Posljednjih nekoliko dana zabilježen je povećan broj lažnih ucjenjivačkih poruka kojima napadač pokušava iznuditi novčanu dobit od žrtve, upozorili su u utorak MUP i nacionalni CERT - organizacijski entitet koji reagira na računalno-sigurnosne incidente, te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava.

Metodu kojom napadač pokušava ostvariti financijsku dobit temelji na objavljivanju navodnih osjetljivih podatka žrtve koja je primila ucjenjivačku poruku ako žrtva ne izvrši uplatu u Bitcoin vrijednosti.

Gotovo uvijek u tekstu poruke ucjenjivač spominje posjedovanje žrtvine kompromitirane lozinke nekog internetskog servisa. Također, navodi da posjeduje snimke s web kamere žrtvinog računala kojoj je pristupio dok je žrtva navodno pregledavala web stranice pornografskog sadržaja. Pri tome prijeti objavom navodne "ponižavajuće" video snimke svim žrtvinim kontaktima koje je prikupio s Messengera, Facebooka i e-maila.

Iako se može dogoditi da poruka sadrži lozinku koju možda koristite ili ste koristili, to je vjerojatno zbog činjenice da postoje određeni servisi s bazom kompromitiranih lozinki (primjerice već ugašeni Leakedsource.com) s kojih je ucjenjivač preuzeo bazu kompromitiranih podataka. Poznati su slučajevi s kompromitiranim računima popularnih web servisa LinkedIn i MySpace, objavio je nacionalni CERT na svojim internetskim stranicama.

Savjeti za izbjegavanje bilo kakvih budućih neugodnosti ili mogućih kompromitacija

To nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza savjetuje korisnicima e-pošte da promjene postojećih lozinki te da koriste drugačije jače lozinke za svaki pojedini internetski servis.

Također, uvijek treba biti na oprezu kome šaljete povjerljive poruke koje sadržavaju slikovni ili video sadržaj.

Korisnici e-pošte trebaju biti oprezni i kad otvaraju privitke pristigle poštom od nepoznatog pošiljatelja.

Ako nemate namjeru koristiti web kameru svakako provjerite je li isključena prije pregledavanja internetskog sadržaja, savjetuje nacionalni CERT koji je na svojim internetskim stranicama objavio i primjere ucjenjivačkih "scam" poruka.

MUP: Uočena pojava većeg broja prijava građana

MUP je također objavio da je u posljednjih nekoliko dana uočena pojava većeg broja prijava građana koji putem e-pošte primaju poruke u kojima pošiljatelj tvrdi da su im račun e-pošte i računalo kompromitirani i da je na taj način pribavio pristupnu korisničku lozinku koju navodi u poruci. Lozinka može biti točna, ali i ne mora, ili se radi o staroj lozinki koju korisnik više ne koristi.

Počinitelj u svojoj poruci navodi kako je na žrtvino računalo instalirao maliciozni program koji mu je omogućio pristup kameri i korisničkim podacima te je na taj način došao u posjed eksplicitnog

sadržaja žrtve dok je ista navodno pregledavala web stranice pornografskog sadržaja, navodi MUP, dodajući da na temelju navodnog eksplicitnog sadržaja počinitelj vrši ucjenu prema žrtvi uz prijetnju da će, ne uplati li žrtva određeni iznos na počiniteljev bitcoin račun, sav kompromitirajući sadržaj poslati žrtvinim Facebook/Messenger prijateljima, te osobama iz imenika e-pošte i dr.

Korisnicima e-pošte MUP savjetuje da ne otvaraju sumnjive privitke u porukama od pošiljatelja koji nisu poznati jer takvi privitci mogu sadržavati maliciozne programe, da budu oprezni prilikom slanja povjerljivih poruka koje sadrže slikovni ili video sadržaj, da provjeravaju isključenost web kamere ukoliko ju nije potrebno koristiti prilikom pregledavanja internetskog sadržaja.

I MUP savjetuje korisnike da ažuriraju svoje pristupne lozinke uz korištenje sigurnosno jače lozinke za svaki pojedini internetski servis, izbjegavaju ustupanje svojih lozinki i računa e-pošte drugim osobama ili servisima te da instaliraju i redovito ažuriraju antivirusne programe i operativne sustave.

(Hina)