Phishing kampanje

Svi koristimo barem jednu email adresu, bez obzira na naše svakodnevno zanimanje. Stoga je većina vektora napada koristi iz lažnih razloga zbog krađe akreditiva radi pristupa vašem računaru ili telefonu; takvi e-mailovi poznati su kao „phishing“ e-mailovi. Postoje dve vrste zlonamernih kampanja:

1. One koje se masovno šalju entitetima sa mnogo većom ciljnom publikom - koje se lako mogu otkriti;
2. Ciljani e-mailovi koji su izrađeni posebno za strane koje primaju zahtev, ponekad čak i na njihovom maternjem jeziku i sa tačnim informacijama.

Masovne kampanje

Pogledajmo sledeći neciljani e-mail:


From: Message Centre <3610sa@makerspacect.com>
Sent: Friday, September 13, 2019 12:39 PM
To: [redacted]
Subject: ResetPassword Friday, September 13, 2019

Office-365

Hi [redacted]

Due to request that you created ID: 3610
We need to confirm you as a owner of this email [redacted]
This validation valid until 13 September, 2019.

Confirm Ownership here for [redacted]

Thanks
mirosoft Corporation. All rights reserved. 2019 .

U ovom email-u postoji veći broj ključnih crvenih zastavica:

1. Adresa „od“ je jasno sumnjiva;
2. Poruka je loše oblikovana i strukturisana;
3. Rok podrazumeva osećaj hitnosti da vas prevari da kliknete na link što je pre moguće;
4. Prelazak kursorom preko linka otkriva potpuno nerelevantni domen:
   http://boutiquesque.com/cl/?
5. Reference u podnožju stranice se odnose na Microsoft koji je pogrešno napisan i nije relevantan u ovom kontekstu;
6. Nisu uključeni nikakvi kontakt podaci.

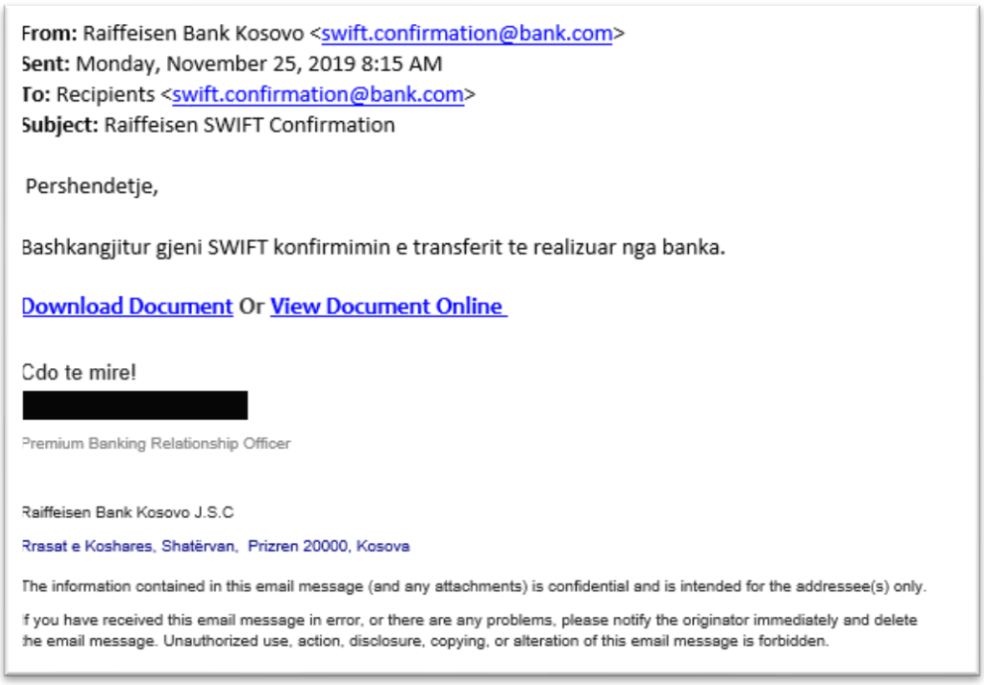
Preporučujemo da jednostavno zanemarite takve slučajeve i blokirate adresu pošiljaoca ili potpuno izbrišete poruku.

Spear Phishing

Kampanje poznate pod imenom „spear phishing“ opasne su jer mogu izgledati sasvim realno čak i ljudima koji se razumeju u tehnologiju. Napredni napadači će se predstavljati kao entiteti nakon što prikupe što više informacija. Na primer, strani glumci pokušaće da pošalju e-mailove na maternjem jeziku primaoca sa prilozima ili linkovima prema njihovoj struci ili interesima.

Nažalost, protokol e-maila nije zaštićen dizajnom; napadači vam mogu slati e-mail-ove sa legitimnim adresama entiteta (poznato kao „lažiranje e-mail-a“). Međutim, u tim će slučajevima ugledni pružaoci usluga e-maila, poput Microsoft Outlooka i Gmail-a, automatski otkriti i klasifikovati veliku većinu njih kao neželjenim poštama. Stoga napadači pokušavaju da izbegnu lažni e-mail i umesto toga koriste domene koji su gotovo identični izvornom.

Da bismo najbolje razumeli ovu tehniku, navešćemo drugi scenarijo koji se obično koristi ciljano i izgleda da će biti poslat iz naše banke:



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

The information contained in this email message (and any attachments) is confidential and is intended for the addressee(s) only.

If you have received this email message in error, or there are any problems, please notify the originator immediately and delete the email message. Unauthorized use, action, disclosure, copying, or alteration of this email message is forbidden.

Na prvi pogled, e-mail izgleda legitimno - na maternjem je jeziku primaoca klijenta, sadrži potpis sličan onome koji koristimo, a koristi i domen „*bank.com*“ koji se možda neće smatrati sumnjivim na početku, ali zapravo jeste; možda je dobro vreme za podsetnik da nikada ne koristimo bilo koji drugi naziv domena osim službenog „*raiffeisen-kosovo.com*“. Pored toga, takvi su e-mail-ovi gotovo svaki put neočekivani pa biste trebali biti posebno oprezni pre nego što nastavite.

Kao i uvek, najbolji način da dođete do zaključka je da postavite kursor na linkove i obratite pažnju na domen na koji se poziva. Ako se ne podudara sa našim službenim domenom, najverovatnije je lažni i eventualno ga treba proslediti na siguria@raiffeisen-kosovo.com ili korisničkoj službi na+383 (0)38 222 222.