Sigurnosne prijetnje na Internetu

Dark web

Vjekoslav Radošević, 11.12.2024.

Pregled predavanja

- Pitanja za ispite
- Motivacija
- Slojevi weba
- Kako radi dark web
- Aktivnosti na dark webu
- Zaključak
- Literatura

Pitanja za ispite

- Navedite slojeve weba i ukratko objasnite svaki od njih.
- Što su skrivene web usluge?
- Navedite i ukratko objasnite dva spomenuta načina pretraživanja dark weba.
- Opišite način korištenja Tor2Web usluge.
- Navedite neke aktivnosti kibernetičkog kriminala koje se provode na dark webu.

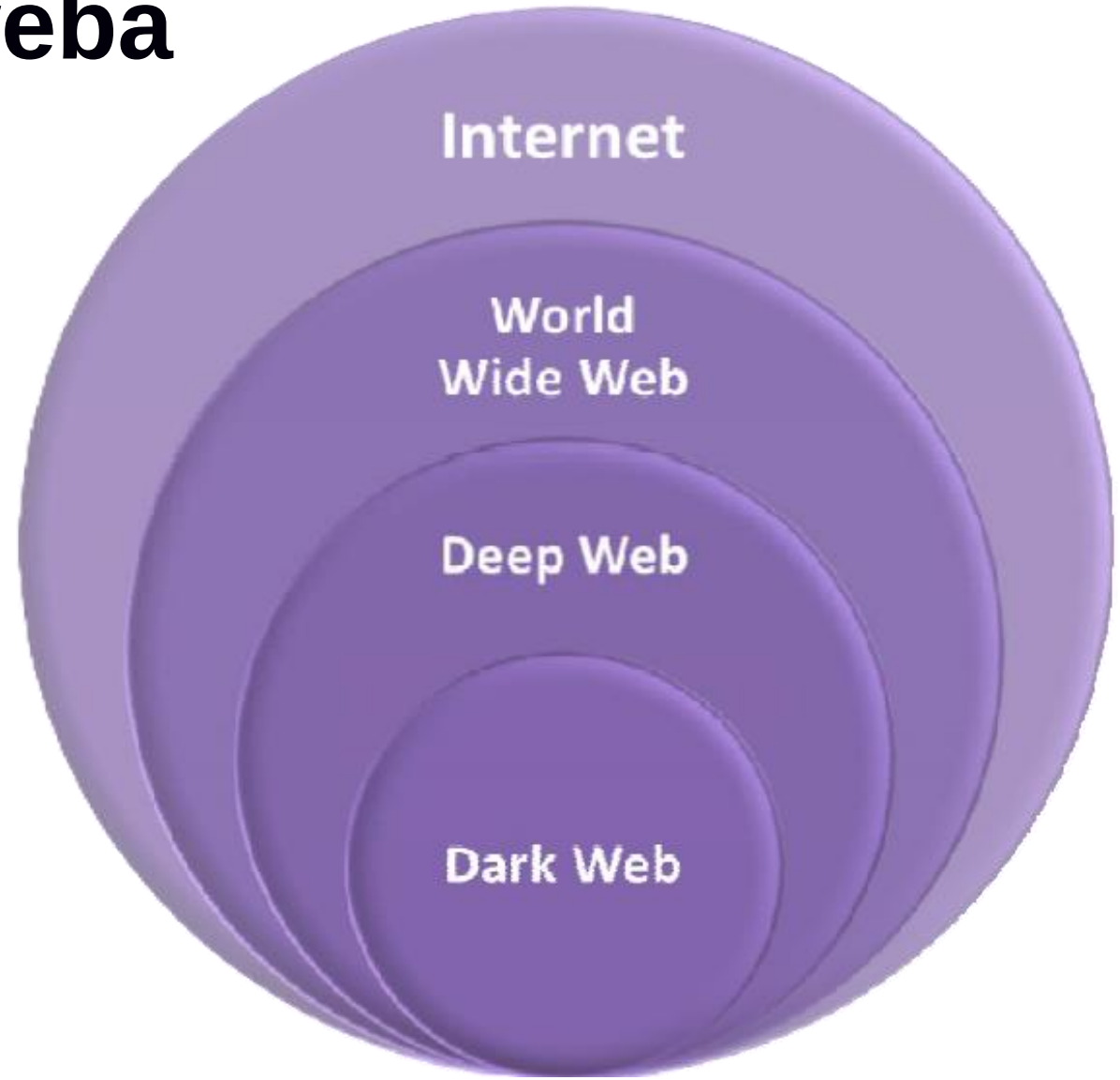
Motivacija

- Dvostruka uloga dark weba:
  - Omogućuje kriminalcima iskorištavanje anonimnosti za provođenje ilegalnih i neetičnih aktivnosti
  - Omogućuje pristup necenzuriranom web sadržaju uz dodatnu razinu zaštite
- Potrebno je razumjeti principe rada dark weba kako bi ga mogli sigurno koristiti

Slojevi weba

- Površinski web
  - Web sadržaj pronađen posebnim programima (eng. web crawlers) i indeksiran web tražilicama koje korisniku kasnije nude rangirani skup poveznica na stranice
  - Web sadržaj dohvatljiv standardnim web klijentima, npr. web preglednicima
- Deep web
  - Web sadržaj koji nije moguće indeksirati
  - Budući da nije indeksiran, nije ga moguće dohvatiti korištenjem web tražilica
- Dark web
  - Web sadržaj na anonimnim web poslužiteljima kojima je moguće pristupiti samo korištenjem posebne programske podrške
  - Dio deep weba

Slojevi weba



Skrivene web usluge

- Skrivena web usluga je usluga čija IP adresa nije poznata, a pristupa joj se isključivo posebnom programskom podrškom
- Dark web je kolekcija skrivenih web usluga
- Razlozi zašto IP adresa web usluge mora ostati tajna:
  - Vlasnik skrivene usluge ne želi otkriti svoj identitet otkrivanjem IP adrese web usluge
  - Želi se spriječiti filtriranje prometa prema web usluzi na temelju njene IP adrese

Tor skrivene usluge

- Tor skrivenoj usluzi klijent **ne pristupa izravno** niti mu je potrebna IP adresa te usluge kako bi joj pristupio
- Domensko ime Tor skrivene usluge sastoji se od:
  - Javnog ključa Tor skrivene usluge
  - .onion sufiksa (domene)
  - Primjer: vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion
- .onion domena nije poznata DNS poslužiteljima zbog čega ne mogu domensko ime skrivene usluge povezati s odgovarajućim IP adresama

Protokol Tor skrivenih usluga

- Skrivena usluga odabire i uspostavlja puteve do nasumično odabrana tri čvora Tor mreže tj. **čvorova za upoznavanje** (eng. introduction nodes)
- Javni ključ skrivene usluge i identifikatori čvorova za upoznavanje čine **deskriptor** skrivene usluge kojega ona potpisuje svojim tajnim ključem i objavljuje u raspodijeljenoj tablici deskriptora na Tor mreži
- Klijent dohvaća i provjerava ispravnost deskriptora javnim ključem skrivene usluge i uspostavlja put do **čvora za sastanak** (eng. rendezvous node)
- Klijent nasumično odabire jedan od čvorova za upoznavanje i predaje mu IP adresu čvora za sastanak i jednokratni kod
- Čvor za upoznavanje prosljeđuje IP adresu skrivenoj usluzi koja odlučuje hoće li uspostaviti komunikaciju s klijentom preko čvora za sastanak ili ne

Pretraživanje dark weba – direktoriji

- Dark web moguće je pretraživati korištenjem usluga koje izlažu poveznice na druge dark web stranice
- Na Tor mreži se te usluge zovu *Hidden Wiki* usluge
  - Također skrivene usluge
  - Organiziraju sadržaj po kategorijama (forumi, tržnice, vijesti...)
  - Sadrže poveznice na legalne i ilegalne usluge – **korisnik mora biti oprezan**
- Dark web stranice često prestaju i ponovno počinju s radom, pa direktoriji moraju redovito ažurirati svoje poveznice

Pretraživanje dark weba – tražilice

- Dark web moguće je pretraživati korištenjem posebnih dark web tražilica
  - DuckDuckGo (nije ograničena na dark web)
  - Ahmia (pretraga Tor skrivenih usluga)
  - Grams (pretraga Tor tržnica, aktivna od 2014. do 2017. godine)
- Problem: stranice dark weba nisu dobro povezane kao stranice na površinskom webu, a često i prestaju s radom
- korisnici predlažu dodatne poveznice na temelju kojih pretraživači proširuju svoju pretragu

Tor2Web

- Usluga na **površinskom webu** koja korisniku omogućuje pristup Tor skrivenim uslugama korištenjem standardnog preglednika (znači bez korištenja Tor programske podrške)
- Način korištenja:
  - Korisnik pronalazi URL Tor skrivene usluge kojoj želi pristupiti
  - Korisnik mijenja domensko ime iz URL-a tako da adresira Tor2Web poslužitelj
    - npr. ABC.onion -> ABC.onion.to
  - Korisnik šalje HTTP zahtjev Tor2Web poslužitelju na novi URL
  - Tor2Web poslužitelj izvlači URL skrivene usluge i pristupa joj preko Tor mreže
  - Tor2Web poslužitelj korisniku prosljeđuje odgovor skrivene usluge
- Tor2Web **ne osigurava** anonimnost korisnika

Tržnice dark weba

- Web trgovine pokrenute kao skrivene usluge u cilju zaštite svojih vlasnika, prodaju legalne i/ili ilegalne proizvode i usluge
- Plaćanje kriptovalutama
  - Bitcoin (pseudo-anoniman)
  - Monero, Zcash (anonimni, privacy coins)
- Primjeri tržnica: Silk Road, Silk Road 2.0, AlphaBay, Hansa
- Sustav reputacije kao zamjena za sustav verifikacije [4]
  - pozitivna reputacija prodavača povlači (u teoriji) manju vjerojatnost prijevare kod prodaje
  - Zbog toga, prodavači s boljom reputacijom često podižu cijene svojih usluga
  - Bitno poštivati pravila tržnica – u protivnom isključenje i gubitak pozitivne reputacije

Dobra strana dark weba

- Nekim je korisnicima pristup dijelovima weba ograničen (npr. The Great Firewall of China [2])
- Organizacije poslužuju replike svojih stranica kao skrivene usluge [1]
  - Vijesti (ProPublica), društvene mreže (Facebook)
  - CIA za anonimne dojave
- Svi korisnici mogu pristupati tim skrivenim uslugama budući da nije moguće filtrirati promet na temelju IP adrese skrivene usluge
- Šifriranje veze s kraja na kraj (eng. end-to-end encryption)

Neetične i ilegalne aktivnosti na dark webu

- Govor mržnje
- Prodaja droge i oružja
- Pornografija i prikazivanje nasilja
- Ekstremističke skupine šire svoje ideologije, provode novačenje članova, skupljaju financijska sredstva [2]
- Kibernetički kriminal

Kibernetički kriminal na dark webu

- Command & control poslužitelji aktivni kao skrivene usluge
- Prodaja ranjivosti nultog dana (eng. zero-day vulnerabilities) uz pomoć skrivenih usluga
- Prodaja ukradenih vjerodajnica i brojeva kreditnih kartica (Card shops [3])
- Forumi za edukaciju i koordiniranje aktivnosti kibernetičkih kriminalaca
- Crime-as-a-Service

Zaključak

- Neke dobre primjene... i mnogo loših
- Ulaganje u razvoj tehnologija za deanonimizaciju korisnika, suradnja država i provođenje operacija za gašenje ilegalnih skrivenih usluga zahtijevaju vrijeme i resurse koji bi se mogli upotrijebiti na druge načine (kada dark web ne bi bio problem)

Literatura

- [1] Kumar, Aditi, and Eric Rosenbach. "The truth about the dark web." Finance and Development 56.3 (2019): 22-25
- [2] Gupta, Abhineet, Sean B. Maynard, and Atif Ahmad. "The dark web phenomenon: A review and research agenda." arXiv preprint arXiv:2104.07138 (2021)
- [3] Finklea, K. "Dark Web", Congressional Research Service, March 10, 2017
- [4] Schäfer, Matthias, et al. "BlackWidow: Monitoring the dark web for cyber security information." 2019 11th International Conference on Cyber Conflict (CyCon). Vol. 900. IEEE, 2019
- [5] Tor zajednica, *How do Onion services Work?,* https://community.torproject.org/onion-services/overview/, pristupljeno: 5.11.2024.
- [6] Editorial, *What is Tor2web? History, Security, Uses & Advantages*, 13.5.2024., https://thecyberexpress.com/what-is-tor2web/, pristupljeno: 16.11.2024.

Dodatna literatura

- Kim Zetter, *How the Feds Took Down the Silk Road Drug Wonderland*, 18.11.2013., https://www.wired.com/2013/11/silk-road/, pristupljeno: 11.11.2024.
- I2P zajednica, *Garlic routing*, https://geti2p.net/en/docs/how/garlic-routing, pristupljeno: 16.11.2024.

Hvala!