OUCH! | 2016.gada marts

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Kas ir ļaunatūra

Pārskats

Iespējams, sarunās par kiberdrošību esat dzirdējuši tādus terminus, kā vīrusi, trojāni un izspiedējvīruss. Visi šie vārdi raksturo programmu veidus, ko noziedznieki izmanto, lai inficētu datorus un ierīces. Kopējais termins, ko lieto, lai aprakstītu visas šīs dažādās programmas, ir ļaunatūra. Šajā izdevumā mēs izskaidrosim, kas ir ļaunatūra, kas to rada un kāpēc, un pats svarīgākais, ko jūs varat darīt, lai aizsargātu sevi.

Viesredaktors

Lenny Zeltser nodrošina klientu IT operāciju drošību NCR Corp un SANS institūtā māca, kā cīnīties ar ļaunatūru. Lenny ir aktīvs Twitter kā **@lennyzeltser** un raksta drošības blogu **zeltser.com**.

Kas ir ļaunatūra?

Vienkārši runājot, ļaunatūra ir programmatūra (datorprogramma), ko izmanto, lai veiktu ļaunprātīgas darbības. Faktiski termins ļaunatūra ir radies no vārdiem ļaunprātīga un programmatūra. Noziedznieki instalē ļaunprātīgu programmatūru uz jūsu datoriem vai ierīcēm, lai iegūtu kontroli pār tām, vai piekļūtu informācijai, kas tajās atrodas. Pēc instalēšanas, ļaunatūru var izmantot, lai novērotu Jūsu ikdienas aktivitātes tiešsaistē, nozagtu Jūsu paroles vai failus, vai izmantotu Jūsu sistēmu uzbrukumu veikšanai. Ļaunatūra var pat liegt pieeju Jūsu pašu failiem, pieprasot samaksāt izpirkumu, lai atgūtu šos failus.

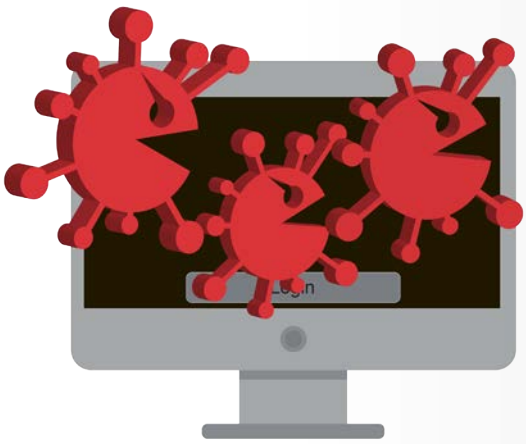
Daudzi cilvēki nepareizi uzskata, ka ļaunatūra ir problēma tikai uz Windows datoriem. Protams, Windows ir plaši izmantots un veido lielu skaitu potenciālo mērķu, taču ar ļaunatūru var inficēt jebkuru ierīci, ieskaitot Mac datorus, viedtālruņus vai planšetdatorus. Jo vairāk datorus un ierīces noziedznieki inficē, jo vairāk naudas viņi var iegūt. Tāpēc ikviens ir mērķis, ieskaitot jūs.

Kas rada ļaunatūru?

Ļaunatūru vairs nerada tikai zinātkāri vai amatieru hakeri, bet labi organizēti un izglītoti kibernoziedznieki. Viņu mērķis ir pelnīt naudu no inficētā datora vai ierīces, iespējams, pārdodot jums nozagtos datus, sūtot surogātpasta vēstules, uzsākot pakalpojumu atteices uzbrukumus vai veicot izspiešanu. Cilvēki, kas rada, izplata un gūst labumu no ļaunatūras, var būt gan atsevišķi indivīdi, kas rīkojas paši savās interesēs, gan labi organizētas noziedzīgas grupas vai pat valsts organizācijas.

Kas ir ļaunatūra

Cilvēki, kas rada šodienas ļaunatūru, bieži strādā pie tās izveides kā pilna laika darbu. Turklāt, kad viņi attīsta savu ļaunatūru, viņi bieži vien pārdod to citām personām vai organizācijām, pat sniedzot saviem "klientiem" regulārus atjauninājumus un atbalstu.



Aizsargājiet sevi no ļaunatūras, piesardzīgi izturoties pret aizdomīgām ziņām, regulāri atjauninot savas iekārtas un uzstādot aktuālu antivīrusa programmatūru.

Kā sevi aizsargāt

Plaši izplatīts aizsardzības pasākums ir uzstādīt uzticamu pārdevēju piedāvātu antivīrusa programmatūru. Šādi instrumenti, dažkārt saukti arī par antiļaunatūras programmatūru, ir izveidoti, lai atklātu un apturētu ļaunatūru. Taču antivīrusi nespēj bloķēt vai izdzēst visas kaitīgās programmas. Kibernoziedznieki nepārtraukti pilnveidojas, attīstot aizvien jaunas un sarežģītākas ļaunatūras, kas izvairās no atklāšanas. Savukārt, antivīrusu ražotāji nepārtraukti pilnveido savus produktus ar jaunām iespējām, kā atklāt ļaunatūru. Praktiski tā ir kļuvusi par ieroču sacensību, kur abas puses cenšas viena otru apmānīt. Diemžēl sliktie parasti ir vienu soli priekšā. Tā kā Jūs nevarat pilnībā paļauties tikai uz antivīrusiem, šeit ir daži papildu pasākumi, ko Jūs varat darīt, lai aizsargātu sevi:

- Kibernoziedznieki parasti inficē datoru, izmantojot ievainojamības programmatūrā. Parasti jaunāku vai atjauninātu versiju programmatūrā ir mazāk ievainojamību, tādēļ tās ir grūtāk inficēt. Tādēļ pārliecinieties, ka Jūsu operētājsistēmās, aplikācijās un iekārtās ir uzstādīta automātisko atjauninājumu uzlikšanas iespēja.
- Vēl noziedznieki var inficēt mobilās iekārtas, izveidojot viltotu mobilo aplikāciju, publicējot to Internetā un pievilinot cilvēkus lejupielādēt un instalēt šo programmatūru. Tādēļ aplikācijas lejupielādējiet un instalējiet tikai no uzticamiem tiešsaistes veikaliem. Papildus centieties uzstādīt tikai tādas aplikācijas, kas ir bijušas pieejamas ilgāku laiku, ir pietiekami populāras un kurām ir daudzas pozitīvas atsauksmes.
- Datoros (ikdienā) izmantojiet standarta lietotāja kontu ar ierobežotām pieejas tiesībām, nevis priviliģētu kontu kā, piemēram, "Administrators" vai "root". Tas nodrošina papildu aizsardzību, neļaujot daudzām ļaunatūrām uzstādīt pašām sevi.
- Kibernoziedznieki bieži apmāna cilvēkus, lai tie paši uzstādītu ļaunatūru. Piemēram, viņi var nosūtīt Jums e-pastu, kas izskatās ticams un satur pielikumu vai saiti. Iespējams, izskatās, ka šis e-pasts nācis no Jūsu bankas vai kāda drauga. Tomēr, ja Jūs nospiedīsiet saiti, vai atvērsiet pielikumu, tiks aktivizēts ļaundabīgs kods, kas instalēs

Kas ir ļaunatūra

ļaunatūru Jūsu sistēmā. Ja e-pasta ziņa rada steidzamības sajūtu, izraisa apjukumu, vai izskatās pārāk laba, lai būtu patiesība, tas var būt uzbrukums. Esiet piesardzīgi, labākā aizsardzība bieži ir veselais saprāts.

- Regulāri veiciet Jūsu sistēmas rezerves kopiju veidošanu, piemēram, izmantojot "mākoņa" pakalpojumus, vai saglabājiet savas rezerves kopijas bezsaistē, piemēram, uz tīklam nepieslēgtiem cietajiem diskiem. Tas aizsargās Jūsu rezerves kopijas gadījumos, kad ļaunatūra mēģinās izdzēst vai aizšifrēt failus. Rezerves kopijas ir ārkārtīgi būtiskas - bieži tas ir vienīgais veids, kā atjaunot sistēmas darbību pēc ļaunatūras infekcijas.

Galu galā, labākais veids, kā aizsargāties pret ļaunatūru, ir regulāri atjaunināt programmatūru, uzstādīt uzticamu antivīrusu programmatūru no labi zināmiem pārdevējiem un būt piesardzīgiem un neļaut sevi apmānīt vai ievilināt savas sistēmas inficēšanā.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni http://www.securingthehuman.org.

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.

Resursi

Pikšķerēšana:	https://securingthehuman.sans.org/ouch/2015#december2015
Sociālā inženierija:	https://securingthehuman.sans.org/ouch/2014#november2014
Mobilo aplikāciju droša izmantošana:	https://securingthehuman.sans.org/ouch/2015#january2015
Jūsu planšetes drošība:	https://securingthehuman.sans.org/ouch/2016#january2016
Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2015#august2015

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Tulkojums: Edgars Tauriņš