Esplorando Internet lungo i meandri del WEB

Author : Salvatore Lombardo

Date : 25 Febbraio 2019

Nel 1969 nasceva la rete **Arpanet**, un progetto realizzato dal Dipartimento della Difesa degli Stati Uniti nell'ambito dello sviluppo di tecnologie militari, che sarebbe stata l'**archetipo della grande rete mondiale** che oggi conosciamo con il nome di Internet e che, dagli anni '90, si è ampiamente diffusa grazie all'avvento del World Wide Web.

Negli stessi anni i servizi segreti americani adottavano, per la protezione delle proprie comunicazioni, il progetto **TOR (The Onion Router)**, la rete segreta di Internet. Anche questo progetto, inizialmente militare, si modificò nel tempo e fu utilizzato dapprima in ambito scientifico e di ricerca, fino a diventare di uso comune con l'omonimo programma di navigazione. Oggi TOR è un browser libero [1] e disponibile su vari sistemi operativi, **noto per la sua peculiare caratteristica di garantire l'anonimato sul web e l'accesso alla sua darknet.**

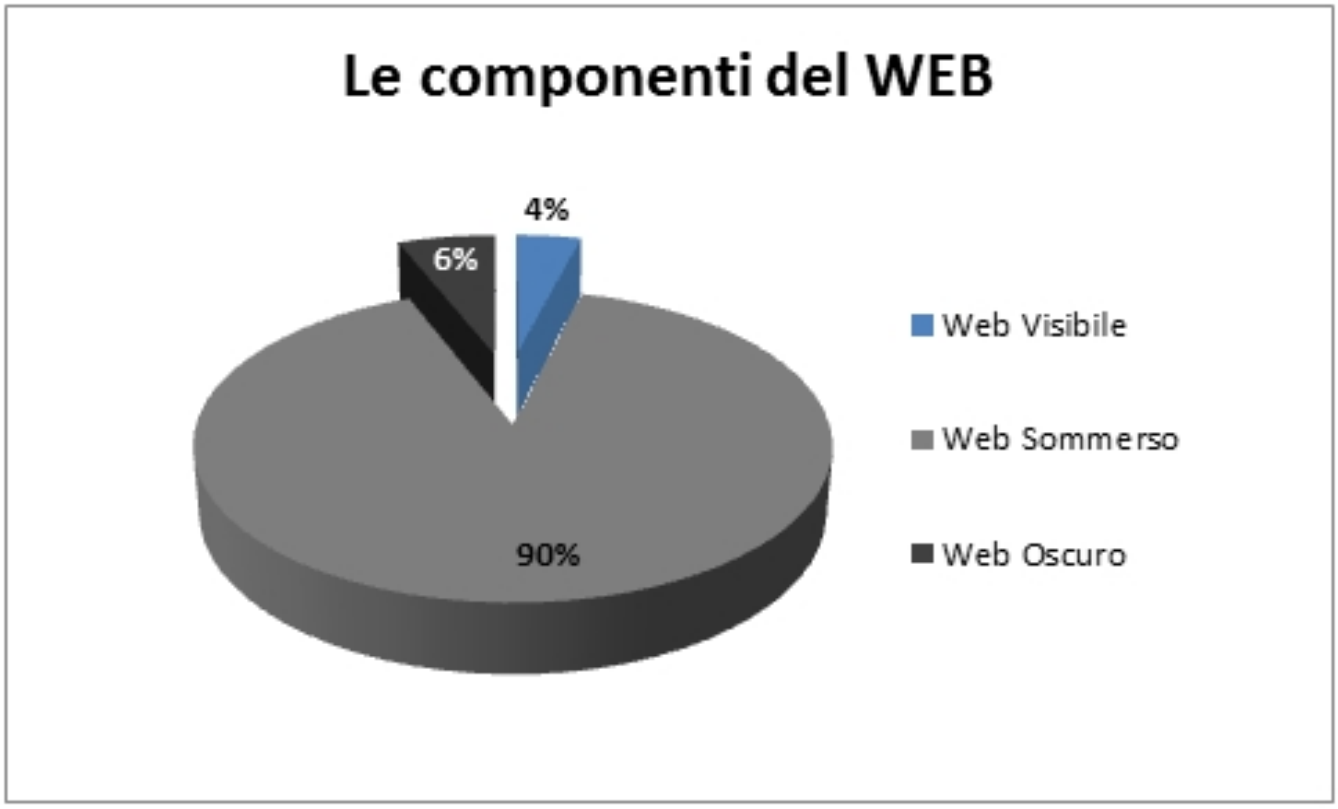
Con questo articolo intendo parlare di alcuni aspetti nascosti del web a puro scopo informativo, *senza pertanto voler promuovere alcuna attività illecita, che va sempre e comunque perseguita e contrastata*.

Il Web non è solo quello che noi vediamo, ma è anche costituito:

- dall'insieme dei contenuti non indicizzati dai comuni motori di ricerca. Sappiamo che, per facilitare la ricerca di informazioni su internet da parte degli utenti, è fondamentale la cosiddetta indicizzazione web. Ovvero il processo automatizzato svolto dagli stessi motori di ricerca attraverso l'ausilio di bot specializzati che, attraverso una scansione della rete, aggiornano il proprio registro degli indirizzi;
- dall'insieme dei contenuti che, se pur accessibili pubblicamente, risiedono in spazi web il cui indirizzo IP è volutamente nascosto.

Riguardo alla stima delle **effettive proporzioni** degli insiemi appena definiti, nel corso degli anni si sono espressi diversi esperti di sicurezza internazionale. Si può comunque con buona approssimazione ipotizzare uno scenario, espresso in percentuale, di questo tipo: si stima che circa il **4%** dei contenuti di internet risulti indicizzato e rappresenti la componente visibile del web. Il restante **96%** dei contenuti copre le altre due componenti, rispettivamente la parte

sommersa (90%) e quella oscura (6%).



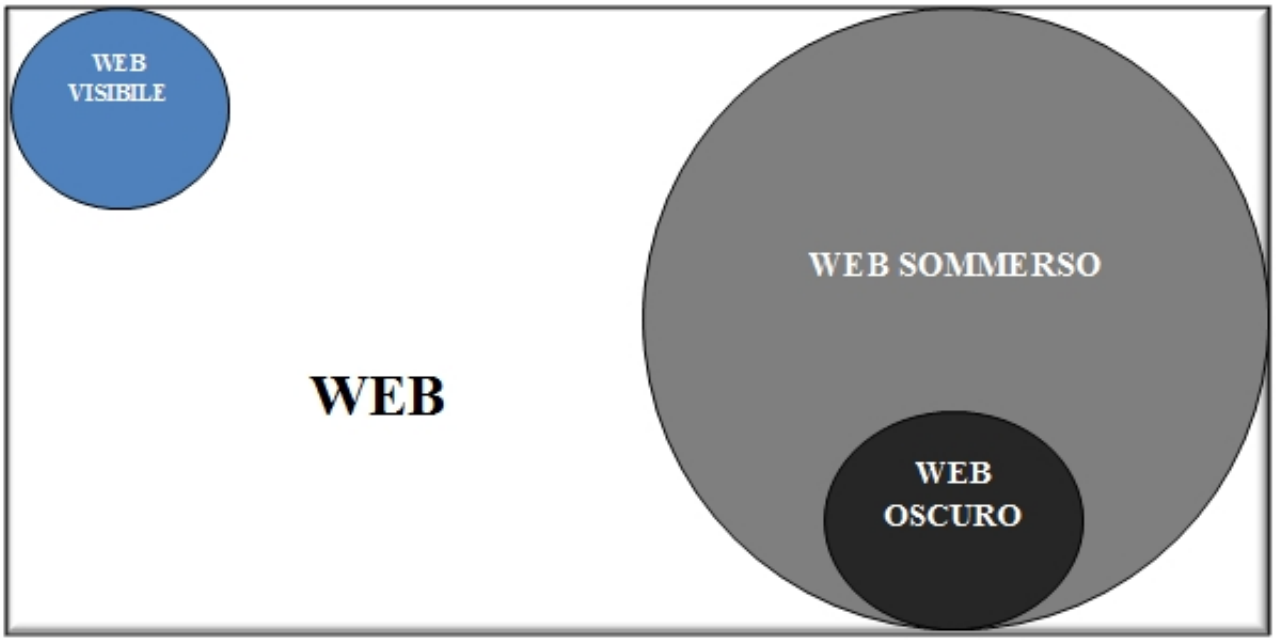
Le componenti del WEB	
La componente Visibile (Surface Web)	*Tutti i contenuti indicizzati*
La componente Sommersa (Deep Web)	*Contenuti non indicizzati ma che sono accessibili tramite un normale browser se noti i relativi indirizzi. Ad esempio fanno parte dello spazio sommerso le aree riservate, le intranet, le caselle webmail*
La componente Oscura (Dark Web)	*Contenuti non indicizzati e che non sono accessibili tramite i comuni browser. Per consultare i contenuti pubblicati sul dark web, occorre barcamenarsi tra molteplici sotto reti chiuse e private, le cosiddette darknet quali TOR, Freenet, Project I2P e ricorrere per la navigazione ad applicativi specializzati. In particolare per esplorare le pagine .onion della ben nota darknet TOR (The Onion Router) è necessario l'omonimo browser*

Ricorrendo all'utilizzo della teoria degli insiemi, come riportato nella successiva figura, se consideriamo il WEB come l'insieme ***Universo*** si può affermare che le sue componenti visibile e sommersa siano due sottoinsiemi disgiunti e propriamente inclusi nell'insieme WEB:

- ***WEB VISIBILE ? WEB SOMMERSO;***
- ***WEB VISIBILE ? WEB;***
- ***WEB SOMMERSO ? WEB;***

e che la componente oscura sia un sottoinsieme propriamente incluso nel sottoinsieme sommerso del WEB:

- ***WEB OSCURO ? WEB SOMMERSO ?***



TOR e la sua darknet

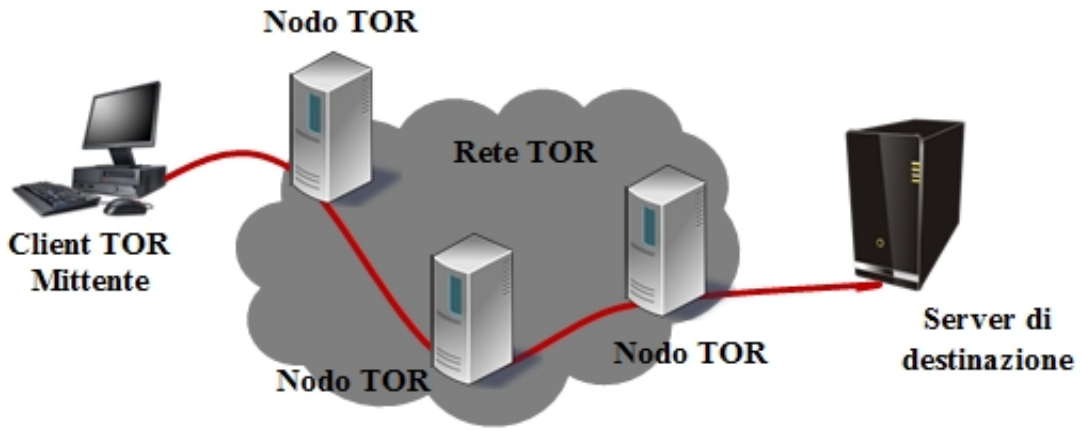
Il browser TOR altro non è che il fratellastro di Firefox e, come già detto, rappresenta il client per navigare e scambiare dati sulla medesima rete TOR. Viene utilizzato un meccanismo di crittografia a strati di cipolla (come suggerisce l'acronimo TOR) che se utilizzato in modo appropriato, tramite l'uso congiunto di una buona VPN, può garantire un certo livello di anonimato (l'indirizzo IP pubblico viene nascosto e si assicura una protezione della privacy e della sicurezza delle comunicazioni) durante la propria visita lungo le maglie del lato oscuro del web. È bene precisare che anche questo browser non è immune da vulnerabilità e, pertanto, è sempre consigliabile un aggiornamento periodico. A differenza di un comune browser, TOR permette una navigazione in sicurezza sia nella web in chiaro che in quello oscuro.

Come avviene la navigazione sulla Darknet TOR

Sul web visibile, quando digitiamo l'indirizzo di un sito (ovvero il suo URL: Uniform Resource Locator) nella barra degli indirizzi del nostro client, questo inoltrerà una richiesta ai cosiddetti **DNS (Domain Name Server)**, i quali hanno il compito di:

- convertire l’URL in un indirizzo **IP;**
- evadere la richiesta mettendoci in collegamento con il sito web desiderato (che registrerà a sua volta l’**indirizzo IP** del nostro pc, rendendoci visibili in rete).

Con il browser *TOR* la nostra navigazione non transiterà direttamente dal client al server di destinazione, per il tramite dei server DNS, ma passerà, in modo stratificato, attraverso un certo numero di nodi Tor lungo un percorso virtuale che custodisce il nostro indirizzo IP. Questo tipo di approccio rende complicata l’identificazione del client mittente, assicurando di fatto connessioni anonime e servizi occultati.

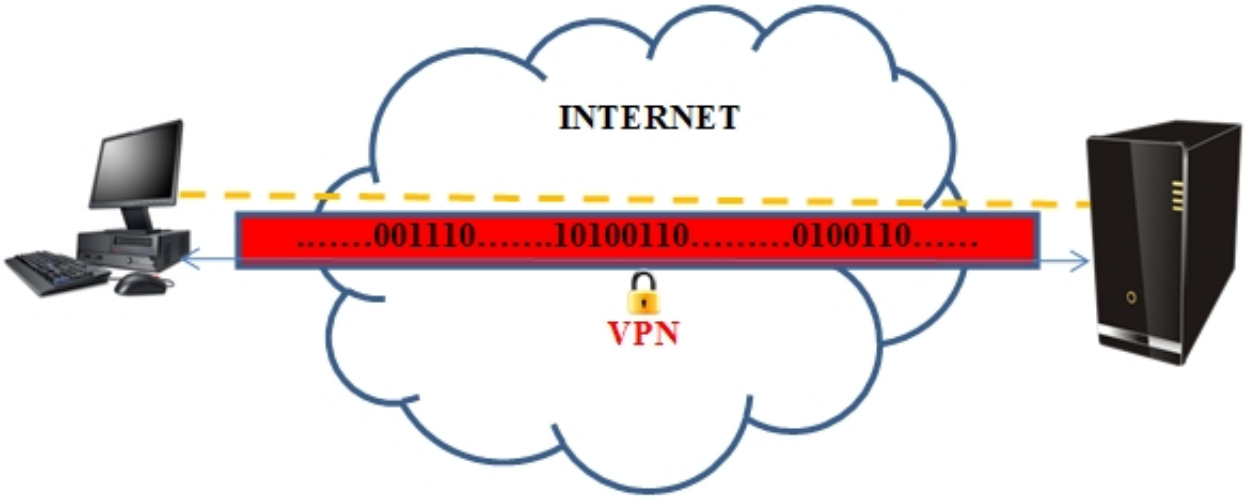


Anonimato e Privacy

Per garantire la riservatezza, la sicurezza e la protezione delle comunicazioni durante una navigazione internet, scegliere di utilizzare una VPN (Virtual Private Network) risulta vincente. La crittografia del canale di comunicazione e l’oscuramento dell’indirizzo IP pubblico assegnato consentono, infatti, di nascondere all’ISP (Internet Service Provider) tutte le proprie attività di rete. Una buona VPN (di solito a pagamento!) consente anche un certo livello di protezione della nostra privacy.

Se si vuole davvero blindare l’esplorazione sulle darknet, è consigliabile adoperare una VPN che:

- sia compatibile con il browser TOR;
- sia acquistabile, per ovvi motivi di rintracciabilità, in criptovaluta;
- non generi file di log;
- consenta, tramite le funzionalità killswitch, la gestione delle possibili perdite DNS che possono essere responsabili della nostra visibilità durante la connessione.



L’ecosistema delle reti oscure

Le darknet rappresentano a tutti gli effetti un ecosistema, in cui distinguiamo:

- gli utilizzatori (gli organismi viventi) che interagiscono con l’ambiente. Troviamo giornalisti, politici, esperti di comunicazioni, semplici curiosi, ma anche criminali ed utenti propensi ad attività illegali. Per quest’ultimo motivo, le reti oscure sono frequentate anche dalle forze di polizia e dai servizi di intelligence.

- I mercati neri, innumerevoli negozi online proponenti prodotti e servizi illegali. Esiste una vera e propria mappa dei black market specializzati in determinati settori di mercato, eccone alcuni:

  - servizi e vendita dispositivi e servizi per l’hacking;
  - servizi per frodi di carte di credito;
  - vendita di armi e documenti falsi;
  - spaccio di stupefacenti.

Il mercato oscuro può offrire, a prezzi sorprendentemente non proibitivi, ogni tipo di strumenti e prodotti illeciti e anche servizi su commissione, basati su modelli di vendita noti come *Criminal as a Service* (CaaS) o *Ransomware as a Service* (RaaS). Ovviamente, per garantire sicurezza e non rintracciabilità degli acquisti, le criptovalute (Bitcoin e/o Monero) rappresentano il mezzo di pagamento utilizzato.

Conclusioni

Il Web ha consentito negli anni lo sviluppo e la diffusione dell’informazione e della ricerca scientifica, così come la lotta alla censura; ma nel contempo l’altra faccia della medaglia ha sfruttato l’anonimato per perpetrare fini per nulla degni di merito.

Tutti i **beni e servizi illeciti non sono, però, prerogativa esclusiva del dark web**. Siti

pedopornografici, hacker, gruppi criminali si trovano anche sulla rete indicizzata, e bisogna fare un plauso agli organi di polizia preposti per il loro costante impegno nella lotta contro i reati commessi in rete.

Allo stesso modo, **il dark web non è solo un contenitore di attività criminali** ma può offrire anche numerosi servizi leciti e alternativi. Sulla rete TOR, ad esempio, è possibile trovare delle versioni underground di alcuni social media e motori di ricerca, musica in streaming, store online.

Ovviamente a far pendere l'ago della bilancia sul bene o sul male è sempre e comunque **il peso delle azioni e delle intenzioni umane**. Per fortuna, così come accade nella vita reale, anche quando si esplora internet lungo i meandri del Web, ognuno di noi ha il potere di scegliere in autonomia gli scopi del proprio agire.

Note

[1] https://www.torproject.org/

Riferimenti Sitografici

https://www.silicon.it/security/deep-e-dark-web-oltre-le-colonne-dercole-del-web-conosciuto-122315?inf_by=5c1a1e30671db848718b535b

https://darkwebnews.com/help-advice/access-dark-web/

https://www.cybersecurity360.it/cultura-cyber/cose-il-deep-web-e-il-dark-web-cosa-si-trova-e-come-si-accede-tutte-le-istruzioni/

https://www.hdblog.it/2016/11/24/dark-web-deep-cosa-e-sicurezza-rete-internet/

https://www.iusinitinere.it/fenomeno-del-web-sommerso-lecito-illecito-622

http://www.i-forensics.it/i-forensics-news/118-tor-la-porta-del-deep-web

https://www.giorgiosbaraglia.it/deep-web-dark-web-non-la-stessa-cosa/

Articolo a cura di **Salvatore Lombardo**