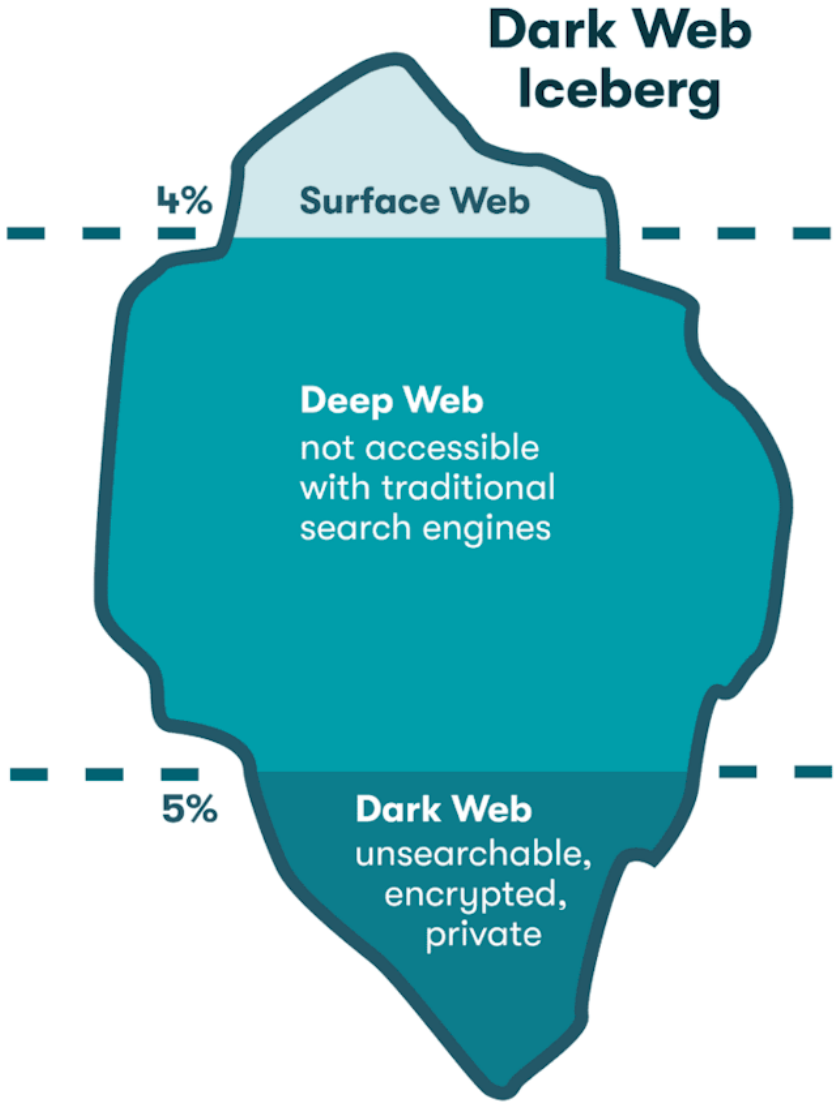
RISCURILE DE SECURITATE ALE NAVIGĂRII PE DARK WEB

HINCU ALICE RAMONA

CE ESTE DARK WEB?

- Dark Web este **o parte a internetului ascunsă de motoarele de căutare obișnuite** și accesibilă doar prin rețele speciale care asigură anonimatul, precum Tor.
- În țări unde guvernul controlează strict informațiile și media, Dark Web-ul oferă o cale pentru jurnaliști:
  - de a comunica liber;
  - de a schimba informații;
  - de a raporta încălcări ale drepturilor omului;
- Exemplu: utilizarea rețelei Tor în timpul Primăverii Arabe pentru a ocoli cenzura și a organiza proteste.



- Surface Web: Informațiile sunt ușor accesibile prin intermediul motoarelor de căutare tradiționale și nu necesită autentificare specială.
- Deep Web: Deși nu este indexat de motoarele de căutare, conținutul din Deep Web poate fi accesat dacă ai link-ul direct sau permisiunea necesară (de exemplu, autentificare cu nume de utilizator și parolă).
- Dark Web: Necesită software special și configurații specifice pentru acces (de exemplu, Tor Browser), iar adresele web sunt diferite, folosind de obicei sufixul .onion.

TOR: PILONUL ANONIMATULUI PE INTERNET

- Tor, scurt pentru "The Onion Router", este un software gratuit care permite comunicarea anonimă pe internet. Este unul dintre principalele instrumente utilizate pentru a accesa Dark Web-ul.
- Cum Funcționează Tor?
  - Criptarea Straturilor: Datele sunt criptate în mai multe straturi și trimise printr-o serie de relee alese aleatoriu, fiecare dezvăluind doar locația nodului anterior și a celui următor.
  - Nodurile: Cuprinde noduri de intrare, relee intermediare, și noduri de ieșire. Fiecare are un rol specific în asigurarea anonimatului și securității datelor.

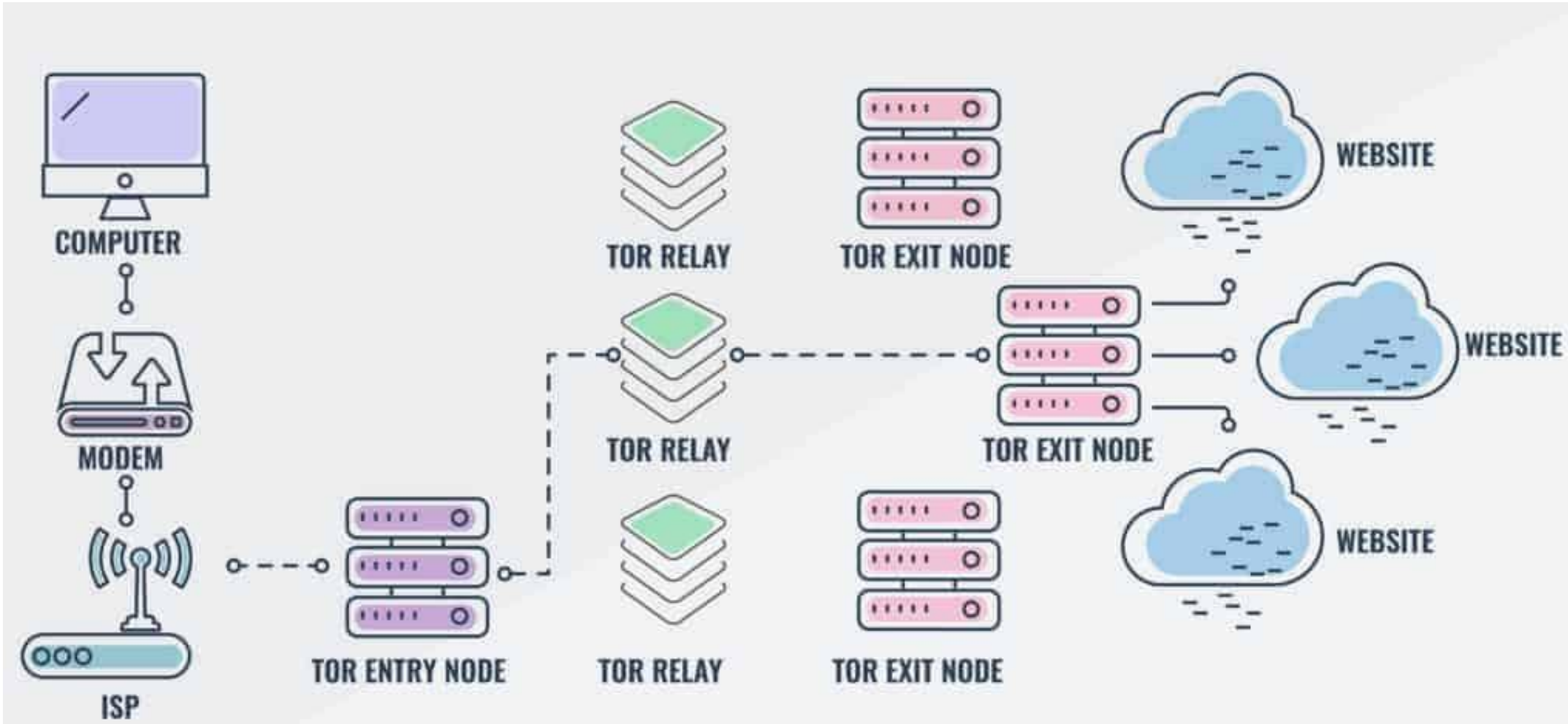


FIG: Simplified Tor Connection

Explicare diagramă:

- Semnalul este trimis de la computerul utilizatorului, trecând prin modemul său și ajungând la furnizorul de servicii de internet (ISP). ISP-ul poate vedea că utilizatorul este conectat la rețeaua Tor, dar nu poate vedea ce anume accesează utilizatorul.
- De la ISP, comunicația este redirecționată către primul nod Tor, cunoscut ca nod de intrare. Acest nod vede adresa IP a utilizatorului, dar nu cunoaște destinația finală a datelor.
- Comunicația este apoi transmisă printr-o serie de relee Tor. Fiecare releu decriptează un strat al criptării, însă fiecare vede doar adresa nodului anterior și a următorului nod din lanț, nu și adresa inițială a utilizatorului sau destinația finală a datelor.
- Ultimul nod în rețea este nodul de ieșire Tor. Acest nod decriptează ultimul strat de criptare și trimite datele către destinația finală pe internet. La acest punct, nodul de ieșire poate vedea datele trimise către website, dar nu cunoaște sursa originală a acestora (adică adresa IP a utilizatorului).
- Datele ajung în final la website-ul dorit. Website-ul vede cererea ca venind de la nodul de ieșire Tor, nu de la utilizatorul real, astfel menținându-se anonimatul utilizatorului.

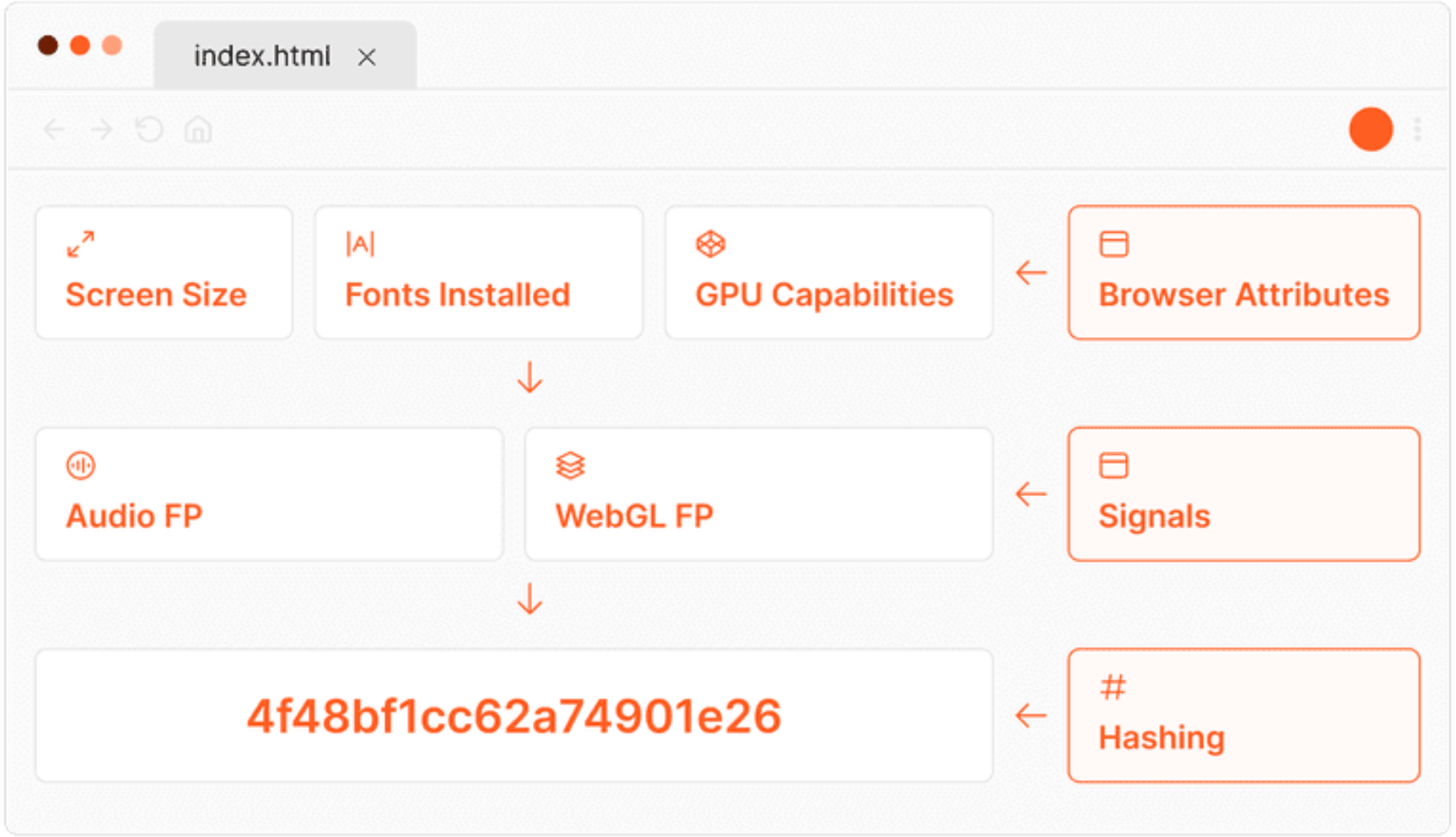
EXEMPLE DE VULNERABILITĂȚI ASOCIATE CU DARK WEB

1. BROWSER FINGERPRINTING

Amprenta digitală a browserului este o tehnică avansată de urmărire care colectează informații despre dispozitivul și browserul unui utilizator pentru a crea un identificator unic. Reprezintă o formă de **vulnerabilitate asociată cu expunerea și colectarea de date**, care poate afecta confidențialitatea utilizatorilor pe internet

- Aceasta colectează detalii precum:
  - tipul și versiunea browserului
  - sistemul de operare
  - rezoluția ecranului
  - fonturile instalate
  - setările de limbă
  - fus orar, și multe altele.

Diferit de cookie-uri, amprenta digitală nu poate fi ștearsă simplu prin curățarea cache-ului browserului, fiind astfel mai persistentă și invazivă.


index.html
Screen Size
Fonts Installed
GPU Capabilities
Browser Attributes
Audio FP
WebGL FP
Signals
4f48bf1cc62a74901e26
Hashing

CUM SĂ MINIMIZEZI AMPRENTA DIGITALĂ A BROWSERULUI

- Amprenta digitală a browserului este mai puțin unică când mai mulți utilizatori împărtășesc aceleași caracteristici și setări ale browserului.

- Dacă nu sunt personalizate setările browserului, este mai probabil ca un user să se "amestece în mulțime", ceea ce face mai dificilă urmărirea și identificarea.

- Utilizarea setărilor standard ale browserului și evitarea instalării pluginurilor neobișnuite sau a extensiilor poate ajuta la reducerea unicității amprentei digitale.

EXEMPLU: MODIFICAREA REZOLUTIEI ECRANULUI

Cum afectează dimensiunile ferestrei browserului Tor anonimatul ?

- Maximizarea browserului Tor pe un ecran cu o rezoluție standard (cum ar fi 1280x1024 sau 1080p) nu este extrem de riscantă, deoarece multe persoane au ecrane cu aceste dimensiuni.
- Cu toate acestea, anumite rezoluții pot sugera dacă este folosit un PC sau un laptop, ceea ce ar putea oferi indicii suplimentare despre identitatea userului.
- Redimensionarea manuală a browserului Tor la dimensiuni neobișnuite poate crea o amprentă digitală unică, facilitând astfel urmărirea activităților utilizatorului pe mai multe site-uri, chiar dacă IP-urile utilizate de Tor se schimbă.

2. ACCES NEAUTORIZAT LA HARDWARE

Accesul neautorizat la camera web reprezintă o altă vulnerabilitate serioasă de securitate, adesea clasificată ca **vulnerabilitate de tip acces la hardware**. Aceasta implică capacitatea unor aplicații sau site-uri web de a accesa și controla camera web a unui dispozitiv fără permisiunea explicită a utilizatorului.

În unele cazuri, software-ul rău intenționat poate chiar dezactiva LED-ul indicator al camerei web, care în mod normal ar lumina când camera este activă. Aceasta înseamnă că utilizatorii pot fi spionați fără să știe că camera lor este în funcțiune.

EXEMPLU DE EXPLOATARE SPECIFICĂ

- **Nume Vulnerabilitate:** CVE-2017-11292
- Adobe Flash Player a fost o țintă comună pentru atacatori datorită răspândirii sale largi și a multiplelor sale vulnerabilități de securitate. Una dintre aceste vulnerabilități notabile a fost CVE-2017-11292, o vulnerabilitate de execuție de cod la distanță care a fost exploatabilă prin intermediul unui clip Flash special conceput.
- Atacatorii puteau crea un fișier SWF (Shockwave Flash) malițios care, odată deschis de victime prin intermediul unui browser cu Adobe Flash Player instalat, permitea executarea de cod arbitrar pe mașina victimei.
- Acest cod arbitrar putea include scripturi pentru activarea camerei web și microfonului fără a lumina LED-ul de notificare al camerei, ceea ce însemna că utilizatorii puteau fi filmați sau înregistrați fără știrea lor.

EXEMPLU DE EXPLOATARE SPECIFICĂ

Cum erau păcălite victimele în a deschide fisierele ? Social Engineering.

- Pe Dark Web, unde anonimatul și lipsa de reglementare fac mai dificilă verificarea conținutului, fișierele SWF pot fi ascunse ca fiind alt tip de conținut, cum ar fi filme, muzică sau software. Utilizatorii care caută să descarce astfel de materiale pot sfârși să descarce și să execute fișiere malițioase.
- Unii utilizatori de pe Dark Web pot fi motivați de curiozitatea de a explora conținutul disponibil, inclusiv fișierele multimedia care necesită Flash pentru a fi vizualizate. Acest lucru îi poate face vulnerabili la deschiderea și rularea de fișiere SWF fără a realiza riscurile de securitate asociate.

3. VULNERABILITĂȚI TOR

Deanonimizarea la Nodurile de Ieșire Tor: Tehnica EPICFAIL

- Tehnica EPICFAIL este o metodologie de eavesdropping utilizată de NSA (National Security Agency) pentru a deanonimiza utilizatorii rețelei Tor la nodurile de ieșire. Aceasta este parte dintr-o serie de tehnici care exploatează comportamentele inadecvate sau "naive" ale utilizatorilor, pe care NSA le numește „Dumb Users”.
- Mecanismul de Funcționare:
  - Interceptarea Traficului de Ieșire: La nodurile de ieșire, traficul de la utilizatorii Tor este decriptat înainte de a fi trimis către destinațiile finale pe internetul obișnuit. Aceasta permite observatorilor la aceste noduri să captureze și să analizeze traficul fără criptare.
  - Identificarea Informațiilor Personale: Utilizatorii care se loghează pe site-uri personale sau utilizează identificatori unici în timp ce sunt conectați la Tor pot fi deanonimizați. De exemplu, dacă un utilizator se autentifică pe un cont de email personal sau pe rețele sociale folosind conexiunea Tor, detaliile furnizate pot fi direct corelate cu identitatea lor reală.

3. VULNERABILITĂȚI TOR

Analiza Pasivă a Traficului în Rețeaua Tor

- Analiza pasivă a traficului este o tehnică folosită pentru deanonimizarea utilizatorilor Tor, prin monitorizarea și corelarea traficului la nodurile de intrare și de ieșire. Aceasta se bazează pe identificarea și urmărirea caracteristicilor unice ale traficului și sistemului utilizatorilor. Analiza pasivă a traficului este considerată o **vulnerabilitate de tip corelare a traficului**.
- Corelarea Traficului:
  - Atacatorii pot corela timpul și caracteristicile traficului de la nodurile de intrare și ieșire pentru a lega activitatea din rețeaua Tor cu traficul neanonimizat pe internet.
  - Exemplu: Dacă un set unic de atribute de sistem și comportamente de trafic sunt observate atât la nodul de intrare, cât și la nodul de ieșire, atacatorul poate deduce identitatea utilizatorului.
- Măsură de protectie: folosirea unui VPN pentru a ascunde adresa IP reală.

Monitorizarea Nodurilor de Intrare:

- Nodurile de intrare sunt primele puncte de
  contact pentru traficul care intră în rețeaua Tor. Aceste noduri pot vedea adresa IP reală a utilizatorului și alte informații de identificare.
- Vulnerabilitate: Dacă un atacator monitorizează un nod
  de intrare, poate colecta adrese IP și alte date
  ale utilizatorilor care accesează rețeaua Tor.

Monitorizarea Nodurilor de Ieșire:

- Nodurile de ieșire sunt punctele unde traficul părăsește rețeaua Tor și se îndreaptă spre destinațiile finale
  pe internetul obișnuit. Aici, traficul este decriptat, dezvăluind conținutul său.
- Vulnerabilitate: Un atacator care controlează sau monitorizează nodurile de ieșire poate intercepta și analiza traficul de ieșire, identificând comportamente și pattern-uri unice.

3. VULNERABILITĂȚI TOR

Atacul de Reconstrucție a Circuitului în Rețeaua Tor

- Atacul de reconstrucție a circuitului este o metodă prin care un cineva creează și controlează un număr mare de noduri Tor pentru a intercepta și corela traficul anonim cu traficul neanonimizat, compromițând astfel anonimatul utilizatorilor.
- Exemplu: Dacă există 9000 de noduri Tor și un adversar controlează 3000 dintre ele, există o probabilitate de 30% ca un nod Tor selectat aleatoriu să fie compromis.
- Impactul Controlului Multiplu: Dacă un utilizator selectează un circuit de trei noduri, probabilitatea ca toate nodurile să fie compromise crește exponențial.

3. VULNERABILITĂȚI TOR

Atacul de Reconstrucție a Circuitului în Rețeaua Tor

Cum funcționează?

- Crearea de Noduri Malitioase: Adversarul configurează și introduce un număr mare de noduri Tor în rețea, crescând probabilitatea ca un utilizator să aleagă noduri controlate de adversar pentru circuitul său.
- Controlul Nodurilor de Intrare și Ieșire: Dacă adversarul controlează atât nodul de intrare, cât și nodul de ieșire din circuitul Tor al unui utilizator, poate corela traficul care intră și iese din rețea pentru a identifica utilizatorul.
- Reconstrucția Circuitului: Adversarul folosește datele colectate pentru a reconstrui circuitul complet utilizat de un utilizator, identificând astfel punctele de origine și destinație ale traficului.

DEMO