OUCH! | 2016.gada aprīlis

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Mani ir “uzlauzuši”, ko darīt?

Pārskats

Mēs zinām, Jums rūp Jūsu datora un mobilo ierīču drošība, un Jūs veicat pasākumus, lai tās aizsargātu. Tomēr, neatkarīgi no tā, cik droši jūs izmantojat tehnoloģijas, agrāk vai vēlāk Jūsu ierīces var “uzlauzt” vai “kompromitēt”. Šajā izdevumā jūs uzzināsiet, kā noteikt, vai Jūsu dators vai mobilā ierīce ir “uzlauzta”, un ko Jūs varat darīt tādā gadījumā. Galu galā, jo ātrāk Jūs atklāsiet, ka kaut kas nav kārtībā, jo ātrāk varēsiet reaģēt un jo lielāka ir iespēja samazināt kaitējumu, ko Jums var nodarīt kiber uzbrucējs.

Viesredaktors

Samantha Davison (**@sam_e_davison**) ir par drošību informējošās un izglītojošās programmas vadītāja uzņēmumā “Uber”, kur izglīto darbiniekus vairāk kā 350 pilsētās visā pasaulē.

Pazīmes, kas liecina par “uzlaušanu”

“Uzlaušanu” nav viegli pamanīt, jo nav vienas konkrētas pazīmes, pēc kuras to vārētu noteikt. Tā vietā hakeri parasti atstāj vairākas pazīmes vai indikatorus. Jo vairāk Jūsu sistēma atbilst šiem indikatoriem, jo lielāka ir iespēja, ka tā ir “uzlauzta”.

- Jūsu antivīrusu programma ir paziņojusi par sistēmas infekciju, īpaši, ja tā nespēj izdzēst vai ievietot karantīnā inficētos failus.
- Jūsu tīmekļa pārlūka mājas lapa ir negaidīti mainījusies vai pārlūks atver mājas lapas, ko Jūs neesat atvēruši.
- Jūsu datorā vai ierīcē parādās jauni konti, ko Jūs neesat izveidojis, vai jaunas programmas, ko Jūs neesat instalējis.
- Jūsu dators vai aplikācijas nepārtraukti beidz darboties vai “uzkaras”, parādās dīvaini logi vai nezināmas aplikācijas.
- Programma prasa Jūsu atļauju veikt izmaiņas sistēmā, lai gan Jūs tajā brīdī neko neinstalējat un neatjaunojat aplikācijas.
- Vairs nedarbojas Jūsu parole sistēmai vai tiešsaistes kontam, lai arī Jūs zināt, ka parole ir pareiza.
- Draugi prasa Jums, kāpēc Jūs sūtiet viņiem e-pasta mēstules (SPAMu), lai arī Jūs neesat neko sūtījis.
- Jūsu mobilā telefona rēķinā parādās nesaprotamas izmaksas par paaugstinātas maksas īsziņām.
- Jūsu ierīce pēkšņi sāk strauji tērēt bateriju vai datu apjomu.

Mani ir “uzlauzuši”, ko darīt?

Kā rīkoties

Jo ātrāk Jūs reaģējat gadījumā, ja Jums ir aizdomas par datora vai ierīces “uzlaušanu”, jo labāk. Ja tas ir darba dators vai ierīce, vai Jūs to izmantojat darbam, labāk nemēģiniet paši risināt problēmu. Jūs ne tikai izdarīsiet vairāk ļauna, nekā laba, bet arī potenciāli varat iznīcināt vērtīgus pierādījumus izmeklēšanai. Tā vietā nekavējoties paziņojiet par incidentu darba devējam, sazinoties ar palīdzības dienestu, drošības komandu vai vadītāju. Ja kāda iemesla dēļ nevarat sazināties ar darba devēju vai esat satraukts par kavēšanos, atslēdziet iekārtu no tīkla un tad izslēdziet to, vai ieslēdziet lidojuma režīmu. Pat ja Jūs neesat pārliecināts, ir labāk drošības pēc paziņot. Ja tas ir personīgais dators vai iekārta, tad šeit ir daži pasākumi, ko varat veikt.

Agrāk vai vēlāk Jūsu dators vai ierīce var tikt kompromitēta. Jo ātrāk Jūs atklājat incidentu un spējat reaģēt, jo labāk.

- **Nomainiet paroles**: Ne tikai datora un mobilo iekārtu paroles, bet arī visu tiešsaistes kontu paroles. Paroļu maiņai neizmantojiet “uzlauzto” datoru. Paroļu maiņai izmantojiet iekārtu, par kuras drošību esat pārliecināti.
- **Antivīruss**. Ja antivīrusa programma ziņo par inficētu failu, sekojiet tās rekomendācijām. Parasti tas nozīmē faila ievietošanu karantīnā vai dzēšanu. Vairums programmu norādīs saites, kur varat uzzināt vairāk par attiecīgo infekciju. Ja Jums ir šaubas, ievietojiet failu karantīnā. Ja tas nav iespējams, izdzēsiet to.
- **Atjaunošana**. Ja nespējat novērst infekciju, vai gribat būt pilnīgi pārliecināts, ka sistēma ir salabota, visdrošākā iespēja ir to pilnībā atjaunot. Datora gadījumā sekojiet ražotāja instrukcijām. Vairumā gadījumu tas nozīmē izmantot ražotāja rīkus, lai pārinstalētu operētājsistēmu. Ja tas nav iespējams - attiecīgie rīki nav atrodami vai ir bojāti, sazinieties ar ražotāju vai meklējiet informāciju mājas lapā. Nepārinstalējiet operētājsistēmu no rezerves kopijām, jo tajās varētu būt tās pašas nepilnības, kas ļāva hakerim iegūt pieeju. Rezerves kopijas jāizmanto tikai datu atjaunošanai. Mobilajām ierīcēm sekojiet ražotāja vai pakalpojuma sniedzēja instrukcijām, tām vajadzētu būt pieejamām arī attiecīgajās mājas lapās. Vairumā gadījumu tas nozīmē atjaunot rūpnīcas iestatījumus. Ja neesat pārliecināts par atjaunošanas procesu, meklējiet palīdzību pie profesionāļiem. Vai, ja Jūsu dators vai ierīce ir veca, var apsvērt domu par jaunas iegādi - tas varētu būt lētāk un vienkāršāk. Visbeidzot, ja esat iegādājies jaunu ierīci

Mani ir “uzlauzuši”, ko darīt?

vai atjaunojis veco, pārliecinieties, ka tā ir pilnībā atjaunināta un tajā ir aktuālā programmatūras versija, kā arī ir iespējota automātiskā atjaunināšana, ja tas ir iespējams.

- **Rezerves kopijas**. Svarīgākais solis, ko varat veikt savai aizsardzībai, ir regulāri sagatavot rezerves kopijas. Jo biežāk tiek gatavotas rezerves kopijas, jo labāk. Daži risinājumi automātiski veidos rezerves kopijas jauniem vai izmainītiem failiem katru stundu. Neatkarīgi no tā, kādu rezerves kopiju risinājumu izmantojiet, pārliecinieties, ka failu atjaunošana no tiem ir iespējama. Bieži gadījumos, kad esat “uzlauzts”, vienīgais veids, kā atgūt Jūsu datus, ir atjaunot tos no rezerves kopijām.
- **Tiesībsargājošās iestādes**: Ja Jūtaties jebkādā veidā apdraudēts, ziņojiet par incidentu attiecīgajām tiesībsargājošajām iestādēm.

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

Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2015#august2015
Paroles:	https://securingthehuman.sans.org/ouch/2015#april2015
Kas ir ļaunatūra:	https://securingthehuman.sans.org/ouch/2016#march2016
Jūsu jaunā planšetdatora drošība:	https://securingthehuman.sans.org/ouch/2016#january2016

License

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