DEEP & DARK WEB

Uvod u razumevanje pojmova i razlike između deep web-a i dark web-a...

OSNOVNI POJMOVI

- **Surface Web:**
  - Predstavlja deo world wide web-a dostupan preko standardnih intrernet pretraživača (Google,Bing,Yahoo,…).
  - Standardni pretraživači indeksiraju web stranice što omogućava korisnicima tih pretraživača da pronađu željene stranice.
- **Deep Web: (**Deepnet, Invisible Web, Undernet, Hidden Web**)**
  - Deo web-a koji nije dostupan preko standarnih internet pretraživača.
  - Ne treba mešati pojam sa Dark Web-om.
  - Predstavlja sav neindeksiran sadržaj web stranica, (čak iako je tom sadržaju moguće pristupiti preko indeksiranih sajtova).
- **Dark Web:**
  - Mali deo Deep Web-a koji je s namerom sakriven kako bi bio nepristupačan preko standardnih pretraživača.

ČESTI NESPORAZUMI

- Dark Web nije isto što i Deep Web
- Ni Dark Web ni Deep Web nisu ilegalni niti sadrže SAMO ilegalan sadržaj
- Na Deep Web-u deo sadržaja jeste ilegalan ali je veliki deo jednostavno neindeksiran

- Fun Fact:
  - Ogroman deo web sajtova koje su studenti ove škole host-ovali kao projekte za predmete Web Dizajn i Web programranje su deo Deep Web-a.

KAKO DEEP WEB OSTAJE SKRIVEN?

- Najjednostavnije rečeno, standardni pretraživači koriste web crawler-e, koji koriste linkove na web site-u kako bi navigirali kroz njegove stranice.
- Deep Web sajtovi ostaju skriveni tako što koriste:
  - Dinamični sadržaj (*Stranice kojima se pristupa submit-ovanjem posebnih query-ja ili putem html formi*)
  - "Nelinkovan" sadržaj (*Stranice kojima se pristupa preko linka koji nije pristuan nigde na indeksiranim stranama web site-a*)
  - Private Web (*Sajtovi sa zaštićenim pristupom – Potreban korisnički nalog*)
  - Sadržaj sa ograničenim pristupom (*Korišćenje Robots Exclusion Standard, CAPTCHA, itd…*)
  - Skriptovan sadržaj (*Stranice kojima je moguće pristupiti jedino preko linkova koje generiše java script ili linkova koji se dinamički dobijaju ajax-om ili flash-om*)
  - Non-HTML/Tekstualni sadržaj (*Tekstualni sadržaj koji je hardkodovan u multimedijalne fajlove kao što su slike ili video i korišćenje formata koje web crawler-i ne prepoznaju*)
  - Poseban software (Tor, I2P,...)

KAKO PRISTUPITI DEEP WEB-U?

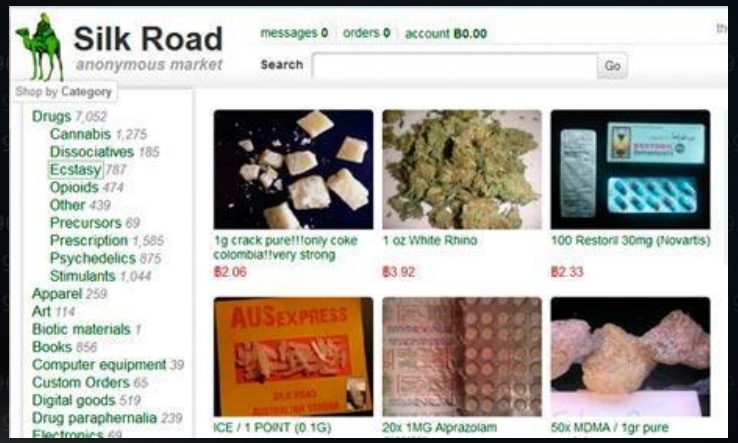
- Pristup Deep Web-u nije moguć preko komercijalnih browser-a kao što su Chrome, Firefox, Internet Explorer, itd...
- Potrebno je skinuti TOR Browser Bundle (TOR – The Onion Router):
  - **TOR Browser Bundle** je browser zasnovan na izvornom kodu Firefox-a, koji korisničku konekciju čini anonimnom tako što koristi TOR relay network (TOR Anonymity Network).
  - TOR Anonymity Network korisiti Onion Routing odakle i potiče ime browsera.
    - Onion Routing: *Podaci su enkapsulirani unutar višestrukih slojeva enkripcije i šalju se preko serije mrežnih node-ova, gde svaki node "ljušti" samo jedan sloj enkrpcije kako bi saznao na koji node da prosledi podatke. To omogućava da svaki node zna samo adresu sa koje su podaci stigli i adresu na koju treba da ih prosledi, tako da kada se dekriptuje poslednji sloj enkripcije podaci su stigli na svoje odredište a pošiljalac je ostao anoniman.*
  - Nakon instaliranja TOR-a nije potrebno vršiti dodatna podešavanja jer je prekonfigurisan za bezbedno korišćenje.
  - Poslednji korak je otići na adresu: **http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page - Ovo je link ka necenzurisanoj Hidden Wiki stranici koja sadrži putanje ka raznim sajtovima na deep web-u.**

DODATNE MERE PREDOSTROŽNOSTI

- I pored toga što sam TOR nudi dovoljan nivo zaštite za korisnike poželjno je primeniti još neke mere predostrožnosti:
  - Koristiti Tails OS (Poželjno ga je pokretati sa USB-a, DVD-a ili Memorijske kartice) ili Linux Kali preko virtualne mašine.
  - Koristiti VPN.
  - Ne verujte nikome koga sretnete na Deep Web-u.
  - Ne skidajte nikakve fajlove sa Deep Web-a
  - Ne koristite servise za torentovanje dok surfujete Deep Web-om
  - # Neki ljudi predlažu i prekrivanje web kamere neprovidinim materijalom zbog navodnih slučajeva špijuniranja korisnika.

DEEP WEB NIJE ILEGALAN!!!

- Zbog same tajanstvene prirode oba pojma i njihovog čestog poistovećivanja, slabije informisani korisnici smatraju, kako je pristup sajtovima koje ova dva pojma obuhvataju, ilegalan.
- Ilegalan je pristup Dark Web-u (Zavisi od državnih zakona), ali pristup Deep Web-u nije.
- Klasifikacione razlike izmedju pojmova su pokrivene na početnom slajdu i te razlike nisu faktor koji razdvaja legalno od ilegalnog.
- Ilegalna priroda Dark Web-a je u sadržaju koji on obuhvata:
  - Prodaja oružja i narkotika (Silk Road – Crno tržište)
  - RED ROOM (Ubistva uživo)
  - Snuff filmovi
  - Dečija pornografija
  - Ilegalno Kockanje
  - Unajmljivanje ubica
  - Sobe za mučenje, itd...



DEEP WEB NIJE ILEGALAN!!!

- Za razliku od Dark Web-a Deep Web nije ilegalan.
- Na Deep Web-u se mogu pronaći izuzetno korisne stvari:
  - Akademske informacije
  - Naučna istraživanja
  - Pravni dokumenti
  - Državni dokumenti
  - Sajtove studenata Visoke ICT :)
  - Itd...

BITNE INFORMACIJE

- Operacija Darknet:
  - U Oktobru 2011. godine grupa Anonymous haktivista je pokrenula operaciju Darknet koja je obuhvatala skup DDoS napada na Lolita City, website koji je hostovao dečiju pornografiju.
- Silk Road:
  - Online crno tržište na kom se uglavnom prodaju oružje i narkotici. Novčane transakcije se obavljaju pomoću bitcoin-a.
- Freedom Hosting Network:
  - Mreža slobodnog hostovanja čiji je vlasnik Eric Eoin, 28-godišnji Irac uhapšen u avgustu 2013 godine od strane FBI-a , zbog optužbi da je distibuirao i promovisao dečiju pornografiju. Dan nakon hapšenja više od pola skrivenih servisa na Freedom Hostig Network su pretrpeli malware napade i skinuti su sa mreže.
- Bitcoin :
  - Glavna valuta korišćena na Dark Web-u.

ZAVRŠNA REČ

- Najprimamljiviji aspekt pristupa Deep Web-u jeste anonimnost koju pruža sam TOR pretraživač, kao i prilika da se korisnik edukuje na poljima internet zaštite kako bi svoju privatnost dodatno osigurao (pored ugrađenih mera sigurnosti).
- Moguće je sprovesti značajna istraživanja zahvaljujući pristupu informacijama nedostupnim standardnim korisnicima interneta.
- Bez obzira na propagandu, standardni browser-i ne pružaju dovoljan stepen sigurnosti i anonimnosti, a neki prikupljanje informacija o korisnicima svojih usluga opravdavaju stavkama u dugačkim uslovima korišćenja (Terms of Service) na koje korisnici pristaju bez detaljnog isčitavanja.