OUCH! | 2017 m. birželio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Apžvalga
- Pataisų diegimas
- Atsarginės kopijos
- Sukčiavimas

Ko galime pasimokyti iš „WannaCry“ atakų?

Apžvalga

Tikriausiai pastebėjote, jog neseniai žiniasklaidos atstovai išplatino daugybę naujienų apie naujausią viruso „WannaCry“ kibernetinę ataką. „WannaCry“ virusas užkrėtė daugiau nei 200 000 kompiuterių, panaikindamas įvairių organizacijų, įskaitant Jungtinės Karalystės ligoninių, prieigą prie jų turėtų duomenų. Ši ataka tokio didžiulio dėmesio sulaukė dėl kelių priežasčių. Visų pirma, ji staigiai išplito pereidama nuo vieno kompiuterio prie kito, taikydamasi į gerai žinomas ir pažeidžiamiausias „Windows“ operacinės sistemos vietas. Visų antra, tai buvo toks kenkimo programos tipas, kuris įprastai yra vadinamas „išpirkos reikalaujančia programa“. Tai reiškia, jog tokiam virusui užkrėtus kompiuterį, jis užšifruos visus jūsų turėtus failus ir panaikins prieigą prie šių duomenų. Vienintelis būdas, kuriuo galėtumėte atgauti savo duomenis, būtų juos atkurti iš atsarginės jų kopijos arba sumokėti kibernetiniam nusikaltėliui 300 $ išpirką už tai, kad visi jūsų duomenys būtų iššifruoti. Visų trečia ir svarbiausia yra tai, kad ši ataka galėjo niekada neįvykti. „Microsoft“ įmonė gerai žinojo „Windows“ operacinės sistemos pažeidžiamas vietas, į kurias nusitaikė „WannaCry“ virusas, todėl likus keliems mėnesiams iki atakos, išleido reikiamas pataisas. Tačiau dauguma organizacijų šių pataisų neįdiegė arba vis dar naudojo tokias senesnes operacinės sistemos versijas kaip „Windows XP“, kurioms pataisos jau seniai nebekuriamos. Toliau pateikiame tris paprastus veiksmus, kurių turėtumėte imtis, siekdami, jog tokie virusai kaip „WannaCry“ niekada neužkrėstų jūsų kompiuterio.

Kviestinė redaktorė

Dr. Johannes Ullrich yra SANS technologijų instituto mokslinių tyrimų fakulteto dekanas ir svetainės DShield.org įkūrėjas. Institute jis yra atsakingas už šiuolaikinių kibernetinio saugumo grėsmių stebėjimo sistemą „**SANS Internet Storm Center**“. Taip pat Johannes dėsto paskaitas apie internetinių programų saugą (**DEV522**), įsibrovimų aptikimą (**SEC503**) ir naująją interneto protokolo versiją IPv6 (**SEC546**).

Pataisų diegimas

Pirmiausiai įsitikinkite, jog kompiuteriai, mobilieji įrenginiai, programos ir kiti prietaisai, kuriuos jungiate prie interneto, yra atnaujinti. Kibernetiniai nusikaltėliai jūsų naudojamų įrenginių programinėje įrangoje nuolat ieško naujų pažeidžiamų vietų. Jas aptikę, jie naudoja specialias programas, kuriomis bando įsilaužti į jūsų įrenginius. Tuo tarpu, šių įrenginių programinę įrangą sukūrusios įmonės sunkiai dirba, siekdamos pažeidžiamas vietas panaikinti, išleisdamos naujinius. Įsitikindami, jog jūsų kompiuteriuose ir mobiliuosiuose įrenginiuose yra įdiegti šie naujinimai, jūs užsitikrinate, jog į juos svetimam asmeniui bus žymiai sudėtingiau įsilaužti. Štai kodėl „WannaCry“ viruso išplitimas yra toks apmaudus. Siekdama užkirsti kelią tokiai

© SANS Institute 2017

Ko galime pasimokyti iš „WannaCry“ atakų?

atakai, „Microsoft“ atnaujinimus išleido iki atakos likus dviem mėnesiams. Jei organizacijos būtų atsinaujinusios savo kompiuterių operacines sistemas, įvykdyti šios atakos niekada nebūtų pavykę. Norėdami užtikrinti, jog turimos operacinės sistemos versija bus pati naujausia, jei tik įmanoma, įjunkite automatinį naujinimą. Ši taisyklė galioja beveik bet kuriai, prie tinklo prijungtai, technologijai, ne tik jūsų kompiuteriams ir mobiliesiems įrenginiams, bet ir prie interneto prijungtiems televizoriams, namuose esantiems maršruto parinktuvams, žaidimų pultams, o kada nors ateityje, galbūt net jūsų automobiliui. Jei jūsų operacinės sistemos arba įrenginiai yra tokie seni kaip „Windows XP“ operacinė sistema, kad apsaugos naujiniai jiems jau nebekuriami, pakeiskite šiuos įrenginius naujais, kuriems ši paslauga būtų teikiama.

Geriausia jūsų gynyba nuo tokių atakų kaip „WannaCry“ yra imtis trijų paprastų veiksmų: atnaujinti savo kompiuterių sistemas, saugotis sukčiavimo atakų ir daryti sistemoje esančių duomenų atsargines kopijas.

Atsarginės kopijos

Kai kada tokių kibernetinių atakų metu, kuomet reikalaujama išpirkos, gali būti užkrėstos net atnaujintos operacinės sistemos. Dar vienas būdas, kuriuo galite apsisaugoti, yra pasidaryti savo duomenų atsarginę kopiją. Atsarginės kopijos tai kur nors kitur, nei jūsų kompiuteryje ar mobiliajame įrenginyje laikomos atsarginės jūsų informacijos kopijos. Praradę vertingus duomenis, juos galite atkurti iš turimų atsarginių kopijų. Deja, daugybė žmonių reguliariai nedaro atsarginių kopijų, net jei jas kurti yra paprasta ir nebrangu. Sukurti atsarginę savo duomenų kopiją galite dviem būdais: įkeldami juos į fizinę laikmeną arba debesija paremtą saugyklą. Kiekvienas būdas turi savų privalumų ir trūkumų. Jei nesate tikri, kurį būdą turėtumėte naudoti, galite naudoti abu būdus tuo pat metu.

Fizinės laikmenos tai jūsų naudojamas atminties įtaisas, pavyzdžiui, išoriniai atmintukai arba per belaidį namų ar biuro tinklą naudojami įrenginiai. Naudodami savo fizinę laikmeną galite greitai daryti atsargines kopijas ir atkurti didelius duomenų kiekius. Šio būdo trūkumas yra tas, kad įrenginį užkrėtus išpirkos reikalaujančia kenkimo programa, atitinkamai galite užkrėsti ir atsarginių kopijų laikmeną. Jei atsarginių kopijų darymui naudojate fizines laikmenas, tuomet atsargines kopijas turėtumėte laikyti visiškai kitoje, saugioje vietoje. Įsitikinkite, jog bet kokios turimos atsarginės kopijos būtų tinkamai pažymėtos. Debesija paremti sprendimai tai internetinės paslaugos, kurių metu jūsų failai yra saugomi internete. Įprastai tai atliekama kompiuteryje įdiegiant programą, kuri viskuo pasirūpina. Debesija paremtų sprendimų privalumas yra naudojimo paprastumas. Be to, jūsų operacinę sistemą užkrėtus išpirkos reikalaujančiam virusui, įprastai jis negalėtų prisijungti prie debesijoje saugomų atsarginių kopijų. Šio metodo trūkumas yra tas, kad didelio duomenų kiekio atsarginių kopijų darymas

© SANS Institute 2017

Ko galime pasimokyti iš „WannaCry“ atakų?

ar jų atkūrimas gali ilgai užtrukti. Pasidomėkite apie debesijoje laikomų atsarginių kopijų privatumą ir saugumą. Pavyzdžiui, ar atsarginių kopijų darymo paslauga patikimai užšifruos jūsų duomenis ir ar siūlys patikimą vartotojo identifikavimo būdą.

Sukčiavimas

Galiausiai, blogų kėslų turintys asmenys visada atnaujina ir keičia savo puolimo taktikas. Kibernetiniai nusikaltėliai dažnai naudoja „sukčiavimu“ vadinamą puolimo būdą, kuriuo taikosi į numatytas operacines sistemas, siekdami jas užkrėsti. Sukčiaujama yra tuomet, kai kibernetiniai nusikaltėliai jums atsiunčia el. laišką, siekdami jus įtikinti atidaryti užkrėstą priedą arba apsilankyti kenksmingoje svetainėje. Atlikus vieną iš minėtų veiksmų, užkrečiama jūsų kompiuterio operacinė sistema. Nors „WannaCry“ virusas nenaudojo tokio puolimo būdo, tačiau jis yra neretai naudojamas daugumoje kitų atakų, įskaitant daugumą išpirkos reikalaujančių programų rūšių. Be to, neabejojame, kad „WannaCry“ virusą sukūrę asmenys, siekdami užkrėsti daugiau operacinių sistemų, artimiausiu metu atnaujins savo puolimo būdus ir naudos naujas technikas, įskaitant sukčiavimą. Geriausia jūsų gynyba nuo tokių el. laiškais paremtų atakų, yra naudotis sveiku protu. Jei el. laiškas ar žinutė atrodo keistai, įtartinai ar skamba pernelyg gerai, kad būtų tiesa, greičiausiai tai bus skirta puolimui.

SUŽINOKITE DAUGIAU

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

Šaltiniai

Kas yra kenkimo programa?:	https://securingthehuman.sans.org/ouch/2016#march2016
Išpirkos reikalaujančios programos:	https://securingthehuman.sans.org/ouch/2016#august2016
Atsarginės kopijos:	https://securingthehuman.sans.org/ouch/2015#august2015
Sukčiavimas:	https://securingthehuman.sans.org/ouch/2015#december2015
Kaip saugiai naudotis debesija?:	https://securingthehuman.sans.org/ouch/2016#november2016

Licencija

OUCH! Yra leidžiamas SANS Securing The Human instituto ir platinamas pagal Creative Commons BY-NC-ND 3.0 licensiją. Jums leidžiama naudoti ir platinti šį naujienlaiškį su sąlyga, kad niekas nebus keičiama. Norėdami gauti daugiau informacijos susisiekite su mumis ouch@securingthehuman.org.

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