OUCH! | 2016.gada augusts

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Šifrējošie vīrusi

Kas ir šifrējošie vīrusi?

Šifrējošie vīrusi ir īpaša veida ļaunatūra, kas šobrīd aktīvi izplatās internetā, apdraudot upuru dokumentus un citus failus. Ļaunatūra ir programmatūra - datorprogramma, kas tiek izmantota ļaundabīgiem mērķiem. Lai arī šifrējošie vīrusi ir tikai viens no ļaunatūras veidiem, tie ir ļoti izdevīgi noziedzniekiem, tāpēc kļuvuši ļoti izplatīti. Kad šifrējošais vīruss ir inficējis Jūsu datoru, tas nošifrē noteiktus failus vai pat visu cieto disku. Tad Jūs vairs nespējat piekļūt sistēmai vai nevarat atvērt savus dokumentus, fotogrāfijas vai citus failus. Ļaunatūra tad Jūs informē, ka vienīgais veids, kā atšifrēt failus vai atgūt sistēmu, ir samaksāt izpirkuma maksu (no tā arī cēlies nosaukums angļu valodā - ransomware). Visbiežāk izpirkuma maksa tiek prasīta digitālā valūtā, piemēram, Bitkoinos. Šifrējošie vīrusi izplatās tāpat, kā cita veida ļaunatūra. Populārākā metode ir kaitīgi e-pasti, kuri mudina atvērt pievienotos failus vai noklikšķināt saiti, lai Jūsu dators tiek inficēts.

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**.

Vai maksāt izpirkuma maksu?

Tas nav viegls jautājums. Problēma ir tāda, ka, jo vairāk cilvēku maksās noziedzniekiem, jo lielāka motivācija tiem būs turpināt inficēt citus. No otras puses - Jums var nebūt citas iespējas atgūt failus. Tomēr atceraties, pat ja samaksājat izpirkumu, nav garantijas, ka saņemsiet savus failus atpakaļ. Noziedznieki var neatšifrēt Jūsu failus vai pat, ja viņi Jums nosūta atšifrēšanas instrukcijas, atšifrēšanas process var neizdoties, vai Jūsu datorā var būt kāda cita ļaunatūra.

Rezerves kopijas

Iespējams, labākais veids, kā atgūt failus un nemaksāt izpirkuma maksu, ir atjaunot failus no rezerves kopijām. Šādā veidā, pat ja Jūsu dators tiek inficēts, Jums ir iespēja atgūt failus un atjaunot un iztīrīt datoru. Tomēr ņemiet vērā, ja

Šifrējošie vīrusi

rezerves kopijas ir pieejams no inficētā datora, šifrējošais vīruss var izdzēst vai nošifrēt arī rezerves kopijas. Tādēļ ir svarīgi veidot rezerves kopijas vai nu uzticamos tiešsaistes servisos, vai glabāt rezerves kopijas ārējā diskā, kas nav pastāvīgi pieslēgts sistēmai. Izplatīta kļūda ir, ka cilvēki nepārbauda, vai rezerves kopijas darbojas kā paredzēts un no tām tiešām ir iespējams atjaunot failus. Tāpēc regulāri pārbaudiet, vai rezerves kopijas strādā, un pārliecinieties, vai ir iespējams atjaunot failus. Rezerves kopijas palīdz Jums arī gadījumā, ja fails tiek nejauši izdzēsts vai cietais disks tiek bojāts.

Šifrējošie vīrusi ir ļaunatūra, kas inficē Jūsu datoru un nošifrē failus, tādejādi neļaujot Jums tiem piekļūt.

Citas aizsardzības metodes

Jūs varat aizsargāties no šifrējošajiem vīrusiem tieši tāpat, kā no cita veida ļaunatūras. Sāciet ar aktuālu pretvīrusu aizsardzības programmu no uzticama ražotāja. Šāda aizsardzība ir radīta, lai atklātu un apturētu ļaunatūru. Tomēr antivīrusu aizsardzība nevar bloķēt vai izdzēst visas ļaundabīgās programmas. Kibernoziedznieki nepārtraukti izgudro un attīsta jaunus programmu veidus, kas var izvairīties no atklāšanas. Tāpat antivīrusu ražotāji nepārtraukti pilnveido savus ražojumus, lai atklātu jauna veida ļaunatūru. Tā ir sacensība, kurā abas puses cenšas viena otru pārspēt. Diemžēl ļaundari parasti ir soli priekšā, tādēļ Jums jāveido rezerves kopijas un jāpielieto citas aizsardzības metodes, piemēram, šīs:

- Kibernoziedznieki bieži inficē datorus vai iekārtas, izmantojot ievainojamības programmatūrā. Programmatūrām, kas tiek regulāri atjauninātas, ir mazāk zināmu ievainojamību, līdz ar to noziedzniekiem ir grūtāk inficēt Jūsu sistēmu. Tādēļ centieties vienmēr atjaunināt savas operētājsistēmas, aplikācijas un iekārtas, ja, iespējams, aktivizējot automātisko atjauninājumu instalēšanu.
- Datorā izmantojiet standarta lietotāja kontu ar ierobežotām tiesībām, nevis priviliģētos kontus kā “Administrators” vai “root”. Tas nodrošina papildus aizsardzību, neļaujot daudzu tipu ļaunatūrai pašai instalēt sevi datorā.
- Noziedznieki bieži apmāna cilvēkus, lai tie instalētu ļaunatūru. Piemēram, viņi var nosūtīt Jums e-pastu, kas neizskatās aizdomīgs un kurā ir saite uz mājas lapu, vai kuram ir pielikums. Šāds e-pasts var izskatīties kā nācis

Šifrējošie vīrusi

no bankas vai kāda Jums pazīstama cilvēka. Tomēr, ja Jūs atvērtu failu vai noklikšķinātu uz saites, tiktu aktivizēts ļaundabīgs kods, kas instalē ļaunatūru Jūsu sistēmā. Ja e-pasta ziņojums rada steidzamības sajūtu, izraisa apjukumu, izskatās pārāk labs, lai būtu patiesība, vai tajā ir neatbilstoša valoda, tas, iespējams, ir uzbrukums. Esiet piesardzīgi, bieži labākā aizsardzība ir veselais saprāts.

Aizsargājiet sevi, piesardzīgi klikšķinot uz saitēm vai atverot e-pastu pielikumus, uzturot aktuālu antivīrusu programmatūru un regulāri veidojot rezerves kopijas, kā arī pārliecinoties, ka failus no rezerves kopijām tiešām iespējams atjaunot.

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 securingthehuman.sans.org/ouch/archives.

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
Kas ir ļaunatūra:	https://securingthehuman.sans.org/ouch/2016#march2016
Šifrēšana:	https://securingthehuman.sans.org/ouch/2016#june2016
Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2015#august2015
Microsoft raksts:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 Kursi - Ļaunatūras izpēte:	https://sans.org/for610

License

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