OUCH! | 2016 m. rugpjūčio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

Išpirkos reikalaujančios programos

Kas yra išpirkos reikalaujanti programa?

Išpirkos reikalaujanti programa yra tam tikra kenkimo programos rūšis, kuri šiais laikais yra aktyviai platinama internetu, grasinant sunaikinti „aukos“ dokumentus ir kitus failus. Kenkimo programa – tai programinė įranga (arba kompiuterinė programa), skirta atlikti kenkėjiškus veiksmus. Nors išpirkos reikalaujanti programa yra tik viena iš skirtingų kenkimo programų rūšių, tačiau nusikaltėliams ji yra labai pelninga, todėl pastaruoju metu ji ir yra dažnai naudojama. Išpirkos reikalaujančiai programai užkrėtus jūsų kompiuterį, ji užšifruoja tam tikrus failus arba visą kietąjį diską. Tada netenkate prieigos prie visos sistemos ir nebegalite atsidaryti tokių svarbių failų kaip dokumentai ar nuotraukos. Tuomet kenkimo programa jus informuoja, kad vienintelis būdas iššifruoti jūsų failus ir atstatyti sistemos veiklą yra sumokėti išpirką kibernetiniam nusikaltėliui. Štai todėl ji vadinama išpirkos reikalaujančia programa. Dažniausiai išpirkos turi būti sumokėtos kokia nors skaitmeninės valiutos forma, pavyzdžiui, bitkoinais. Išpirkos reikalaujanti programa yra platinama lygiai tokiais pačiais būdais, kaip kitos kenkimo programos. Dažniausiai aukoms yra išsiunčiamas kenkėjiškas el. laiškas, kuriame kibernetiniai nusikaltėliai bando jas priversti atidaryti užkrėstą priedą arba paspausti nuorodą, kuri jas nukreiptų į nusikaltėlio interneto svetainę.

Kviestinė redaktorė

Lenny Zeltser „NCR Corp“ įmonėje rūpinasi klientų IT operacijų saugos klausimais ir SANS institute moko kaip kovoti su kenkimo programomis. Lenny aktyviai dalyvauja Twitter paskyroje **@lennyzeltser**, o svetainėje **zeltser.com** rašo tinklaraštį apie saugumą.

Ar turėtumėte sumokėti išpirką?

Tai sudėtingas klausimas. Problema yra ta, kad kuo dažniau, užkrėtus kompiuterius, žmonės sumoka šiems nusikaltėliams, tuo labiau jie yra motyvuojami užkrėsti daugiau kompiuterių. Viena vertus, jūs galite neturėti jokio kito pasirinkimo kaip kitaip atkurti savo failus. Kita vertus, turėkite omenyje, kad nėra garantijos, jog sumokėję išpirką atkursite savo failus. Juk susidūrėte su nusikaltėliais, kurie nebūtinai iššifruos failus, o jei ir nurodys, kaip tai padaryti, sumokėjus pinigus, kažkas šifravimo metu gali nepavykti arba jūsų kompiuterį gali užkrėsti dar viena kenkimo programa.

Pasidarykite savo failų kopijas

Gali būti, kad užkrėtus kompiuterį išpirkos reikalaujančiai programai ir pasirinkus nemokėti išpirkos, geriausias būdas atkurti

Išpirkos reikalaujančios programos

savo failus yra pasinaudoti failų kopijomis. Tokiu būdu, kompiuterį užkrėtus išpirkos reikalaujančiai programai, galėsite savo failus atidaryti juos atkūrę arba iš naujo įdiegę kompiuterio sistemą. Turėkite omenyje, kad prisijungus prie atsarginių failų kopijų iš užkrėstos sistemos, išpirkos reikalaujanti programa gali ištrinti arba užšifruoti jūsų atsargines failų kopijas. Todėl labai svarbu atsargines failų kopijas daryti naudojant debesija paremtas paslaugas arba atsargines kopijas laikyti išoriniuose diskuose, kurie ne visada yra prijungti prie sistemos. Be to, dažniausiai žmonių daroma klaida, susijusi su atsarginėmis kopijomis, yra manymas, kad failai atsidarys prieš tai nepabandžius jų atkurti. Reguliariai patikrinkite, ar veikia jūsų turimos atsarginės kopijos ir įsitikinkite, jog užkrėtus kompiuterio sistemą išpirkos reikalaujančiai programai, galėsite juos atkurti. Atsarginės failų kopijos yra svarbios dar ir todėl, kad jas galite atkurti failus netyčia ištrynę arba tiesiog sugedus kietajam diskui.

Išpirkos reikalaujanti programa yra kenkimo programos rūšis, kuri užšifruoja failus jūsų kompiuteryje ir uždraudžia prieigą prie jų.

Kitos apsaugos priemonės

Apsisaugoti nuo išpirkos reikalaujančios programos galite tokiu pat būdu, kuriuo saugotumėtės nuo kitų kenkimo programos rūšių. Pirmiausiai, įsitikinkite, kad esate atnaujinę iš patikimo tiekėjo įsigytą antivirusinę programą. Tokios priemonės, kartais dar vadinamos programine įranga prieš kenkimo programas, yra sukurtos siekiant aptikti kenkimo programas ir sustabdyti jų veiklą. Tačiau antivirusinės programos negali blokuoti ar pašalinti visų kenkimo programų. Kibernetiniai nusikaltėliai nuolat tobulėja, kurdami vis naujesnes ir išmanesnes kenkimo programas, kurios gali išvengti aptikimo. Savo ruožtu, antivirusinių programų pardavėjai taip pat atnaujina savo produktus, papildydami juos naujomis funkcijomis, kurios gali aptikti kenkimo programas. Daugeliu atžvilgių tai tapo ginklavimosi varžybomis, kurių metu abi pusės siekia pranokti viena kitą. Deja, blogiukai įprastai pirmauja, todėl turite įsitikinti, kad esate pasidarę atsargines failų kopijas ir imtis keleto papildomų veiksmų siekdami apsisaugoti:

- Kibernetiniai nusikaltėliai dažnai užkrečia kompiuterius arba įrenginius, bandydami pasinaudoti silpniausiomis programinės įrangos vietomis. Kuo naujesnė jūsų programinės įrangos versija, tuo mažiau silpnų vietų yra sistemoje ir tuo sudėtingiau kibernetiniams nusikaltėliams ją užkrėsti. Todėl įsitikinkite, kad jūsų operacinėse sistemose, programose ir įrenginiuose yra įjungtas automatinis atnaujinimas.

Išpirkos reikalaujančios programos

- Kompiuteriuose naudokite standartinę paskyrą, kuri turi ribotas teises, o ne privilegijuotas paskyras, turinčias „Administratoriaus“ ar „šaknies“ valdymo teises. Tai suteiks papildomą apsaugą, draudžiant patiems įdiegti daugybę kenkimo programos rūšių.
- Kibernetiniai nusikaltėliai dažnai stengiasi įtikinti žmones įdiegti kenkimo programas už juos. Pavyzdžiui, jie gali jums atsiųsti teisėtai atrodantį el. laišką su prisegtu priedu arba pateikta nuoroda. Gali atrodyti, kad šį el. laišką atsiuntė jūsų bankas arba draugas. Tačiau, atidarę failą arba paspaudę nuorodą, suaktyvintumėte kenkimo programos kodą, kuris sistemoje įdiegtų kenkimo programą. Jei žinutėje raginama imtis skubių veiksmų, o tekstas skamba painiai arba per gerai, kad būtų tiesa, tai gali būti puolimas. Dažniausiai geriausia apsauga yra įtarumas ir sveikas protas.

Apsisaugokite nuo išpirkos reikalaujančių programų išlikdami budriais, kai tenka atidaryti prie el. laiško prisegtus priedus ar spausti nuorodas. Įsitikinkite, jog esate atnaujinę savo antivirusinę programą ir reguliariai darote atsargines failų kopijas, kurios, prireikus, gali būti atkurtos.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę securingthehuman.sans.org/ouch/archives.

Šaltiniai

Sukčiavimas:	https://securingthehuman.sans.org//ouch/2015#december2015
Kas yra kenkimo programa?:	https://securingthehuman.sans.org/ouch/2016#march2016
Užšifravimas:	https://securingthehuman.sans.org/ouch/2016#june2016
Atsarginės kopijos:	https://securingthehuman.sans.org/ouch/2015#august2015
„Microsoft“ straipsnis:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS instituto FOR610 kursas „Atvirkštinė kenkimo programų inžinerija“:	https://sans.org/for610

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.