OUCH! 2025. gada jūnijs

Jūsu ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Aizsardzība pret ļaunatūru: neredzamais ienaidnieks

"Nekaitīgs" e-pasts ar postošām sekām

Sāra ir talantīga pašnodarbināta grafikas dizainere, kuras radošums un iztikas līdzekļi ir atkarīgi no viņas personāldatora. Kādā pēcpusdienā, kad projektu termiņi tuvojās un darbs bija saspringts, viņa saņēma e-pasta vēstuli no potenciāla klienta. Tēmas laukā bija rakstīts: "Aizraujoša projekta iespēja." Sūtītāja vārds šķita pazīstams, iespējams, tas bija ieteikums no kāda iepriekšējā klienta. Vēloties izpētīt jauno darbu, Sāra atvēra e-pasta vēstuli, lai atrastu šķietami patīkamu ziņu, kurā bija izklāstīts potenciālais projekts, un pielikums ar norādi "ProjectBrief.pdf". Viņa nekavējoties atvēra pielikumu, cerot iegūt informāciju par jauno uzdevumu.

Sārai nezinot, šis viens klikšķis aizsāka virkni notikumu, kas drīz vien sagrāva viņas profesionālo un personīgo dzīvi. Pielikums bija prasmīgi maskēta ļaunatūra, kas bija izstrādāta, lai nemanāmi iekļūtu datora sistēmā. Turpmākajās dienās Sāra pamanīja nelielas izmaiņas: pasliktinājās viņas personāldatora veiktspēja un negaidīti pārstāja darboties programmas. Viņa šīs problēmas uzskatīja par tipiskām tehniskām kļūmēm, saistot tās ar savas ierīces vecumu un tās intensīvo lietošanu.

Tomēr drīz vien situācija pasliktinājās. Kad Sāra mēģināja pieslēgties savai internetbankai, lai pārskatītu norēķinu kontu un krājkontus, viņa atklāja, ka esošā parole vairs nedarbojas. Viņu pārņēma panika, kad viņa sazinājās ar savu banku un uzzināja, ka trīs ārvalstu kontos ir veiktas ievērojamas naudas izmaksas. Viņas gadiem ilgi rūpīgi krātie ietaupījumi, kas bija nopelnīti smagā darbā, bija pazuduši. Sāra drīz vien saprata, ka ir kļuvusi par ļaunatūras uzbrukuma upuri, kas inficēja viņas personālo datoru, sagrāva viņas finansiālo drošību un, potenciāli, apdraudēja arī viņas profesionālo reputāciju.

Kas ir ļaunatūra?

Ļaunatūra ir kibernoziedznieku radīta datorprogramma, kas bez jūsu piekrišanas vai ziņas iekļūst datorsistēmās vai mobilajās ierīcēs un tās sabojā vai kontrolē. Šis termins ir vārdu "*ļaunprātīgs*" un "*programmatūra*" kombinācija. Droši vien esat dzirdējuši par datorvīrusiem, trojāņiem (slepeni ieviesta ļaunprogrammatūra, kas saskaņā ar hakera iecerēm veic manipulācijas mērķsistēmā.;), izspiedējvīriem un spiegprogrammatūru. Šie ir ļaunatūras veidi.

Ļaunatūra ir bīstama tāpēc, ka, tiklīdz jūsu dators vai ierīce ir inficēta, kibernoziedznieks var iegūt pilnīgu kontroli pār to, jums pat nezinot par to. Tā var nemanāmi fiksēt jūsu darbības, tostarp to, ar ko sazināties, ko sakāt, kā arī jūsu svarīgāko kontu piekļuves datus un paroles.

Ļaunatūra var arī nemanāmi iegūt visus jūsu failus, tostarp attēlus, videoklipus vai svarīgus dokumentus. Tā var inficēt gandrīz jebkuru sistēmu, viedtālruņus, viedpulksteņus vai pat viedierīces jūsu mājās, piemēram, termoregulatoru un durvju slēdzenes. Arī Apple iPhone un Mac datorus ļaunatūra var inficēt, ja tie nav pietiekami aizsargāti.

Nostipriniet savu aizsardzību: stratēģijas drošībai

Par laimi, jau tagad iespējams veikt vairākus vienkāršus pasākumus, lai pasargātu datoru no vīrusu iekļūšanas.

1. **Uzturiet atjauninātu sistēmu**: regulāri atjauniniet operētājsistēmu, programmatūru un mobilās lietotnes, lai nodrošinātu, ka zināmās ievainojamības ir novērstas un ka ir instalētas jaunākās drošības funkcijas. Vieglākais veids, kā to izdarīt, ir ieslēgt automātiskos atjauninājumus.
2. **Esiet piesardzīgi ar e-pastiem un ziņām** : viens no izplatītākajiem veidiem, kā kibernoziedznieki inficē jūsu ierīces, ir ar viltu panākt, lai jūs atverat inficētu pielikumu, lejupielādējat inficētu programmatūru vai noklikšķināt uz kaitīgas saites. Uzmanieties no aicinājumiem rīkoties nekavējoties, vai no ziņām, kas ir pārāk labas, lai būtu patiesas.
3. **Izmantojiet spēcīgu un unikālu paroli**: paroles ir jūsu drošības atslēga. Ja kibernoziedznieks uzlauž kādu no tām, viņš var pārņemt un inficēt konkrēto ierīci vai kontu. Aizsargājiet visas ierīces ar unikālām, spēcīgām parolēm vai frāžveida parolēm. Paroles garumam ir izšķiroša nozīme. Ja vien tas ir iespējams, izmantojiet daudzfaktoru/divfaktoru autentifikāciju (MFA vai 2FA).
4. **Lejupielādējiet tikai no uzticamiem avotiem**: lejupielādējiet programmatūru, multivides failus vai lietotnes tikai no oficiālām vai uzticamām vietnēm. Bieži sastopams veids, kā kiberuzbrucēji inficē mobilās ierīces, ir maldinot jūs, liekot lejupielādēt neautorizētas mobilās lietotnes, kas paredzētas, lai pārņemtu jūsu ierīci.
5. **Antivīrusu programmatūra**: kad tas ir iespējams, instalējiet drošu un uzticamu pretvīrusu programmatūru un iestatiet tās automātisku atjaunināšanu. Ne visās sistēmās vai ierīcēs var uzstādīt antivīrusu un antivīrusu programmatūra nevar atpazīt visas ļaunatūras, taču tā to var palīdzēt daudzās situācijās.

Viesredaktore

Šerija Pena ir galvenā privātuma aizsardzības speciāliste uzņēmumā Agora. Savu karjeru viņa sāka vietējā pašvaldībā un pēc maģistra grāda iegūšanas informācijas drošībā/kiberdrošībā pārgāja strādāt privātajā sektorā. Šerija gandrīz desmit gadus ir strādājusi drošības jomā un pašlaik ir WiCyS Colorado vadītāja.

Resursi

Frāzveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase/
Paroļu pārvaldnieku iespējas: https://www.sans.org/newsletters/ouch/power-password-managers/
Atjauninājumu nozīme: https://www.sans.org/newsletters/ouch/power-updating/
Lejupielādes risks: kā izvairīties no kaitīgām mobilajām lietotnēm:
https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps/

CERT.LV