Dark web
Deep web
Surface web

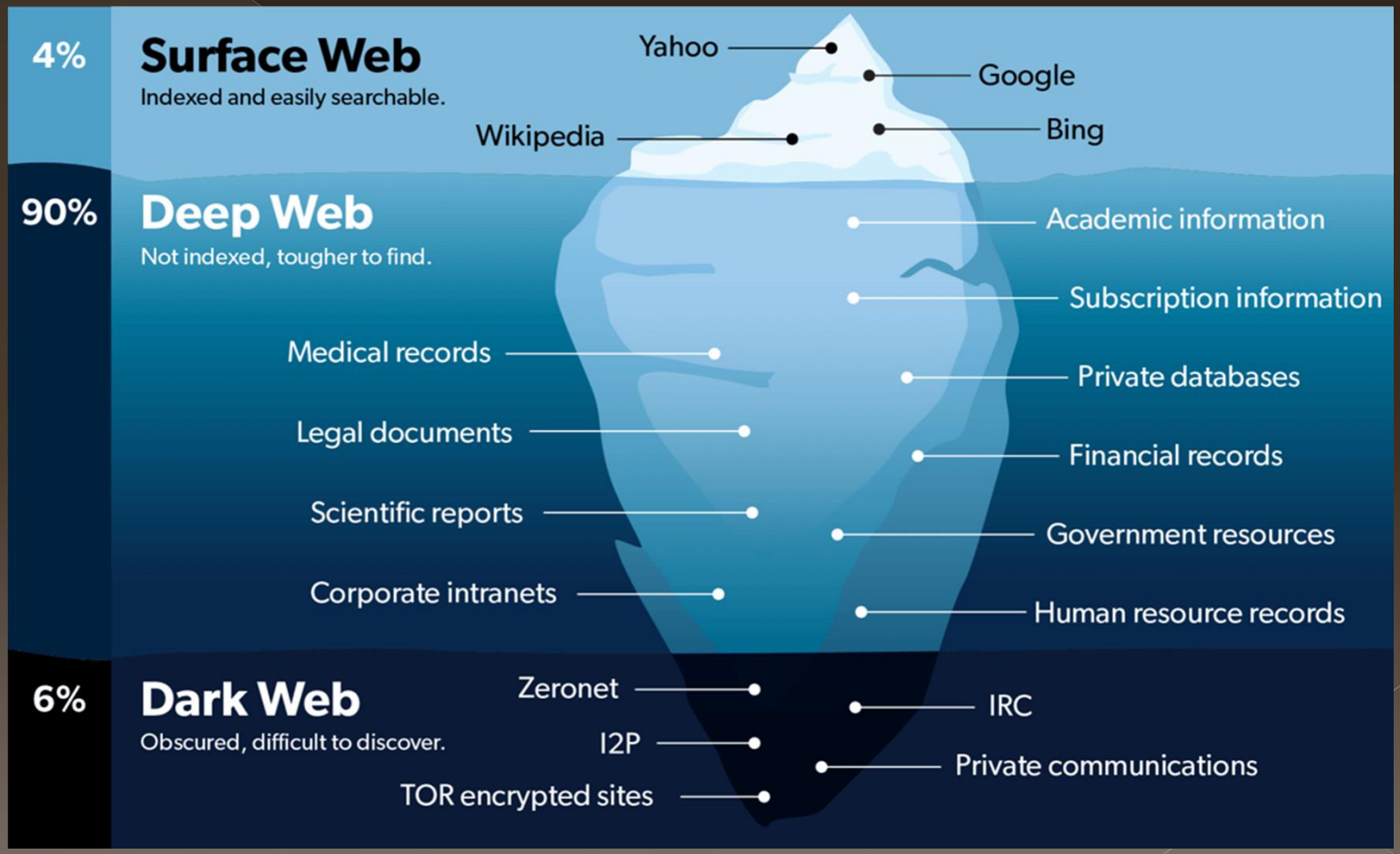
!!! IMPORTANTE !!!

IL MIO NON E' UN INVITO AD ACCERE AL DARK WEB MA E' SEMPLICEMENTE DIVULGAZIONE DI INFORMAZIONI.

Introduzione

Parlando di Cybercrimine come fatto nella descrizione delle varie tipologie di attacco non possiamo non finire a parlare di Dark Web perché esso rappresenta l'ecosistema all'interno del quale si annida questa criminalità.

Struttura:


4%
Surface Web
Indexed and easily searchable.
Yahoo
Google
Wikipedia
Bing
90%
Deep Web
Not indexed, tougher to find.
Academic information
Subscription information
Medical records
Private databases
Legal documents
Financial records
Scientific reports
Government resources
Corporate intranets
Human resource records
6%
Dark Web
Obscured, difficult to discover.
Zeronet
IRC
I2P
Private communications
TOR encrypted sites

Dark web e Deep web sono la stessa cosa?

- Assolutamente no ma spesso i due termini vengono usati come fossero la stessa cosa;
- Il Dark web però è una piccola parte del Deep web.

Surface web, il Deep web e il Dark web (1/2)

Tutti e tre ruotano intorno a quello che sono i motori di ricerca:

- **Surface Web**:

  rappresenta tutte quelle pagine web e quei documenti che vengono indicizzati dai motori di ricerca;

- Il **Deep Web**:

  indica tutte quelle pagine web e quei contenuti che non sono indicizzati dai motori di ricerca, convenzionali e quindi non possono essere trovate tramite una semplice ricerca su Google.

Surface web, il Deep web e il Dark web (2/2)

- Il **Dark Web**:

  Definisce quella parte del Deep web che non è accessibile attraverso i normali programmi, ma che richiede l'impiego di accorgimenti e programmi particolari.

  Sostanzialmente, possiamo definirlo come la porzione di internet che è intenzionalmente nascosta dai motori di ricerca, utilizzando indirizzi IP nascosti.

Motivi dietro le pagine non indicizzate:

- Le pagine web non vengono indicizzate principalmente per 3 motivi differenti:
  1. Perché sono delle pagine dinamiche ossia create al momento in seguito a delle azioni che noi effettuiamo sulla piattaforma;
  2. Includono delle informazioni private e personali e quindi per forza non devono essere indicizzate;
  3. Chi ha creato quelle pagine non vuole che siano indicizzate poiché contengono informazioni che non si vuole far visualizzare e trovare facilmente da tutti con una semplice ricerca.

Struttura del Web:

Dark web

- Sott'insieme del Deep web
- Contiene pagine dove tendenzialmente si effettuano della attività illegali:
  - DROGHE
  - ARMI
  - DOCUMENTI FALSI
  - CONTI BANCARI RUBATI;
  - SERVIZI HACKING
  - PORNOGRAFIA ILLEGALE
  - FINTI TITOLI DI STUDIO
  - FORUM (scambio di idee senza filtri)
- Le pagine non devono essere indicizzate altrimenti la giustizia ci metterebbe pochissimo ad essere individuati dalla giustizia che procederebbe alla chiusura del servizio.

E’ legale o illegale accedere al Dark web?

- Di base accedere non è illegale perché noi entriamo per visitare delle pagine non indicizzate;
- Se mi trovo a **GUARDARE** dei siti che vengono sostanze stupefacenti o armi non è illegale e non sto commettendo alcun reato;
- Se effettuo una compravendita compio un **REATO** per il quale subirò delle conseguenze.

Qual è il rischio più grande nel Dark web?

Quello di venire truffati mentre state voi stessi truffando

- Spesso abbiamo sentito parlare " Hackerato lo shopping o un tale servizio e rubati milioni di dati" → Tutto ciò finisce nel Dark Web;
- Il maggior commercio nel Dark web si focalizza su dati di carte di credito di paypall, carte regalo amazon ecc…
- Molto spesso l'acquisto di questi dati avviene tramite criptovalute

Truffe e Trappole

- Per esempio preso dall'euforia e dalle opportunità decido di comprare un conto PayPall che mi farà avere molti più soldi rispetto a quelli che vado ad investire nell'acquisto;
- Il sistema mi chiede di pagare in criptovalute

POSSO INCAPPARE IN DELLE TRAPPOLE

Conseguenze

1. Ho appena commesso un reato;
2. Ho appena effettuato una transazione, loro hanno preso le vostre criptovalute (Bitcoin/LiteCoin/Monero/l'Ethereum che non tengono traccia di alcun tipo di movimento) ma voi non avete ricevuto assolutamente nulla in cambio o vi hanno inviato un servizio che non funziona.
3. Ho effettuato la transazione, ho perso i soldi, ho commesso un reato e sono vittima di un **Cybercriminale** che a sua volta è entrato in possesso di alcuni dei miei dati personali

Quali sono gli altri rischi del Dark Web? (1/3)

- Se navigo nel Surface web esistono delle barriere di sicurezza create dall'autore dei siti stessi, nel Dark web e nel Deep Web queste barriere non esistono ;

- Se navigo su YouTube su Google ecc… posso stare abbastanza tranquillo perché il proprietario di questi siti investe soldi sulla sicurezza ;

- Nel Dark Web non esiste una supervisione dei siti anzi molto spesso i link vengono creati per attrarre clienti e curiosi e poi truffarli.

Quali sono gli altri rischi del Dark Web? (2/3)

- Nel Dark Web sono ad alto rischio di Virus e quindi se navigo devo stare 10 volte più attento rispetto ad una normale navigazione sul Surface Web;

COME FACCIO A PROTEGGERMI ?

Rischi nel Dark Web? (3/3)

- Il modo principale per prendere un virus sul computer normalmente è l'azione diretta da parte di un utente ossia si scarica un file, si avvia la lettura di un allegato da una mail , un file trasportato su una chiavetta ecc…
- Sul Dark web qualsiasi cosa io scarico o qualsiasi link che clicco sono potenziali virus
- Un Malware abbiamo visto che può rimanere silente nel nostro pc e rubare i nostri dati privati oppure può essere trasmesso ad altri fino a creare una catena di dati rubati.
- Nel Dark web i link che ci portano ai siti non sempre esplicitano ciò che realmente poi si trova.

E’ un bene entrare nel Dark web?

Se non volete commettere reati o acquistare cose proibite

NO

Se voglio solo osservare perché curioso

SI

Come si entra sul Dark Web:

- Si deve effettuare una connessione alla rete Tor (Browser) che è un rete di server;
- E' necessario scaricarlo da Torproject.org e poi seguire le istruzioni fornite.
- Per accedere a dei particolari domini, per esempio i .Onion bisogna riuscire a farsi invitare da qualcuno.
- I domini .onion ,costituiscono la rete Onion ,hanno dei tempi di transazione molto breve e sono fuori da qualunque tipologia di controllo o sorveglianza.

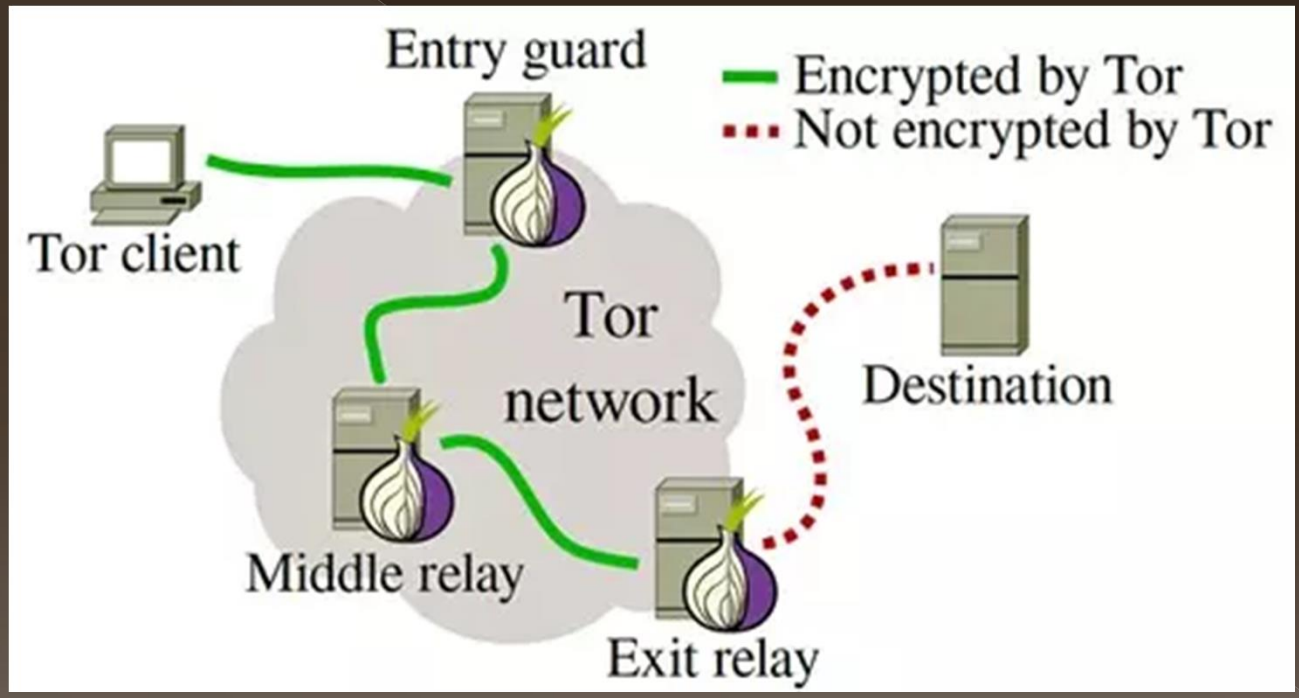
!!!!IMPORTANTE!!!!

- L’utilizzo di Onion consente solo di non far sapere con chi si comunica, ma non di navigare in modalità totalmente anonima.
- Per evitare di essere rintracciati in qualsiasi modo si può utilizzare un hotspot WiFi pubblico o la rete di un Internet Point che non richieda il rilascio di alcun documento di identità.
- Per navigare nel Dark web le due accortezze principali da usare sono oscurare la telecamera del pc e parlare il meno possibile.

Tor

- Tor è l'acronimo di The Onion Router è una rete decentralizzata costituita da migliaia di server sparsi in tutto il mondo e si basa su una struttura a strati proprio come la "cipolla";
- I dati di navigazione non transitano direttamente dal client al server, come accade per la navigazione normale. I pacchetti passano attraverso dei router e realizzano un circuito virtuale crittografato a strati.

Struttura Tor



Ma chi ha inventato Tor?

- Tor è un protocollo (una serie di regole per il trasferimento delle informazioni) sviluppato nella metà degli anni Novanta dagli Uffici per le ricerche navali degli Stati Uniti (United States Naval Research Laboratory) per proteggere le comunicazioni dell'intelligence, e oggi, conta approssimativamente 2,5 milioni di accessi quotidianamente.
- Gli URL della rete Tor hanno il TLD (Top Level Domain) che non è il classico .com o .it, ma .onion.
- Posso usare Tor anche per normali connessioni web ma ovviamente deve rimbalzare fra diversi server e quindi la connessione è più lenta ma ho una navigazione anonima.

Cosa è Tor:

- Tor è una tecnologia per proteggere la privacy e mantenere un anonimato;
- Non è esclusivamente l'accesso al Dark Web e commettere cose illegali;
- Usare Tor è legale e posso tranquillamente collegarmi anche a Facebook.

Differenza fra una normale navigazione e con l'uso di Tor (1/3):

- Normalmente se mi connetto ad un sito es. facebook dal nostro pc parte una richiesta di collegamente al server dove risiede il servizio, e digitiamo nome utente e pwd e accediamo → Connessione rintracciabile anche utilizzando delle VPN (non sempplice ma possibile);
- Con Tor si hanno più nodi(proxy) che può essere chiunque da un serve potentissimo sparso nel mondo ad un pc di casa;
- Se effettuo su Tor una richiesta per es su Youtube la richiesta prima di arrivare al server youtube passa attraverso vari nodi Tor (2-3-4-100)

Differenza fra una normale navigazione e con l'uso di Tor (2/3):

- I pacchetti spediti hanno tutti la stessa lunghezza per riuscire a vedere tutti i pacchetti identici (512 byte);
- Il pacchetto viene criptato ogni volta che passa da un nodo;
- Se per esempio il pacchetto passa da 3 nodi avrà tre chiavi di cifratura → strati di cipolla
- Avrò il mio messaggio al centro e 3 strati di cifratura sopra a protezione;
- Il nostro computer manda il messaggio al primo nodo Tor che conosce solo la chiave di cifratura del primo strato quello più esterno;

Differenza fra una normale navigazione e con l'uso di Tor (3/3):

- Dalla decriptazione questo nodo avrà solo l'informazione di collegamento al successivo nodo Tor;
- Il secondo nodo Tor avrà la chiave ci cifratura per togliere il secondo strato e stessa cosa saprà solo a quale nodo successivo inviare il pacchetto;
- Il terzo nodo Tor avrà la chiave di cifratura dell'ultimo strato e lui leggerà di collegarsi a youtube;
- Procedimento inverso di criptaggio del pacchetto per arrivare al mittente della richiesta. Il nostro pc ovviamente ha tutte le chiavi di criptaggio e decifra il messaggio.

Deep web

- Nel Deep web trovo moltissime informazioni interessanti;
- Il Deep web non è l'Internet che siamo abituati ad utilizzare tutti i giorni nelle nostre normali ricerche;
- Non ci sono sistemi interattivi;
- Non troverò una grafica ben curata.
- Noi tutti i giorni navighiamo anche nel Deep web semplicemente entrando in pagine interne ad un'azienda o pagine protette da pwd

Sistemi che consentono l'anonimato nella navigazione:

- **DuckDuckGo**;
- **UltraSurf** un piccolo programma per Windows che permette di navigare anonimi su Internet camuffando il proprio indirizzo IP con un indirizzo IP statunitense;
- **Freegate** piccolo programma gratuito che permette di navigare in maniera anonima su Internet e di bypassare le censure imposte in molti Paesi senza dover configurare nulla.
- **HotSpot Shield** è una soluzione molto efficace per nascondere la propria identità online camuffando l'indirizzo IP con un IP americano
- **Ricco VPN** è un sistema di VPN molto valido che permette di camuffare la propria identità online con l'ausilio di indirizzi IP stranieri.