Izspiedējvīrusi

Kas ir izspiedējvīruss?

Izspiedējvīrusi ir ļaundaru radītas programmatūras (ļaunatūras), kas paredzētas, lai sašifrētu jūsu failus vai datoru un turētu kā ķīlniekus, pieprasot samaksu par to atguvi. Izspiedējvīrusi ir kļuvuši ļoti populāri, jo tas ir viegls un ērts veids, kā ļaundariem gūt peļņu.

Kā lielākā daļa ļaunatūru, izspiedējvīruss sākas ar jūsu datora inficēšanu, proti, atverot inficētu e-pasta pielikumu vai uzklikšķinot uz saites pikšķerēšanas e-pastā. Kad ļaunatūra inficē jūsu datoru, tā šifrē failus cietajā diskā, iespējams, pat visu disku un jebko citu, kas pievienots datoram, lai vairs nevarat piekļūt saviem failiem. Tad tā jūs informē, ka vienīgais veids, kā atgūt jūsu failus, ir samaksāt ļaundariem izpirkumu, tādēļ tos sauc par šifrējošiem izspiedējvīrusiem. Dažkārt ļaundari draud publicēt jūsu failus, ja izpirkuma maksa netiks samaksāta. Noziedznieki var pieprasīt samaksu arī neizsekojamā virtuālā valūtā, piemēram, Bitcoin. Ja jūs veiksiet izpirkuma maksu, ļaundari, iespējams, jums atjaunos piekļuvi failiem, taču tam nav garantijas. Dažkārt tie paņem jūsu naudiņu, un, jums nezinot, atstāj jūsu datoru inficētu, vai arī turpina prasīt aizvien vairāk naudas.

Kā aizsargāties pret infekciju

Jūs savu datoru varat pasargāt no izspiedējvīrusiem gluži tāpat, kā no jebkuras citas ļaunatūras. Šeit apkopoti trīs svarīgākie soļi:

- **Atjauniniet sistēmas un programmatūru**: Kibernoziedznieki visbiežāk inficē datorus un iekārtas, kurām nav novērstas programmatūras kļūdas (pazīstamas kā ievainojamības). Jo jaunāka ir jūsu programmatūra, jo mazāk tai ir zināmu ievainojamību, un kibernoziedzniekiem to ir grūtāk inficēt. Tāpēc pārliecinieties, vai operētājsistēmām, programmām un ierīcēm ir automātiska atjaunināšana.

- **Uzstādiet antivīrusu programmu**: Izmantojiet jaunāko antivīrusu programmatūru no uzticama piegādātāja. Šādi rīki ir paredzēti, lai atklātu un apturētu ļaunatūras. Tomēr antivīrusu programma nevar bloķēt vai likvidēt visas ļaunatūras, un parasti tā nevar arī atjaunot failus pēc izspiedējvīrusa uzbrukuma. Kibernoziedznieki nepārtraukti veic uzlabojumus, izstrādā jaunas un sarežģītākas uzbrukumu un inficēšanas metodes, lai izvairītos no to atklāšanas. Tāpat arī

antivīrusu ražotāji nepārtraukti papildina savus produktus ar jaunām spējām atklāt ļaunatūru. Daudzējādā ziņā tā ir kļuvusi par bruņošanās sacensību starp abām pusēm, mēģinot vienai otru apsteigt.

- **Esiet modri**: Kibernoziedznieki, izmantojot pikšķerēšanas e-pastu uzbrukumus, bieži panāk, ka cilvēki paši uzinstalē izspiedējvīrusus un citas ļaunatūras. Piemēram, ļaundaris var nosūtīt jums e-pastu, kas izskatās ticams un satur pielikumu vai saiti. Iespējams, izskatās, ka e-pasts nāk no jūsu bankas vai drauga. Tomēr, atverot pievienoto failu vai noklikšķinot uz saites, jūs varat aktivizēt ļaunatūru, kas inficē datoru. Ja ziņojums satur steidzamības faktoru vai izskatās pārāk labs, lai būtu patiesība, tas visticamāk būs uzbrukums. Esiet modri - kibernoziedznieki darbojas, izmantojot jūsu emocijas. - Veselais saprāts parasti ir jūsu labākā aizsardzība.

Veidojiet failu rezerves kopijas

Tā kā pieņemt, ka vienmēr varēsiet novērst uzbrukumu, ir nesaprātīgi, tad rezerves kopijas ir jūsu labākā aizsardzība pret izspiedējvīrusiem. Ja jums ir jūsu svarīgo dokumentu un citu failu rezerves kopijas, uzbrukuma gadījumā jums ir iespēja failus atjaunot no kopijām, nevis maksājot izpirkuma maksu. Ir svarīgi, lai rezerves kopiju veidošanai izmantojat kādu no automatizētiem rīkiem, kuri regulāri veic visu jūsu failu kopēšanu, un lai failu atjaunošanas procedūra ir pārbaudīta, pārliecinoties, ka nepieciešamības gadījumā varēsiet veikt datu atjaunošanu. Ir pieejama virkne vienkāršu mākoņpakalpojumu un lokālu rezerves datu glabāšanas risinājumu, kurus jūs varat uzinstalēt uz sava datora un droši lietot, lai veidotu failu rezerves kopijas.

Viesredaktors

Lenny Zeltser ir galvenais informācijas drošības eksperts kiberdrošības aktīvu pārvaldības uzņēmumā Axonius. Viņš arī pasniedz SANS Institūta kursu par ļaunatūras apkarošanu un analīzi. Lenny ir aktīvs Twitter lietotājs @lennyzeltser un raksta blogu par drošību zeltser.com.

Resursi

Rezerves kopijas?: https://www.sans.org/security-awareness-training/resources/got-backups
Kā atpazīt pikšķerēšanu: https://www.sans.org/security-awareness-training/resources/stop-phish
Kāpēc svarīgi veikt atjauninājumus: https://www.sans.org/security-awareness-training/resources/power-updating
SANS FOR610 Course - Ļaunatūras reversā inženierija: https://sans.org/for610

Tulkojums: CERT.LV

 Redakcija: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley