Iknedēļas ziņas
Sagatavotas 21.02.2017.
Numurs 2017/5

Turpinās uzņēmēju apkrāpšanas gadījumi

Kāda uzņēmuma grāmatvede saņēma uz darba e-pastu vēstuli, it kā no uzņēmuma vadītāja par steidzamu maksājuma veikšanu. Sūtītais e-pasts izrādījās viltots, jo tam nebija nekāda saistība ar uzņēmuma vadītāju.

Uzņēmums ziņoja par krāpniecību un lūdza CERT.LV šo e-pasta ziņojumu pārbaudīt. Krāpnieki nebija pacentušies šo vēstuli sūtīt no uzņēmuma adreses, bet no kādas speciāli pielāgotas yandex e-pasta adreses.

Krāpnieciskā teksta paraugs:
"Mums nepieciešams veikt SEPA maksājumus €13,805(Euros) uz Angliju. Kādu informāciju jums ir nepieciešams saņemt šo izdarīt tagad?"

Šīs vēstule ir daļa no vēstulēm, kas tiek izsūtītas ar mērķi izkrāpt uzņēmēju naudas līdzekļus. Uz šādu krāpniecisko e-pastu nav ieteicams atbildēt.

Kārtējais "Everest-trade" krāpniecības upuris

Arī šonedēļ pie CERT.LV vērsies vīrietis, kas cietis no krāpniecības nelicenzētājā "Everest trade" akciju tirdzniecības platformā. Tirdzniecība ar akcijām sākusies ar nelielu summu, 500 dolāriem, taču ar laiku vīrietis ticis pārliecināts investēt arvien vairāk.

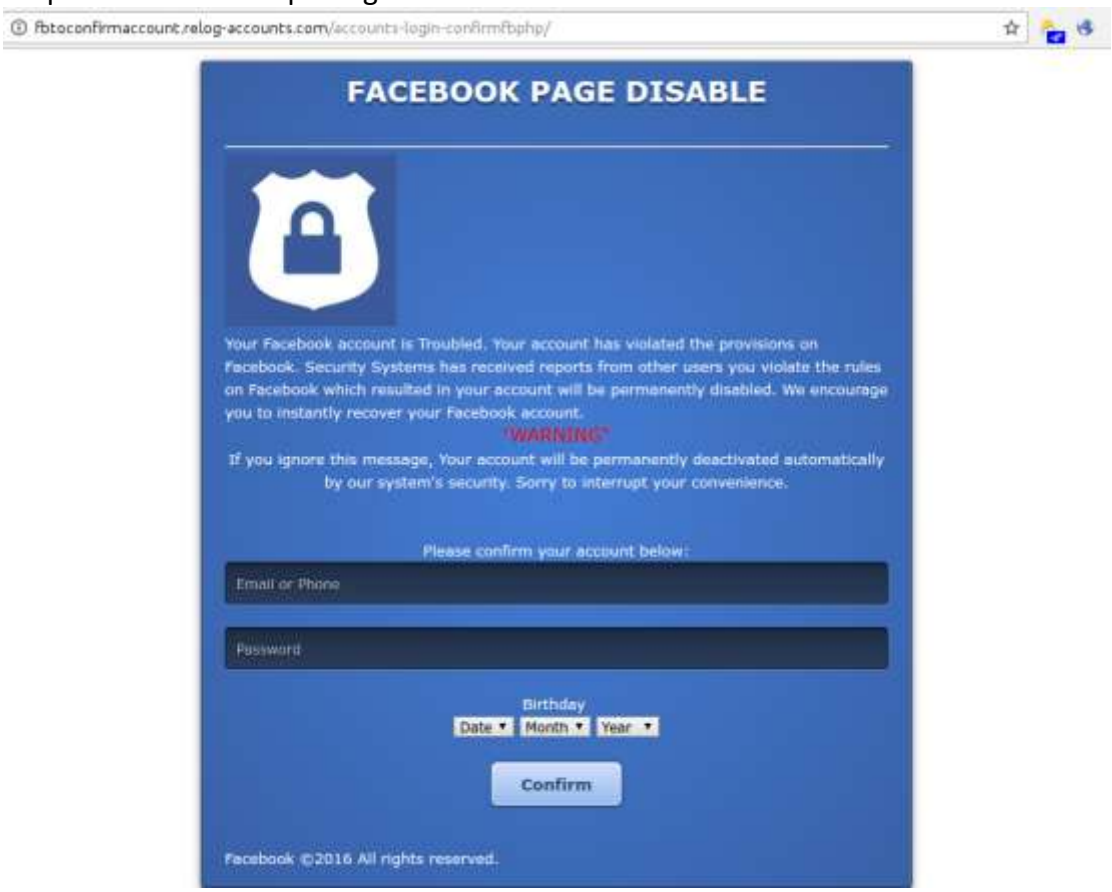
Kopumā vīrietis ieguldījis ap desmit tūkstošiem savas naudas, bet kopējā akciju tirdzniecības bilance uzrādījusies lielāka - pat līdz 45 tūkstošiem, taču, lai naudu izņemtu, bija jāiemaksā vēl 15 tūkstoši eiro, operācijas pabeigšanai. Līdzīga situācija atkārtojusies vēl vairākas reizes, kamēr bilance izaugusi līdz 100 tūkstošiem, bet prasīts ieskaitīt vēl naudu operācijas pabeigšanai un konvertācijai. Ne ieguldīto, ne nopelnīto naudu vīrietim neizdevās saņemt, tāpēc viņš vērsās pie pašas platformas, ar ko strādā "Everest trade", taču arī tur nav saņēmis nekādu palīdzību naudas atgūšanai.

CERT.LV ieteica vīrietim vērsties ar iesniegumu policijā. Arī Finanšu un kapitāla tirgus komisija (FKTK) brīdina par nelicencētas atvasināto finanšu instrumentu tirdzniecības platformas "Everest Trade" finanšu pakalpojumiem tās interneta vietnē https://everest.trade/en/. FKTK norāda, ka minētajam pakalpojumu sniedzējam nav tiesību nodarboties ar ieguldījumu pakalpojumu un ieguldījumu blakus pakalpojumu sniegšanu, tajā skaitā uzturēt atvasināto finanšu instrumentu tirdzniecības platformu.

Facebook lapas izkrāpj paroles

CERT.LV saņēma informāciju par Facebook paroļu izkrāpšanas mēģinājumu. Sākumā lietotājs saņem brīdinājumu par to, ka lietotāja konts tiks deaktivizēts, un lai tas nenotiktu, jānospiež uz saites. Lai neradītu aizdomas, lietotājs tiek pārvirzīts uz it kā leģitīmu Facebook saiti. Tas tiek panākts ar pašizveidotas Facebook lapas palīdzību, līdz ar to paziņojums izskatās autentiski. Tālāk lietotājam jāapstiprina savs konts. Nospiežot uz saites, lietotājs tiek pārvirzīts uz viltotu lapu un aicināts ievadīt savu e-pastu un Facebook paroli.
Ja lietotājs ievadījis savus datus kaitnieciskā vietnē, parole nekavējoties jāmaina, lai nebūtu iespējamas krāpnieciskas manipulācijas ar kontu.

Krāpnieciskās vietnes paraugs:



Macro ļaunatūra izplatās arī Mac OS

Windows vidē ļaundari jau pāris gadus izmanto macro, lai izplatītu ļaunatūru, taču tagad iespējams inficēt arī Mac OS platformā strādājošos.
Drošības pētnieki atklājuši, ka ļaundari iesūta kaitnieciskus Word dokumentus, kuros iespējots macros, lai instalētu ļaunatūru Mac datoros un zagtu lietotāja datus.
Nospiežot uz kaitnieciskā dokumenta, tas izpilda funkciju, kas lejupielādē ļaunatūru, kas inficē datoru, ļaujot uzbrucējam pārvaldīt webkameras, piekļūt pārlūka vēsturei un nozagt paroles un šifrēšanas atslēgas.
Labākais, kā sevi pasargāt, ir liegt atļauju iespējot macros Word dokumentos.