OUCH! | 2016m. kovo mėnuo

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Kas yra kenkimo programa
- Kas kuria kenkimo programas?
- Apsisaugojimas

Kas yra kenkimo programa?

Apžvalga

Tikriausiai esate girdėję tokius kibernetinio saugumo terminus kaip virusas, Trojos arklys, išpirkos reikalaujančios kenkimo programos ar šakninis virusas. Visi šie žodžiai apibūdina tą patį dalyką – nusikaltėlių naudojamų programų rūšis, siekiančias užkrėsti kompiuterius ir kitus įrenginius. Norint apibūdinti visas šias skirtingas programas, dažnai naudojamas bendras terminas – kenkimo programos. Šiame naujienlaiškyje paaiškinsime, kas yra kenkimo programos, kas ir kodėl jas kuria ir, svarbiausia, ką galite padaryti, siekdami apsisaugoti.

Kviestinė redaktorė

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

Kas yra kenkimo programa?

Trumpai tariant, kenkimo programa yra kompiuterio programinė įranga, naudojama atlikti tyčinius veiksmus. Iš tiesų, terminas kenkimo programa yra sudarytas iš dviejų terminų: kenkimas ir programinė įranga. Kibernetiniai nusikaltėliai kenkimo programas diegia į kompiuterius, siekdami juos užvaldyti arba gauti prieigą prie jų turinio. Įdiegę kenkimo programą, šie nusikaltėliai gali šnipinėti jūsų internetinę veiklą, vogti slaptažodžius ir failus arba naudotis jūsų sistema, siekdami vykdyti nusikaltimus prieš kitus. Kenkimo programa netgi gali panaikinti prieigą prie jūsų pačių failų, reikalaudama nusikaltėliui sumokėti išpirką už tai, kad atgautumėte minėtąją prieigą.

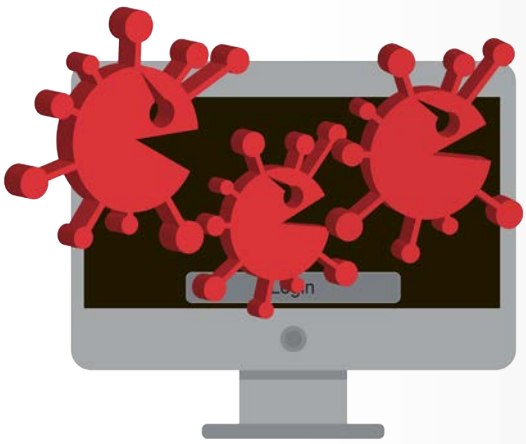
Dauguma žmonių klaidingai mano, kad kenkimo programa yra tik Windows operacinę sistemą turinčių kompiuterių problema. Windows operacinė sistema yra gana plačiai naudojama, todėl ji tampa dideliu taikiniu. Visgi, kenkimo programomis galima užkrėsti bet kurį įrenginį, įskaitant Mac kompiuterius, išmaniuosius telefonus ar planšetinius kompiuterius. Kuo daugiau kompiuterių ir įrenginių nusikaltėliai užkrečia, tuo daugiau pinigų jie uždirba. Todėl taikiniu gali tapti bet kas, įskaitant ir jus.

Kas kuria kenkimo programas?

Kenkimo programas dabar kuria ne vien tik smalsūs mėgėjai ar neprofesionalūs programišiai, bet ir patyrę kibernetiniai nusikaltėliai. Jų tikslas yra užsidirbti pinigų iš užkrėsto kompiuterio arba įrenginio, parduodant pavogtus jūsų duomenis, el. paštu siunčiant brukalus, paleidinėjant aptarnavimo perkrovos atakas ar prievartaujant turtą. Žmonėmis, kuriančiais,

Kas yra kenkimo programa?

platinančiais ar gaunančiais naudos iš kenkimo programų, gali būti tiek pavieniai asmenys, veikiantys gerai organizuotose nusikaltėlių grupėse, tiek vyriausybinės organizacijos. Žmonės, kuriantys šių laikų išmaniąsias kenkimo programas, dažnai yra pasišventę šiam tikslui, todėl kenkimo programų kūrimas yra jų darbas pilnu etatu. Be to, vos tik sukūrę kenkimo programą, jie dažnai ją parduoda kitiems asmenims arba organizacijoms, o kartais net įdiegia ją savo „klientų“ įrenginiuose kartu su įprastais atnaujinimais ir teikiama pagalba.



Saugokitės kenkenčių programų skeptiškai reaguodami į įtartinas žinutes, įdiekite naujausius įrenginių, programų, operacinių sistemų ir antivirusinių naujinimus kai tik įmanoma.

Apsisaugojimas

Norint apsisaugoti, dažniausiai reikia įdiegti antivirusinę programą, įsigytą iš patikimų pardavėjų. Tokios priemonės, kartais dar vadinamos programine įranga prieš kenkimo programas, yra sukurtos siekiant aptikti kenkimo programas ir sustabdyti jų veiklą. Visgi, antivirusinės programos negali blokuoti ar pašalinti visų kenkimo programų. Kibernetiniai nusikaltėliai nuolatos atnaujina, kuria naujesnes ir išmanesnes kenkimo programas, kurios gali išvengti aptikimo. Savo ruožtu, antivirusinių programų pardavėjai taip pat nuolatos atnaujina savo produktus, papildydami juos naujomis funkcijomis, kurios gali aptikti kenkimo programas. Tai tapo tarsi ginklavimosi varžybomis, kurių metu abi pusės stengiasi pergudrauti viena kitą. Deja, blogiukai įprastai pirmauja. Kadangi negalite pasikliauti vien tik antivirusine programa, pateikiame keletą papildomų veiksmų, kurių turėtumėte imtis, 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. Įsitikinkite, kad jūsų operacinėse sistemose, programose ir įrenginiuose yra įjungtas automatinis atnaujinimas.
- Įprastai kibernetiniai nusikaltėliai mobiliuosius įrenginius užkrečia sukurdami netikras mobiliąsias programėles, paskelbdami apie jas internete ir stengdamiesi įtikinti žmones jas parsisiųsti bei įsidiegti. Todėl programas siųskitės ir diekite tik iš patikimų internetinių parduotuvių. Be to, diekite tik tas mobiliąsias programėles, kurios internete yra paskelbtos jau kurį laiką, kurias parsisiunčia daugybė žmonių ir kurios turi daug teigiamų atsiliepimų.
- 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.

Kas yra kenkimo programa?

- 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 šis el. laiškas buvo atsiųstas iš jūsų banko arba draugo. 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.
- Reguliariai darykite savo sistemos ir failų atsargines kopijas, naudodamiesi debesija paremtomis paslaugomis arba laikykite šias atsargines kopijas nepasiekiamas internetu, pavyzdžiui, atjungiamuose išoriniuose diskuose. Taip apsaugosite savo atsargines kopijas, jei kenkimo programa bandytų užšifruoti arba ištrinti jas. Atsarginės kopijos yra itin svarbios, kadangi tai gali būti vienintelis būdas atkurti kenkimo programos paveiktus failus.

Galiausiai, geriausias būdas apsisaugoti nuo kenkimo programų yra nuolat atnaujinti turimą programinę įrangą, įdiegti patikimą antivirusinę programą, gautą iš gerai žinomų pardavėjų ir išlikti budriais, kai kas nors mėgins jus apgauti arba įtikinti užkrėsti jūsų turimą sistemą.

SUŽINOKITE DAUGIAU

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

Šaltiniai

Sukčiavimas:	https://securingthehuman.sans.org/ouch/2015#december2015
Socialinė inžinerija:	https://securingthehuman.sans.org/ouch/2014#november2014
Saugus mobilių programų naudojimas:	https://securingthehuman.sans.org/ouch/2015#january2015
Jūsų naujos planšetės apsauga:	https://securingthehuman.sans.org/ouch/2016#january2016
Atsarginės kopijos:	https://securingthehuman.sans.org/ouch/2015#august2015

Licencija

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