SANS SECURITY AWARENESS

OUCH!

Mėnesinis informacinio saugumo naujienlaiškis Tau

Taip, jūs esate taikiniai

Apžvalga

Dauguma žmonių klaidingai mano, kad jie nėra kibernetinių nusikaltėlių taikiniai, nes jie, jų naudojamos sistemos ar turimos paskyros yra visiškai nevertingos. Deja, tai netiesa. Jei darbe ar namie naudojate kokias nors technologijas, patikėkite, nusikaltėliai tikrai jose ras ką nors vertingo. Laimei, geriausia apsauga nuo šių kibernetinių atakų esate jūs patys.

Kodėl esate taikiniai?

Šiais laikais internete yra daugybė įvairių kibernetinių nusikaltėlių, turinčių skirtingas motyvacijas. Kodėl kuris nors iš jų norėtų jus pulti? Nes įsilauždami į jūsų sistemą, jie gali įgyvendinti savo tikslą. Štai pora dažniausiai pasitaikančių kibernetinių nusikaltėlių tipų ir priežasčių, dėl kurių jie gali į jus nusitaikyti.

⚠ **Kibernetiniai nusikaltėliai.** Šie piktadariai siekia gauti kaip įmanoma daugiau pinigų. Internetas jiems yra toks vertingas todėl, kad vos vienu mygtuko paspaudimu, jie gali paprastai nusitaikyti į bet ką pasaulyje. Be to, yra DAUGYBĖ būdų kaip jie gali iš jūsų pasipelnyti. Pavyzdžiui, pavogti pinigus iš jūsų banko arba pensijų sąskaitų, jūsų vardu užsisakyti kredito kortelę ir atsiųsti jums sąskaitą, pasinaudoti jūsų kompiuteriu, siekiant įsilaužti į kitų žmonių sistemas arba įsilaužti į jūsų socialinį tinklalapį ar žaidimų paskyras ir jas parduoti kitiems nusikaltėliams. Būdų, kaip piktadariai gali iš jūsų pasipelnyti, sąrašas yra beribis. Yra šimtai tūkstančių žmonių, kurie kasryt pabudę turi tikslą pasinaudoti kiek įmanoma daugiau žmonių, įskaitant jus.

☆ **Kryptingai veikiantys nusikaltėliai.** Tai yra itin kvalifikuoti kibernetiniai nusikaltėliai, kurie dažnai dirba įvairioms vyriausybėms, nusikalstamos gaujos arba į jus darbe nusitaikę konkurentai. Jei manote, kad jūsų darbas neatkreipia daug dėmesio, galite labai nustebti.

- **Jūsų tvarkoma darbo informacija yra itin vertinga įvairioms įmonėms ir vyriausybės organizacijoms.**
- **Kryptingai veikiantys nusikaltėliai gali į jus darbe nusitaikyti ne todėl, kad nori jus užpulti, o todėl, kad jumis pasinaudotų, siekiant įsilaužti į vieno iš jūsų bendradarbių arba kitas sistemas.**
- **Tokie nusikaltėliai gali į jus darbe nusitaikyti vien dėl su jumis bendradarbiaujančių kitų įmonių arba partnerių interesų.**

Turiu antivirusinę programą, todėl aš saugus

Gerai, vadinasi, aš taikinys. Nieko tokio. Tiesiog savo kompiuteryje įdiegsiu antivirusinę programą ir įjungsiu ugniasienę, tuomet būsiu saugus, tiesa? Na, ne visai. Dauguma žmonių mano, jog įdiegę kokias nors apsaugos priemones bus saugūs. Deja, tai netiesa. Kibernetiniai nusikaltėliai vis tobulėja ir daugelis jų puolimo metodų šiais laikais lengvai apeina bet kokias apsaugos technologijas. Pavyzdžiui, jie dažnai sukuria specialią kenkimo programą, kurios jūsų antivirusinė programa neaptiks. Taip pat jie apeis el. pašto filtrus, naudodami individualiai pritaikytą sukčiavimo būdą arba paskambins jums telefonu ir įtikins jus atskleisti savo kredito kortelės duomenis, pervesti pinigus ar pasakyti slaptažodį. Jus saugančios technologijos atlieka itin reikšmingą vaidmenį, tačiau geriausiai apsisaugoti galite tik patys.

Laimei, išlikti saugiu nėra taip sudėtinga, nes geriausia jūsų apsauga yra sveikas protas ir keli paprasti veiksmai. Jei gavote el. laišką, žinutę arba jums kas nors paskambino ir pranešta žinia skamba neįprastai skubiai, keistai ar įtartinai, tai gali būti puolimas. Įsitikinkite, kad jūsų kompiuteriai ir prietaisai yra saugūs, įjungdami automatinį jų atnaujinimą. Galiausiai, kiekvienoje iš savo paskyrų naudokite patikimą ir unikalią slaptafrazę. Geriausias būdas apsisaugoti internete yra likti atidžiais. Nežinote nuo ko turėtumėte pradėti? Apsvarstykite galimybę užsiprenumeruoti kasmėnesinį „OUCH!“ naujienlaiškį svetainėje sans.org/ouch

Kviestinis redaktorius

Matt Bromiley *(@mbromileyDFIR) yra reagavimo į incidentus ir skaitmeninės ekspertizės specialistas, sukaupęs daugiau nei 8 metų patirtį ir dirbantis su organizacijomis bei sprendžiantis incidentus visame pasaulyje. Matt taip pat dirba dėstytoju, vedančiu SANS FOR508 ir FOR572 kursus apie skaitmeninę ekspertizę ir reagavimą į incidentus.*

SANS SECURITY AWARENESS

Šaltiniai

Apsisaugokite nuo kenkimo programų:	https://www.sans.org/u/L1J
Socialinė inžinerija:	https://www.sans.org/u/L1O
Sukčiavimas telefonu:	https://www.sans.org/u/L1T
Slaptafrazės:	https://www.sans.org/u/L1Y
Plakatas – jūs esate taikiniu:	https://www.sans.org/u/L23