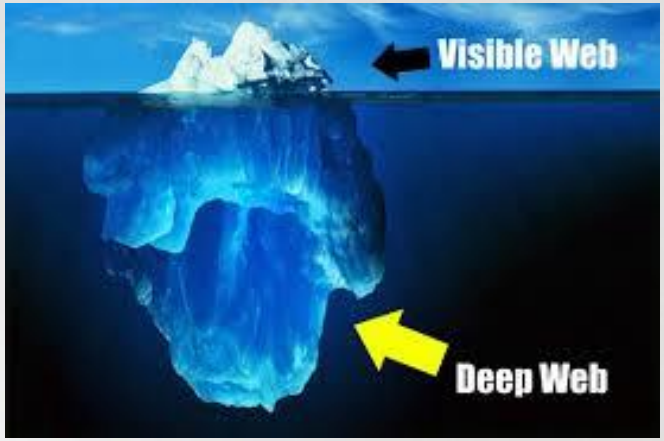
Franco Sivilli

Psicologia della salute, vecchie e nuove dipendenze

Il DEEP WEB: il lato oscuro della Rete

Il Deep Web: le origini e la dimensione



Il termine **"deepweb"** è usato per indicare una classe di contenuti su Internet che, per diversi motivi tecnici, non è indicizzato dai motori di ricerca.

Nasce per poter comunicare in maniera anonima in Rete, consentire agli utenti della rete di salvaguardare il proprio diritto alla privacy ma favorire anche la crescita di veri e propri servizi online per la fornitura di ogni genere di illegalità

Il deep web stimato è circa **500** volte il web visibile.

Il Deep Web: i contenuti

- **Pagine web dinamiche**: pagine generate dinamicamente sulla richiesta HTTP richiamate solo compilando un form o a risposta di una particolare richiesta;
- **Pagine non linkate:** pagine Web che non sono collegate a nessun'altra pagina Web
- **Siti privati**: pagine che richiedono la registrazione e l'autenticazione login/password impedendo ai motori di ricerca di accedervi e indicizzarle;
- **Script:** pagine che possono essere raggiunte solo attraverso *link* realizzati in java script o in Flash e che quindi richiedono procedure particolari
- **Reti ad accesso limitato**: contenuti su siti che non sono accessibili a tutto il pubblico Internet
- **Darknet** e infrastrutture di routing alternative: siti ospitati su infrastrutture che richiedono uno specifico software per accedere ai loro contenuti (client dedicato)

Il Deep Web: gli utenti

- Attivisti informatici, politici e religiosi (informazioni sensibili es. wikileaks)
- Servizi di prevenzione per sondare pericoli internazionali e per catturare tendenze in anteprima;
- Professionisti delle informazioni (*data mining* o *information brokering)*
- Dark user: utenti della **darknet (la parte illegale della Rete)**

Il Deep Web: le reti che lo compongono

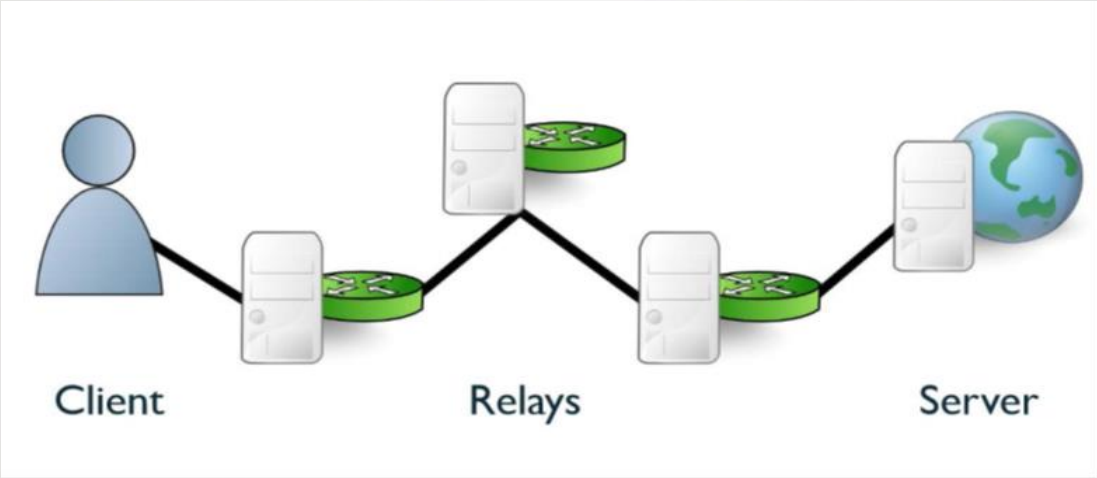
- TOR*
- P2P
- FREENET

* La più usata

Il Deep Web: la rete TOR

TOR: La rete TOR è stata originariamente sviluppata dalla US Naval Research Laboratory ed introdotta nel 2002 per consentire comunicazioni anonime tramite una rete basata su una serie di nodi chiamati relay, costituiti da server intermediari (onion) attraverso i quali transitano i dati prima di arrivare a destinazione.
In pratica, i dati prima di arrivare al server del sito web richiesto, **passano in questi nodi casualmente** utilizzando sempre un percorso differente. Arrivati al nodo prescelto, viene selezionato immediatamente il successivo e così via. La rete è strutturata in modo tale da **modificare il percorso** dei dati ogni dieci minuti e automaticamente. Ne consegue che i siti web non capiscono da dove ricevono la richiesta. Per aumentare la sicurezza, tutti i dati scambiati tra i server sono **crittografat**i in modo tale da impedirne la lettura.

Il Deep Web: la rete TOR



Il Deep Web: la rete TOR

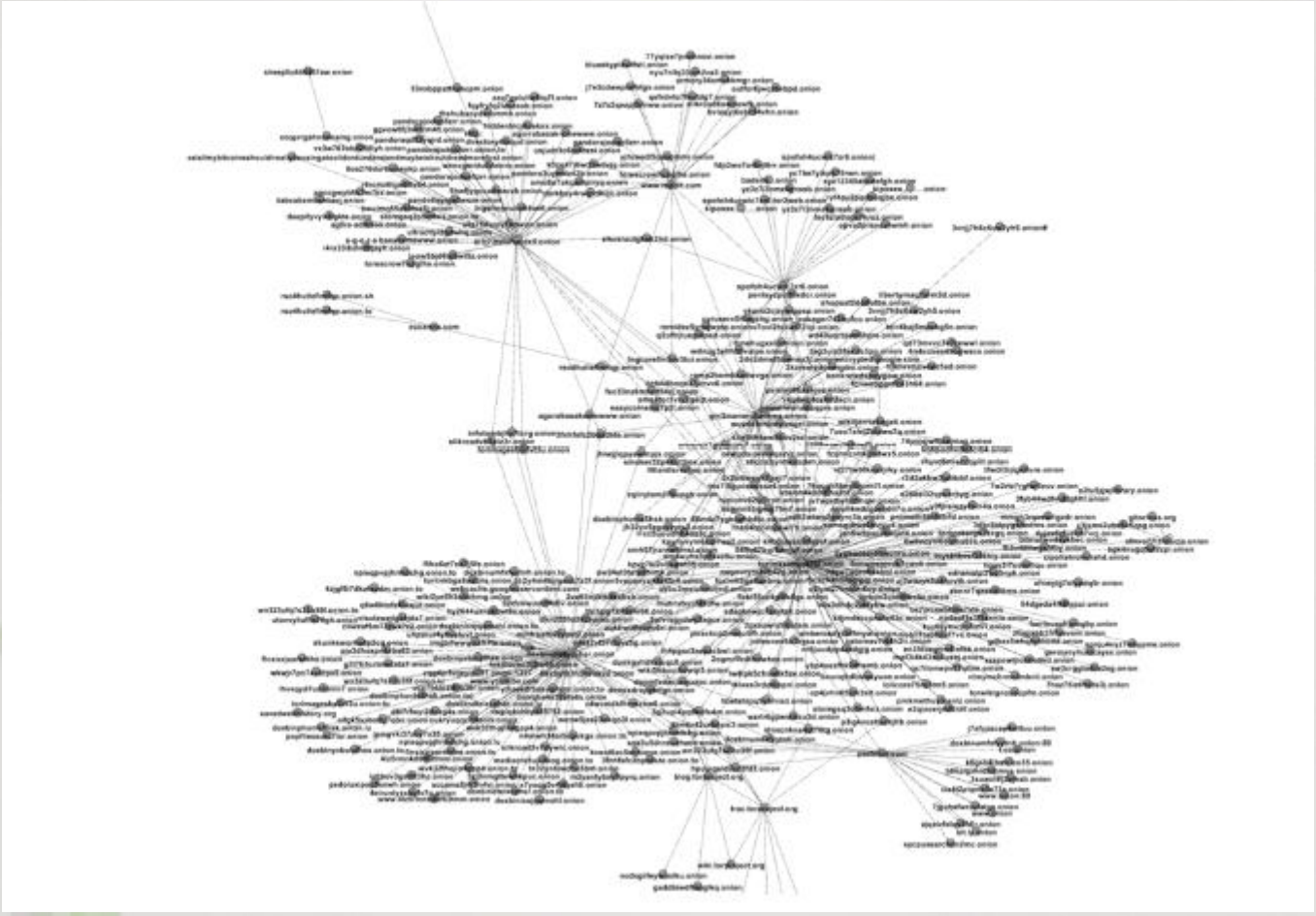
L'adozione di questo meccanismo di crittografia ha i seguenti vantaggi:

- ogni nodo (server) all'interno del circuito conosce **solo l'hop precedente e successi**vo per una richiesta ma non può decifrare il contenuto né scoprire la sua destinazione finale;
- un server, quindi, vede la richiesta ricevuta come emanata dall'ultimo nodo del circuito TOR ed è praticamente impossibile individuare l'origine di una richiesta;
- **l'unico nodo TOR in grado di visualizzare la richiesta non cifrata è il nodo di uscita,** ma anche questo non conosce l'origine della richiesta, ma solo l'hop precedente nel circuito.

Il Deep Web: la rete TOR

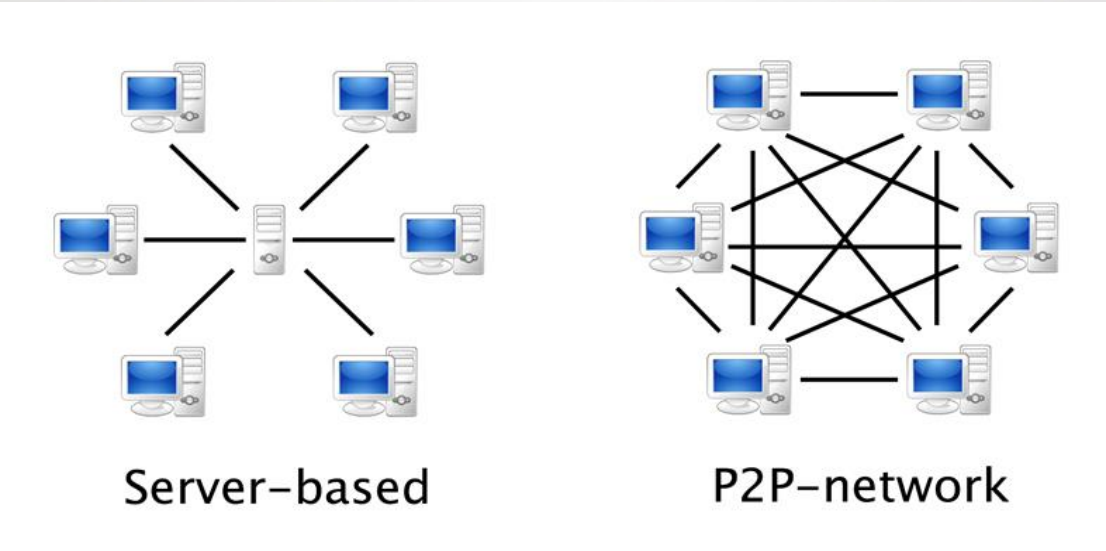
La gamma di prodotti offerti in TOR's hidden services è abbastanza vasto e si estende praticamente su ogni forma di voce relativa ad attività illegali (ad esempio, droghe, armi, sicari, ecc).

Il Deep Web: la rete TOR (i nodi onion censiti)



Il Deep Web: la rete P2P

E’ l’antitesi del modello Client/Server, trattasi di rete formata da nodi equivalenti (*peer* appunto) che fungono sia da client che da server verso altri nodi della rete. Qualsiasi nodo è in grado di avviare o completare una transazione ed ha una propria configurazione locale che può differire da quella degli altri nodi nella velocità di elaborazione, nell’ampiezza di banda e nella quantità di dati memorizzati.



Il Deep Web: la rete P2P

L’esempio classico di P2P è la rete per la condivisione di file (*file sharing*) come Gnutella, FastTrack che forniscono il libero scambio di file tra i computer connessi a Internet. I tipi di file maggiormente condivisi in queste reti sono quelli multimediali (musica e film). Ciò ha portato molte compagnie, soprattutto quelle discografiche e i media, a considerarle una minaccia per i loro interessi.

Il Deep Web: la rete P2P

Tecnicamente, le applicazioni peer-to-peer dovrebbero implementare solo protocolli di *peering* che non riconoscono il concetto di "server e di client". Tale applicazioni o reti "pure" sono in realtà molto rare. Molte reti e applicazioni che si descrivono come peer-to-peer fanno però affidamento anche su alcuni elementi "non-peer", come per esempio il DNS. Inoltre, applicazioni globali utilizzano spesso protocolli multipli che fungono simultaneamente da client, da server, e da peer.

Il Deep Web: la rete Freenet

"Without anonymity there can never be true freedom of speech". Ian Clarke

Nasce per salvaguardare ed esaltare il diritto di libertà.
Essa risale ai primi anni del nuovo millennio ed è stata fondata per garantire l'anonimato e la sicurezza degli utenti e dei loro dati.

Il Deep Web: la rete Freenet

Tecnicamente è costituita da due parti:

- il database distribuito, suddiviso tra tutti i computer connessi alla sua rete,
- gli strumenti per navigare nel database e comunicare coi vari computer connessi.

Il Deep Web: la rete Freenet

Quando si inserisce un file nel DB distribuito, si riceve in cambio una **chiave di cifratura** mentre il file **viene collocato in più computer**, detti nodi, presenti in rete.
Per recuperare il file, bisogna consegnare a Freenet la chiave e in cambio si riceve il file corrispondente, scaricandolo dai vari nodi su cui è stato immagazzinato appunto **“a pezzi”.**

Il Deep Web: Freenet vs P2P

La **differenza** di Freenet, rispetto ad altre reti di condivisione, è **l'assenza di controllo** sui files immagazzinati. Tutti i files inseriti in Freenet, infatti, sono prima di tutto **frammentati** in pezzi più piccoli, per agevolare lo scambio, e poi **cifrati**: soltanto l'utente con la chiave corrispondente sa quale file stia scaricando, mentre tutto il resto della Rete non ne saprà nulla.

Il Deep Web: Freenet vs P2P

Ogni nodo, quindi, **conterrà** soltanto un cumulo più o meno grande di **frammenti anonimi di files**, **cifrati** e indistinguibili: in questo modo, nessuno può sapere quali files si trovino nel proprio computer e nessuno può formalmente essere ritenuto responsabile di ciò che è condiviso attraverso il suo nodo (almeno davanti al tribunale della propria coscienza).Proprio perché nessuno sa dove si trovi esattamente un determinato file e in quante copie sia presente, **non ci sono facili sistemi per rimuovere un file**:ciò lo rende resistente alle censure ed è proprio questo uno degli obiettivi perseguiti dal creatore di Freenet.

Il Deep Web: strategie di Freenet

I file sono **conservati** in base alla loro **popolarità**, ossia alla frequenza con cui sono cercati e scaricati: un file popolare continuerà a rimanere attivo e disponibile in molte copie, mentre un file che non interessa più a nessuno, pian piano, diventerà sempre più **raro** fino a **scomparire** per “selezione naturale” dalla rete. Se si vuole eliminare un file, dunque, l’unico sistema è sperare che a nessuno interessi più.

Il Deep Web: strategie di Freenet

Un’altra strategia utilizzata da Freenet per resistere alle censure è quella di essere strutturata come **rete decentralizzata** e composta da innumerevoli **sottoreti più piccole**. Ogni nodo **conosce soltanto una ristretta cerchia di nodi** a esso adiacenti e soltanto con loro si può collegare; questi nodi, a loro volta, conoscono soltanto una ristretta cerchia di altri nodi e si possono collegare soltanto con loro; e così via, fino a coprire l’intera rete. Tutti i nodi, inoltre, hanno lo stesso valore: **non esiste distinzione tra client e server**, cioè fra un nodo che funge da deposito (server) e un altro che si collega per attingere (client), come avviene in altre reti. Tutti i nodi sono sia server che client; **un nodo molto potente** (ossia un nodo che cede molta banda di connessione e un grande spazio di storage), può talvolta assumere un ruolo da server (inteso come maggiore contributo che riesce a dare alla Rete).

Il Deep Web: la rete darknet

La **Darknet si riferise ad una classe di reti che hanno lo** scopo di garantire l'accesso anonimo e non tracciabile ai contenuti Web e l'anonimato di un sito.
La struttura composita della rete **Freenet (ma anche TOR)** la rende utilizzabile come **darknet** ovvero come sottorete composta soltanto da nodi conosciuti e di fiducia, creata manualmente da uno specifico utente.

Il Deep Web: contenuti della darknet

- Portali pedopornografici come Lolita City o OnionPedo;
- Portali per rovinare in maniera anonima la reputazione di terzi come RespiraTor;
- Laboratori rivoluzionari politico-informatico come Revolution Bunker o LiberaTor per costruirsi un arsenale domestico, confezionare ordigni esplosivi e organizzare agguati e attentati
- Hacker Services che mette a disposizione virus informatici per attaccare persone o aziende sgradite e sistemi di ricerca delle password altrui;
- Contract killer: offre omicidi a pagamento, con tariffe dettagliate. Cinquemila euro di spese anticipate per un delitto in Europa, diecimila per una trasferta extracontinentale. C'è una sorta di regolamento: l'obiettivo deve avere almeno 16 anni, e il costo dell'operazione è di 20 mila euro per una persona normale, 50 mila per un poliziotto, un criminale o un paparazzo, 100 mila per un boss, un funzionario di polizia o un giornalista, fino a 200 mila per un manager. Due mesi di tempo dal primo pagamento per completare la missione.

Il Deep Web: la rete darknet (alcuni indirizzi)

Address	Descriptio	Note
http://rso4hutlefirefqp.onion/	EuCanna -	First Class Cannabis Healthcare
http://newpdsuslmzqazvr.onion/	Peoples Drug Store	The Darkweb's Best Online Drug Supplier!
http://k4btcoezc5tlxyaf.onion/	Kamagra for Bitcoin	Same as Viagra but cheaper!
http://tuu66yxvrnn3of7l.onion/	UK Guns and Ammo	Selling Guns and Ammo from the UK for Bitcoins.
http://2ogmrlfzdthnwkez.onion/	Rent-A-Hacker	Hacking, DDOS, Social Engeneering, Espionage, Ruining people.
http://3dbr5t4pygahedms.onion/	ccPal	CCs, CVV2s, Ebay, Paypals and more.
http://ybp4oezfhk24hxmb.onion/	Hitman Network	Group of contract killers working in the US, Canada and EU.
http://en35tuzqmn4lofbk.onion	USfakeIDs	High quality USA Fake Drivers Licenses

Il Deep Web: la moneta della darknet

Gli acquirenti e i venditori di questi siti, conducono tutte le loro transazioni con il **Bitcoin**, una moneta virtuale detta anche criptomoneta, che si basa sul concetto dell'anonimato e della prova di scambio, oltre ad avere, di norma, uno schema di emissione pre concordato. Valute di questo tipo hanno poco a che fare con quelle emesse dalle banche nazionali. La loro nascita risale idealmente alla fine del 2008 da Satoshi Nakamoto che pubblicò sul sito *metzdowd.com* un documento chiamato Bitcoin sancendo la nascita dell'idea alla base di tutte le criptomonete.

Il Deep Web: non è tutto negativo

Ian Walden (professore di Information and Communications Law alla *Queen Mary University* di Londra), sostiene che l'attrazione per il deepweb deriva «dall'uso di tecniche che danno la possibilità alle persone di comunicare anonimamente e in maniera onesta».

Navigare nel completo anonimato provoca sensazioni strane, quasi di euforia che non sono troppo lontane da quelle che probabilmente hanno provato un quarto di secolo fa i primi utenti di Internet.

Il Deep Web: non è tutto negativo

Walden sottolinea che « nei regimi dove la censura è all'ordine del giorno, i social media non favoriscono le proteste politiche, poiché è molto facile identificare gli utenti» e che il deepweb permette di «comunicare nel lungo periodo senza mettere a rischio l'incolumità dei propri cari».

TOR per i giornalisti è una vera manna, serve per poter comunicare segretamente con le loro fonti.

Conclusioni

La sfida dei prossimi anni sarà quella di pretendere una Rete che consenta di mantenere privato ciò che il privato cittadino non vuole divulgare del suo essere (Privacy), e permetta la più totale accessibilità dei dati e dei processi, sia delle Pubbliche Amministrazioni sia degli individui.

fsivilli@unich.it