G Data press release 2012

Noul tip de malware merge la cumparaturi

MMarketPay.A comanda automat aplicatii platite

Bucuresti (Romania) 01.08.2012 – Expertii de la G Data Security Labs au descoperit un nou tip de malware pentru Android care descarca aplicatii platite fara stirea utilizatorului de smartphone sau tableta. Malware-ul este ascuns in aplicatii false, de genul GO Weather, Travel Sky sau E-Strong File Explorer si este distribuit catre diverse website-uri chinezesti si catre provideri de aplicatii mobile. Pentru moment, atacatorii vizeaza clientii China Mobile, un important provider international de aplicatii mobile. Troianul foloseste accesul la magazinul de aplicatii al furnizorului si apoi descarca si instaleaza malware sau aplicatii platite. G Data SecurityLabs atentioneaza ca acesta se poate raspandi in toata Europa, inclusiv in Romania.

Infractorii cibernetici folosesc malware-ul MMarketPay.A ca pe o noua forma de a face bani din infractiuni online. In prealabil, s-au concentrat pe furtul de date personale, spionaj sau trimit-erea de SMS-uri cu suprataxa. Acum ei izbutesc sa patrunda pentru prima data in magazinul de aplicatii al unui furnizor. Pentru a face asta, malware-ul schimba numele punctului de acces al dispozitivului mobil (APN) si il conecteaza la China Mobile. Punctul de acces al unui smartphone sau al unei tablete este uzual folosit de provideri pentru a furniza update-uri de sistem, de ex-emplu. Aici, troianul intercepteaza mesajul de confirmare si trimite un raspuns printr-un server special.

Malware-ul poate astfel accesa magazinul de aplicatii al China Mobil fara sa se inregistreze, apoi cumpara si instaleaza orice aplicatie pe cheltuiala victimei.

"Am observat dezvoltarea unui nou si profitabil model de business pentru infractorii cibernetici. Odata cu MMarketPay.A a fost lansata pe piata o noua specie de aplicatii daunatoare gandita in scopul de a sustrage bani", **explica Ralf Benzmuller, sef al G Data SecurityLabs.** ***"In consecinta, noi ne gandim ca este foarte posibil ca o versiune modificata a acestei aplicatii va aparea in Europa si ii va viza pe clientii furnizorilor de aplicatii mobile europeni."***

Captura de ecran: Atacatorii au infectat aceasta aplicatie pretinsa a fi GO Weather cu MMarketPay.A, care apoi va putea fi cumparata fara ca utilizatorul sa stie.

Sfaturi de securitate pentru utilizatorii de Android:

- Folositi o solutie eficienta de securitate care sa va protejeze dispozitivele mobile.
- Instalati intotdeauna cele mai recente update-uri pentru a tine sistemul de operare, programele si aplicatiile folosite complet actualizate. Acestea inchid bresele de securitate pe care infractorii ar putea sa le exploateze pentru a ataca.
- Descarcati aplicatii doar din surse de incredere, precum Google Play sau website-urile producatorilor. Atunci cand alegeti aplicatiile acordati atentie modului in care acestea au fost descarcate. Cu cat o aplicatie a fost mai descarcata, cu atat este mai de incredere. Trebuie totodata sa verificati ce autorizatii are aplicatia. Fiti atenti cu aplicatiile care pot, de exemplu, initia apeluri telefonice sau pot trimite mesaje text. In general, ar trebui sa instalati doar aplicatii de care aveti cu adevarat nevoie.
- Ignorati mesajele cu origini necunoscute primite pe smartphone-uri si tablete. Utilizatorii care doresc sa fie in siguranta, pot verifica online ce mesaje sunt reale sau pot suna la serviciul de relatii cu clientii al furnizorului.
- Verificati factura telefonica. Daca aceasta include incarcari suplimentare de servicii pe care nu le-ati folosit, ati putea fi victima unei fraude.

-###-