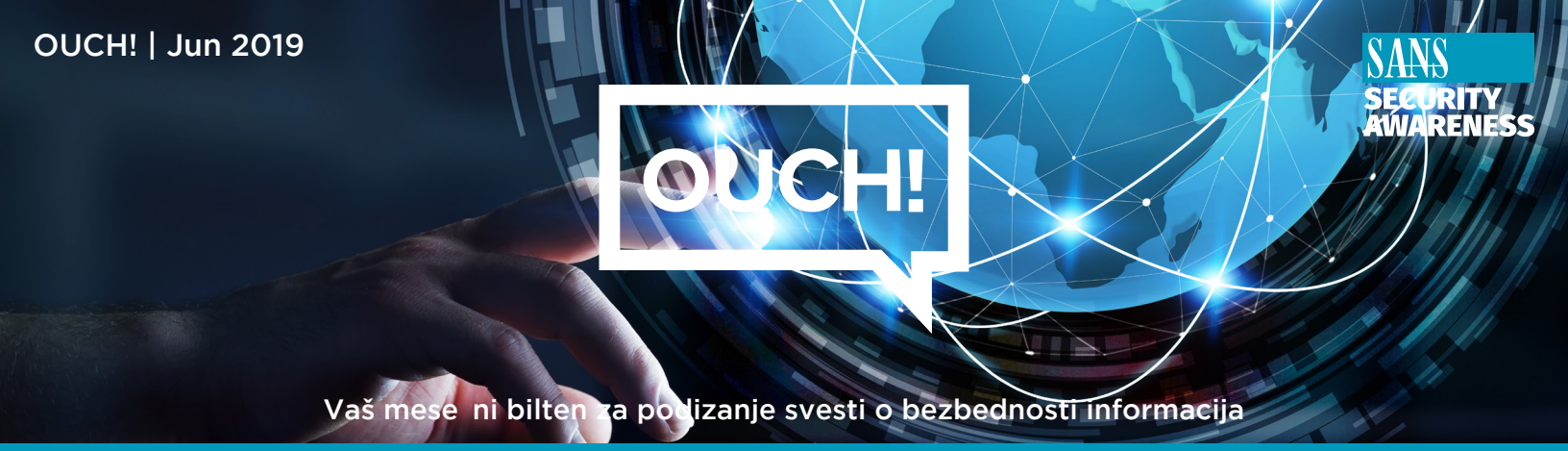

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Dark veb – mračna strana interneta

Uvod

Verovatno ste već čuli za pojam “Dark veb” i možda ste se pitali šta je to i da li biste nešto trebali da preduzmete u vezi sa tim. U nastavku teksta ćemo objasniti šta je Dark veb i kakav značaj može imati za vas.

Šta je to?

Dark veb (u doslovnom prevodu: mračni internet) se sastoji od sistema na internetu koji omogućavaju anonimnu komunikaciju i razmenu informacija na bezbedan način. Ne postoji jedan Dark veb, on nije poput Fejsbuka kojim upravlja jedna organizacija. Dark veb je skup različitih sistema i mreža koje održavaju različiti ljudi i koji se koriste u najrazličitije svrhe. Ti sistemi su ipak povezani na internet i njegov su deo, ali ih uglavnom nije moguće pronaći korišćenjem standardnih pretraživača. Najčešće je potrebno da na svom računaru instalirate poseban softver da biste mogli da ih pronađete i da im pristupite. Jedan od primera je Tor Project. Da biste pristupili ovom Dark vebu, neophodno je da preuzmete i instalirate Tor Browser. Kada korišćenjem ovog softvera pristupite veb serverima, taj enkriptovani saobraćaj prolazi i druge računare koji takođe koriste Tor. IP adresa izvorišta saobraćaja se u tim prelascima s računara na računar menja što znači da kada saobraćaj koji ste generisali dospe do veb sajta, vaša aktivnost biva praktično anonimizovana. Drugi primeri Dark veb mreža su Zeronet, Freenet i I2P.

Ko ga koristi?

Sajber kriminalci su veliki korisnici Dark veba. Oni na Dark vebu održavaju veb sajtove i forume koji su podrška njihovim kriminalnim aktivnostima kao što su trgovina drogom ili preprodaja gigabajtova hakovanih podataka, i to na anoniman i bezbedan način. Na primer, kada sajber kriminalac hakuje banku ili internet prodavnicu, on nastoji da ukrade što više informacija koje će potom preprodati drugim sajber kriminalcima koristeći sajtove na Dark vebu.

Postoje i legitimne svrhe upotrebe Dark veba. Na primer, ljudi u zemljama u kojima je nivo cenzure visok mogu da koriste Dark Veb mreže za razmenu informacija i upoznavanje sa dešavanjima u svetu, dok istovremeno imaju zaštićenu privatnost i ostaju anonimni. Novinari, uzbunjivači i ljudi koji se zalažu za privatnost mogu koristiti Dark veb u cilju postizanja anonimnosti i

zaobilaženja cenzure. Pored toga, navedeni pojedinci mogu koristiti tehnologije kao što je Tor Browser ne samo da za pristup Dark vebu, već i anonimnu pretragu standardnog Interneta.

Šta da preduzmem?

Osim ako nemate poseban razlog da pristupate Dark vebu, savetuje se da ga ne koristite. Neki Dark Veb sajtovi koriste se u ilegalne svrhe, mnogi sajtovi će koristiti vaš računar u mreži ravnopravnih računara (peer network) kroz koje saobraćaj prolazi da bi ostvarile svoje ciljeve, a u nekim slučajevima vaš računar može čak biti i cilj probe ili napada. Iako postoje kompanije koje nude usluge praćenja i obaveštavanja o tome da li su vaše ime ili druge informacije ukradene od strane sajber kriminalaca pronađene na Dark vebu, stvarna vrednost ovih usluga je upitna. Najbolji način da se zaštitite je da pretpostavite da su neke od vaših informacija već prisutne na Dark vebu i da ih sajber kriminalci uveliko koriste. U cilju sopstvene zaštite:

- **Budite sumnjičavi prema telefonskim pozivima ili elektronskoj pošti jer ih mogu uputiti osobe koje se samo pretvaraju da su zvanične organizacije koje će vas pri tom često požurivati da preduzmete neku radnju, poput plaćanja kazne. Kriminalci u okviru personalizovanih prevara često koriste i informacije koje su o vama pronašli na standardnom internetu.**
- **Uvek nadgledajte korišćenje vaših platnih kartica i platnih naloga. Koristite notifikacije o izvršenim transakcijama. Na taj način ćete najbrže primetiti ako se desi neka finansijska prevara. Ako uočite takvu transakciju, o tome odmah obavestite vašu banku.**

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Mika Hofman *(@WebBreacher) je glavni istražitelj u kompaniji Spotlight Infosec LLC, sertifikovani instruktor SANS instituta i autor SANS OSINT obuka. Njegova strast prema sajber bezbednosti i pretraživanju javno dostupnih resursa na internetu ogleda se u projektima u kojima učestvuje, obukama koje kreira i načinu na koji te obuke sprovodi.*

Dodatni materijal

Personalizovane prevare:	https://www.sans.org/u/RfW
Socijalni inženjering:	https://www.sans.org/u/Rg1
Pregledač Tor:	https://www.torproject.org/
SANS OSINT obuka:	https://sans.org/sec487