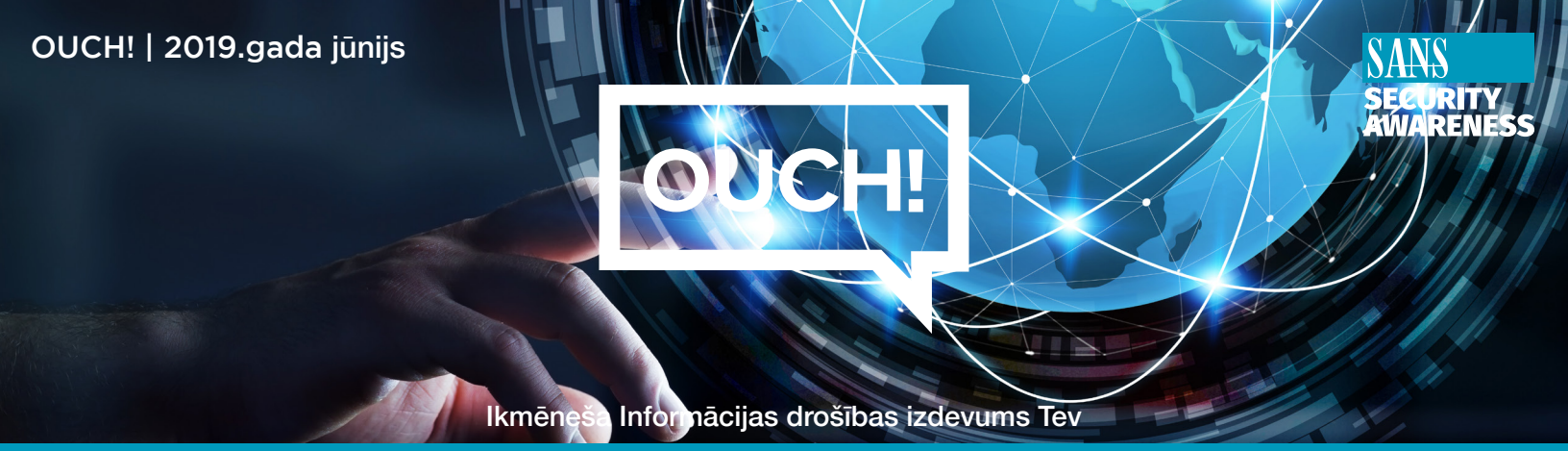

Ikmēneša Informācijas drošības izdevums Tev

Tumšais tīmeklis

Pārskats

Iespējams, esat dzirdējuši medijos vai kādu citu lietojam terminu "tumšais tīmeklis" (dark web) un brīnījušies, "*kas ir šis tumšais tīmeklis?*" vai arī "*vai man kaut kas šajā sakarā būtu jāpasāk?*". Šodien mēs izskaidrosim, kas ir "tumšais tīmeklis", un ko tas nozīmē jums.

Kas tas ir?

Tumšais tīmeklis sastāv no Interneta sistēmām, kas ir radītas, lai sazinātos vai veiktu informācijas apmaiņu droši un anonīmi. Nav viena "tumšā tīmekļa"; tas nav kaut kas līdzīgs Facebook, kuru pārvalda viena organizācija. Tā vietā tumšais tīmeklis ir dažādu sistēmu un tīklu kopums, kuru pārrauga dažādi cilvēki, un kas tiek izmantots visdažādākajiem mērķiem. Šīs sistēmas ir savienotas un ir daļa no Interneta, taču jūs to neatradīsiet, izmantojot savus ierastos interneta meklētājus. Bieži vien jums ir nepieciešama specializēta programmatūra, lai tos atrastu un tiem piekļūtu. Viens piemērs ir Tor projekts. Lai piekļūtu šim tumšajam tīmeklim, jums jālejuplādē un jāuzstāda Tor Browser pārlūks. Kad jūs pieslēdzaties tīmekļa serveriem, izmantojot Tor Browser, jūsu šifrētā datu plūsma ceļo, izmantojot citas iekārtas, kurās arī ir Tor. Pārvietojoties no vienas iekārtas uz citu, izejošā IP adrese mainās, un tas nozīmē, ka tad, kad nokļūstat tīmekļa vietnē, jūsu aktivitātes ir tikušas anonimizētas. Citi tumšā tīmekļa piemēri ir Zeronet, Freenet un I2P.

Kas to izmanto?

Tumšo tīmekli izmanto kibernoziedznieki. Viņi tumšajā tīmeklī uztur tīmekļa vietnes un forumus, lai padarītu iespējamas savas pretlikumīgās aktivitātes, piemēram, narkotiku iegādi vai liela apjoma (gigabaiti) zagtu datu pārdošanu - viss anonīmi un droši. Piemēram, kad kibernoziedznieki uzlauž banku vai tiešsaistes tirdzniecības vietni, tie nozog tik daudz informācijas, cik vien spēj, tad pārdod šo informāciju citiem kibernoziedzniekiem tumšā tīmekļa vietnēs.

Ir arī leģitīmi tumšā tīmekļa izmantošanas veidi. Piemēram, cilvēki valstīs, kurās ir smaga cenzūra, var izmantot tumšo tīmekli, lai dalītos ar informāciju un redzētu, kas citur pasaulē notiek, saglabājot savu privātumu un paliekot anonīmi. Žurnālisti, trauksmes cēlāji, uz privātumu orientēti cilvēki var izmantot tumšo tīmekli, lai saglabātu savu anonimitāti un apietu cenzūru. Papildus tam,

šādi indivīdi var izmantot tehnoloģijas, tādas kā Tor Browser, ne tikai, lai piekļūtu tumšajam tīmeklim, bet arī, lai anonīmi sērfotu parastajā Internetā.

Kas man jādara?

Ja vien jums nav specifiskas vajadzības piekļūt tumšajam tīmeklim, mēs aicinātu jūs to nedarīt. Dažas tumšā tīmekļa vietnes tiek izmantotas pretlikumīgiem mērķiem, daudzas vietnes izmantos jūsu datoru P2P tīklā (peer network), lai sasniegtu savus mērķus, un dažos gadījumos jūsu dators var tikt pat skenēts vai tam var uzbrukt. Dažas kompānijas piedāvā monitoringa pakalpojumus, kas jūs brīdinātu, ja jūsu vārds vai citi jūsu dati tiktu nozagti un parādītos tumšajā tīmeklī. Šo servisu patiesā vērtība ir apšaubāma. Labākais vaids, kā sevi pasargāt, ir pieņemt, ka daļa jūsu informācijas jau ir tumšajā tīmeklī un to jau izmanto kibernoziedznieki. Rezultātā...

⚠

- **Ar aizdomām izturieties pret telefona zvaniem un e-pastiem, kas uzdodas par iestādēm vai organizācijām un steidzina jūs veikt darbību, piemēram, samaksāt sodu. Noziedznieki var pat izmantot par jums atrastu informāciju, lai izveidotu personalizētu uzbrukumu.**
- **Sekojiet līdzi savām maksājumu kartēm un bankas izrakstiem. Varbūt pat iespējojiet paziņojumus par dienā notikušajām transakcijām. Tādejādi jūs pamanīsiet, ja būs notikusi kāda finanšu krāpniecība. Ja jūs to pamanāt, nekavējoties par to paziņojiet savam maksājumu karšu izsniedzējam vai bankai.**
- **Iesaldējiet savu kredītreitingu (ASV). Tas neietekmē jūsu kredītkartes izmantošanu, bet ir viens no efektīvākajiem soļiem, kā varat sevi pasargāt no identitātes zādzības.**

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.

Viesredaktors

Micah Hoffman *(@WebBreacher) ir Spotlight Infosec LLC vadošais eksperts, sertificēts SANS institūta instruktors un SANS OSINT kursu autors. Micah aizraušanās ar kiber un publiskos avotos pieejamu informāciju parādās viņa projektos, kursu programmā un mācību stilā.*

Resursi

Personalizēti uzbrukumi	https://www.sans.org/u/RfW
Sociālā inženierija:	https://www.sans.org/u/Rg1
Identitātes zādzība:	https://www.identitytheft.gov
Kredīta iesaldēšana:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser:	https://www.torproject.org/
SANS OSINT kurss:	https://sans.org/sec487

Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV