Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

Sustabdykime kenkimo programinę įrangą
Sustabdykime kenkėjiškas programas

Apžvalga

Kalbant apie kibernetinį saugumą, turbūt ne kartą girdėjote tokias sąvokas kaip virusas, Trojos arklys, išpirkos reikalaujanti programa ransomware ar slapto tipo kenkimo programa rootkit. Tai skirtingų tipų kenkimo programinė įranga, angliškai vadinama malware, kurią kibernetiniai nusikaltėliai pasitelkia, kad užkrėstų jūsų kompiuterius ir kitus prietaisus. Kai tik yra įdiegiamos, jos gali daryti ką tik nori. Sužinokite, kas yra kenkimo programinė įranga, kokias grėsmes ji kelia ir, svarbiausia, ką galite padaryti, kad nuo jos apsisaugotumėte.

Kas yra kenkimo programinė įranga?

Paprastai tariant, kenkimo programinė įranga – kompiuterinė programa – naudojama siekiant atlikti kenkimo veiksmus. Ši sąvoka (angl. – malware) yra sudaryta iš dviejų žodžių: kenksmingas (angl. – malicious) ir programinė įranga (angl. - software). Kibernetiniai nusikaltėliai įdiegia kenkimo programinę įrangą jūsų kompiuteriuose ar kituose prietaisuose, kad galėtų juos valdyti. Įdiegus kenkimo programinę įrangą, nusikaltėliai gali sekti jūsų veiksmus internete, vogti jūsų slaptažodžius ir failus, arba pasitelkti jūsų sistemą atakoms prieš kitus vartotojus. Kenkimo programinė įranga net gali užvaldyti jūsų failus ir pareikalauti išpirkos už tai, kad jie būtų sugrąžinti. Daugelis žmonių mano, jog kenkimo programinė įranga sukelia problemų tik kompiuteriams, dirbantiems su Windows operacine sistema. Deja, kenkimo programinė įranga gali užkrėsti bet kokį prietaisą, pradedant Mac kompiuteriais, išmaniaisiais telefonais ir baigiant skaitmeniniais vaizdo įrašymo prietaisais bei apsaugos kameromis. Kuo daugiau kompiuterių ir prietaisų kibernetiniai nusikaltėliai užkrečia, tuo didesnes pinigų sumas jie gali uždirbti. Todėl bet kuris iš mūsų gali tapti jų taikiniu, įskaitant ir jus.

Apsaugokite save – sustabdykite kenkimo programinę įrangą

Galbūt manote, kad jums tereikia įdiegti apsaugos programą, pavyzdžiui, nuo virusų apsaugančią programą, ir būsite apsaugotas nuo bandymų užkrėsti jūsų įrangą. Deja, antivirusinės programos negali sustabdyti visos kenkimo programinės įrangos. Kibernetiniai nusikaltėliai nuolat sukuria naujas ir sudėtingesnes kenkimo programas, kurių gali būti neįmanoma nustatyti. Savo ruožtu, parduodantys nuo virusų apsaugančias programas, nuolat atnaujina savo produktus ir gerina jų galimybes nustatant kenkimo programas. Daugeliu atžvilgiu tai jau tapo savotiškomis ginklavimosi varžybomis, o blogiukai paprastai yra vienu žingsniu priekyje. Kadangi negalima pasikliauti vien tik nuo virusų apsaugančiomis programomis, toliau pateikiami papildomi žingsniai, kurių galite imtis, kad apsisaugotumėte:

Kibernetiniai nusikaltėliai dažnai užkrečia kompiuterius arba prietaisus pasinaudodami jūsų programinės įrangos silpnybėmis. Kuo naujesnė bus jūsų programinė įranga, tuo mažiau bus silpnų vietų jūsų sistemose ir tuo

sunkiau bus kibernetiniams nusikaltėliams jas užkrėsti. Pasirūpinkite, kad jūsų operacinės sistemos, programos, naršyklė, joss papildiniai bei prietaisai būtų nuolat atnaujinami ir nepasenę. Tai lengviausia užtikrinti įgalinus, kai tai įmanoma, automatinį atnaujinimą.

Paprastai kibernetiniai nusikaltėliai užkrečia kompiuterius arba mobiliuosius prietaisus sukurdami netikras kompiuterių programas arba mobiliąsias taikomąsias programas, paskelbdami jas internete ir apgaule priversdami jas atsisiųsti bei įdiegti. Tad siųskitės ir diekite programas arba taikomąsias programas tik iš patikimų elektroninių parduotuvių. Taip pat venkite mobiliųjų taikomųjų programų, kurios yra visiškai naujos, turi nedaug teigiamų įvertinimų, yra retai atnaujinamos, arba kurias atsisiuntė labai nedidelis kiekis vartotojų. Nebesinaudojate kompiuterio programa ar mobiliąja taikomąja programa? Ištrinkite ją.

Kibernetiniai nusikaltėliai dažnai apgaule priverčia žmones įsidiegti kenkimo programinę įrangą. Pavyzdžiui, jie gali atsiųsti jums žinutę elektroniniu paštu, kuri atrodo teisėta ir kurioje yra pridėtas priedas arba nuoroda. Galbūt susidaro įspūdis, kad elektroninė žinutė yra atsiųsta jūsų banko ar kurio nors iš draugų. Tačiau, jei atidarysite pridėtą failą arba spustelėsite ant pridėtos nuorodos, aktyvuosite kenkimo kodą, kuris įdiegs kenkimo programą jūsų sistemoje. Jei pranešimo turinyje raginama skubiai imtis kokių nors veiksmų arba jis atrodo per daug geras, kad tai būtų tiesa, tai gali būti ataka. Būkite įtarūs, sveikas protas dažniausiai yra geriausia jūsų apsauga.

Reguliariai darykite savo sistemos ir failų kopijas, talpindami jas nuotolinių „debesies“ išteklių saugyklose, arba saugokite atsargines kopijas neinternetinėse talpyklose, pavyzdžiui, interneto ryšio neturinčiuose išoriniuose atminties įtaisuose. Taip apsaugosite savo atsargines kopijas tuo atveju, jei kenkimo programa bandys užkoduoti arba ištrinti jūsų failus. Turėti atsargines kopijas yra itin svarbu, nes jos dažnai yra vienintelis būdas ištaisyti kenkimo programinės įrangos padarytą žalą.

Galiausiai, geriausias būdas apsisaugoti nuo kenkimo programinės įrangos, yra nuolatos atnaujinti visą savo programinę įrangą ir prietaisus, jei įmanoma, įdiegti patikimą nuo virusų apsaugančią programinę įrangą ir būti budriems bei nepasiduoti bandymams jus apgauti ir užkrėsti jūsų sistemą. Kai visi šie būdai nepadeda, reguliarus atsarginių kopijų darymas dažnai būna vienintelis būdas viską atkurti.

Kviestinė redaktorė

Lenis Zeltseris *(Lenny Zeltser) kovoja su kenkimo programinės įrangos plitimu Minerva Labs kurdamas saugumo produktus galutiniams vartotojams ir dėstydamas SANS institute. Lenis aktyviai dalyvauja tviteryje, jo paskyra –* @lennyzeltser , bei rašo saugumo tinklaraštį adresu zeltser.com.

Šaltiniai

Išpirkos reikalaujančios programos (Ransomware): https://www.sans.org/u/EdI

Atsarginės kopijos (Backups): https://www.sans.org/u/EdN

Sustabdykime duomenų vagystes (Stop That Phish): https://www.sans.org/u/EdS