Sigurnosne prijetnje na Internetu

Tor

Marko Lipovac, 13.11.2024.

Pregled predavanja

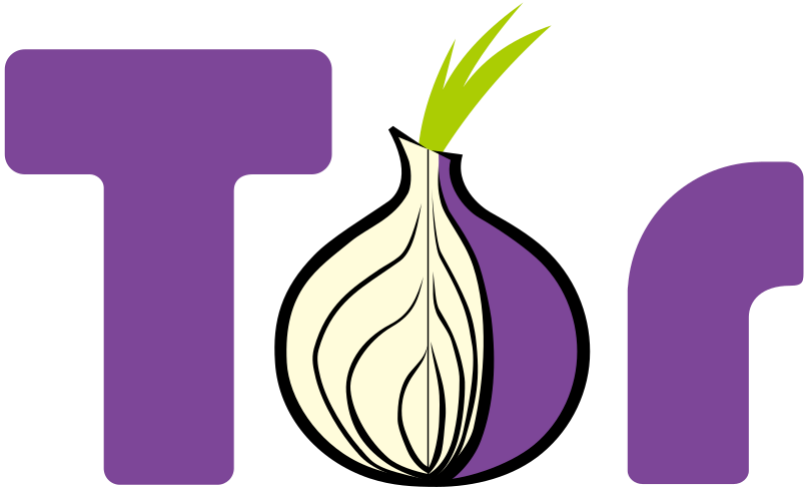
- Motivacija
- Pitanja za ispit
- Tor
- Ranjivosti Tor-a
  - Unos privatnih podataka
  - Zaraženi čvorovi
  - FBI-ovi NIT
- Zaključak

Pitanja za ispite

- Što je Tor i kako je najčešće implementiran?
- Što je Onion Routing i o čemu ovisi koliko slojeva enkripcija postoji?
- Kako se može otkriti identitet korisnika na Tor-u?
- Što je skrivena usluga?
- Što je ECID u FBI-ovom NIT i kako on nastaje?

Motivacija

- Najčešći razlog korištenja Tor-a je privatnost
- Tor koristi oko 2 miljuna korisnika dnevno
- Mnogi korisnici vjeruju da su tijekom korištenja Tor-a u potpunosti sigurni



Tor

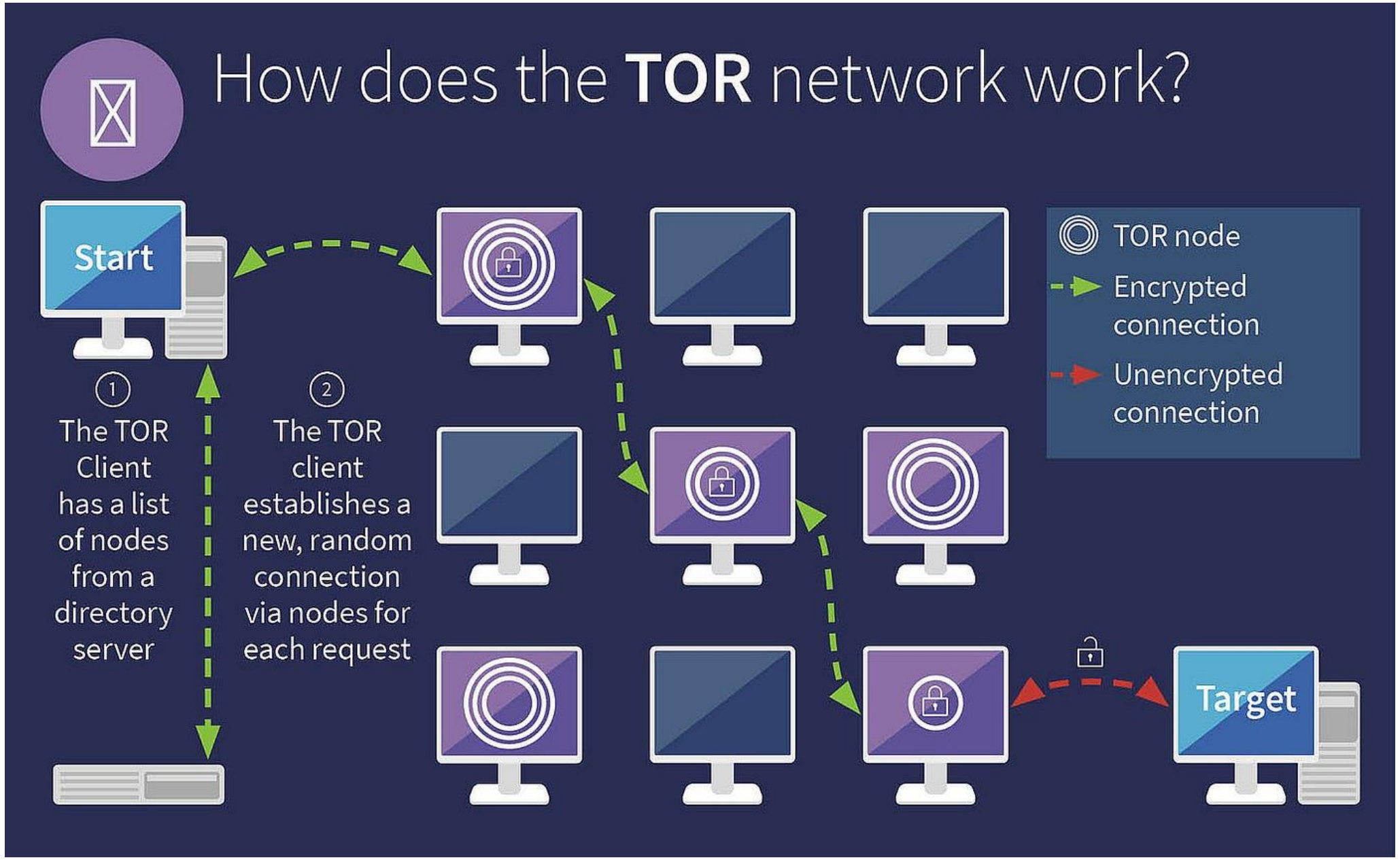
- Tor (The Onion Router) je program i mreža koji pomaže zaštiti privatnosti njegovih korisnika
- Tor Browser je verzija Firefox-a koja rješava mnoge probleme s privatnošću (najčešća implementacija Tor-a)
- Tor je neprofitna organizacija - sav prihod koristi za njezin cilj, a ne dobit osnivača

Tor

- Onion Routing je metoda anonimnog usmjeravanja podataka na internetu koja koristi višeslojno šifriranje.
- Pri slanju, podatci se šifriraju višestruko. Za svaki čvor postoji jedna šifra.

Tor

- Svaki čvor dekriptira samo jedan sloj enkripcije i ostatak prosljeđuje.
- Svi sudionici mreže imaju samo adrese onih računala od kojih su primili podatke ili kojima trebaju poslati podatke
- Zahtjev sa izlaznog čvora na server nije šifriran od strane Tor-a


How does the TOR network work?
Start
TOR node
Encrypted connection
Unencrypted connection
1
The TOR Client has a list of nodes from a directory server
2
The TOR client establishes a new, random connection via nodes for each request
Target

Tor

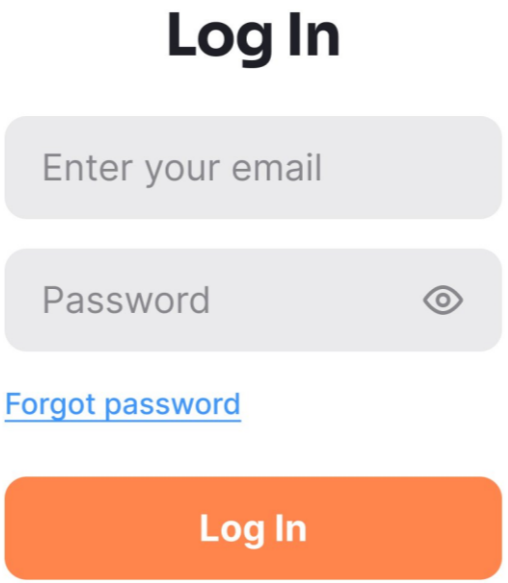
- Skrivena usluga je tip web stranice ili usluge koja djeluje na mreži koja je dizajnirana za pružanje anonimnosti korisnicima i samoj usluzi
- Skrivene usluge nisu dostupne putem standardnih web preglednika

Tor

- Nedostatci Tor preglednika:
  - Sporiji je nego normalni preglednik
  - Većina dodataka (eng. Plugins) neće raditi radi sigurnosti
  - Neke stranice neće raditi kako je zamišljeno ili uopće

Ranjivosti Tor-a

- Unos osobnih podataka
  - Najčešći način otkrivanja identiteta korisnika Tor-a
  - Osjetljivi podatci ne moraju nužno biti ime i prezime, nego mogu biti i šifre te korisnička imena
- Zaraženi čvorovi
  - Moguće je spojiti se na 3 čvora koja pripadaju istoj organizaciji/osobi i ona bi mogla spojiti korisnika s podatcima koji su poslani (vrlo mala vjerojatnost)



Ranjivosti Tor-a

- FBI-ov NIT(Network Investigative Technique)
- Sastoji se od više komponenata:
  - FBI-ove skrivene usluge
  - Flash aplikacije
  - Socket veze
  - FBI servera (cornhusker)

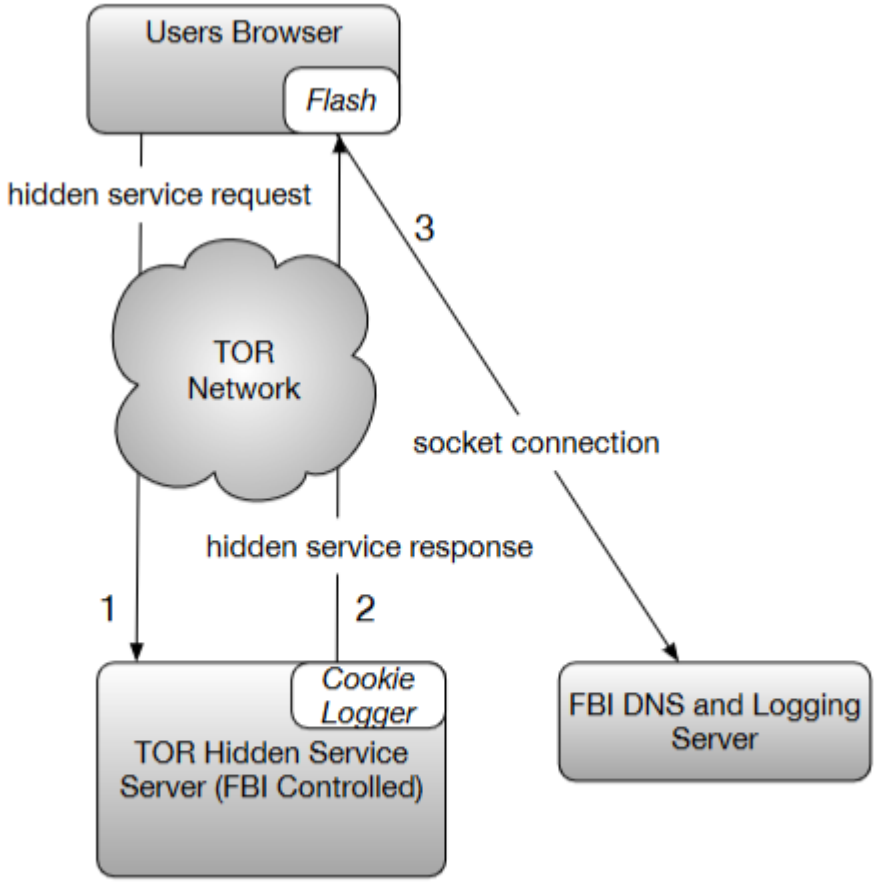


Figure 1. NIT High Level Overview

FBI NIT – Serverski dio koda

- Tijekom pristupa stranici, datoteka gallery.php unutar iframe-a veličine 1x1 piksela, bi se pokrenula.
- gallery.php bi stvorio SessionID svaki put pri pokretanju koji je nasumično generiran broj.
- FBI bi tada pratio podatke koji sadržavaju ID-ove

```
82    <p class="unimportant" style="text-align:center;"></p>  <iframe src="/gallery.php?b=girls&t=1481&u=%2Fgirls%2Fres%2F1481.html&m=0"
      width="1" height="1" frameborder="0"></iframe></body>
83    </html>
```

Figure 3. Tracked Webpage 1481.html

FBI NIT – Serverski dio koda

- Iz prikupljenih podataka ustanovio bi se korišteni preglednik, te se svakom pripadajućem pregledniku priključuje i pripadajuća flash datoteka
- Za preglednik Rekonq, datoteka gallery.php bi uključivala flash datoteku pod nazivom gallery.swf te bi proslijedila ID flash objektu

FBI NIT – Serverski dio koda

- ECID (Encrypted Session ID) stvoren korištenjem FBI-ove generate-cookie (koristi GALLERY_API_KEY i SessionID)
- Svi podatci su šifrirani s nasumičnim IV i ključem nazvanim GALLERY_API_KEY kojeg je jedino moguće pročitati na serveru

FBI NIT – Serverski dio koda

```
1680    function generate_cookie($key, $method, $session_id)
1681    {
1682      // Create the @-delimited plaintext structure
1683      $data = "2@" . $method . "@" . $session_id . "$";
1684
1685      // Generate a random IV and encrypt the plaintext
1686      $ivlen = mcrypt_get_iv_size(MCRYPT_BLOWFISH, MCRYPT_MODE_CBC);
1687      $iv    = mcrypt_create_iv($ivlen, MCRYPT_DEV_URANDOM);
1688      $enc   = mcrypt_encrypt(MCRYPT_BLOWFISH, $key, $data, 'cbc', $iv);
1689
1690      // Concatenate the IV and ciphertext and then base32-encode the output
1691      return join('.', str_split(strtoupper(bin2hex($iv . $enc)), 40));
1692    }
```

Figure 8. ECID Generation in fuctions.php

FBI NIT – Flash aplikacija

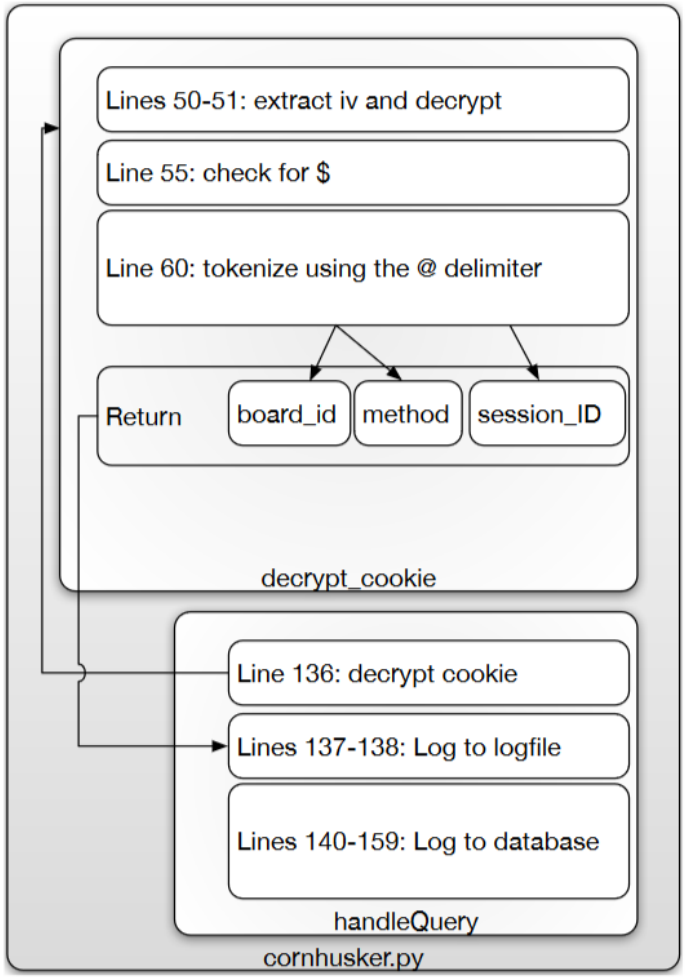
- Poziva se funkcija loadGallery koja provjerava ako postoji ECID (nije null) te stvara socket vezu na domenu „96.126.124.96.ECID.cpimagegallery.com”
- Kad je cpimagegallery.com mapiran od strane DNS resolvera, vraća adresu FBI servera (cornhusker)

FBI NIT – Flash aplikacija

- Flash će napraviti DNS zahtjev kako bi se mapirala domena cornhuskera
- Nakon što se mapirala domena poziva se funkcija onConnect koja stvara podatak tipa String koji sadrži podatke o operacijskom sustavu računala, arhitekturi procesora i ECID-u
- Taj podatak se šalje cornhusku preko TCP socket veze koja ignorira bilo kakve proxy postavke

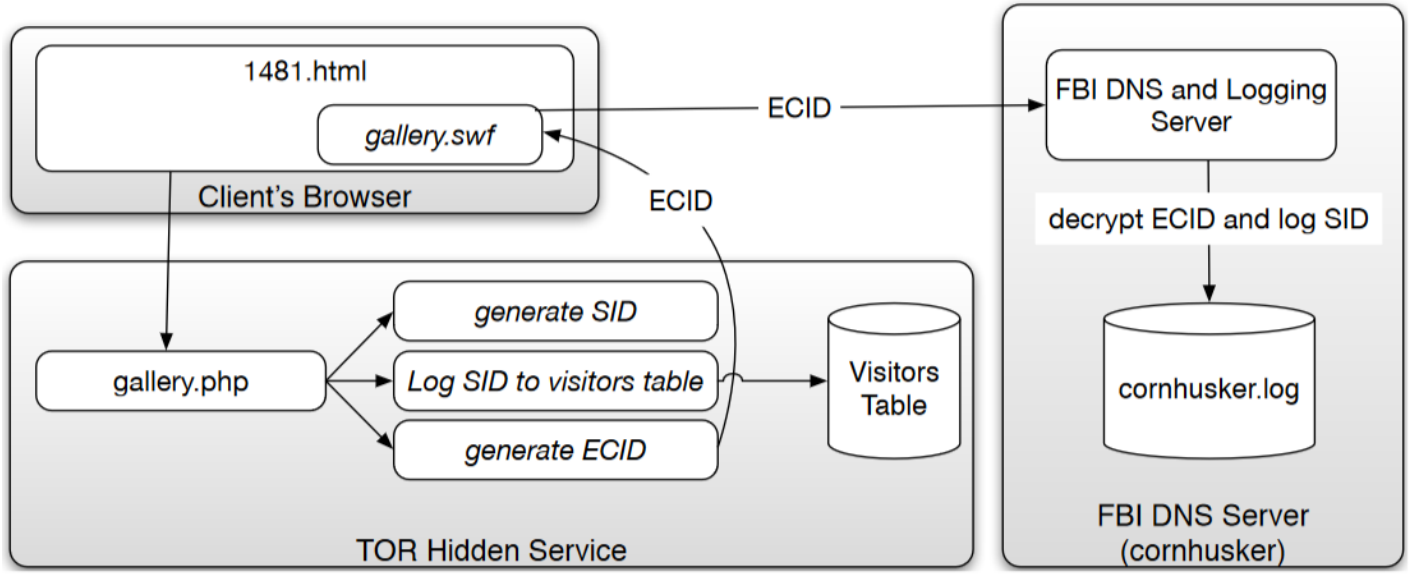
FBI NIT – Čitanje i bilježenje DNS-a

- Proveden na cornhuskeru
- Poziva se funkcija decrypt_cookie
- Vraćeni podatci spremaju se u log datoteku
- Zapisani podatci se spremaju u bazu podataka



FBI-ov NIT – Analiza podataka

- Usporedbom ID-ova dvaju servera povezali bi se prikupljeni podatci s korisnikom stranice



FBI-ov NIT - Sažetak

- Korisniku koji je pristupio FBI-ovoj sakrivenoj usluzi putem Tor-a, pokreće se php datoteka koja dodaje Flash aplikaciju na korisnički preglednik
- Zatim Flash aplikacija uspostavlja TCP socket vezu sa FBI-ovim serverom (cornhusker)

FBI-ov NIT - Sažetak

- Nakon uspostave veze, šalju se podatci o korisniku preko socket veze na cornhusker (zaobilazi Tor)
- Iz toga FBI može doći do IP adrese korisnika i identificirati ga, te usporedbom ID-ova s dvaju servera, poveže se njegov identitet sa stranicama koje je posjetio

Zaključak

- Tor se smatra kao siguran način pretraživanja internetom, ali možemo vidjeti da čak ni on nije u potpunosti siguran
- Većina slučaja otkrivanja identiteta korisnika je bila zbog korisničke greške

Literatura

- Tor – What is Tor? -https://support.torproject.org/about/what-is-tor/ - pristupljeno 11.11.2024.
- GeeksforGeeks – Working of Tor Browser - https://www.geeksforgeeks.org/working-of-tor-browser/ - pristupljeno 11.11.2024.
- Computerphile -TOR Hidden Services - Computerphile - https://www.youtube.com/watch?v=lVcbq_a5N9I&ab_channel=Computerphile – pristupljeno 11.11.2024.
- Miller, Matthew, Joshua Stroschein, and Ashley Podhradsky. "Reverse Engineering a Nit That Unmasks Tor Users." (2016). – pristupljeno 11.11.2024.
- Medium – Let’s connect to TOR - https://jaydev-joshi-blog.medium.com/lets-connect-to-tor-8fd1dd3171e3 - pristupljeno 13.11.2024.

Dodatna literatura

- Computerphile - TOR Hidden Services – Computerphile - https://www.youtube.com/watch?v=lVcbq_a5N9I – pristupljeno 11.11.2024.
- MalwarebytesLABS - Tor Browser and Firefox users should update to fix actively exploited vulnerability - https://www.malwarebytes.com/blog/news/2024/10/tor-browser-and-firefox-users-should-update-to-fix-actively-exploited-vulnerability - pristupljeno 11.11.2024.

Hvala!