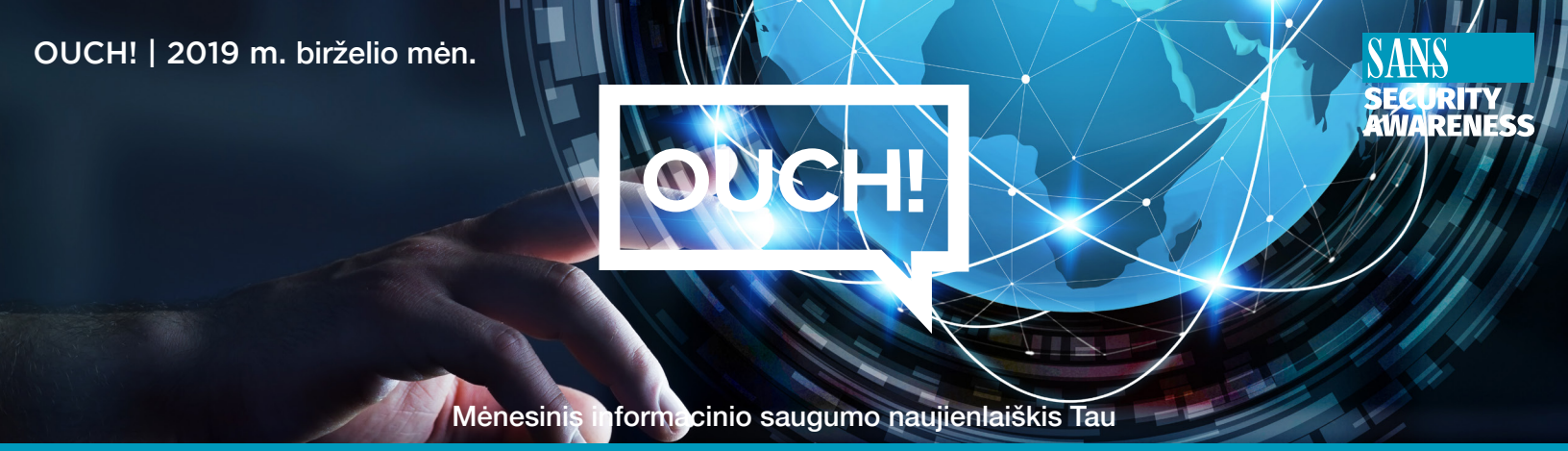

Mėnesinis informacinio saugumo naujienlaiškis Tau

Tamsusis saitynas (dark web)

Apžvalga

Tikriausiai esate girdėję kitų žmonių arba žiniasklaidos naudojamą terminą „tamsusis saitynas“ ir susimąstę *„Kas gi yra tas tamsusis saitynas?“* arba *„Ar man reikėtų imtis kokių nors veiksmų dėl jo?“*. Šiandien paaiškinsime, kas yra tamsusis saitynas ir ką jis jums turėtų reikšti.

Kas tai yra?

Tamsųjį saityną sudaro saugiam ir anonimiškam bendravimui bei informacijos dalinimuisi sukurtos interneto sistemos. Nėra tik vieno „tamsiojo saityno“, kadangi tai nėra kažkas panašaus į „Facebook“ svetainę, kurią valdo viena organizacija. Tamsusis saitynas labiau primena skirtingų sistemų ir tinklų, kuriuos valdo atskiri žmonės, rinkinį, naudojamą įvairiems tikslams. Prie šių sistemų vis dar yra jungiamasi internetu, todėl jos yra laikomos interneto dalimi, tačiau įprastai tradicinėmis paieškos sistemomis jų nerasite. Be to, dažniausiai, norint jas atrasti ir prie jų prisijungti, reikės kompiuteryje įdiegti specialią programinę įrangą. Vienas iš pavyzdžių - „Tor Project“. Norėdami prisijungti prie tamsiojo saityno, turite parsisiųsti ir kompiuteryje įdiegti „Tor“ naršyklę. Prisijungus prie saityno serverių per „Tor“ naršyklę, jūsų šifruotasis duomenų srautas keliaus per kitus kompiuterius, kuriuose taip pat naudojama „Tor“. Jam keliaujant per šiuos kompiuterius, jūsų pradinis kompiuterio adresas keisis, o tai reiškia, kad jums patekus į svetainę, jūsų internetinė veikla bus anonimiška. Kiti tamsiojo saityno pavyzdžiai yra platformos „Zeronet“, „Freenet“ ir „I2P“.

Kas juo naudojasi?

Dažniausiai tamsiuoju saitynu naudojasi kibernetiniai nusikaltėliai. Jame jie prižiūri svetaines ir forumus, kuriuose anonimiškai ir saugiai vykdoma tokia nusikalstama veika kaip narkotikų pirkimas ar neteisėtais būdais gautų duomenų pardavimas. Pavyzdžiui, kibernetiniams nusikaltėliams įsilaužus į banką ar internetinės prekybos parduotuvę, jie pavogia kiek įmanoma daugiau informacijos, kurią vėliau parduoda kitiems kibernetiniams nusikaltėliams tamsiojo saityno svetainėse.

Kartais tamsiuoju saitynu naudojamasi teisingumo tikslais. Pavyzdžiui, žmonės, gyvenantys šalyse, kuriose yra paplitusi cenzūra, gali naudotis tamsiojo saityno tinklais, kad išsaugodami savo privatumą, anonimiškai pasidalintų informacija ir pamatytų, kas

vyksta pasaulyje. Tamsiuoju saitynu taip pat gali naudotis žurnalistai ar asmenys, pranešantys apie pažeidimus, ir privatumo norintys žmonės, siekiantys padidinti savo anonimiškumą ir apeiti cenzūrą. Be to, tokie asmenys gali naudoti „Tor“ naršyklės technologijas ne tik tam, kad gautų prieigą prie tamsiojo saityno, bet kad anonimiškai naršytų įprastame internete.

Kaip turėčiau elgtis?

Jei neturite konkrečios priežasties jungtis prie tamsiojo saityno, rekomenduojame prie jo nesijungti. Kai kurios tamsiojo saityno svetainės yra naudojamos neteisėtiems tikslams ir daugumoje svetainių jūsų kompiuteris bus naudojamas tarpusavyje sąveikaujančiame tinkle, skirtame įgyvendinti svetainių naudotojų tikslus, o kai kuriais atvejais gali būti bandoma gauti prieigą prie jūsų kompiuterio ar net į jį įsilaužti. Kai kurios įmonės siūlo stebėjimo paslaugas, skirtas išsiaiškinti ar kibernetiniai nusikaltėliai nežino jūsų vardo ir ar nebuvo pavogta kita jūsų informacija, kuri po to yra paskelbiama tamsiajame saityne. Reali tokių paslaugų vertė yra abejotina. Geriausias būdas apsisaugoti yra manyti, kad dalis jūsų informacijos jau yra patekusi į kibernetinių nusikaltėlių naudojamą tamsųjį saityną. Todėl:

- **būkite įtarūs, sulaukę bet kokių telefono skambučių arba el. pašto laiškų nuo asmenų, apsimetančių oficialių organizacijų atstovais ir darančių psichologinį spaudimą imtis kokių nors veiksmų, pavyzdžiui, sumokėti baudą. Nusikaltėliai netgi gali naudoti apie jus rastą informaciją tam, kad sukurtų individualizuotą apgaulingą laišką.**
- **stebėkite savo kredito kortelės ir banko išrašus. Galbūt net nustatykite kasdieninius pranešimus, kuriuos gautumėte atlikus bet kokias operacijas. Tokiu būdu galėtumėte nustatyti, ar yra vykdomas koks nors finansinis sukčiavimas. Nustatę tokią nusikalstamą veiką, nedelsdami apie ją praneškite savo kredito kortelės bendrovei arba bankui.**

Kviestinis redaktorius

Micah Hoffman *(@WebBreacher) įmonėje „Spotlight Infosec LLC“ dirba pagrindiniu tyrėju, o taip pat yra sertifikuotas „SANS instituto“ dėstytojas ir „SANS instituto“ kursų apie atvirųjų šaltinių žvalgybą medžiagos autorius. Micah aistrą kibernetikos ir atvirųjų šaltinių žvalgybos sričiai galima įžvelgti jo projektuose, mokomojoje medžiagoje ir net mokymo stiliuje.*

Šaltiniai

Individualizuoti apgaulingi laiškai: https://www.sans.org/u/RfW
Socialinė inžinerija: https://www.sans.org/u/Rg1
Federalinės prekybos komisijos svetainė, kurioje galima pranešti apie asmens tapatybės duomenų vagystę: https://www.identitytheft.gov
„Tor“ naršyklė: https://www.torproject.org/
„SANS“ instituto kursas apie atvirųjų šaltinių žvalgybą: https://sans.org/sec487