Kampanjat “Phishing”

Të gjithë ne, pavarësisht profesionit tonë të përditshëm, përdorim së paku një e-mail adresë. Prandaj, shumica e sulmuesve e përdorin atë për qëllime mashtruese siç janë vjedhja e kredencialeve me qëllim të fitimit të qasjes në kompjuterin ose telefonin tuaj; e-mail të tillë njihen si e-mail për “phishing”. Ekzistojnë dy lloje të kampanjave dashakeqe:

1. Ato që iu dërgohen masivisht subjekteve, në target audienca më të mëdha – të cilat mund të zbulohen lehtësisht;
2. E-mail të targetuar, të cilat bëhen posaçërisht për palët pranuese, nganjëherë edhe në gjuhën e tyre amtare dhe me informacione të sakta.

Fushatat masive

Le t’ia hedhim një sy e-mail të mëposhtëm jo të targetuar:

Në këtë e-mail ka shenja të shumta të rrezikut:

1. Adresa "from" (nga) është qartazi e bërë për qëllime të phishing;
2. Formati dhe struktura e mesazhit janë jo të mira;
3. Afati nënkupton ndjesi të urgjencës për t'iu mashtruar juve për të klikuar linkun sa më parë;
4. Mbajtja e kursorit mbi linkun ekspozon domen krejtësisht jo relevant:
   http://boutiquesque.com/cl/?
5. Në footer ka referencë të Microsoft që në këtë rast është shkruar gabimisht dhe nuk është relevante në këtë kontekst;
6. Nuk ka informacione të kontaktit.

Ne rekomandojmë që thjesht të injoroni tentativat e tilla dhe të bllokoni adresën e dërguesit ose të fshini mesazhin.

"Spear Phishing"

Kampanjat e njohura si "spear phishing" janë të rrezikshme pasi që ato mund t'i duken mjaft të vërteta madje edhe njohësve të mirë të teknologjisë. Sulmuesit e avancuar mund të paraqiten si subjekte pasi të kenë grumbulluar sa më shumë informacione që të munden. Për shembull, akterët e huaj mundohen të dërgojnë e-mail në gjuhën amtare të pranuesit me shtojca ose linqe që lidhen me profesionin ose interesat e tyre.

Për fat të keq, protokolli i email-it nuk është i sigurt; sulmuesit mund të ju dërgojnë e-mail nga adresat legjitime të një subjekti (procedurë e njohur si "email spoofing"). Megjithatë, në këto raste, ofruesit e njohur të shërbimeve të e-mail si Microsoft Outlook dhe Gmail i zbulojnë automatikisht ato dhe i klasifikojnë shumicën e tyre si spam/junk. Prandaj, sulmuesit mundohen t'i shmangen e-mail të falsifikuar dhe në vend të kësaj përdorin domene, të cilat janë pothuajse identike me origjinalin.

Për ta kuptuar më mirë këtë teknikë, do të përshkruajmë një skenar tjetër të rastit, i cili zakonisht përdoret në mënyrë të targetuar, që duket sikur është dërguar nga banka jonë:

From: Raiffeisen Bank Kosovo <swift.confirmation@bank.com>
Sent: Monday, November 25, 2019 8:15 AM
To: Recipients <swift.confirmation@bank.com>
Subject: Raiffeisen SWIFT Confirmation

Pershendetje,

Bashkangjitur gjeni SWIFT konfirmimin e transferit te realizuar nga banka.

Download Document Or View Document Online

Cdo te mire!

[redacted]

Premium Banking Relationship Officer

Raiffeisen Bank Kosovo J.S.C

Rrasat e Koshares, Shatërvan, Prizren 20000, Kosova

Në shikim të parë e-mail duket të jetë legjitim – i njëjti është në gjuhën amtare të klient pranues, përmban nënshkrimin i cili është i ngjashëm me atë që përdorim ne, dhe gjithashtu përdor domenin "*bank.com*", i cili në fillim mund të mos duket i dyshimtë, por në fakt është; mos harroni se ne nuk përdorim asnjëherë domen tjetër përveç atij zyrtar "*raiffeisen-kosovo.com*". Gjithashtu, e-mail të tillë janë gati gjithmonë të papritur, kështu që ju duhet të jeni tepër të kujdesshëm përpara se të vazhdoni më tutje.

Si gjithmonë, mënyra më e mirë për të arritur në përfundim është të mbani kursorin mbi linkun (linqet) dhe t'i kushtoni rëndësi domenit i cili referohet. Nëse nuk është i njëjtë me domenin tonë zyrtar, atëherë ka shumë gjasa të jetë mashtrues dhe si i tillë duhet të përcillet (të bëhet forward) në adresën siguria@raiffeisen-kosovo.com ose në Shërbimin për Klientë në numrin +383 (0)