OUCH! | 2016m. balandžio mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- **Apžvalga**
- **Užuominos, padedančios suprasti, kad į jūsų įrenginį buvo įsilaužta**
- **Kaip spręsti šias problemas?**

Įsilaužė, o kas toliau?

Apžvalga

Mes žinome, kad jūs norite apsaugoti savo kompiuterį ir mobiliuosius įrenginius, todėl imatės veiksmų, kurie padėtų tai padaryti. Tačiau, kad ir kaip saugiai naudotumėtės technologijomis, anksčiau ar vėliau, į šiuos įrenginius vis vien gali būti įsilaužta arba jie gali būti pažeisti. Šiame naujienlaiškyje sužinosite ir išmoksite, kaip atpažinti, ar į jūsų kompiuterį arba mobilųjį įrenginį buvo įsilaužta ir, jei taip, kokių veiksmų galėtumėte imtis. Galų gale, kuo greičiau nustatysite, kad kažkas yra blogai, ir kuo greičiau tai sutvarkysite, tuo mažiau žalos kibernetinis programišius galės padaryti.

Kviestinė redaktorė

Samantha Davison (**@sam_e_davison**) yra „Uber“ įmonės švietimo saugumo klausimais ir informuotumo programos vadovė, mokanti įmonės darbuotojus 350 pasaulio šalių.

Užuominos, padedančios suprasti, kad į jūsų įrenginį buvo įsilaužta

Kadangi dažnai nėra vienintelio būdo, galinčio padėti išsiaiškinti, ar į jūsų įrenginį buvo įsilaužta, tai padaryti gali būti sudėtinga. Tačiau įprastai programišiai palieka keletą užuominų, iš kurių galite apie tai spręsti. Kuo daugiau šių užuominų pastebite sistemoje, tuo labiau tikėtina, kad į jūsų įrenginį buvo įsilaužta. Užuominos:

- Jūsų antivirusinė programa perspėjo, kad jūsų sistema buvo užkrėsta, ypač, jei pranešime nurodyta, jog ji negalėjo pašalinti arba izoliuoti pažeistų failų.
- Netikėtai pasikeitė jūsų naršyklės pagrindinis puslapis arba jūsų naršyklė jus nukreipia į puslapius, kuriuose neketinote lankytis.
- Jūsų kompiuteryje arba kitame įrenginyje atsiranda naujų paskyrų, kurių jūs nekūrėte, arba veikia naujos programos, kurių jūs neįdiegėte.
- Jūsų kompiuteris arba programos nuolat stringa, darbalaukyje atsiranda nežinomų programų piktogramos arba iškyla keisti langai.
- Programa jūsų prašo suteikti leidimą sistemoje atlikti pakeitimus, nors jūs aktyviai nediegėte ir neatnaujinote jokių programų.
- Bandant prisijungti prie sistemos arba internetinės paskyros, jūsų slaptažodis nebeveikia, nors žinote, kad jis yra teisingas.

Įsilaužė, o kas toliau?

- Draugai jūsų klausia, kodėl jiems el. paštu siunčiate brukalus, kurių iš tiesų nesiuntėte.
- Jūs gaunate mobiliojo telefono sąskaitas už niekada nesiųstas SMS žinutes mokamais numeriais.
- Jūsų mobilusis įrenginys staiga dėl neaiškių priežasčių pradėjo naudoti itin daug duomenų, o baterija pradėjo itin greitai sekti.

Anksčiau ar vėliau į jūsų kompiuterį ar kitą įrenginį gali būti įsilaužta. Kuo anksčiau tai aptiksite ir reaguosite – tuo geriau.

Kaip spręsti šias problemas?

Jei manote, kad į jūsų kompiuterį arba kitą mobilųjį įrenginį buvo įsilaužta – kuo greičiau imsitės veiksmų, tuo bus geriau. Jei kompiuterį arba kitą įrenginį jums davė darbdavys arba jis naudojamas darbo paskirčiai, nebandykite šių problemų spręsti savarankiškai. Taip galite pridaryti ne tik daugiau žalos, bet ir sunaikinti vertingus įkalčius, kurie gali būti panaudoti tyrimo metu. Vietoj to, nedelsdami praneškite apie tai savo darbdaviui. Įprastai tai galite padaryti susisiekę su pagalbos skyriumi, saugumo komanda arba prižiūrėtoju. Jei dėl kokios nors priežasties su savo organizacija negalite susisiekti arba esate sunerimęs dėl delsimo, tada atjunkite savo kompiuterį arba kitą įrenginį nuo tinklo ir jame įjunkite miego, veikimo pristabdymo arba skrydžio veikseną. Net jei nežinote, ar į jį buvo įsilaužta, dėl viso pikto geriau būtų apie tai nedelsiant pranešti. Jei kompiuteris arba kitas įrenginys priklauso jums ir jūs jį naudojate asmeniniams tikslams, pateikiame keletą veiksmų, kurių galite imtis:

- **Slaptažodžių keitimas**. Tai reiškia, kad slaptažodžiai turi būti pakeisti ne tik jūsų kompiuteriuose ir mobiliuose įrenginiuose, bet ir visose jūsų turimose internetinėse paskyrose. Įsitikinkite, jog keisdami slaptažodžius nenaudojate to paties kompiuterio, į kurį buvo įsilaužta. Slaptažodžių keitimui naudokite kitą kompiuterį arba įrenginį, kurį laikote saugiu.
- **Antivirusinė programa**. Jei apie užkrėstą failą praneša antivirusinė programa, galite imtis jos rekomenduojamų veiksmų. Tai įprastai reiškia failo izoliavimą, išvalymą arba ištrynimą. Dauguma antivirusinių programų jums pateiks nuorodas, kurias paspaudę galėsite gauti daugiau informacijos apie konkretaus užkrato tipą. Jei nežinote, ką daryti, rinkitės failo izoliavimą. Jei to padaryti neįmanoma – ištrinkite jį.
- **Sistemos atkūrimas**. Jei užkrato neįmanoma sutvarkyti arba norite būti tikri, kad jūsų sistema buvo pataisyta, tada saugesnis variantas yra ją atkurti. Kompiuteriuose vadovaukitės sistemos gamintojo nurodymais. Dauguma atvejų turėsite panaudoti esamas paslaugų programas, kurios operacinę sistemą įdiegs iš naujo. Jei šių paslaugų

Įsilaužė, o kas toliau?

programų nerandate, kad yra pažeistos arba užkrėstos, tada dėl tolimesnių veiksmų susisiekite ir pasitarkite su įrenginio gamintoju arba apsilankykite jo internetinėje svetainėje. Nediekite operacinės sistemos iš jos atsarginių kopijų, kadangi jos gali būti tokios pat pažeidžiamos ir programišiui suteikti prieigą pakartotinai. Atsargines kopijas turėtumėte naudoti tik duomenų atkūrimui. Mobiliuosiuose įrenginiuose vadovaukitės įrenginio gamintojo arba paslaugų teikėjo nurodymais, kurie turėtų būti pateikti jų internetinėse svetainėse. Dauguma atvejų tai padaryti gali būti taip pat paprasta, kaip atkurti mobiliojo įrenginio gamyklinius nustatymus. Jei nesate tikri, kaip atkurti sistemą, apsvarstykite galimybę pasinaudoti profesionalų paslaugomis, kurie jums šioje srityje padėtų. Arba, jei jūsų kompiuteris arba kitas įrenginys yra seno modelio, paprasčiau ir pigiau būtų tiesiog įsigyti naują. Galiausiai, atkūrę kompiuterio arba kito įrenginio sistemą arba įsigiję naują įrenginį, įsitikinkite, kad jo sistema yra atnaujinta ir, jei tik yra įmanoma, įjunkite automatinį jos atnaujinimą.

- **Atsarginės kopijos**. Svarbiausias veiksmas, kurio galite imtis siekdami iš anksto apsisaugoti, yra reguliariai daryti atsargines kopijas. Kuo dažniau darysite atsargines kopijas, tuo bus geriau. Kai kur šios atsarginės kopijos bus automatiškai daromos kas valandą, sukūrus naujus failus arba juos pakeitus. Nepriklausomai nuo to, kokį atsarginių kopijų darymo variantą pasirinksite naudoti, periodiškai patikrinkite, ar galite tuos failus atkurti. Gana dažnai vienintelis būdas viską atkurti po įsilaužimo, yra atkurti duomenis iš atsarginės kopijos.
- **Teisėsauga**. Jei jums kas nors kokiu nors būdu grasina, praneškite apie tai vietos teisėsaugai.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę http://www.securingthehuman.org.

Šaltiniai

Atsarginės kopijos:	https://securingthehuman.sans.org/ouch/2015#august2015
Slaptafrazės:	https://securingthehuman.sans.org/ouch/2015#april2015
Kas yra kenkimo programa?:	https://securingthehuman.sans.org/ouch/2016#march2016
Jūsų naujos planšetės apsauga:	https://securingthehuman.sans.org/ouch/2016#january2016

Licencija

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus