Ikmēneša informācijas drošības biļetens ikvienam

Stāties pretī ļaunatūrai

Pārskats

Saistībā ar kiberdrošību jūs droši vien esat dzirdējuši tādus terminus kā vīruss, trojānis un izspiedēvīruss. Tie ir apzīmējumi dažādu veidu ļaundabīgām programmatūrām, ko dēvē arī par ļaunatūru, un ko kibernoziedznieki izmanto, lai inficētu datorus un citas ierīces. Ja šāda programmatūra tiek uzstādīta, ļaundaris iegūst rīcības brīvību. Turpinājumā par to, kas īsti ir ļaunatūra, kādi ir ar to saistītie riski un kā sevi no tās pasargāt.

Kas ir ļaunatūra?

Ļaunatūra būtībā ir datora programmatūra, ko izmanto pretlikumīgiem nolūkiem. Termins radies savienojot vārdus „programmatūra" un „ļaundabīgs". Kibernoziedznieki uzstāda ļaunatūru datoros vai ierīcēs, lai iegūtu pār tām kontroli. Pēc uzstādīšanas ļaunatūra dod iespēju noziedzniekam novērot jūsu tiešsaistes aktivitātes, nozagt paroles vai failus, kā arī izmantot jūsu sistēmu, lai uzbruktu citiem. Ļaunatūra var arī pārņemt kontroli pār jūsu failiem un pieprasīt izpirkumu, lai jūs tos varētu atgūt. Parasti cilvēki uzskata, ka ļaunatūra ir tikai Windows datoru problēma, diemžēl ļaunatūra var inficēt praktiski jebkuru ierīci, sākot no Apple datoriem līdz drošības kamerām. Jo vairāk ierīču tiek inficētas, jo lielāka iespēja ļaundariem ir iegūt naudu. Tādēļ ikviens ir uzskatāms par potenciālu mērķi.

Aizsargājiet sevi – apturiet ļaunatūru

Pārsvarā valda uzskats, ka pietiek uzstādīt drošības programmu, piemēram, antivīrusu, lai pasargātu sevi no inficēšanās ar ļaunatūru. Diemžēl antivīrusa programmas nespēj apturēt visu ļaunarūru. Kibernoziedznieki nepārtraukti izstrādā jaunu un sarežģītāku programmatūru, kas var izvairīties no antivīrusiem. Protams, antivīrusu izstrādātāji nepārtraukti uzlabo arī savus risinājumus. Tās ir sava veida bruņošanās sacensības, diemžēl ļaundari bieži ir vienu soli priekšā. Papildu antivīrusa programmatūrai, jūs varat veikt sekojošus pasākumus, lai sevi pasargātu:

Kibernoziedznieki izmanto ievainojamības jūsu programmatūrā. Jo jaunāka/aktuālāka programmatūras versija jums ir, jo tai ir mazāk ievainojamību. Tāpēc ieteicams regulāri atjaunināt jūsu operētājsistēmas, lietotnes, pārlūkus, to paplašinājumus un citas programmas. Vienkāršākais risinājums parasti ir uzlikt automātisku atjauninājumu uzstādīšanu.

Izplatīts veids, kā kibernoziedznieki inficē datorus un mobilās ierīces, ir izstrādājot viltotas datorprogrammas vai mobilās lietotnes, publiskojot tās internetā un apmānot cilvēkus, lai tie brīvprātīgi uzstādītu šos viltojumus. Tādēļ lejupielādējiet un uzstādiet programmas tikai no uzticamiem tiešsaistes veikaliem, turklāt izpētiet atsauksmes par programmām un izvairieties no tām, kas ir maz izmantotas vai kurām ir tikai dažas pozitīvas atsauksmes. Tāpat izdzēsiet lietotni vai programmu, kas jums vairs nav nepieciešama.

Kibernoziedznieki bieži manipulē ar cilvēkiem, lai tie paši uzstādītu ļaunatūru, piemēram, tie var nosūtīt jums e-pastu, kas satur pielikumu vai saiti tekstā, un iespējams, izskatās kā nācis no drauga vai jūsu bankas. Diemžēl, kad jūs noklikšķināt uz saites vai lejupielādējat pielikumu, jūsu sistēmā tiek uzstādīta ļaunatūra. Ja saņemtais ziņojums izskatās pārāk labs, lai būtu patiesība, vai arī tas rada mānīgu steidzamības sajūtu, tas var būt uzbrukums. Esiet piesardzīgi, jo jūsu labākā aizsardzība ir jūsu veselais saprāts.

Regulāri veidojiet rezerves kopijas jūsu sistēmām un failiem, vai nu mākonī, vai bezsaistē, piemēram, uz ārējā cietādiska. Tas pasargās jūsu failus uzbrukuma gadījumā. Rezerves kopijas bieži vien ir vienīgais risinājums, kā atgūt jūsu failus pēc izspiedējvīrusa uzbrukuma.

Labākais veids, kā pasargāt sevi no ļaunatūras, ir uzturēt programmas aktuālas, instalēt uzticamu antivīrusa risinājumu un būt uzmanīgiem, lai veiksmīgi atpazītu mēģinājumus jūs apmānīt. Kad nekas vairs nelīdz, jūsu sistēmas palīdzēs atjaunot regulāri veiktās rezerves kopijas.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Lenny Zeltser *cīņai ar ļaunatūru veido drošības risinājumus Minerva Labs, kā arī pasniedz lekcijasSANS institūtā. Lenny ir aktīvs Twitter lietotājs -* @lennyzeltser, *un raksta arī blogu* zeltser.com *par IT drošību.*

Resursi

Izspiedējvīrusi:	https://www.sans.org/u/EdI
Rezerves kopijas:	https://www.sans.org/u/EdN
Aizsardzība pret pikšķerēšanu:	https://www.sans.org/u/EdS

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Tulkojums: Edgars Tauriņš