G Data press release 2013

Infractiuni cibernetice 3.0: aplicatii periculoase vizeaza tranzactiile bancare

G Data a descoperit presupuse certificate de securitate pentru dispozitive mobile cu OS Android

Bucuresti (Romania) 29.04.2013 - Infractorii cibernetici vizeaza in mod curent dispozitivele mobile cu OS Android pentru a sustrage TAN-urile (numere de autentificare ale tranzactiilor) si PIN-urile conturilor online bancare, prin intermediul unei autentificari pe email presupuse a fi din partea Postbank, care incearca sa-i convinga pe utilizatori sa instaleze un „certificat SSL". Atunci cand utilizatorul acceseaza link-ul din email de pe smartphone sau tableta, ajunge pe un website care furnizeaza un certificat SSL insotit de instructiuni de instalare. Odata instalata, aplicatia, care insinueaza ca securizeaza tranzactia de online banking, spioneaza TAN-ul si PIN-ul si le trimite atacatorilor. Aceasta actiune permite infractorilor sa manipuleze tranzactiile de online banking si sa deturneze banii spre alte conturi. Utilizatorii solutiei G Data MobileSecurity 2 sunt protejati impotriva acestei amenintari.

Smartphone-urile si tabletele sunt printre dispozitivele utilizate in cadrul procesului de autentificare bidirectional. Ca parte a acestui proces, banca trimite un SMS cu un numar de tranzactie (TAN) receptionat pe smartphone sau tableta. Asta inseamna ca aceste dispozitive sunt tinte pretioase pentru infractorii 3.0, deoarece multi utilizatori nu au instalata o solutie de securitate pe dispozitivele mobile.

In acest caz, atacatorii pretind ca lucreaza în cadrul departamentului de suport clienti al Postbank si trimit milioane de email-uri prin care ii indemna pe destinatarii sa instaleze presupuse „certificate SSL". In locul unei aplicatii de securitate acestia instaleaza, de fapt, un program malware care directioneaza instant toate TAN-urile catre infractori.

Exemplul unui email pretins a fi de la Postbank:

Cand e accesat de pe un dispozitiv mobil, link-ul inclus in textul mail-ului conduce la un website incarcat cu un banner Postbank, care furnizeaza aplicatia de securitate falsa si

instructiunile de instalare. Daca website-ul este accesat de pe un computer, utilizatorii primesc doar un mesaj care precizeaza ca certificatul a fost instalat cu succes.

Screenshot cu instructiunile de descarcare si instalare a aplicatiei:

Odata ce aplicatia a fost instalata, utilizatorului i se solicita introducerea numarului de cont si PIN-ul. Suplimentar, programul solicita o serie de autorizatii, care ii permit sa acceseze, printre altele, mesajele SMS primite. Atacatorii sunt astfel capabili sa sustraga datele necesare pentru efectuarea tranzactiilor de online banking si sa manipuleze transferul bancar.

De data aceasta, cei vizati au fost clientii Postbank, in viitorul apropiat, cei vizati ar putea fi clientii altor banci, din alte tari europeane, atentioneaza specialistii de la G Data. Scenariul se poate repeta, in conditii similare, iar cei prinsi nepregatiti se vor numara printre victime.

-###-