



# DATA SHIELDS

---



## Osservazione Critica Dark Web

In questa relazione analizzeremo oggettivamente la parte opposta al clear web, ovvero il dark net. Questo percorso attraverserà una parte generale di Onion, delle sue componenti e dei riferimenti alla legalità fino ad arrivare ad esempi con una descrizione nel dettaglio dei principali malware che si possono incontrare.

Il report effettuato è puramente per scopi illustrativi e divulgativi sull'argomento.

## Introduzione Onion

Tor Browser è un browser web incentrato sulla privacy, sviluppato dal Tor Project. L'obiettivo principale di questo strumento è quello di proteggere l'anonimato degli utenti online, mascherando le loro informazioni personali e la loro ubicazione geografica. Tor Browser si avvale della tecnologia della rete Tor (The Onion Router), la quale indirizza il traffico internet attraverso una vasta rete di relay gestiti da volontari in tutto il mondo. Questo meccanismo, denominato "onion routing", impiega una crittografia a strati che incapsula i dati in diversi livelli di sicurezza, rendendo estremamente complicato risalire all'origine del traffico.

### Dettaglio specifiche Onion Layer di protezione di Tor

Il processo di onion routing è fondamentale per la sicurezza garantita da Tor. Ogni nodo della rete, o "onion router", decifra un singolo strato di crittografia prima di passare i dati al successivo router. Questo metodo impedisce a qualsiasi singolo punto della rete di avere accesso sia alla sorgente sia alla destinazione finale dei dati, garantendo così un alto livello di anonimato.

**- Funzionalità e Sicurezza:** Tor Browser è studiato per proteggere gli utenti dalla sorveglianza di massa e dal tracciamento online. In termini pratici, ogni sessione di navigazione termina con l'eliminazione automatica di cookie e dati di sessione, mentre i tentativi di finger printing del browser vengono sistematicamente bloccati

**-Accesso al Darkweb:** Qui si trovano i siti .onion, che offrono un grado ancora maggiore di privacy e anonimato, essendo inaccessibili tramite i normali browser. Questi siti sono spesso utilizzati per garantire la libera espressione o la comunicazione sicura lontano dagli occhi indiscreti, ma possono anche includere mercati non regolamentati che vendono una vasta gamma di prodotti e servizi.

**-Navigazione Sicura e Personalizzazione:** Gli utenti devono rimanere vigili e adottare pratiche di sicurezza informate per mitigare rischi specifici associati a queste aree di Internet. Tor Browser offre la possibilità di personalizzare le impostazioni di sicurezza, permettendo agli utenti di bilanciare tra facilità d'uso e livelli elevati di protezione.



## Componenti Principali

- **Anonimizzazione: Tor** maschera l'indirizzo IP dell'utente rendendo difficile per i siti web o altre entità identificare e tracciare l'utente.

-**Routing a Strati:** Il nome "Onion" deriva dal modo in cui il traffico viene incapsulato in strati di crittografia, come una cipolla. Ogni strato viene decifrato da un nodo successivo nella catena, rivelando l'informazione necessaria per raggiungere il nodo successivo.

-**Nodi:** La rete Tor è composta da migliaia di nodi volontari:

- **Nodo di ingresso (Entry Node):** Il primo nodo che riceve il traffico dall'utente.
- **Nodo di inoltro (Relay Node):** Nodi intermedi che trasportano il traffico all'interno della rete Tor.
- **Nodo di uscita (Exit Node):** L'ultimo nodo che invia il traffico alla destinazione finale sul web.

- **Circuito :** Ogni volta che un utente inizia una sessione Tor, viene creato un circuito, una sequenza casuale di nodi attraverso cui passerà il traffico. Il circuito viene cambiato periodicamente per migliorare la sicurezza.

- **Crittografia a Strati:** Il messaggio dell'utente è incapsulato in più strati di crittografia:

- Quando l'utente invia una richiesta, viene crittografata con la chiave pubblica del nodo di uscita.
- Poi viene nuovamente crittografata con la chiave pubblica del nodo intermedio. Infine, viene crittografata con la chiave pubblica del nodo di ingresso.



## Processo di Connessione

### Creazione del Circuito:

Il client Tor seleziona casualmente una serie di nodi e stabilisce un circuito criptato:

- Ogni nodo conosce solo l'indirizzo IP del nodo precedente e del nodo successivo, mantenendo così l'anonimato tra i nodi

### Inoltro del Traffico:

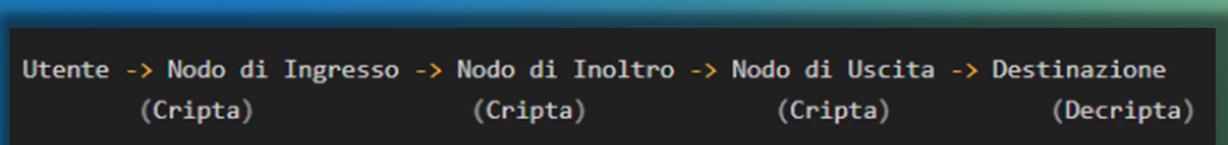
- L'utente invia la richiesta attraverso il nodo di ingresso, che rimuove il primo strato di crittografia.
- La richiesta passa al nodo di inoltro, che rimuove un altro strato
- Infine, il nodo di uscita rimuove l'ultimo strato e invia la richiesta al server di destinazione

### Risposta del Server:

- La risposta del server segue il percorso inverso attraverso i nodi, ciascuno dei quali aggiunge uno strato di crittografia

## Schema del Funzionamento

Per visualizzare meglio il processo, ecco un semplice schema:



## **Motori Di Ricerca**

A differenza del web normale (clearnet), dove i motori di ricerca come Google, Bing e Yahoo dominano, il dark web richiede l'uso di motori di ricerca specializzati che possono indicizzare e cercare siti .onion. Ecco una panoramica dei motori di ricerca più usati su Tor:

### **1. Ahmia**

Offre la possibilità di cercare siti .onion, permettendo agli utenti di accedere a risorse che non sono indicizzate dai normali motori di ricerca. Ahmia si impegna a escludere contenuti illegali dalle sue ricerche, offrendo una piattaforma relativamente più sicura per la navigazione.

### **2. DuckDuckGo**

DuckDuckGo è ben conosciuto per la sua politica di non tracciare gli utenti e viene spesso utilizzato come motore di ricerca predefinito in Tor Browser. Sebbene non sia esclusivo al dark web, DuckDuckGo può cercare e indicizzare siti .onion, rendendolo un'opzione versatile per gli utenti che cercano privacy sia nel web normale sia nel dark web.

### **3. notEvil**

notEvil è un altro motore di ricerca che attinge al design e al funzionamento di Google, offrendo una vasta gamma di risultati da siti .onion senza tracciare gli utenti. Il suo nome è un riferimento alla vecchia filosofia di Google "Don't be evil".

### **4. Candle**

Candle è un motore di ricerca ispirato a Google, ma molto più basilare. Non offre le stesse capacità di filtraggio o sicurezza di altri motori di ricerca più sofisticati, ma può essere utile per ricerche semplici e dirette nel dark web.

### **5. Haystak**

Haystak è un motore di ricerca premium che vanta di avere indicizzato più pagine .onion di qualsiasi altro motore di ricerca. Offre anche funzionalità avanzate di ricerca per gli utenti che scelgono la versione premium.



## **Parliamo di Legalità**

### **Legalità di Tor Browser**

Tor Browser stesso è completamente legale nella maggior parte dei paesi del mondo. È uno strumento progettato per garantire la privacy e la sicurezza online, ed è utilizzato legittimamente da giornalisti, attivisti per i diritti umani, forze dell'ordine e persone comuni per proteggere la loro identità su internet

### **Navigazione nel Darkweb**

Sebbene accedere al darkweb tramite Tor sia legale, le attività svolte su di esso possono non esserlo. Il darkweb è spesso associato a mercati neri, vendita di sostanze illegali, servizi di hacking, e altre attività criminali. Partecipare a queste attività, anche solo navigando consapevolmente in siti che le facilitano, può essere considerato illegale a seconda delle leggi locali

### **Responsabilità Legale**

Gli utenti di Tor devono essere consapevoli che mascherare la propria identità per commettere atti illegali o accedere a materiale illegale (come pornografia infantile, traffico di droga, armi, etc.) è considerato un reato in molti paesi. Inoltre, anche il solo possesso di determinati tipi di dati scaricati dal darkweb può essere illegale.

### **Conformità alle Leggi sulla Soveglia**

In certe giurisdizioni, le agenzie governative possono avere il potere legale di richiedere dati dagli ISP o da altri intermediari di servizi internet

### **Rispetto Delle Leggi Locali**

È essenziale per gli utenti di Tor conoscere e rispettare le leggi locali relative all'uso di internet e alla privacy. Questo include la comprensione delle implicazioni legali dell'accesso o della distribuzione di materiali protetti da copyright attraverso Tor.



**Vendita Botnet:**

<http://blackypezbmbgvmmI4vllavvdvjjh6dkuth7ngnj2qx3x56xl6eaq7qd.onion/product-tag/ddos-attack-botnet/>

La Botnet consiste in una raccolta di dispositivi infettati dal malware. La rete di dispositivi infetti viene detta zombie network o zombienet per il fatto che tali dispositivi restano passivi fin quando l'attaccante non invia un comando di attivazione ai dispositivi compromessi, infatti il malware è programmato per rimanere inattivo e non individuabile sul dispositivo finché non riceve il comando. Questo tipo di attacco può provocare un DoS o DDoS verso il bersaglio prescelto.

**Vendita Informazioni Personaliali:**

<http://darkleakyqmv62eweqtyw4dnhaijg4m4dkburo73pzuqfdumcntqdokyd.onion/articles/article-95.html>

La vendita di informazioni personali sia PII che SII è un furto di dati sensibili (dal numero di telefono, ai dati bancari e dati sanitari). La vittima in questo caso subisce un furto di identità più o meno grave che può portare anche ad ingenti perdite economiche e perdita di credibilità per le aziende.

**Vendita Ramsonware:**

<http://blackujuzctwajhtduhrza3kjngotya7k4rg4apymlbj7plinnrsvtid.onion/product/jigsaw-ransomware-decrypted-windows/%20%3C@369027659331534859%3E%20questo%20%C3%A8%20il%20ran>

Questo tipo di malware agisce crittografando interi devices o server rendendoli inutilizzabili, in modo da poter chiedere un riscatto al proprietario. In seguito a quest'azione non è assicurata la decifratura dei dati.

**KEYLOG:**

<http://kw4zlnfhxje7top26u57iosg55i7dzuljjcyswo2clgc3mdliviswwyd.onion/product/ardamax-keylogger/>

Questo tipo di attacco informatico è una tipologia specifica di spyware che mira al monitorare e spiare il dispositivo target, riportanto in tempo reale tutto quello che fa la vittima, all'ideatore dello script. Questi sono specializzati nel registrare tutto ciò che viene digitato (utilizzati comunemente per rubare le password)



## **Conclusione**

Durante questo processo di ricerca e osservazione abbiamo effettuato un'analisi olistica sulla parte oscura del web, ovvero il dark net. Passando dal Tor Broswer abbiamo avuto accesso ad un mondo di infinite informazioni che sul clear web non sono accessibili. Nel concreto abbiamo constatato la facilità di creazione, diffusione e acquisto di malware e SPII che possono creare non poco disagio tra qualsiasi tipo di utente da quello più esperto e soprattutto utenti medi e poco esperti.

