci iz Trend Microa identificirali su još devet aplikacija (koje su preuzete gotovo pola milijuna puta), a koje se potiho spajaju na sumnjive servere i mogu preuzeti do 3000 različitih malwarea među kojima su i neki koji se, bez znanja korisnika, ulogiravaju u njihove Facebook i Google račune i šire dalje.

Ako imate instaliranu neku od ovih aplikacija:

Shoot Clean–Junk Cleaner, Phone Booster, CPU Cooler
Super Clean Lite — Booster, Clean & CPU Cooler
Super Clean — Phone Booster, Junk Cleaner & CPU Cooler
Quick Games — H5 Game Center
Rocket Cleaner
Rocket Cleaner Lite
Speed Clean — Phone Booster, Junk Cleaner & App Manager
LinkWorldVPN
H5 gamebox;

obavezno ju uklonite sa svog uređaja i promijenite lozinke na Google i Facebook profilima. Također, provjerite je li vam aktivan Play Protect skener koji je dio Google Play Storea kako bi vas na vrijeme upozorili o sumnjivim aplikacijama.

A onda još malo...

Istraživači iz Cofense Phishing Defense Centra također su primijetili pojačanu zarazu trojancem Anubisom i to upravo uređaja koji koriste Android. Radi se o veoma nezgodnom malwareu koji je originalno korišten za kibernetičku špijunažu i krađu bankovnih podataka.

Anubis, pojašnjavaju iz CPDC-a, u potpunosti preuzima kontrolu nad uređajem, krade podatke, snima telefonske razgovore, a može čak i zaključati podatke i tražiti otkupninu od vlasnika uređaja. Skriva se u privitku e-mail poruke koji izgleda poput računa. Kad korisnik otvori privitak, pojavljuje se poruka koja od njih traži aktivaciju "Google Play Protecta". No umjesto da zaista aktivira taj zaštitni mehanizam, korisnik zapravo daje mnoštvo privola koje malwareu omogućuju preuzimanje kontrole nad njegovim uređajem.

Malware cilja uređaje s operativnim sustavom Android 4.0.3 ili novije, a na popisu se našlo čak 250 ciljanih aplikacija među kojima su većinom bankarske aplikacije, blockchain aplikacije, aplikacije za trgovanje kriptovalutama, ali i Amazon. Puni popis možete pogledati ovdje.

U svakom slučaju, korisnici bi trebali biti izuzetno oprezni kad instaliraju aplikacije, čak i one s Google Play Storea, ali i kad otvaraju različite e-mailove koji im stižu s nepoznatih adresa, piše Zimo.

This entry was posted on Friday, February 7th, 2020 at 6:59 pm and is filed under Nekategorizirano You can follow any responses to this entry through the Comments (RSS) feed. Responses are currently closed, but you can trackback from your own site.