DNSC&ING Bank: Persoanele juridice, vizate de hackeri cu mesaje false de actualizare a datelor si apeluri false în numele ANAF

Directoratul National de Securitate Cibernetica (DNSC) si ING Bank avertizeaza asupra a doua tentative de frauda care vizeaza tot mai intens persoanele juridice - atacuri de tip phishing care solicita actualizarea urgenta a datelor, precum si apeluri false (spoofing) în care infractorii sustin ca suna din partea Agentiei Nationale de Administrare Fiscala (ANAF).

"Scopul infractorilor este obtinerea unor câstiguri financiare, prin manipularea potentialelor victime sa îsi introduca date bancare pe site-uri false sau sa efectueze transferuri de bani. În ambele situatii, atât paginile clona, cât si conturile bancare în care ajung banii sunt controlate integral de atacatori. În acest scenariu, victimele primesc e-mailuri, SMS-uri sau mesaje pe retele sociale care par sa provina de la banci, autoritati sau institutii publice, fiind îndemnate sa îsi "confirme" sau "actualizeze" informatiile personale. Atacatorii folosesc un ton urgent în mesaje ("contul va fi blocat" sau "nu vei mai avea acces la produsele si serviciile detinute") si includ elemente grafice care par legitime, întrucât reproduc identitatea vizuala a entitatii pe care o imita", precizeaza Directoratul, într-un comunicat de presa transmis, miercuri, AGERPRES.

Conform expertilor, odata cu accesarea link-urilor suspecte incluse în mesaje, potentialele victime sunt redirectionate catre site-uri false. Astfel, site-ul clona arata similar cu cel al entitatii în care atacatorii se deghizeaza, fiind creat special pentru a colecta informatii sensibile, precum date bancare, parole sau coduri de securitate (OTP), si care vor fi ulterior folosite pentru acces neautorizat la conturi sau initierea de tranzactii frauduloase.

"În ING, investim masiv în sisteme avansate de monitorizare a tranzactiilor, capabile sa identifice în timp real activitati suspecte si abateri de la comportamentul obisnuit al utilizatorilor. În paralel, acordam o importanta majora preventiei, prin informarea clientilor cu privire la cele mai frecvente tipuri de fraude digitale. Ne dorim sa consolidam parteneriatul dintre banca si client, întrucât majoritatea tentativelor de frauda se bazeaza pe manipularea utilizatorilor pentru a-si divulga singuri datele bancare sau pentru a autoriza transferuri de bani. Este esential ca fiecare client sa înteleaga faptul ca nicio banca nu va trimite, sub nicio forma, mesaje sau e-mail-uri care sa contina link-uri (URL-uri) prin care sa solicite introducerea userului, parolei, codurilor de autentificare sau datelor cardului. Preventia este cruciala, deoarece în majoritatea cazurilor de frauda, sansele de recuperare a banilor sunt extrem de reduse", a declarat, în comunicatul citat, Alin Becheanu, Head of Faud Monitoring & Prevention, ING Bank România.

În acelasi timp, a fost descoperita o campanie de apeluri telefonice false în numele ANAF.

"Acest tip de frauda este în prezent unul dintre cele mai active în România si se bazeaza pe tehnici de inginerie sociala. În unele cazuri, infractorii din spatele apelurilor încearca sa convinga potentiala victima sa introduca date de autentificare la conturile de internet banking pe site-uri frauduloase, ori chiar sa efectueze tranzactii în conturi controlate direct sau indirect de atacatori. În alte instante, atacatorii încearca sa obtina acces de la distanta pe dispozitivul victimei. Numitorul comun în aceste initiative frauduloase este folosirea identitatii vizuale si a numelui ANAF, pentru a convinge victimele sa transfere bani, sa ofere date bancare sau acces la conturile lor. De regula, schema frauduloasa debuteaza cu un apel telefonic fals din partea ANAF. De fapt, în spatele apelului sunt infractori online bine instruiti, care actioneaza asemanator unui operator de call center. Apelantul comunica potentialei victime faptul ca are "o returnare de taxe", "o rambursare de impozit" sau "o suma de recuperat" si o îndeamna sa acceseze un link", explica specialistii în securitate cibernetica.

Şi în acest caz, urmatorul pas al atacatorului poate varia, în functie de context.

În unele cazuri solicita instalarea unei aplicatii de control la distanta pe dispozitivul victimei, sub pretextul ca va primi banii mai rapid. Prin instalarea acestor aplicatii de acces la distanta, precum AnyDesk sau AirDroid, infractorii obtin acces direct la telefon si la datele bancare. Acestia se conecteaza în contul victimei, initiaza tranzactii, pot seta dispozitive noi pentru autorizare sau pot modifica limitele de plata. În final, banii sunt transferati rapid în conturi ale unor carausi de bani sau în alte conturi controlate de atacatori, folosite pentru a îngreuna depistarea traseului acelor sume. În alte situatii, atacatorii încearca sa determine victimele sa transfere chiar ele soldurile disponibile într-un cont fals de rambursare, controlat de atacatori", noteaza DNSC.

Expertii vin cu o serie de recomandari pentru utilizatori, pe care acestia ar trebui sa le respecte pentru a evita aparitia problemelor: sa nu actioneze în graba si sa nu ia decizii financiare în timpul unui apel telefonic; sa nu instaleze aplicatii de control de la distanta la solicitarea unor persoane necunoscute; sa nu introduca date de autentificare sau date bancare în urma unor apeluri sau indicatii telefonice; sa închida apelul si sa verifice informatiile exclusiv pe canalele oficiale ale institutiilor; sa tasteze manual adresele site-urilor în browser si sa nu urmeze indicatii primite telefonic.

"Infractorii din mediul online nu mai sunt neaparat acei hackeri cu gluga pe care îi vedem adesea în filme. De cele mai multe ori sunt persoane care pot fi persuasive, care au abilitati de comunicare si, uneori, experienta în relatia cu clientii. Ei se folosesc de tehnici de inginerie sociala si de scenarii atent gândite în prealabil, care se bazeaza puternic pe generarea emotiei pozitive ("ai o suma de recuperat") sau negative ("contul tau va fi blocat"), la care adauga de fiecare data urgenta, pentru a face potentiala victima mai putin atenta la detalii, mai putin doritoare sa faca anumite verificari si susceptibila sa actioneze impulsiv. Trebuie sa vorbim cât mai mult despre aceste povesti pe care ni le servesc infractorii, la telefon, prin SMS, email sau social media, astfel încât sa ne construim treptat reflexe de securitate pentru a evita astfel de capcane", a subliniat Mihai Rotariu, manager Directia Comunicare, Media si Marketing din cadrul DNSC.

Reprezentantii Directoratului mentioneaza faptul ca, pentru a recunoaste tentativele de frauda online si a nu le cadea victima, este imperios necesar ca utilizatorii sa se informeze constant despre acestea din surse de încredere, precum site-ul DNSC si sectiunea de securitate de pe site-ul ING Bank.