Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica (Classe L-31)

Deep Web: la parte nascosta di Internet

Laureando

Simone Squadroni

Relatore

Prof. Fausto Marcantoni

A.A. 2019/2020

Indice

Elenco delle figure

1. Introduzione

1.1 Cos'è il Deep Web

Con il termine Deep Web ci si riferisce a quella porzione del Web che non può essere indicizzata dai tradizionali motori di ricerca, come Google, Yahoo o Bing. Le credenziali per entrare negli account dei vari siti Web, i dati personali, le informazioni riservate, fanno tutti parte dei dati che devono essere tenuti al sicuro e che non devono essere pubblici ma devono essere protetti. Anche questo genere di dati oltre ai siti non indicizzati sono presenti e vengono memorizzati nel Deep Web, il luogo dove possono essere tenuti al sicuro.

1.1.1 Differenza tra Surface Web, Deep Web e Dark Web

Per differenziare meglio Surface Web, Deep Web e Dark Web è possibile immaginarli come se fossero degli strati, dove in superficie c'è il Surface, al centro il Deep ed in fondo il Dark Web.

Nel Surface Web vi è tutto ciò che è accessibile pubblicamente attraverso l'uso di un motore di ricerca, cioè è possibile raggiungere i siti che sono indicizzati; tutti i siti e le aziende che lavorano online utilizzano strumenti per raccogliere quante più informazioni possibili, come ad esempio i cookie, strumenti di profilazione che permettono di prendere dati riguardanti le abitudini, i gusti e le scelte che fa un utente durante la sua navigazione, cosicché questi dati possano essere utilizzati per scopi aziendali o personali. Molto spesso non è possibile disattivarli quando si entra in un sito web, e nel caso che possano essere disattivati, non è possibile farlo con tutti perché alcuni rimarranno attivi senza che l'utente possa far nulla. L'utilizzo di strumenti di ricerca e profilazione di fatto creano un ambiente dove gli utenti non hanno una privacy vera e propria poiché c'è sempre qualcuno che ha la possibilità di sapere cosa fanno.

Il Deep Web è l'opposto del Surface Web, cioè in esso è possibile trovare tutti quei dati che non sono raggiungibili usando un motore di ricerca. I dati presenti nel Deep Web non sono accessibili pubblicamente dato che un utente necessita di avere delle credenziali, come ad esempio username e password, per poterli vedere; un esempio di dato presente nel Deep Web è la password che un utente usa per accedere al suo conto bancario o alla sua email. Solitamente si accostano al Deep Web attività illegali, ma non sarebbe possibile sfruttare ciò che è presente nel Web senza di esso; è la parte del Web dove sono registrati i dati personali, le informazioni importanti e tutto ciò che non si vuole sia accessibile attraverso una semplice ricerca. Proprio perché nel Surface Web non vi è una sicurezza adeguata per i dati degli utenti è stato necessario la creazione di uno spazio dove possano essere tenuti al sicuro. I dati presenti nel Deep Web rappresentano la maggior parte dei dati in tutto il Web, circa più del 90%.

Figura 1.1: Struttura del Web

Il Dark Web è una porzione del Deep Web, alla quale non è possibile accedere utilizzando un normale motore di ricerca; la tecnologia utilizzata per la creazione di questa sezione del Web è stata ideata dai ricercatori militari degli Stati Uniti negli anni 90. L'obiettivo era quello di creare una rete nella quale fosse possibile inviare e ricevere dati rimanendo anonimi e venne chiama "The Onion Router", detta anche Tor. Il nome deriva dal fatto che ci sono diversi strati di crittazione all'interno del protocollo di comunicazione. Un utente al giorno d'oggi può utilizzare le tecnologie e gli strumenti presenti nel Dark Web per comunicare in modo anonimo e di fatto mantenendo intatta la propria privacy; chi vive in un paese dove non c'è la libertà di espressione attraverso questa sezione del Web può comunque dire la sua senza il rischio di essere scoperto. L'anonimato che viene garantito agli utenti che entrano nel Dark Web viene sfruttato anche da chi lo utilizza per attività illegali, dalla vendita di dati sensibili alla vendita di sostanza stupefacenti, proprio per questo è necessario prestare la dovuta attenzione a ciò che si fa in determinati luoghi. La rete di anonimizzazione Tor, la più famosa ed utilizzata al giorno d'oggi, è facilmente raggiungibile attraverso l'utilizzo di Tor Browser, un motore di ricerca specifico che può essere utilizzato da qualsiasi utente. Il livello di sicurezza garantito da Tor è elevato ma non assoluto, infatti la rete è stata vittima di numerosi attacchi e continuerà ad esserlo, perciò viene consigliato anche l'utilizzo congiunto di altre tecnologie per poter godere di una sicurezza ancora maggiore.

1.2 Conseguenze legali

Entrare nel Deep Web e nel Dark Web non è illegale e di per sé non comporta alcun rischio sotto il punto di vista legale; dipende da cosa si fa e cosa si sceglie di cercare: acquistando prodotti illegali o visualizzando certi generi di materiale, si rischiano sanzioni e conseguenze che arrivano fino al penale. Un utente che utilizza Tor Browser per navigare nel Dark Web non viola nessuna legge, a meno che l'accesso alla rete Tor non sia espressamente vietato dallo stato nel quale si trova, come ad esempio in Cina, poiché è possibile trovare anche materiale non illegale come forum e blog che trattano di normali argomenti ma non per questo si può entrare in uno qualsiasi di essi senza prestare la dovuta attenzione. Ciò che viene trattato nei forum e nei blog, vista l'assenza di censura, può riguardare argomenti che incitano all'odio o che incoraggiano comportamenti criminali ed in questi casi anche la sola partecipazione alla discussione porterebbe l'utente a commettere un'azione illegale e quindi sarebbe punibile penalmente. Per dare un'idea della quantità di materiale illegale presente nel Dark Web, nel 2019 uno studio condotto dall'Università del Surrey ha riscontrato un aumento di siti Web pericolosi pari al 20% dal 2016, arrivando a rappresentare circa il 60% del totale. Oltre ai rischi sul piano legale, ad esempio effettuando acquisti imprudenti, il Dark Web espone gli utenti anche a minacce di altro genere, come l'alto rischio di hackeraggio, soprattutto verso gli utenti meno esperti: webcam hackerata, dati sensibili rubati e materiale compromettente messo nell'hard disk dell'utente possono essere solo alcune delle conseguenze che si possono avere navigando in modo sconsiderato in questi ambienti.

2. Perché entrare nel Deep Web e nel Dark Web

2.1 Motivazioni

In questa sezione del Web è possibile trovare informazioni, oggetti, servizi e molto altro che normalmente non sarebbero accessibili. Quando si parla di Deep Web comunemente viene associato il pensiero che ci siano soltanto attività illegali ma non è così; ci sono molti forum, blog, siti di informazione che hanno come scopo quello di divulgare conoscenze che sarebbero difficili da reperire nel Surface Web. Naturalmente vista la sicurezza di cui si dispone in questo ambiente sono ancor più diffuse le attività illegali, che vanno dalla vendita di documenti falsi al poter acquistare droghe o commissionare un attacco informatico ai danni di un determinato soggetto.

2.1.1 Sicurezza e rischi

La sicurezza garantita da questo ambiente deriva dagli strumenti necessari per accedere ai contenuti che si trovano al suo interno; ad esempio per accedere alla rete Tor è necessario utilizzare Tor Browser il quale permette di entrare nei siti con dominio ".onion" che si trovano appunto all'interno della rete Tor. Tutto il traffico interno alla rete viene crittografato e rimbalzato tra vari relay prima di arrivare al destinatario in modo da garantire una maggiore sicurezza agli utenti. La rete Tor non è l'unica che dispone di caratteristiche adatte per mantenere l'anonimato e per comunicare in modo sicuro, ma è la più facile alla quale accedere. Oltre ai benefici che si traggono dall'utilizzare queste reti sono presenti anche dei rischi, sopratutto per il fatto che sono popolate da moltissimi utenti che non hanno buone intenzioni. Mentre si naviga per il Deep Web e soprattutto nel Dark Web è importante prestare attenzione a ciò che si fa ed ai dati che si usano perchè si rischia di farsi rubare dati sensibili senza nemmeno accorgersene o di contrarre malware che comprometterebbero significativamente la propria privacy; è sconsigliato l'utilizzo di dati personali, come ad esempio la propria email per registrarsi ad un sito.

2.2 Trackography

Trackography è un progetto open source creato da Tactical Tech che mostra come gli utenti vengono tracciati online e dove finiscono i dati personali di essi una volta che si accede ad un sito web. In particolare vengono mostrati:

- Le aziende che fanno tracking online;
- I paesi che ospitano i server che hostano i siti web ai quali si accede;
- I paesi che ospitano i server delle aziende che fanno tracking online;
- I paesi che ospitano l'infrastruttura di rete necessaria a raggiungere i server dei siti web e le aziende di tracking;
- Informazioni su come molte "società di monitoraggio a livello globale" gestiscono i dati in base alle loro politiche sulla .

I dati che vengono raccolti da Trackography sono liberi e possono essere usati come "risorsa" da ricercatori, giornalisti o chiunque voglia utilizzarli. Un utente tramite l'utilizzo di Trackography può vedere come i propri dati vengano raccolti non appena accede ad un sito web, sia con il suo consenso che senza; molti stati hanno una propria politica relativa alla privacy ma questa non protegge l'utente nel caso la raccolta di dati venga effettuata da una società di un altro stato il quale ha politiche differenti. Questo tool permette di visualizzare in modo semplice ed efficace tramite un'interfaccia grafica come avvengono questi procedimenti sui vari siti Web di informazione di ogni stato presente nel database; accedendo a "trackography.org" come prima cosa bisogna scegliere lo stato, tra quelli colorati in blu, dal quale stiamo "accedendo" ad Internet. In questo esempio è stata scelta l'Italia e successivamente, tramite un nuovo banner nella pagina, vengono mostrati i canali di informazione dello stato scelto tra i quali possiamo scegliere, come ad esempio blog, National media o local media.

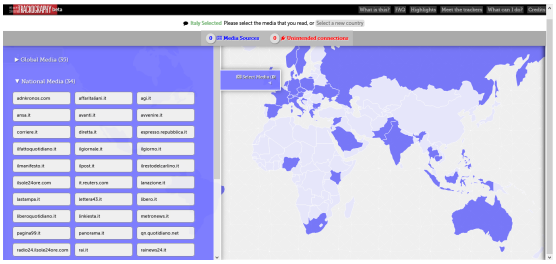

Figura 2.1: fonte: "https://trackography.org/"

Una volta scelto il sito Web che si preferisce, in questa occasione "ansa.it", verrà mostrata la mappa aggiornata nella quale sono presenti archi di due colorazioni:

- Rosso = rappresentano le connessioni Internet ai server delle aziende che stanno monitorando l'utente attraverso il sito Web scelto. Questo tipo di connessioni vengono definite "connessioni non intenzionali";
- Blu = mostrano il percorso che viene effettuato dal traffico Internet dell'utente per raggiungere i server del sito Web scelto.

Oltre agli archi nella mappa determinati stati assumono una diversa colorazione in base al modo in cui sono coinvolti con il sito Web scelto:

- Verde = nazione nella quale siamo connessi;
- Blu = nazione/nazioni che hostano il sito Web;
- Viola = nazione/nazioni che hanno l'infrastruttura Web;
- Rosso = nazione/nazioni che hostano il servizio di tracking;

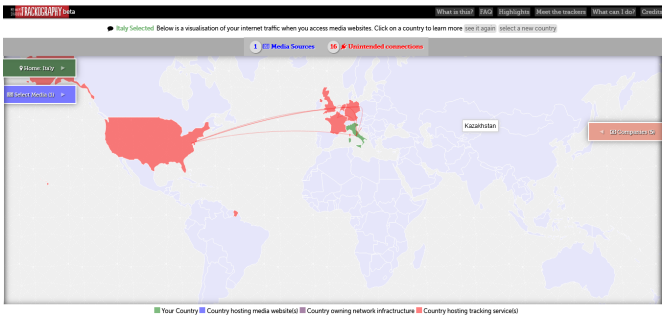

Figura 2.2: fonte: "https://trackography.org/"

È possibile vedere in un banner uno schema con le società che tracciano i dati degli utenti ed in che modo li utilizzano attraverso quel preciso sito Web; cliccando su uno stato invece è possibile vedere più precisamente quali sono le società situate in esso.

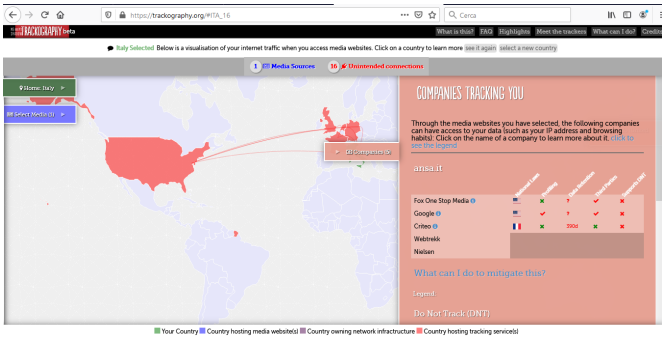

Figura 2.3: fonte: "https://trackography.org/"

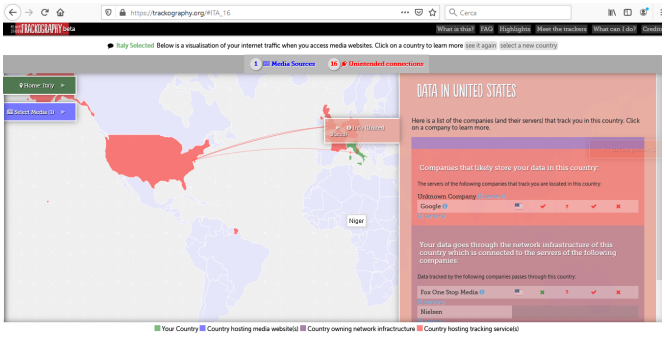

Figura 2.4: fonte: "https://trackography.org/"

Trackography tiene sotto controllo più di 2500 siti Web in 38 nazioni; i siti che vengono presi in considerazione sono siti di informazioni che vengono consultati giornalmente da moltissimi utenti ed il tool li suddivide in quattro categorie principali: governo e politica; finanza; salute; sociale. Ognuna delle categorie maggiori poi ha altre sotto-categorie in modo da classificare con maggior precisione i vari siti.

Per dare un esempio della quantità di dati che vengono intercettati da un singolo paese, tra tutti i siti Web analizzati il 90% hanno almeno una connessione che passa attraverso l'infrastruttura di rete degli Stati Uniti; colossi come Google, Facebook e Twitter, che hanno la loro infrastruttura Web negli USA, sono presenti nelle connessioni dell'87,32% dei Web media analizzati.

2.3 Black Market

Nel Dark Web è possibile comprare qualsiasi tipo di merce o servizio, sia illegale che legale e questo viene reso possibile dall'esistenza dei Black Market, negozi online dove gli utenti possono vendere e comprare ciò che vogliono. Hanno funzionalità molto simili a quelle di un normale negozio online, ad esempio ogni venditore ha una propria reputazione, che varia in base ai feedback rilasciati dai clienti ed attraverso questa è possibile farsi un'idea sull'affidabilità del venditore, ma comunque è un'informazione da non considerare vera al 100% poiché può essere manomessa e modificata dal diretto interessato. Una buona parte dei Black Market utilizzano un "central escrow service", un servizio di sicurezza con il compito di controllare che il commercio venga effettuato in modo corretto, sia dal lato del cliente che da quello del venditore; ad esempio nel caso in cui un prodotto acquistato da un acquirente non venga consegnato, quest'ultimo può contattare il central escrow service e chiedere il risarcimento. Anche in questo caso, essendo gestito da persone, c'è la possibilità che quest'ultime vengano corrotte e che il servizio poi non funzioni a dovere. Vengono adottati altri metodi di sicurezza come ad esempio la 2-FA[1] , codici mnemonici e pin di sicurezza. Alcuni Black Market offrono agli utenti un proprio servizio di messaggistica sul quale usano il software di crittografia PGP, che permette di crittografare i messaggi in modo da renderli visibili soltanto al destinatario; in questo modo gli utenti una volta entrati nel market non dovranno nemmeno uscire da esso per comunicare con il venditore. Negli ultimi anni sono aumentati notevolmente i modelli as-a-service[2] e tutorial online che permettono agli utenti di sfruttare al meglio i servizi offerti nei marketplace; uno dei prodotti più richiesti e costosi sono le vulnerabilità zero-day, cioè vulnerabilità sfruttabili in un sistema per le quali ancora non è stata trovata una soluzione. Le zero-day vengono usate per lo spionaggio aziendale ed infatti le grandi aziende hanno creato programmi "bug bounty" per evitare che le zero-day vengano vendute nei Black Market; i programmi bug bounty prevedono un premio in denaro, spesso molto elevato, per chi scopre queste vulnerabilità e le segnalano alla rispettiva azienda. Nei Black Market i pagamenti vengono effettuati soltanto attraverso l'utilizzo di criptovalute, come i più conosciuti Bitcoin, poiché grazie alle loro caratteristiche rendono molto più difficile il tracciamento di un utente tramite un acquisto. Esistono vari Black Market ed ognuno offre merci e servizi differenti; nell'immagine 2.5 vengono mostrate le caratteristiche più importanti di alcuni di essi.

Caratteristiche	World Market	DarkMarket Marketplace	Torrez Market	DeepSea Marketplace
Da Quanto è On	09/11/2020	1 anno	10/12/2019	Maggio 2020
N° Di Prodotti	600	10.000+	4.500+	1.000+
Sicurezza	2-FA, Mnemonic Code, 6-digit Pin, Escrow	Escrow, 2-FA, PGP	Multisig Transactions, Escrow, Wallet-less mode, 2-FA, Secutiry Pin	Escrow, 2-FA, Mnemonic Code, 6-digit Pin, Login Phrase
Criptovalute Accettate	Bitcoin	Bitcoin, XMR	Bitcoin, Litecoin, ZCash, Monero	Bitcoin
Registrazione	Richiesta	Richiesta	Richiesta	Richiesta
Commissione Di Vendita	50 dollari	500 dollari	250 dollari	150 dollari

Figura 2.5: Black Market

[1] Autenticazione a due fattori

[2] servizio d'applicazione software erogato attraverso il Web dal venditore o rivenditore. Il cliente avrà accesso a un'interfaccia di utilizzo del software via browser, senza la necessità di alcun download applicativo o istallazione.

2.4 Criptovalute

Nel Deep Web e nel Dark Web, vista la privacy e l'anonimato che vengono garantiti, sono molto diffusi i traffici di merci illegali; i pagamenti necessitano di mantenere un elevato livello di sicurezza e per questo ogni transazione viene effettuata attraverso l'utilizzo di criptovalute, viste le loro caratteristiche. Le criptovalute sono monete digitali con le quali si possono effettuare ogni tipo di operazione, sia di vendita che di acquisto; sono un metodo di pagamento legale ma sono decentralizzate, cioè non sono sotto il controllo di nessuna autorità, a differenza del normale denaro, e vengono trasferite tramite il P2P[3]. Queste valute hanno un'origine digitale, derivano da operazioni di "mining", le quali possono essere effettuate da chiunque abbia le capacità adatte; per "mining" si intende il processo nel quale un computer risolve difficili problemi matematici ed in cambio riceve monete digitali; ogni utente può conservarle in appositi portafogli virtuali, chiamati wallet. Una transazione viene chiamata "blocco" e nel momento in cui viene convalidata, ed accade solo quando si ha l'ok del 50%+1 dei nodi della rete, viene aggiunta alla blockchain, cioè un registro pubblico nel quale è possibile vedere tutte le transazioni che vengono effettuate e di ognuna è possibile sapere l'indirizzo del mittente, del ricevente e quanto denaro viene trasferito. Le criptovalute, come ad esempio i più famosi e conosciuti Bitcoin, non sono valute completamente anonime poiché per esserlo non dovrebbero essere riconducibili a nessuno e quindi non potrebbe essere creato nessun genere di contabilità, ma con le blockchain chiunque può avere informazioni riguardo qualsiasi transazione avvenuta. I portafogli di criptovalute, i cosiddetti wallet, non sono riconducibili nello specifico ad utenti ma a stringhe alfanumeriche e questo rende più complicato associare la stringa che rappresenta un certo portafoglio ad una persona, ma comunque seguendo i movimenti che vengono effettuati con un conto è possibile risalire all'identità fisica del possessore. L'utilizzo delle criptovalute assicura all'utente una maggiore privacy rispetto a l'utilizzo di metodi di pagamento più classici, come carte di credito; esistono criptovalute, come i Monero e gli ZCash, che hanno come obiettivo principale quello di garantire anonimato, non è possibile garantirlo al 100% ma cercano di offrire la miglior sicurezza possibile rendendo il più difficile possibile reperire determinati tipi di informazioni. Nel caso dei Monero, per garantire una maggiore sicurezza, viene reso impossibile risalire a l'indirizzo del mittente e del ricevente di una transazione e viene anche oscurato l'importo della transazione; anche con i Monero, godendo di un alto livello di privacy molto vicino a l'anonimato, una volta che li si vorrà scambiare con altre criptovalute o con la valuta FIAT, ad esempio euro o sterline, si diventerà rintracciabili.

2.4.1 Bitcoin Mixer

Per ovviare al problema della visibilità data dalle blockchain sui movimenti di criptovalute, sono stati creati dei servizi, chiamati "Bitcoin Mixer", che garantiscono un ulteriore livello di sicurezza. Questi Mixer permettono ad un utente di mischiare le proprie criptovalute con un gruppo di monete casuali per poi ritornare all'utente un set di monete nuove; questo meccanismo permette di rimuovere il legame che c'è tra l'acquisizione e la destinazione finale alla quale verranno inviate le criptovalute.

[3]Peer-to-Peer

Il funzionamento dei Bitcoin Mixer è molto semplice: l'utente acquista una certa quantità di criptovalute necessarie ai suoi interessi; le invia ad un Bitcoin Mixer; il mixer le aggiunge alla sua riserva di criptovalute; dopo aver tolto una percentuale di tasse, che varia per ogni mixer, rimanderà indietro la stessa quantità di criptovalute con la differenza che quest'ultime non hanno nessun legame con le transazioni precedentemente effettuate dell'utente. Le monete che un Bitcoin Mixer ha nella sua riserva provengono dalle transazioni effettuate da altri utenti, perciò quando ridà indietro un set di monete "nuove" oltre che non saranno riconducibili a l'utente che le riceve, non saranno riconducibili a nessun'altro utente.
Ogni servizio di mixer ha le sue caratteristiche ed accetta determinati tipi di criptovalute; per scegliere un buon mixer per i propri scopi è necessario considerare alcuni aspetti:

- Livello di anonimato;
- Reputazione;
- Tipologie di criptovalute accettabili;
- Tasse: la quantità di tasse che vengono richieste per il mix e per il controllo degli utenti, nel caso ci siano;
- N° di indirizzi aggiuntivi: è possibile inserire più indirizzi ai quali ricevere le criptovalute, cosicché non verranno inviati tutti ad un solo indirizzo ma verranno suddivisi tra tutti gli indirizzi specificati in modo da rafforzare l'anonimato;
- Caratteristiche avanzate: ad esempio alcuni mixer forniscono un'uscita posticipata delle criptovalute, cioè danno la possibilità di decidere dopo quanto tempo verranno inviate agli indirizzi specificati dall'utente;
- Quantità massima e minima di criptovalute inviabili;
- Conferma richiesta: minore è il numero di conferme richieste prima della procedura, maggiore sarà la velocità di esecuzione;
- No Logs Policy: cioè se il mixer mantiene o meno i file di log e nel caso lo facesse per quanto tempo li tiene registrati.

Nell'immagine 2.6 sono mostrati i servizi offerti da alcuni mixer dove per BTC si intendono i Bitcoin, per BCH i Bitcoin Cash e per LTC i Lightcoin.

Caratteristiche	Blender.io	Bitcoin Mixer	SmartMixer.io
Rating	5/5	4/5	
Tasse	Da 0.5% a 2.5% + 0.0001 BTC per ogni indirizzo aggiuntivo	1% + 0.000001 BTC	Da 1% a 5% + 0.00045529 BTC / 0.01072904 LTC / 0.00273174 BCH
Deposito Minimo	0.001 BTC	0.0002 BTC	0.001 BTC
Indirizzi Aggiuntivi	8	5	8
Conferme Richieste	3		
No Logs Policy	SI	SI	I log vengono mantenuti per 24 ore
Massimo Tempo di Delay	24 ore	SI (non specificato di quanto)	Si(non specificato quanto)
URL	https://blender.io/ http://blenderiocpxfema.onion	https://bitcoinmixer.org http://btcmixnqyq7kljrr.onion	https://smartmixer.io/ http://smrtmxdxognxhv64.onion/

Figura 2.6: Bitcoin Mixer

3. Darknet, StealthNet e AnoNet

3.1 Darknet

Con il termine Darknet si intende una rete virtuale privata nella quale gli utenti possono connettersi con altri utenti che conoscono e di cui si fidano; si può creare un gruppo chiuso e privato dove gli utenti che ne fanno parte comunicano tra loro. Solitamente il termine Darknet si utilizza quando si parla di una rete di condivisione file P2P. I principali motivi per cui si utilizza una Darknet sono:

- Proteggere la propria privacy;
- Esporre notizie, anche riservate, in modo sicuro ed anonimo;
- Compiere crimini informatici, come l'hacking;
- Vendere o acquistare ogni tipo di merce nei Black Market;
- Condividere qualsiasi genere di file.

Ogni Darknet necessita di software e strumenti specifici o configurazioni di rete particolari per poter essere utilizzate. Al momento le maggiori Darknet attive sono:

- The Onion Router, detta anche Tor;
- Invisible Internet Project, chiamato anche I2P: si tratta di un overlay network[1] il quale implementa una darknet;
- Freenet: dalla versione 0.7 può essere eseguita sia come Darknet che come Open-Net[2];
- Retroshare: eseguibile come Darknet per condividere file;
- GNUnet: attivando la topologia di rete F2F[3] può essere considerata una Darknet;
- Zeronet: software open source avente come obiettivo quello di creare una rete di client composta da utenti della rete Tor;
- OneSwarm: eseguibile come Darknet F2F per condividere file;
- Tribler: eseguibile come Darknet per condividere file.

[1] Rete di calcolatori costruita su un'altra rete

[2] I nodi adiacenti vengono scoperti automaticamente e ci si collega anche con utenti sconosciuti purché siano connessi alla rete, con questa modalità viene meno la sicurezza

[3] Friend-to-Friend

3.2 StealthNet

È un client P2P libero basato sulla rete Rshare, una rete P2P anonima non più in uso, che garantisce una migliore sicurezza e privacy rispetto ad un client P2P non anonimo. Utilizzare un servizio P2P non anonimo rende facile effettuare un'analisi del traffico da parte di esterni, poiché il collegamento tra mittente e destinatario è diretto, quindi si può scoprire facilmente chi invia, chi riceve ed il contenuto dello scambio di dati; con StealthNet, essendo basato su Rshare, viene resa molto più difficile l'analisi del traffico poiché che lo scambio di dati non avviene in modo diretto ma i dati, prima di arrivare a destinazione, passano per altri nodi della rete Rshare. Ogni nodo presente nella rete Rshare mette a disposizione la sua banda per instradare dati provenienti da altri nodi oltre che per le proprie necessità. Un altro vantaggio della rete Rshare è che i nodi non vengono identificati tramite l'indirizzo IP ma tramite l'utilizzo del Rshare ID, l'identificatore univoco di ogni nodo il quale non può essere associato all'indirizzo IP del nodo. I dati che vengono scambiati nella rete Rshare vengono criptati point-to-point, cioè tra mittente e destinatario, in modo da assicurare una maggiore sicurezza agli utenti proteggendoli da tecniche di analisi del traffico. I client Rshare utilizzano le Web cache, le quali hanno il compito di ricordare l'indirizzo IP, la porta TCP ed i nodi in linea; a differenza di altre reti P2P anonime, qui la Web cache non memorizza i file che vengono condivisi dal nodo e non ha la funzione di ricerca di file o di fonti per il download. Gli utenti hanno la possibilità di utilizzare il proprio host come Web cache per la rete Rshare se hanno sul loro sistema operativo un Web server PHP e MySQL.

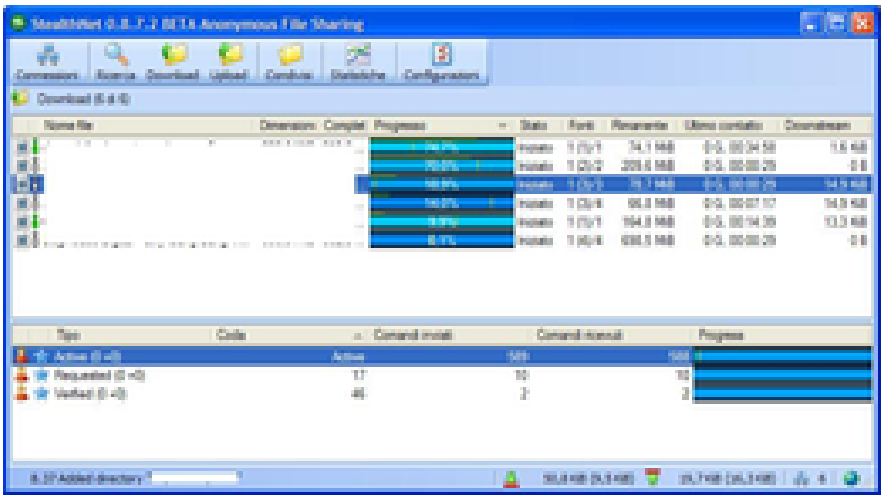

Figura 3.1: Fonte: "https://www.wikizero.com/it/StealthNet"

3.3 AnoNet

AnoNet è una rete F2F[4] decentralizzata costruita utilizzando programmi router BGP[5] e VPN[6]. L'obiettivo di questa rete è quello di rendere difficile conoscere l'identità degli utenti presenti nella rete dando loro la possibilità di ospitare anonimamente servizi IPv4 e IPv6. Nelle reti F2F, come nelle reti P2P, vengono utilizzate delle chiavi crittografiche che permettono agli utenti di connettersi ad una specifica rete; AnoNet utilizza chiavi pubbliche RSA[7] che vengono create da OpenVPN, software che ha anche la funzione di connettere tra loro più nodi presenti nella rete. L'unico modo per accedere alla rete AnoNet è che un utente ottenga almeno una chiave di autorizzazione da uno degli utenti già presenti nella rete. OpenVPN utilizza queste chiavi di crittografia per creare connessioni sicure tra i nodi della rete AnoNet; questi "tunnel" che vengono creati permettono di nascondere il contenuto delle connessioni tra due nodi in modo da mantenere un certo livello di privacy. AnoNet, oltre ad utilizzare OpenVPN, garantisce l'anonimato ai suoi utenti svincolando gli indirizzi IP che identificano i nodi della rete dall'identità degli utenti. Nella rete AnoNet viene utilizzato un blocco di indirizzi IP che è compreso tra 1.0.0.0 e 2.255.255.255, chiamato blocco "1.0.0.0/8", il quale essendo un blocco di indirizzi mai utilizzato, garantisce che non ci sia una collisione tra l'indirizzo utilizzato da Internet e quello utilizzato da AnoNet, dando di fatto la possibilità agli utenti di essere collegati contemporaneamente ad entrambe le reti.

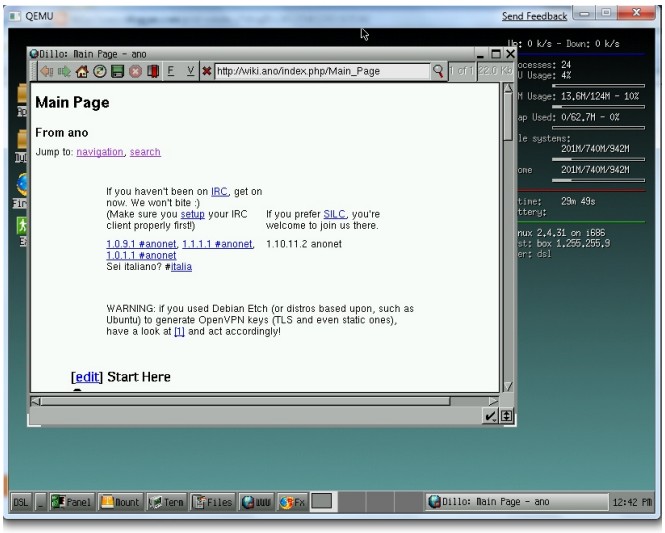

Figura 3.2: Fonte: "https://virtuallyfun.com/wordpress/category/anonet/"

In AnoNet non c'è un'autorità che assegna gli indirizzi IP, ogni utente può andare nell'apposito database e prendere per sé uno o più blocchi di indirizzi, ognuno dei quali può contenere da 2 a 256 indirizzi differenti.

[4] Friend-to-Friend

[5] Border Gateway Protocol: protocollo di routing usato per connettere tra loro più router appartenenti a sistemi autonomi differenti

[6] Virtual Private Network

[7] Algoritmo di crittografia asimmetrica

Ogni utente deve usare almeno due indirizzi IP differenti perché uno viene utilizzato per navigare in modo "passivo" nella rete AnoNet e l'altro per fare da host ad eventuali servizi "attivi", come un server Web. Per il routing viene utilizzato il programma Quagga[8], che necessita di essere installato in ogni nodo della rete, mentre per la risoluzione dei nomi utilizza il software BIND, lo stesso utilizzato da Internet, ma con un database differente. Grazie alle sue meccaniche di assegnazione degli indirizzi IP, AnoNet rende molto difficile identificare un utente tramite il suo indirizzo IP poiché esso non è registrato; possono sorgere dei problemi quando ci sono peer[9] collegati direttamente tra loro dato che ogni nodo deve conoscere l'indirizzo IP di Internet dei suoi peer per potersi connettere con loro tramite OpenVPN e così potrebbe risalire alla loro identità. Su AnoNet è possibile disporre degli stessi servizi che si hanno su Internet, dato che sono identici sia per software sia per architettura, ma si differenzia per l'utilizzo di indirizzi IP diversi, oltre alle caratteristiche che permettono di garantire sicurezza ed anonimato ai propri utenti. Si possono creare delle AnoNet private e collegarle successivamente tramite un preciso gateway o un normale nodo ad AnoNet.

[8]Suite software di routing di rete utilizzato sopratutto per i sistemi Linux, Solaris, FreeBSD e NetBSD

[9]Nodi equivalenti o paritari che possono essere sia client che server verso gli altri nodi terminali, host, della rete.

4. Come e con quali strumenti accedere al Deep Web ed al Dark Web

4.1 Come accedere alla rete Tor

La rete Tor è la più famosa ed utilizzata quando si tratta di accedere al Deep Web ed al Dark Web ed è possibile sfruttarla su tutti i principali sistemi operativi; si può accedere ad essa su Windows, Linux, macOS, Android, iOS e iPadOS. Utilizzare Tor Browser è il metodo più comodo e sicuro, si tratta di una versione modificata del browser Mozilla Firefox nella quale al suo interno ci sono già tutte le impostazioni necessarie a connettersi e sfruttare la rete Tor garantendo anonimato all'utente; il download è gratuito e può essere utilizzato sia da PC che da smartphone e tablet. Nel sottocapitolo 4.3 parlerò più approfonditamente dei vari aspetti riguardati la rete Tor, mentre in questo capitolo di come entrarci utilizzando vari sistemi operativi.

4.1.1 Tor Browser

Windows e macOS

Per scaricare Tor Browser basta andare sul sito ufficiale[1], scegliere la versione giusta per il proprio sistema operativo ed effettuare il download; una volta scaricato verrà chiesto di scegliere la cartella di destinazione dove installare il software. Prima di poter avviare Tor Browser, dopo aver eseguito il programma, l'utente dovrà cliccare sul bottone "Connetti" ed una volta terminato il procedimento sarà tutto pronto per iniziare a fare le proprie ricerche nella rete Tor. Nel caso in cui ci si trovi in un paese dove l'accesso alla rete Tor è vietato per legge, prima di stabilire la connessione, cliccando sul pulsante "Configura" verrà chiesto se il proprio ISP[2] blocca la connessione alla rete Tor, se il PC richiede l'utilizzo di un proxy locale per connettersi ad Internet, di scegliere il tipo di bridge[3] da usare per superare le restrizione dell'ISP e di inserire i dettagli del proxy da utilizzare per connettersi ad Internet; terminato questo procedimento l'utente potrà accedere senza problemi alla rete Tor. Una volta terminata la propria navigazione basterà chiudere Tor Browser per interrompere la connessione alla rete Tor; sia la cronologia che tutti i dati di navigazione non verranno salvati in alcun modo nel computer.

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

[2] Internet Service Provider

[3] Strumento utilizzato per permettere la connessione alla rete Tor anche nei paesi dove è vietato rendendo impossibile sapere se l'utente si sia connesso alla rete

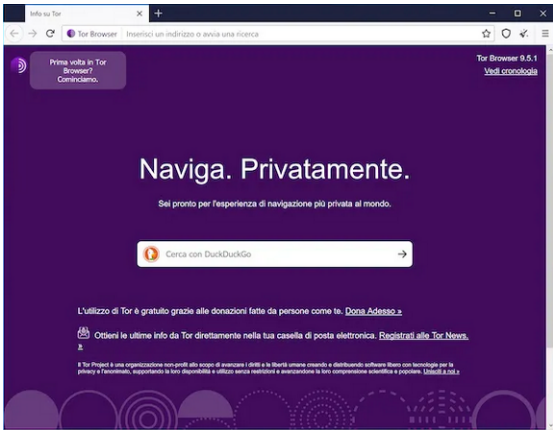

Figura 4.1: fonte: "https://www.aranzulla.it/come-usare-tor-1026046.html#chapter1"

Linux

Per scaricare ed avviare Tor Browser sul proprio sistema operativo Linux le operazioni sono molto simili a quelle necessarie per farlo su Windows e macOS. Per prima cosa bisogna andare sul sito ufficiale[4] e scaricare la versione adatta al proprio sistema operativo Linux; una volta terminato il download, se non si ha l'opzione "estrai qui" da scegliere direttamente sul file ".xz" bisognerà aprire il terminale, entrare nella directory dov'è salvato il file ed estrarre il file di installazione con il comando "tar -xvJf nomeDelFile" dove per "nomeDelFile" si deve scrivere il nome con il quale è stato salvato il file; finita l'estrazione verrà creata una cartella contenente il file manager. Successivamente si potrà scegliere se:

- Aprire Tor Browser direttamente dalla directory e per farlo sarà necessario entrare nella directory dov'è salvato il file manager da terminale ed eseguire il comando "nomeFileManager/Browser/start-tor-browser &";
- Oppure scegliere di installare Tor Browser seguendo una differente procedura: per prima cosa si dovrà spostare il file manager nella directory "/opt" eseguendo da terminale nella directory contenete il file manager il comando "sudo mv nomeFileManager /opt". Ora sempre da terminale andando nella nuova directory contenente il file manager, usando il comando "ls" si vedrà un file con l'estensione ".desktop"; eseguendo il comando "nomeFile.desktop –register-app" si registrerà Tor Browser come un app sul desktop.

Come ultimo procedimento, prima di poter iniziare a navigare, una volta aperta la finestra di Tor Browser bisognerà cliccare sul pulsante "Connect", dopo aver configurato un proxy o un bridge cliccando sul pulsante "Configure" nel caso siano necessari, ed aspettare che venga instaurata la connessione alla rete Tor; una volta stabilita la connessione l'utente potrà navigare nella rete utilizzando Tor Browser.

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

Android

Nel caso si voglia accedere alla rete Tor dal proprio smarthphone o tablet con sistema Android si dovrà scaricare dal playstore, se disponibile, o in alternativa dal sito ufficiale[5] la versione per Android di Tor Browser. Una volta installata l'applicazione basterà cliccare su "Connetti" o su "Configura", nel caso serva configurare un bridge o inserire un proxy, ed aspettare che la connessione alla rete Tor avvenga con successo per iniziare a navigare. Un'alternativa è quella di scaricare l'app Orbot che può essere sfruttata per instradare tutte le altre app del dispositivo sulla rete Tor.

IOS

Per navigare nella rete Tor dal proprio iPhone o iPad basterà andare nell'app store e scaricare l'app "Onion Browser". Finita l'installazione ed aperta l'applicazione l'utente potrà scegliere tra "Configure Bridges" e "Connect to Tor"; dopodiché non appena la connessione alla rete Tor sarà stabilita uscirà la schermata del browser la quale indica che il collegamento è stato effettuato correttamente e l'utente può iniziare la sua navigazione.

4.1.2 Chrome

Utilizzare Tor Browser non è l'unico metodo per accedere alla rete Tor, infatti è possibile farlo utilizzando Chrome; non è comunemente usato poiché la procedura da seguire non è semplice e veloce come con Tor Browser. Come prima cosa bisogna avviare Chrome ed aggiungere l'estensione "ProxySwitchy Omega"; successivamente si dovrà impostare il proxy con i seguenti parametri:

- Protocol: SOCKS4;
- Server: 127.0.0.1;
- Porta: 9999.

Non appena finita la configurazione del proxy e salvate le relative impostazioni bisognerà attivarlo utilizzando l'estensione ProxySwitchy Omega. Il prossimo passo prevede prima il download e poi l'avvio dell'applicazione per Chrome "Kronymous", successivamente l'utente dovrà aprire una nuova scheda di Chrome nella quale dovrà cliccare sul pulsante "Start Tor Proxy" presente nella nuova finestra; non appena la connessione alla rete Tor sarà completata l'utente potrà navigare anonimamente. Terminata la navigazione, per tornare alla classica versione di Chrome, l'utente deve selezionare l'opzione "System Proxy" dal menù dell'estensione ProxySwitchy Omega e chiudere poi Kronymous.

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

4.2 GNUnet

È un framework libero per le reti P2P progettato in modo da offrire un protocollo peer-to-peer anonimo, sicuro e che preveda una rigida politica di sicurezza. È scritto interamente in C e funziona su GNU/Linux, BSD[6], macOS, Solaris e Windows; c'è anche una versione scritta in Java ed è disponibile in ogni sistema operativo purché provvisto di una Java virtual machine. È stato ideato con l'intento di creare una rete di file-sharing anonima che fosse resistente alla censura e che consentisse a tutti gli utenti di avere la possibilità di pubblicare e reperire qualsiasi tipo di informazione. La rete è decentralizzata ed ogni scambio di dati viene criptato al momento utilizzando un alto livello di sicurezza; non viene reso possibile conoscere l'IP del nodo con il quale si sta comunicando poiché la comunicazione viene attuata attraverso l'utilizzo di un nodo intermediario. Il nodo che fa da intermediario ha la possibilità di conoscere l'IP di coloro che vogliono instaurare questa connessione, ma non può conoscere il contenuto dei dati che questi stanno scambiando poiché che solo quest'ultimi conoscono la chiave per decriptare il contenuto dei dati; nella rete GNUnet è possibile quindi sapere soltanto o l'IP dei nodi o il contenuto dei dati inviati.
Il file-sharing utilizza il protocollo anonimo GNUnet per gestire le richieste e le risposte; per la ricerca di dati vengono utilizzati messaggi di richiesta ridondanti, cioè a seconda della lettura che verrà effettuata dal nodo successivo i messaggi vengono poi inoltrati a zero o più nodi; quando un nodo arriva ad un livello di stress eccessivo abbassa le richieste da parte nei nodi adiacenti. E' presente l'opzione "topologia F2F" per permettere le connessioni soltanto con utenti di fiducia. GNUnet utilizza degli URI[7] che hanno due sezioni: il modulo e l'identificatore del modulo. Un tipico URI della rete GNUnet è formato da "gnunet://modulo/modulo/identificatore" dove per "modulo" si intende il nome del modulo e per "identificatore" la stringa specifica del modulo. I file condivisi attraverso il protocollo GNUnet sono codificati in ECRS[8]; l'identificatore del modulo ECRS consiste in una delle seguenti istruzioni: CHK, SKS, KSK o LOC seguita da uno slash e da un valore specifico per ciascuna categoria.

- CHK: identifica il file;
- SKS: identifica file all'interno dei namespaces;
- KSK: identifica richieste di ricerca;
- LOC: identifica un dato su una specifica macchina.

[6] Un'alternativa al sistema operativo Unix sviluppata nell'università di Berkeley in California
[7] Uniform Resource Identifier
[8] Encoding for Censoreship-Resistant Sharing

GNUnet include anche un'implementazione di GNS[9], un sostituto decentrato e resistente alla censura dell'attuale DNS[10]. In GNS ogni utente gestisce autonomamente e arbitrariamente la propria zona principale che verrà poi mappata nello spazio comune dei nomi DNS residenti sotto il dominio di primo livello ".gnu". Gli utenti possono anche delegare sottodomini a zone gestite da altri utenti e la loro ricerca viene eseguita utilizzando il modulo DHT[11] di GNUnet. Il problema principale di questo approccio è che non è possibile garantire l'univocità dei nomi a livello globale, il che richiede l'uso di proxy o altre soluzioni compatibili per soddisfare le esigenze delle vecchie applicazioni create per funzionare sotto DNS e non sotto GNS. Per quanto riguarda gli altri domini di primo livello già esistenti, ad esempio ".com", ".org" o ".it", GNS garantisce le stesse identiche funzionalità dell'attuale DNS. Per P2P si intende una rete nella quale i nodi e i partecipanti risultano anonimi; l'anonimato viene reso tale attraverso l'utilizzo di determinate tecniche di instradamento applicate a reti che usano protocolli TCP/IP le quali nascondono l'ubicazione fisica di ogni nodo rispetto agli altri.
Gli utenti che solitamente utilizzano il P2P anonimo lo fanno perché non vogliono essere identificati come fruitori di determinati materiali poiché:

- Quel materiale o la sua diffusione è illegale;
- Non vogliono essere censurati;
- Vogliono tenere riservati i propri dati personali;
- Vogliono mantenere intatta la loro privacy.

Le reti P2P sono sia anonime, cioè nelle quali i nodi sono privi di identificatori, sia pseudonime, cioè i nodi invece che essere identificati tramite appunto un identificatore lo sono tramite uno pseudonimo come una chiave crittografata. Ad esempio, nella rete MUTE, ogni nodo presente nella rete ha un indirizzo overlay, cioè di copertura, derivante dalla propria chiave pubblica crittografata ed accetta solo messaggi diretti ad esso. In una rete P2P anonima ogni nodo è visto sia come un emittente sia come un destinatario universale così da mantenere l'anonimato; nel caso in cui un nodo si comportasse solo come destinatario, i nodi adiacenti saprebbero che le informazioni che richiedeva erano per se stesso e non per altri.

[9] GNU Name System
[10] Domain Name System
[11] Tabella hash distribuita

4.3 The Onion Router - TOR

Tor, acronimo di "The Onion Router", è un software open source che permette di rimanere anonimi quando si naviga sul Web rendendo molto più difficile tracciare un utente. È disponibile su Windows, OS X, Android ed anche sistemi operativi unix-like come Linux e MacOS. Tor come scopo ha quello di rendere complicata l'analisi del traffico e di proteggere la privacy degli utenti; i dati delle comunicazioni non vanno direttamente dal mittente al destinatario ma passano prima attraverso un circuito solitamente formato da tre nodi, chiamati relay, i quali sono sparsi per tutto il mondo e vengono gestiti da volontari o associazioni che vogliono contribuire al funzionamento della rete Tor.
Ai dati che passano all'interno della rete Tor vengono applicati vari livelli di crittografia prima di entrare in un circuito che ha il compito di rendere più forte la sicurezza della comunicazione; un circuito di base è formato da 3 nodi ma modificando il file di configurazione si può aumentare il numero fino ad un massimo di 10 nodi. In ordine i dati passato prima per il Guard node[12], che può essere un bridge nel caso sia necessario, poi per i Middle node ed infine per l'Exit node prima di arrivare al client o server di destinazione. Per ogni nodo viene creata una chiave di cifratura in modo che ad ogni passaggio venga tolto un livello di crittografia fino ad arrivare alla destinazione in chiaro. Tutti i nodi della rete sono pubblici ed è possibile vederli ma nel caso di un Bridge node la sua identità/indirizzo IP non vengono resi pubblici.
Ogni nodo è a conoscenza di determinate informazioni:

Informazioni	Utente	Guard/Bridge node	Middle node	Exit node
Indirizzo IP dell'Utente	Si	Si	No	No
Indirizzo IP del Guard/Bridge Node	Si	Si	Si	No
Messaggio per il Guard/Bridge Node	Si	Si	No	No
Indirizzo IP del Middle node	Si	Si	Si	Si
Messaggio per il Middle node	Si	No	Si	No
Indirizzo IP dell'Exit Node	Si	No	Si	Si
Messaggio per l'Exit node	Si	No	No	Si
Indirizzo IP del Server di destinazione	Si	No	No	Si
Messaggio per il Server di destinazione	Si	No	No	Si

Tabella 4.1: Fonte: "https://gitlab.torproject.org/"

Questa tabella prende in considerazione un circuito formato da 3 nodi e naturalmente è da considerare che sia l'utente sia ogni nodo conoscano il proprio indirizzo IP e che non è possibile nasconderlo al proprio precedessore e successore.

È stato creato un browser apposito, chiamato Tor browser, con lo scopo di sfruttare al meglio la rete Tor. Tor Browser è il mezzo principale con il quale accedere alla rete Tor; è disponibile su tutti i principali sistemi operativi che vengono utilizzati su PC, smarthphone e tablet. Ha una velocità molto ridotta rispetto ai classici motori di ricerca poiché le comunicazioni vengono cifrate e rimbalzate tra i vari relay sparsi per il mondo; essendo una versione rivisitata di Mozilla Firefox ha un'interfaccia molto user-friendly e questo permette anche ad un utente non molto esperto di utilizzarlo

[12]Si può chiamare anche Entry node

senza problemi. Nell'interfaccia, alla sinistra dei link URL, è possibile vedere quale sia il circuito che stiamo usando per connetterci a quel sito, dove si trovino i nodi e quale indirizzo IP abbiano; è possibile scegliere di cambiare circuito sempre dalla stessa interfaccia nel caso lo si voglia. In alto a destra nella finestra del Browser c'è l'icona di una scopa, la quale ha la funzione di ricaricare il browser ed avviare una nuova connessione. Inoltre una volta aperto Tor Browser, andando nelle impostazioni, è possibile modificare diverse cose, come quale motore di ricerca utilizzare come predefinito, ma sopratutto è possibile scegliere quale livello di sicurezza utilizzare durante la navigazione:

- Standard: assicura una migliore usabilità in termini di fluidità;
- Sicuro: disattiva automaticamente Javascript per tutti i siti che non utilizzano il protocollo sicuro HTTPS, abilità il click-to-play per i video HTML5 e disattiva anche il rendering di alcuni font;
- Molto sicuro: disattiva completamente Javascript, disattiva anche la visualizzazione di alcune immagini ed icone.

Sia la rete che il browser supportano la connessione criptata dal computer dell'utente fino al Guard node ed all'interno della rete stessa, ma non assicura che l'indirizzo IP venga nascono nella connessione tra l'Exit node e la destinazione finale; per questo Tor browser impone l'uso di "HTTPS Everywhere"[13] per forzare l'utilizzo di quanti più siti possibili che supportano una connessione cifrata. E' comunque possibile crittografare la comunicazione attraverso l'utilizzo di un algoritmo di crittografia, come SSL, così da nasconderne il contenuto nel tragitto tra l'Exit node e la destinazione finale. È sconsigliato aprire file ".torrent" o tenere aperte applicazioni che utilizzano file ".torrent" mentre si sta utilizzando Tor browser poiché nella "tracker GET request" viene mostrato l'indirizzo IP in chiaro; oltre a questi tipi di file è consigliabile aprire file Word o PDF scaricati soltanto dopo aver disabilitato la connessione ad Internet del dispositivo in quanto possono contenere link di siti Web che potrebbero venir aperti da programmi che non utilizzano la rete Tor per connettersi e quindi verrebbe mostrato in chiaro l'indirizzo IP dell'utente. Un'altra funzionalità molto importante offerta da Tor è la possibilità di fornire anonimato sia ai client che ai server, cioè è possibile ospitare dei server tenendo segreta la propria posizione; vengono definiti "servizi nascosti". Ai servizi nascosti si accede tramite un dominio ".onion" al quale, una volta riconosciuta la richiesta, Tor apre una connessione; uno dei principali vantaggi dei servizi nascosti è che non richiedono indirizzi IP pubblici e quindi possono essere ospitati dietro firewall o NAT[14].

Disabilitare Adobe Reader e Javascript durante l'utilizzo di Tor Browser rende impossibile la visualizzazione dei contenuti di diverse pagine Web, ma non disabilitandoli si possono correre rischi maggiori. La rete Tor non è impenetrabile, per questo è possibile utilizzarla insieme ad una VPN(capitolo 4.6), cioè una rete virtuale privata, oppure ad un proxy(capitolo 4.7); non è indispensabile utilizzarli insieme ma sfruttando i servizi che entrambi forniscono l'utente godrà di una maggiore sicurezza.

[13]Estensione per i browser che fa instaurare ai siti connessioni HTTPS al posto delle HTTP se supportate; con l'opzione Encrypt All Sites Eligible si può bloccare e sbloccare tutte le connessioni del browser che non sono HTTPS

[14]Network Address Translation

4.3.1 Vulnerabilità ed attacchi

La rete Tor permette a chiunque lo voglia di entrare a far parte della sua struttura diventando un relay; i requisiti per diventarlo sono minimi, serve almeno una connessione da 2MByte/s per poter diventare un Guard node altrimenti si può comunque ricoprire il ruolo di un altro nodo. Questo rende la rete estremamente scalabile[15] ma allo stesso tempo vulnerabile. Essendo i nodi controllati anche da privati è possibile che vengano eseguiti degli attacchi alla rete sfruttando questa possibilità, ad esempio eseguendo un man-in-the-middle, il quale diventerebbe ancora più nocivo nell'eventualità in cui l'attaccante riesca a prendere il controllo dell'Exit node e che la comunicazione con il server non sia stata crittografata. Ci sono vari tipi di attacchi che possono essere fatti verso la rete Tor e possono avere uno specifico obiettivo, cioè client, server o la rete stessa; è comunque possibile effettuare attacchi che prendono di mira più entità contemporaneamente. Di seguito riporterò solo alcuni esempi degli attacchi attuabili per ogni target.

4.3.2 Attacchi ai client

Raptor

I routing attack sulla privacy di Tor sono un gruppo di attacchi che possono essere lanciati da un Sistema Autonomo(AS) in modo da togliere l'anonimato dei client. Un attacco è basato sull'analisi del traffico delle comunicazioni asimmetriche che caratterizzano la rete; un altro attacco sfrutta il corso naturale del routing di Internet ed i percorsi BGP per realizzare l'analisi del traffico; l'ultimo attacco si basa sulla manipolazione del routing di Internet sfruttando le attività di dirottamento BGP così da scoprire i Guard node utilizzati dagli utenti.

P2P Information Leakage

Questo attacco ha come obiettivo quello di riconoscere l'identità dei client Tor sfruttando le loro connessioni con sistemi peer-to-peer; si può prendere come esempio il protocollo BitTorret, un utente malevolo può ricavare l'indirizzo IP di un client connesso alla rete Tor che cerca di comunicare con il torrent tracker. Un torrent tracker è un servizio di rete con il quale il client deve comunicare per poter ottenere informazioni riguardanti i peer disponibili che condividono la risorsa desiderata. Le informazioni dei peer vengono fornite come una coppia di indirizzo IP e porta di ascolto. L'utente malevolo sfrutta il fatto che, anche se solitamente le liste dei tracker spesso sono reperibili in modo anonimo tramite Tor, a volte le comunicazioni vengono create in malo modo ed in questi casi si comunica direttamente con il peer; in situazioni simili è possibile per l'attaccante sfruttare la meccanica del man-in-the-middle nella rete Tor e modificare la lista restituita dal tracker torrent inserendoci indirizzi IP di nodi torrent dannosi. Dato che la connessione tra i peer non avviene attraverso Tor è possibile trovare l'indirizzo IP del client che ha inviato la richiesta al tracker.

[15] Capacità di una rete di aumentare o diminuire la sua dimensione in base alle proprie necessità e possibilità

4.3.3 Attacchi al server

Questo genere di minacce puntano ad attaccare il servizio nascosto con l'intento di svelare la sua identità o di indebolirlo; la rete Tor può essere usata sia per accedere al Surface Web sia al Deep Web ed in quest'ultimo caso l'identità del servizio nascosto è sconosciuta al client. Per sviluppare un attacco con l'obiettivo di rivelare l'indirizzo IP di un servizio nascosto sono necessari alcuni presupposti:

- L'utente malevolo deve impersonare un client dannoso ed un guard node;
- Il servizio nascosto deve essere costretto a scegliere un guard node malevolo come entry node di un circuito.

Caronte attack

Caronte è un tool che individua automaticamente le perdite di position leaks nei servizi nascosti. Queste informazioni includono dati sensibili nel contenuto servito dal servizio nascosto o la configurazione del server, potenzialmente sufficienti a scoprire l'indirizzo IP del servizio nascosto. Queste "position leaks" spesso vengono messe volontariamente dall'amministratore del servizio nascosto e quindi non possono essere considerate delle vere e proprie vulnerabilità della rete Tor.

Cell Counting and Padding

Durante questo genere di attacco il servizio nascosto verrà forzato a stabilire una connessione con un RP[16] malevolo. L'utente malevolo invia dei pacchetti/celle appositamente create al punto di introduzione del servizio nascosto specificando l'RP che vuole; poi il punto di introduzione invierà il messaggio al servizio nascosto in modo da indurlo a creare un circuito Tor per raggiungere quel determinato RP. Una volta che l'RP riceve il messaggio, il quale conterrà un token/cookie creato dal client, invierà un numero preciso di celle di "imbottitura", cioè 50, al servizio nascosto utilizzando lo stesso circuito. Queste celle di "imbottitura", che vengono supportate dal protocollo e poi scartate dal servizio nascosto, servono a lasciare tracce sul traffico; a questo punto l'RP chiuderà il circuito. Il Guard node, che si presuppone venga controllato dall'utente malevolo, monitora il traffico dei circuiti che passano attraverso esso; nel caso riceva una cella contenente la chiusura del circuito, verificherà che questa ricezione avvenga dopo aver ricevuto la cella contenente i cookie di conferma e che il numero di celle passate in precedenza siano 3 "up" attraverso il circuito e 53 siano "down" sempre attraverso il circuito. Se queste condizioni vengono soddisfatte, l'utente malevolo può dedurre che il Guard node che controlla è stato scelto dal servizio nascosto per creare il circuito e quindi potrà recuperarne l'indirizzo IP.

[16]Rendezvous point: router in un dominio di rete multicast che agisce come root condivisa per un multicast shared tree

4.3.4 Attacchi alla rete

Per prendere di mira l'intera rete è necessario essere consapevoli che dovranno essere compromessi diversi nodi; in questo caso l'effetto dell'attacco verrà propagato per tutta la rete invece di influenzare un singolo nodo.

Bridge Discovery

L'obiettivo è quello di recuperare informazioni sui bridge node di Tor poiché le informazioni che li riguardano non sono di dominio pubblico. Si possono usare due approcci differenti:

- Si può prendere il controllo di un middle node nella rete Tor così da sfruttare gli algoritmi di routing della larghezza di banda ponderata di Tor per scoprire i bridge node;

- Si potrebbero elencare i vari bridge node di Tor attraverso l'utilizzo di email di massa e server HTTPS su Tor.

Denial of Service(DoS)

Gli attacchi DoS vengono eseguiti per cercare di rendere inattivo un servizio o un componente sulla rete o almeno di diminuirne le disponibilità. Contro la rete Tor gli attacchi DoS sono CellFlood, cioè viene fatta un'inondazione di celle; viene sfruttato il fatto che l'utilizzo di una chiave privata per eseguire operazioni a 1024-bit sui server moderni sia circa 20 volte più lento che eseguire le stesse operazioni usando una chiave pubblica e quindi elaborare una cella di Tor è circa 4 volte più pesante del crearla. Un utente malevolo può inondare uno specifico nodo con celle create appositamente per prosciugare tutte le risorse di calcolo del target così da portare ad una negazione del servizio.

4.3.5 Attacchi verso entità multiple

Traffic Analysis Attack

Questo genere di attacco si basa sull'analisi del traffico della rete; i pacchetti vengono inseriti dal lato del server cercando di osservarli dal lato del client attraverso correlazioni statistiche. L'obiettivo è quello di ricavare il circuito stabilito dal client ed associare ad esso i pacchetti che vengono osservati dall'Exit node. Questo è possibile assumendo che l'utente malevolo sia capace di osservare il traffico in entrata ed in uscita della rete Tor attraverso i nodi in vari punti. Questo attacco cerca di forzare il client a connettersi ad un server malevolo così che quest'ultimo sia in grado di inserire uno specifico traffico nella connessione TCP; l'utente malevolo che è in possesso di una grande quantità di nodi potrà osservare il traffico di dati tra gli entry node ed i client così da poter trovare lo specifico traffico creato dal server malevolo. Una volta che il traffico viene rilevato, attraverso correlazioni statistiche, è possibile associarlo al client e di conseguenza ottenere il circuito Tor utilizzato.

Timing Attack

Questo attacco rappresenta una variante dell'attacco basato sull'analisi del traffico di rete; con questa metodologia si cerca di ottenere una relazione tra client e server osservando i pacchetti scambiati per realizzare una correlazione temporale. L'utente malevolo se vuole effettuare un attacco simile deve avere il controllo sia del Guard node sia dell'Exit node del circuito utilizzato dalla vittima. È possibile associare i pacchetti ad un certo client/server attraverso un'analisi temporale anche non conoscendo il contenuto dei pacchetti. Il traffico verrà interrotto seguendo intervalli predefiniti così da facilitare la correlazione. È possibile utilizzare un approccio identico per effettuare un'analisi del traffico; eseguendo più timing attack sul traffico della vittima ed utilizzando l'analisi del traffico per realizzare una stima della larghezza di banda, l'attacco è in grado di dedurre l'identità di rete di un client anonimo, di un servizio nascosto o dei proxy anonimi.

Di seguito c'è una tabella con tutti gli attacchi eseguibili e verso quale entità:

Attacco	Client	Server	Rete
Torben	✓		
P2P info leakage	✓		
Induced Tor Guard Selection	✓		
Raptor	✓		
Unpopular Ports Exploitation	✓		
Low-resources Routing	✓		
Cell Counting and Padding		✓	
Tor Cell Manipulation		✓	
Caronte		✓	
Off-path MitM		✓	
Bridge Discovery			✓
Denial of Serice			✓
Sniper			✓
Traffic Analysis	✓	✓	
Timing Attack	✓	✓	
Shaping Attack	✓	✓	

Tabella 4.2: Fonte: "Darknet Security: A Categorization of Attacks to the Tor Network"

4.4 Freenet

Freenet è una rete decentralizzata creata per resistere alla censura che sfrutta le risorse messe a disposizione dai suoi utenti per permettere la pubblicazione e l'utilizzo di qualsiasi tipo di informazione. Freenet è stata costruita ricercando anonimato e sicurezza più che la velocità di trasmissione perciò è poco consigliabile usarla se si vuole scambiare file di grosse dimensioni. E' un software libero scritto in Java ed è possibile utilizzarlo su Windows, GNU/Linux, macOS e tutti i sistemi operativi dotati di una Java Virtual Machine; per entrare e navigare in Freenet bisogna diventare un nodo della rete. A differenza della rete Tor e di I2P non è necessario un server per ospitare contenuti perchè tutto ciò che viene caricato su Freenet rimane lì permanentemente.
Il client è possibile scaricarlo direttamente dal sito ufficiale[17]; è necessario assicurarsi di avere una versione di Java uguale o superiore alla 7. Se ci si trova su Linux e non va a buon fine il download dal sito ufficiale, aprendo il terminale si può eseguire il comando "wget https://github.com/freenet/fred/releases/download/build01487/new_installer_offline_1487.jar -O new_installer_offline.jar" e poi "java -jar new_installer_offline.jar"; se il secondo comando non funziona si può utilizzare "java -jar new_installer_offline.jar -console". Nel caso in cui nel proprio sistema non sia installato "wget" lo si può scaricare eseguendo sempre da terminale il comando "sudo apt-get install wget". Per avviarlo oltre ad un Java Runtime Environment è necessario avere anche l'applicazione "IceaTea Java Web Start". Dopo aver scaricato ed avviato il client si aprirà una finestra nella quale è possibile scegliere se connettersi ad una rete di amici, opzione di alta sicurezza, alla rete globale di Freenet, opzione di bassa sicurezza, oppure se configurare personalmente le opzioni di sicurezza. Prima di passare alla configurazione è importante aprire

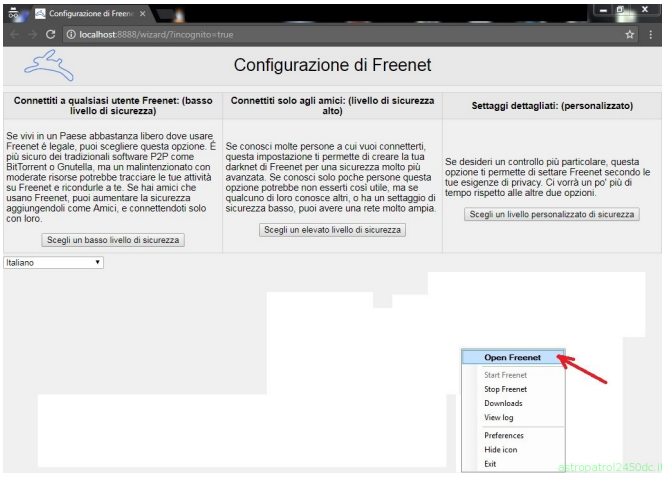

Figura 4.2: Fonte: "http://www.astropatrol2450dc.it/pagineguida/freenet.html"

la finestra del browser in modalità in incognito; step dopo step è possibile scegliere tra le varie opzioni che permettono all'utente di decidere personalmente il livello di sicurezza da adottare durante la navigazione e nei download, la grandezza del datastore e la banda massima da mettere a disposizione mensilmente nel caso si voglia mettere un limite. Finita la configurazione andando nella sezione "Core settings", presente nella voce "Configuration", si potrà visualizzare il valore del "Maximum Memory Usage" il quale si riferisce alla RAM; deve avere come minimo un valore di 512MB per far sì che il tutto funzioni adeguatamente.

[17] https://freenetproject.org/pages/download.html

Terminato anche questo passaggio non resta che cliccare "Apply", tornare alla homepage di Freenet e riavviare il nodo affinché le modifiche vengano applicate. Dopo aver riavviato il nodo si deve configurare il plug-in "WebOfTruth", detto WoT, poichè viene utilizzato dai plug-in di comunicazione per evitare lo spam su supporti non censurabili.

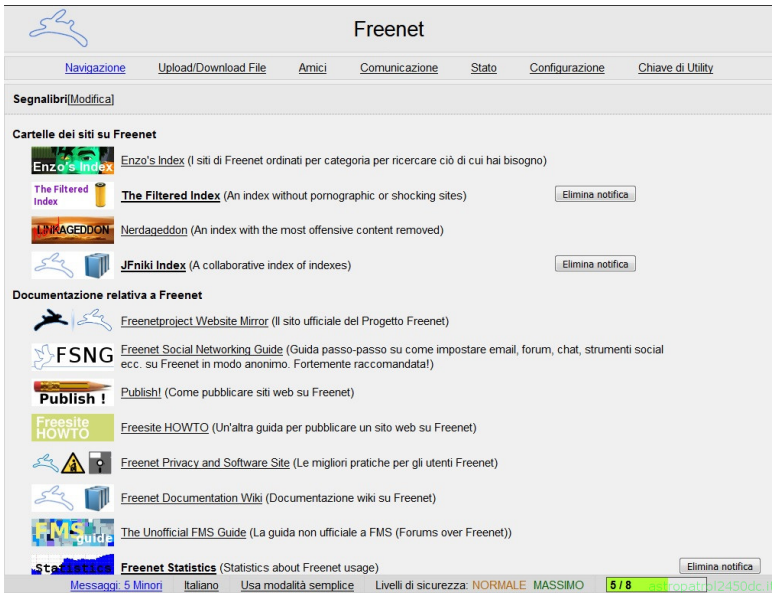

Figura 4.3: Fonte: "http://www.astropatrol2450dc.it/pagineguida/freenet.html"

Freenet mette a disposizione dei propri utenti molti plug-in ed applicazioni tra cui:

- Freemail: permette di creare un account email e poi configurando Mozilla Thunderbird lo si potrà utilizzare mantenendo intatta la propria privacy;
- Frost: applicazione esterna che fornisce una comunicazione in stile Usenet[18] e la possibilità di condividere file sfruttando la rete Freenet;
- Freetalk: plug-in che offre un metodo di comunicazione in stile forum su Freenet;
- FMS: applicazione esterna che fornisce forum ed una comunicazione in stile Usenet su Freenet;
- Sone: plug-in che fornisce una comunicazione in stile social network su Freenet; richiede il plug-in WebOfTruth per trovare altri utenti.

[18]Rete mondiale composta da migliaia di server che raccolgono dati inviati dagli utenti che possono accedere alla rete

Quando si naviga nella rete Freenet è possibile scegliere tra due modalità: Opennet e Darknet.

Opennet

È il meccanismo attraverso il quale la maggior parte dei nodi delle reti Freenet si connettono tra loro; è una rete nella quale le connessioni vengono create direttamente dai nodi. Quando un nodo viene creato ha a disposizione una lista di nodi "seme" ai quali può connettersi. Una volta connessi, i nodi "seme" forniscono a loro volta una lista di altri nodi e così via. Questo procedimento avviene in modo automatico quando un nodo è in esecuzione e non richiede nessun tipo di intervento da parte dell'utente. Le richieste di connessione vengono effettuate attraverso l'invio di "annunci", i quali una volta accettati da un nodo fanno si che la connessione possa essere instaurata. Se un utente decide di diventare un nodo seme deve rispettare alcuni requisiti:

- Rimanere online 24/7;
- Avere un indirizzo IP statico;
- Deve essere in grado di accettare i pacchetti in arrivo sulla propria porta di destinazione;
- Avere una larghezza di banda da almeno 256kbps + upstream.

Tutti i nodi seme sono elencati e visibili nel file "seednode.fref" presente in ogni nodo.

Darknet

Questa modalità è più sicura contro gli attacchi di rete rispetto alla Opennet poiché viene resa più difficile la connessione alla rete; è necessario convincere un user[19] per potersi connettere alla rete. Di fatto in questo modo si creano reti dove tutti gli utenti si conoscono e di fidano l'un l'altro.

La modalità Opennet è più facile da usare per l'utente rispetto alla Darknet ma è più vulnerabile e quindi può essere bloccata molto facilmente; il tracciamento della sorgente da parte degli "aggressori" è molto semplice, il che consente di rintracciare gli autori di determinati contenuti anche avendo risorse limitate e di collegarsi ad ogni nodo della rete potendoli sorvegliare. Scegliendo di navigare e di fatto diventando un nodo della rete Freenet si deve essere consapevoli del fatto che tutto ciò che verrà caricato nella rete verrà frammentato e sparso, rimanendo permanentemente in essa. I nodi della rete mettono a disposizione la loro larghezza di banda e nel proprio PC potrebbe passare qualsiasi genere di dato pertanto prima di entrare a far parte della rete Freenet è necessario sapere che c'è la possibilità che quei dati potrebbero contenere materiale illegale.

[19] Utente

4.5 I2P

I2P, acronimo di Invisible Internet Project, è un livello di rete privato e criptato costruito con l'intento di garantire privacy e sicurezza in modo da proteggere le attività svolte, la posizione e l'identità degli utenti. In questa rete è sempre l'utente a scegliere se condividere dati e con chi farlo, la piattaforma da utilizzare e le connessioni da attuare; I2P offre protezione dai pattern recognition[20] e dalla censura. I2P nasconde l'utente al server e viceversa; tutto il traffico di rete è presente soltanto all'interno della sua rete. Il traffico non interagisce direttamente con Internet poiché si trova ad un livello superiore grazie all'utilizzo di tunnel unidirezionali criptati tra gli utenti della rete, cosicché nessuno possa vedere il contenuto dei dati scambiati, né da dove vengono né dove sono diretti.
Viene fornito agli utenti anche un software da scaricare che permette loro di connettersi alla rete; oltre ai servizi per mantenere intatta la propria privacy, I2P fornisce anche un livello di applicazione che permette la creazione e l'utilizzo di applicazioni di uso quotidiano. Viene fornito anche un DNS, personale di I2P, che permette di farsi da auto-host. Gli utenti hanno anche la possibilità di creare una propria piattaforma che può essere aggiunta alla directory di I2P oppure può essere condivisa solamente con i propri amici. In I2P se l'utente non trova quello che sta cercando, può crearselo autonomamente dato che una volta scaricato il software, esso contiene tutti gli strumenti necessari per connettersi, condividere e creare ciò che si vuole.
I2P utilizza la crittografia per i tunnel che costruisce e per i dati che essi trasportano; questi tunnel utilizzano NTCP2[21] e SSU[22] per nascondere la natura del traffico che trasportano. Viene applicata una crittografia end-to-end per le connessioni, le quali godono anche del forward secrecy[23]. Dato che I2P è indirizzato cripto-graficamente, gli indirizzi sono auto-autenticati ed appartengono solamente all'utente che li ha generati.
La rete è composta da peer, cioè router, e tunnel virtuali unidirezionali sia in uscita sia in entrata; i router comunicano tra loro utilizzando protocolli costruiti utilizzando meccanismi di trasporto già esistenti, come UDP e TCP. Le applicazioni client hanno un proprio identificatore crittografico che gli permette di inviare e ricevere messaggi. I client possono connettersi a qualsiasi router ed autorizzare l'assegnazione temporanea di alcuni tunnel che verranno utilizzati per l'invio e la ricezione di messaggi attraverso la rete. I2P possiede un proprio database interno di rete per la distribuzione di routing e di recapiti sicuri.
La rete I2P è quasi completamente decentralizzata fatta eccezione per i "reseed server", i quali permettono di entrare nella rete; per effettuare la connessione iniziale è necessario ottenere un peer set ed all'indirizzo "http://127.0.0.1:7657/configreseed" nel router Java I2P sono elencati i reseed server che li forniscono. L'utente dovrà connettersi ad un server tramite uno dei router di I2P e quando ne avrà trovato uno raggiungibile potrà costruire "tunnel esplorativi" attraverso esso; una volta connessi è possibile trovare altri peer soltanto attraverso "tunnel esplorativi". I reseed server possono dire che un utente ha avviato la connessione da loro ma nessun'altra informazione relativa al traffico di rete.

[20] Analisi ed identificazione di pattern all'interno di dati grezzi al fine di identificarne la classificazione
[21] Protocollo di autenticazioni delle chiavi
[22] Secure Semireliable UDP: metodo di traporto utilizzato da I2P oltre a NTCP e NTCP2
[23] Proprietà dei protocolli di negoziazione delle chiavi che assicura che, se una chiave di cifratura a lungo termine viene compromessa, le chiavi di sessione generate a partire da essa rimangono riservate

Essendo una rete peer-to-peer distribuita ogni nodo che partecipa al routing di pacchetti renderà noto il suo indirizzo IP agli altri nodi ma nessuno potrà vedere le attività che svolge; non è possibile capire se un determinato nodo stia condividendo file, hostando un sito Web, effettuando ricerche o se contribuisce solamente alla rete offrendo la sua larghezza di banda.
I2P è compatibile con Windows, Linux e macOS ed il sistema operativo deve disporre di Java; è possibile scaricarlo dal sito ufficiale[24]. Una volta installato I2P il software è già pronto per navigare, utilizzando la navigazione in incognito, sia all'interno della sua rete che nel Web esterno. Se l'utente vuole utilizzare un client IRC dovrò configurarlo ma comunque sono già disponibili due server IRC preconfigurati da I2P e pronti all'uso.

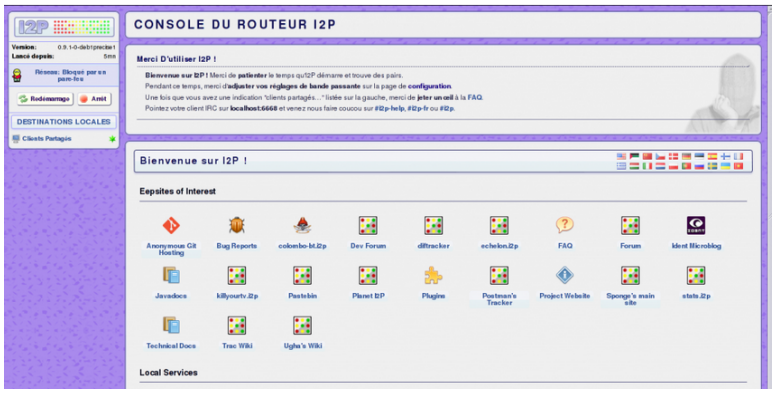

Figura 4.4: Fonte: "https://wizblog.it/come-funziona-i2p"

Utilizzando la porta 7657 del localhost tramite un qualsiasi browser è possibile accedere all'I2P Router Console, la quale viene gestita tramite un'interfaccia grafica dove è possibile scegliere la lingua desiderata. Dall'I2P Router Console andando sulla voce "configurazione manuale proxy" sarà possibile modificare il proxy e lo si dovrà impostare con i seguenti valori: HTTP: 127.0.0.1 – Porta: 4444; poi si dovrà aggiungere l'eccezione nel firewall di I2P andando sulla voce "Bloccato dal Firewall" e mettendo la spunta su "porta UDP" e lasciando la spunta su "Usa la stessa porta" per TCP.
Successivamente è necessario configurare il router e per accedere alle sue impostazioni basterà scrivere nella barra di ricerca del browser l'indirizzo IP 192.168.1.1; una volta entrati nelle impostazioni, nella voce "Configura" si dovrà aggiungere la porta 4444 sia ad UDP che a TCP e poi confermare. Completate queste configurazioni bisognerà salvare le modifiche e riavviare il client; collegandosi di nuovo alla I2P Router Console se uscirà a schermo la stringa "OK" vuol dire che si potrà iniziare ad usare correttamente il software. Durante la prima connessione alla rete, o durante una connessione dopo tanto tempo di inattività, ci sarà un tempo di attesa di qualche minuto durante i quali I2P stabilirà le connessioni con alcuni router della rete. Ci sono molti router connessi alla rete I2P e le prestazioni aumentano all'aumentare degli utenti che entrano a far parte della rete mettendo a disposizione quanta più banda possibile in upload. I dati che passano nella rete I2P sono protetti da vari livelli di crittografia, infatti il mittente ed il destinatario dei pacchetti che vengono scambiati non si conoscono e non sono conoscibili da terze parti; I2P dà la possibilità agli utenti di utilizzarlo contemporaneamente ad un altro browser dove si sta navigando normalmente in Internet.

[24]https://geti2p.net/en/

4.6 VPN

Una VPN[25] consente di creare una rete virtuale privata; permette inoltre di effettuare una connessione sicura alla rete criptando tutti i dati e di connettere il proprio dispositivo a qualsiasi rete pubblica. Ad esempio se in un paese viene bloccato l'utilizzo di una certa applicazione, attraverso l'utilizzo di una VPN si risulta essere connessi da un altro luogo e quindi si può usare l'applicazione. La rete Tor offre un ottimo livello di sicurezza ai suoi utenti ma è comunque possibile utilizzare una VPN insieme ad essa per ottenere una sicurezza maggiore.
Nella rete Tor viene crittografato soltanto il traffico che passa attraverso la rete, ma questo non accade per il traffico Internet in uscita nel tragitto tra l'Exit node ed il destinatario finale; una VPN crittografa tutto il traffico in uscita da un browser o da un'applicazione e lo maschera utilizzando un indirizzo IP secondario. Utilizzare una VPN mentre si naviga nella rete Tor permette all'utente di usufruire di un servizio di crittografia su tutto il traffico, sia interno che esterno al browser. Il procedimento consiste nel far crittografare la connessione da Tor che poi cripta anche la connessione VPN; successivamente la connessione ritornerà a Tor ed infine passerà attraverso Internet utilizzando la VPN. Facendo così ne l'ISP ne il provider della VPN potranno tracciare le attività rendendo di fatto la connessione più sicura. Le VPN gratuite non offrono i servizi adatti ad entrare nel Deep e Dark Web poiché salvano i logs e le attività, perciò la navigazione diventerebbe poco sicura e soprattutto non anonima.
Quando si utilizza una VPN è importante sceglierne una che abbia determinate caratteristiche:

- Controllare se il servizio VPN adotta una politica "No Logs", cioè che non salvano e tengono traccia di nessun movimento ed operazione;
- Alcune VPN condividono online le loro chiavi pre-shared ed è meglio evitarle poiché con queste chiavi i possibili hacker potrebbero effettuare attacchi, come il man-in-the-middle;
- Evitare VPN che hanno la propria sede principale in paesi che non sono privacy-friendly;
- Una VPN deve avere il "Forward-Secrecy", senza il quale l'utente lascerebbe comunque tracce rintracciabili in Internet, ed il "DNS Leak Protection", cioè una prevenzione verso le perdite di dati dal DNS;
- Importante ma non essenziale per una VPN è il "Double-Hop" o chiamato anche "Double-Encryption", cioè la connessione viene instradata tramite due server VPN invece che uno solo;

[25] Virtual Private Network

Alcuni ottimi servizi VPN sono:

- NordVPN: ha più di 3500 server e più di 5000 ISP[26] distribuiti in 62 paesi; la sede centrale è a Panama, un paese che non ha una legislazione severa contro i crimini su Internet. Caratteristiche:
  - Connessione VPN peer-to-peer;
  - Crittografia SSL a 2048 bit che cripta tutti i dati e rende complicata la decodifica;
  - Non mantiene i logs e non lascia tracce delle attività;
  - Offre una velocità maggiore rispetto a molte altre VPN;
  - Ha la funzione "Onion over Tor", ottima se si vuole usare NordVPN insieme a Tor dato che grazie a questa funzionalità prima il traffico di rete passa attraverso la VPN e poi viene automaticamente instradato attraverso la rete Tor.
- ExpressVPN: è situata nelle Isole Vergini ed ha 40 server in totale; il provider VPN ha quattro protocolli, OpenVPN, SSTP[27], L2TP[28] e PPTP[29], tutti molto sicuri. Caratteristiche:
  - Accetta diversi metodi di pagamento come PayPal o l'uso di Bitcoin;
  - Vengono utilizzate chiavi a 4096 bit e TLS per garantire che i dati che vengono trasferiti non vengano visti da una terza parte.
- PrivateVPN: è situata in Svezia ed ha 40 server sparsi nel globo; il provider VPN garantisce un ottimo livello di sicurezza. Caratteristiche:
  - 100% Uptime[30];
  - Port forwarding;
  - Non salva né logs né nessun'altro tipo di traccia;
  - Utilizza un servizio di crittografia a 2048 bit;
  - Consente il torrenting[31] del P2P.
- Torguard: la sede è situata negli USA ma i suoi server sono distribuiti in più di 200 località differenti e questo garantisce anche una velocità maggiore. Caratteristiche:
  - Effettua un riposizionamento istantaneo per non registrare nessun log;
  - Garantisce una connessione VPN P2P molto semplice da usare;
  - Per aumentare la sicurezza utilizza OpenVPN;
  - Consente la condivisione di file crittografati.

[26] Internet Service Provider
[27] Secure Socket Tunneling Protocol
[28] Layer 2 Tunneling Protocol
[29] Point to Point Tunneling Protocol
[30] Tempo nel quale è attivo
[31] Protocollo di condivisione file basato sulla tecnologia P2P. Consente ad un vasto numero di utenti di connettersi e condividere contenuti senza dover fare affidamento su un'unica fonte per i download.

4.7 Proxy

Un proxy è un tipo di server che fa da intermediario per le richieste effettuate dai client che cercano risorse su altri server; un client si connette al server proxy richiedendo un qualche tipo di servizio e quest'ultimo valuta la richiesta e la esegue cercando di gestirla e semplificandola. Gli usi più comuni di un proxy sono:

- Fornire anonimato durante la navigazione in Internet;
- Memorizzare una copia locale degli oggetti Web richiesti in modo da poterli distribuire nuovamente nel caso vengano richiesti senza dover accedere di nuovo al server di destinazione;
- Creare una difesa verso il Web, agendo da filtro per le connessioni, in entrata ed in uscita, monitorando, controllando e modificando il traffico interno.

Esistono dei tipi di proxy che garantiscono maggiore sicurezza e anonimato sul Web e sono gli "Elite proxy"; hanno un numero elevato di funzionalità uniche in aggiunta alle classiche funzioni offerte da un proxy HTTP[32]. Gli "Elite proxy" garantiscono molti vantaggi per quanto riguarda la privacy, ma possono anche nascondere che un utente stia utilizzando un server proxy. Un altro modo per chiamare gli elite proxy è High Anonimity Proxy(HAP).
Un HAP nasconde interamente le informazioni del computer e gli indirizzi IP degli utenti; gli header[33] che vengono normalmente inviati dai proxy, al contrario di come viene comunemente fatto, non contengono l'indirizzo IP. Questo genere di proxy può essere usato insieme ad altre piattaforme così da garantire un livello di sicurezza ancora maggiore.
Un HAP funziona come un normale proxy HTTP; cioè un client HTTP, per esempio un browser Web, invia richieste Web al HAP che le inoltra all'effettivo server Web. Il server Web vedrà il server proxy come se fosse un'altra connessione e risponde normalmente fornendo la risposta HTTP al client. La differenza principale è che l'HAP nasconde interamente la richiesta originale cosicché il Web server non saprà che la richiesta HTTP proviene da un proxy.

L'obiettivo principale quando si utilizza un HAP è quello di proteggere l'anonimato nascondendo l'indirizzo IP; oltre a questo il loro utilizzo può rendere più veloce la processazione delle richieste poiché l'uso della larghezza di banda è ridotto. Alcuni HAP hanno la possibilità di intercettare e successivamente bloccare le richieste provenienti da siti loschi così da proteggere gli utenti dal scaricare involontariamente malware o contenuti contenenti malware.
Un altro utilizzo importante è quello di aumentare il numero di contenuti accessibili nel Web, ad esempio siti che normalmente sarebbero bloccati nel proprio paese diventano accessibili, e vengono bypassati vari controlli di sicurezza; viene migliorata anche la navigazione in quanto la rende più sicura. Usare questo genere di proxy permette ad un utente di avere molte funzionalità aggiuntive senza che debba fare nulla.

[32]Hypertext Transfer Protocol
[33]Parte di un pacchetto contenente informazioni necessarie al funzionamento della rete

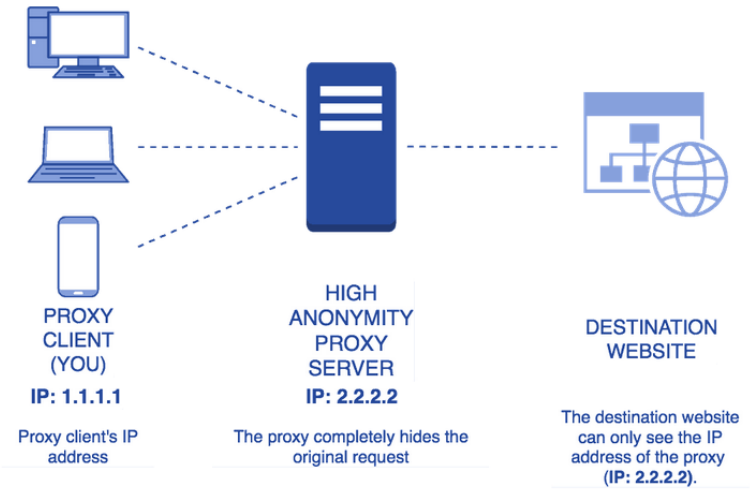

Figura 4.5: Fonte: "https://hide-ip-proxy.com/what-is-high-anonymity-proxy-elite/"

I vantaggi principali nell'utilizzare un Elite proxy/HAP sono:

- Possibilità di accedere a siti Web stranieri e scaricare anche contenuti da essi, dato che il server straniero non sarà in grado di determinare che l'utente si trovi in un'altra nazione;
- Una maggiore protezione per l'utente e per la sua privacy poiché nascondono le sue informazioni personali;
- Diminuire la probabilità di subire attacchi informatici;
- Mantenere al sicuro la propria identità e le proprie informazioni personali quando si naviga sul Web.

Oltre ai vantaggi però ci sono anche degli svantaggi:

- Utilizzando un server proxy c'è il rischio che i dati trasferiti attraverso di esso vengano condivisi con utenti malevoli. Viene chiamato "bad neighbor effect";
- Molto spesso hacker o utenti malevoli presenti nel Web utilizzano questo tipo di proxy e questo può ridurre la velocità di navigazione;
- Nel caso in cui un Elite proxy non venga configurato correttamente, diventa semplice per un utente malevolo riuscire a rubare dati e informazioni, compromettendo di fatto la sicurezza dell'utente.

I proxy di norma inviano tre tipi differenti di header HTTP:

- HTTP_VIA;
- HTTP_X_FORWARDED_FOR;
- REMOTE_ADDR.

Proxy Type	HTTP_VIA	HTTP_X_FORWARDED_FOR	REMOTE_ADDR
Transparent proxy	Proxy's IP address	User's IP address	Proxy's IP address
Anonymity proxy	Proxy's IP address	Proxy's IP address or random IP	Proxy's IP address
High anonymity proxy	blank	blank	Proxy's IP address

Figura 4.6: Fonte: "https://hide-ip-proxy.com/what-is-high-anonymity-proxy-elite/"

Quando viene inviato un header REMOTE_ADDR l'indirizzo IP del server proxy viene sempre incluso, ma questo accade sempre anche quando si naviga senza utilizzare un server proxy.

Open proxy

I servizi proxy premium offrono la possibilità di utilizzare HAP ma comunque si possono trovare proxy gratuiti, detti anche Open proxy; un Open proxy server permette a chiunque sia su Internet di connettersi al proxy del computer e quando un Web browser viene configurato per usare un Open proxy server, le richieste vengono inviate al server proxy prima di andare su Internet. Questo procedimento garantisce anonimato all'utente poiché il server di destinazione invece delle informazioni dell'utente vedrà quelle del proxy. I dati che dovranno andare all'utente, prima di raggiungerlo, passeranno per il server proxy.
Comunemente un Open proxy viene utilizzato quando si vuole nascondere la propria identità durante varie azioni, come può essere il download di un file o la visita di siti Web, oppure per accedere a siti che sono bloccati nel proprio paese.
Gli HAP, così come i proxy HTTP, sono progettati per la navigazione Web e per l'accesso ad Internet; per connettersi ad un proxy dal proprio Web browser ci sono delle opzioni:

- Utilizzare un proxy switch generico che permette di usare un proxy;
- Impostare manualmente il proxy per il browser che si vuole utilizzare;
- Usare Proxifier per deviare le connessioni del browser attraverso un HAP.

Utilizzare un proxy potrebbe essere una possibile opzione in confronto ad utilizzare la rete Tor per accedere al Deep Web, ma c'è una sostanziale differenza; il fornitore di un servizio proxy conosce l'identità degli utenti che lo utilizzano, cosa fanno su Internet e può vedere il traffico di rete mentre passa attraverso il suo server. In alcuni casi è possibile che riesca a vedere all'interno del traffico, anche se è crittografato, mentre lo inoltrano ad esempio verso un sito bancario.

Quando un utente utilizza un servizio proxy deve fidarsi che quest'ultimo non stia monitorando il traffico di rete, che non inserisca i propri annunci nel flusso del traffico o che non registri i dati personali dell'utente.
Utilizzare un proxy per mantenere la propria privacy su Internet non è una cattiva scelta, ma se un utente decide di entrare nel Deep Web o di effettuare azioni/ricerche che vuole mantenere assolutamente private, ci sono opzioni migliori da utilizzare, come la rete Tor.

4.8 Perchè è meglio usare un sistema Linux rispetto ad uno Windows

Windows e Linux sono due sistemi operativi molto diffusi tra gli utenti, ma la maggior parte di loro utilizza Windows per via della sua interfaccia semplice e della sua facilità nell'essere usato anche da un utente poco esperto nel campo dell'informatica, a differenza di Linux che necessita di una conoscenza maggiore per poter essere utilizzato come si deve. È possibile accedere ai contenuti del Deep Web ed al Dark Web utilizzando entrambi i sistemi operativi ma è consigliabile l'utilizzo di un sistema Linux rispetto ad uno Windows poiché:

- I malware ed i virus sono costruiti maggiormente per corrompere un sistema operativo Windows dato che è il sistema operativo più diffuso al mondo;
- Essendo l'anonimato il principale beneficio del Deep e del Dark Web, è sconsigliato utilizzare Windows poiché tiene traccia di tutto quello che viene fatto dagli utenti, e quindi la privacy viene a meno;
- Su Linux a differenza di Windows è più facile individuare bug e successivamente risolverli prima che un hacker possa sfruttarli.

Sono stati creati vari sistemi operativi alternativi che hanno come obiettivo principale quello di garantire anonimato e migliorare la privacy degli utenti durante la loro navigazione; sono principalmente costruiti utilizzando come base il sistema GNU/Linux, ad esempio alcuni di questi sono Tails, Subgraph OS e Whonix.
Tor Browser, il browser più conosciuto ed utilizzato per accedere alla rete Tor, è scaricabile ed utilizzabile sia con Windows sia con Linux, ma vista la maggioranza di sistemi Linux-based costruiti ad hoc per entrare nel Deep Web si può concludere che se si vuole accedere ai contenuti del Deep e del Dark Web è meglio usare un sistema GNU/Linux.

4.9 Migliori sistemi operativi alternativi per accedere al Deep e Dark Web

Oltre ai classici sistemi operativi che tutti conoscono, come ad esempio Windows e Linux, sono stati creati dei sistemi operativi con lo scopo di realizzare un ambiente quanto più sicuro e rivolto al mantenimento della privacy degli utenti. Tra questo genere di sistemi ci sono Tails, Subgraph OS e Whonix; tutti e tre hanno come base un sistema GNU/Linux ed hanno differenti caratteristiche ma comunque ognuno di loro ha l'obiettivo di rendere il sistema il più sicuro possibile.

4.9.1 Tails

Il sistema operativo Tails è una distro[34] Linux che utilizza la rete Tor. Essendo una live distro può essere installata in una chiavetta USB o in un DVD scrivile ed avviata all'accensione del computer al posto del solito sistema operativo; per installarla la chiavetta USB o il DVD devono avere almeno 8GB di memoria disponibile. Il computer deve avere come minimo 2 GB di RAM per lavorare in modo fluido, deve essere a 64-bit poiché dalla versione 3.0 di Tails le successive versioni non sono compatibili con PC a 32-bit ed il processore deve essere compatibile con l'architettura x86-64[35]. Avviandola in questo modo la distro non utilizzerà mai il disco fisso quindi, se il computer al quale connettiamo la nostra periferica o DVD contenente Tails ha dei virus, questi non intaccheranno la distro Linux; potrebbe subire problemi nel caso in cui si utilizzi un computer avente già dei virus al momento dell'installazione di Tails nella periferica/DVD.
Ad ogni avvio il sistema chiederà la lingua e se l'utente vuole aggiungere opzioni extra, come l'utilizzo di un bridge o di un proxy oppure se si vuole impostare una password da amministratore per essere in grado di eseguire attività amministrative come l'installazione di software aggiuntivi o accedere ai dischi rigidi interni del computer. Una volta finita la configurazione iniziale il sistema si presenterà privo di tracce e dati gestiti nelle sessioni precedenti, poiché quando il sistema viene arrestato tutte le attività svolte vengono cancellate. Succede questo perché non scrive nulla sul disco fisso ma utilizza soltanto la memoria RAM del computer, eliminando ogni volta che viene arrestato tutte le tracce possibili.

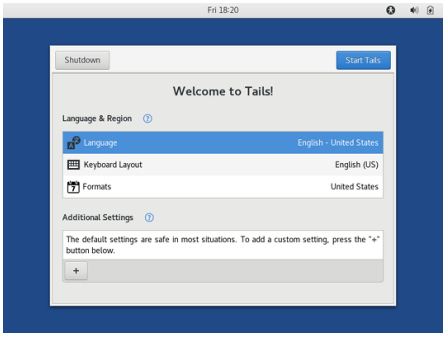

Figura 4.7: Fonte: "https://tails.boum.org/doc/first_steps/welcome_screen/index.it.html"

[34]Distribuzione software del sistema operativo Linux, realizzata dal kernel Linux, un sistema di base GNU e da altri applicativi
[35]Versione a 64-bit del set di istruzioni x86

C'è la possibilità di salvare alcuni file o configurazioni in un volume persistente cifrato all'interno della chiavetta USB; l'utilizzo del volume persistente è un'opzione e si può decidere cosa rendere persistente o meno ed una volta creato il volume possiamo anche scegliere se sbloccarlo o meno all'avvio del sistema. Se si ha l'intenzione di usare Tails per rimanere il più possibile anonimi, creando un volume persistente si deve far attenzione poiché non è nascosto e nel caso qualcuno si impossessi della periferica USB/DVD nella quale è salvato ha la possibilità di vederlo e conoscere i dati che sono salvati al suo interno, ma comunque è possibile impostare una password da inserire per sbloccarlo; un altro problema derivante dall'utilizzo di un volume persistente è che si può minare la sicurezza del sistema nel caso venga usato per sovrascrivere delle impostazioni, perché così facendo c'è la possibilità di compromettere le impostazioni che rendono possibile la sicurezza. Anche avviare il volume persistente da un altro sistema operativo è da evitare poiché c'è la possibilità che vengano create thumbnails, immagini o anche indici del contenuto del volume; è consigliato l'utilizzo di questa opzione solo per lo stretto necessario.
Tails al suo interno ha applicazioni che permettono di lavorare su documenti sensibili e comunicare in modo sicuro; ogni applicazione è già preconfigurata con le giuste impostazioni in modo da evitare errori; alcune delle applicazioni incluse sono:

- Tor Browser con UBlock[36];
- Mozilla Thunderbird con Enigmail, per gestire email cifrate;
- KeePassXC, che permette la creazione e conservazioni di password complesse;
- LibreOffice;
- OnionShare, usato per condividere file attraverso Tor;
- Elecrum Bitcoin Wallet, che permette la creazione e gestione di un personale portafoglio di criptovalute.

Il sistema affinché non vengano effettuati errori ha delle meccaniche già impostate e sono:

- Le applicazioni vengono bloccate in modo automatico quando tentano di connettersi ad internet senza passare per la rete Tor;
- Ogni dato presente nel volume persistente è cifrato;
- Non viene scritto nulla sul disco fisso ed all'arresto viene eliminato tutto.

All'interno della distro Tails tutto ciò che viene fatto su Internet passa per la rete Tor. Tor e Tails sono progetti separatamente ma utilizzati insieme offrono la possibilità di proteggere maggiormente le proprie azioni ed i propri dati; è comunque possibile utilizzarli singolarmente. Si può scaricare Tails dal sito ufficiale[37], è gratuito e tutto il codice del software è pubblico, in modo da permettere a qualsiasi ricercatore o operatore che si occupa di sicurezza informatica di testare se il software funziona in modo ottimale e vedere se ci sono falle nel sistema.

[36] Advertise-blocker
[37] https://tails.boum.org/index.it.html

4.9.2 Subgraph OS

Subgraph è una distro linux progettata per garantire un elevato livello di sicurezza in Internet resistendo agli attacchi dei malware ma anche ad attacchi indirizzati alla rete locale, garantendo una protezione su tutto il sistema operativo come quando si installano delle applicazioni e non solo per il kernel.
Le applicazioni più importanti del sistema operativo lavorano all'interno di una sandbox; questa caratteristica permette di eseguirle in un ambiente controllato e questo fornisce un'ottima protezione dagli attacchi. L'obiettivo che questo sistema operativo si pone è quello di dare all'utente un sistema sicuro nel quale i rischi siano ridotti al minimo cosicché possa lavorare senza la paura di essere vulnerabile ad eventuali attacchi.
Una delle funzionalità più importanti è l'utilizzo di Application Armor, un software di sicurezza per Linux il quale permette all'amministratore di sistema di associare ad ogni programma un profilo di sicurezza che dà la possibilità di restringere le capacità del programma. Subgraph ha un kernel modificato in modo da fornire al sistema la massima sicurezza possibile, includendo anche l'elenco delle patch di Grsecurity e PaX. Ciò rende il kernel più resistente agli eventuali attacchi ed offre un'ottima protezione a tutti i processi in esecuzione.

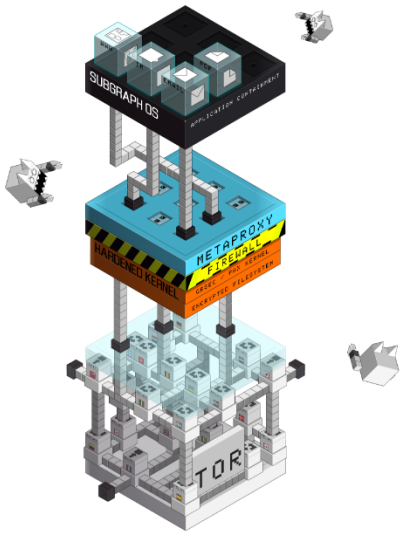

Figura 4.8: Fonte: "https://subgraph.com/"

Grsecurity è un ampio miglioramento della sicurezza per il kernel Linux poiché garantisce una difesa contro molte minacce alla sicurezza attraverso il controllo degli accessi intelligenti, sfrutta una memoria corruption-based ed una serie di altri sistemi che incrementano la protezione i quali generalmente non richiedono alcuna configurazione.
PaX è una patch per il kernel Linux che implementa gli ultimi privilegi di protezione per le pagine di memoria che consentono ai programmi di essere in grado di limitare l'insieme di operazioni che sono autorizzati a eseguire; nel caso di PaX, la capacità di eseguire i dati come codice. Un'altra misura di sicurezza adoperata è l'utilizzo di RAP, un software che previene attacchi dove viene riusato il codice del kernel stesso. Il kernel è programmato con meno funzionalità possibili in modo da dare meno opportunità ad eventuali attacchi.

Le applicazioni vulnerabili o quelle che sono esposte vengono eseguite nella sandbox in modo da isolarle sia tra di loro che dal resto del sistema operativo. Altre caratteristiche della sandbox di Subgraph è l'utilizzo di un ambiente con un file system limitato e l'isolamento del desktop da queste applicazioni. Le applicazioni racchiuse nella sandbox sono:

- Il Web browser;
- Il client per le email con il supporto per la crittografia integrato;
- Il software CoyIM per la messaggistica istantanea;
- Libre Office;
- Il visualizzatore per PDF ed immagini;
- Il riproduttore per i video;
- Hexchat, un software utilizzato per gestire le attività IRC[38];

Oltre a queste misure di sicurezza generali dispone di impostazioni specifiche per utilizzare la rete Tor. Ogni connessione in uscita viene forzata attraverso la rete Tor ed inoltre utilizza lo stream isolation per impedire che lo stesso circuito Tor venga utilizzato da più applicazioni. Il firewall dell'applicazione offre la possibilità di verificare ogni connessione sconosciuta e nuova in uscita così da assicurarsi che sia autentica e non un malware o uno sniffer di dati.

4.9.3 Whonix

Whonix è un software costruito con l'obiettivo di preservare la sicurezza e l'anonimità degli utenti. È disponibile su Windows, Linux e macOS; in Qubes-Whonix e Non-Qubes-Whonix è già preinstallato. Whonix è basato su Kicksecure, una distribuzione Linux che garantisce un ottimo livello di sicurezza; dispone di Tor browser e per proteggere l'anonimato degli utenti in Internet tutte le connessioni vengono forzate a passare attraverso la rete Tor ed in più le applicazioni vengono instradate attraverso percorsi differenti.
Whonix ha diverse caratteristiche che rendono possibile il mantenimento della sicurezza, come ad esempio la "live mode", una modalità nella quale tutte le scritture effettuate sull'hard disk virtuale vengano eliminate dopo l'arresto del sistema poiché vengono effettuate sulla RAM invece che sull'hard disk. Questo procedimento vale anche per le modifiche maligne che vengono apportate dai malware tranne nei casi in cui: la modalità di sola lettura dell'hard disk non è configurata ed il malware ha rimontato il disco come lettura-scrittura o è uscito dalla VM; la modalità di sola lettura dell'hard disk è configurata ed il malware è uscito dalla VM.

[38]Internet Relay Chat: protocollo di messaggistica istantanea su Internet

Vengono utilizzati numerosi meccanismi di sicurezza, come ad esempio:

- Per proteggersi dai "time attack" utilizza il Boot Clock Randomization, che setta in modo randomico l'orologio tra 0 e 180 secondi tra passato e futuro, ed una sicura sincronizzazione del network time attraverso l'uso di sdwdate[39] che imposta l'orologio del sistema attraverso una connessione TCP end-to-end criptata con i Web server di Tor;
- Utilizza AppArmor, il quale permette di associare ad ogni programma un profilo di sicurezza in modo da restringerne le capacità;
- Utilizza il "Console Lockdown" che abilita solo gli appartenenti al gruppo "console" di utilizzarla e di default soltanto l'user fa parte di questo gruppo;
- Utilizza i "Kernel Hardening Settings", impostazioni che rendono il kernel più sicuro le quali sono raccomandate dal KSPP[40].

Whonix ha già diverse applicazioni pre-configurate:

- Tor Browser;
- OnionShare, applicazione che permette di scambiare file di qualsiasi dimensione attraverso la rete Tor;
- Thunderbird;
- KeePassXC, che permette di generare password complesse;
- HexChat, un client IRC open source ;
- VLC Media Player;
- Terminal, cioè un'interfaccia per usare il terminale del sistema;
- Electrum Bitcoin Wallet, per creare e gestire un portafoglio di criptovalute;
- Bitcoin client, un software che facilita la generazione di chiavi private e la loro sicurezza e l'invio di pagamenti per conto di una chiave privata;
- Monero GUI[41] e Monero CLI[42], i quali permettono di gestire un portafoglio di Monero;

Whonix può essere utilizzato come sistema operativo principale ma anche lavorando con due VM[43] contemporaneamente, una come gateway e l'altra come workstation; il gateway sfrutta la rete Tor per garantire sicurezza e privacy così l'utente può esser sicuro che ciò che farà nella workstation rimanga anonimo. Sfruttando le VM si rende più semplice la configurazione di Whonix mentre se lo si vuole installare come sistema operativo principale richiederà una configurazione più lunga e complicata. L'host che verrà usato per avviare Whonix non è importante, ed una volta scaricato il file basta importarlo direttamente in una VirtualBox senza modificare nessuna impostazione per poterlo utilizzare.

[39] Secure Distribuited Web Date
[40] Kernel Self Protection Project
[41] Graphical User Interface
[42] Command Line Interface
[43] Virtual Machine

Figura 4.9: Whonix-Gateway
Fonte:"https://www.whonix.org/wiki/Screenshots"

È importante l'ordine nel quale si avviano le due VM poiché per prima deve essere avviata quella che verrà usata come gateway cosicché possa connettersi subito alla rete Tor; una volta connessa verrà fuori un avviso che richiede un aggiornamento, ma basta chiuderlo e fare da terminale prima il comando "sudo apt-get-update-plus dist-upgrade" e poi "sudo apt-get update && sudo apt-get upgrade –y"; così facendo verrà richiesta una password, che di default sarà "changeme". Una volta terminato si potrà avviare l'altra VM, il Whonix-workstation, ed una volta avviata quando uscirà a schermo un avviso da parte di "whonix setup wizard" basta cliccare l'opzione "understood" e rifare gli stessi comandi da terminale come per il gateway per poi poter iniziare ad utilizzare il sistema.

Figura 4.10: Whonix-workstation
Fonte:"https://www.whonix.org/wiki/Screenshots"

È possibile anche modificare la password sia nel gateway sia nella workstation scrivendo nel terminale il semplice comando "passwd user", poi verrà richiesto di inserire prima la password corrente, poi quella nuova ed infine di verificarla. Ogni volta che si vuole usare Whonix è necessario soltanto ricordarsi di avviare prima il gateway e poi la workstation così da poter agire in sicurezza.

5. Tools e strumenti di ricerca

5.1 Motori di ricerca

Per cercare qualcosa nel Deep e nel Dark Web non è possibile utilizzare un classico motore di ricerca, come Google o Bing, ma è necessario usarne uno che sia capace di accedere alle informazioni contenute in questo ambiente. Ogni motore di ricerca per il Deep Web ha le proprie caratteristiche che lo rendono diverso dagli altri; successivamente ne riporterò alcuni.

Ahmia

È uno dei pochi motori di ricerca per il Deep Web che sono attualmente in funzione; è facile da utilizzare avendo un'interfaccia molto semplice e dato che necessita di poche istruzioni per svolgere una ricerca. Offre un servizio unico tra i motori di ricerca che si chiama "Link Graph" il quale permette di vedere quali connessioni ci sono tra un link ed un altro.

Kilos

Questo motore di ricerca permette di accedere ai contenuti anche del Dark Web; ha un focus particolare per le droghe. Per la ricerca vengono usate keywords[1] e filtri, i quali sono sfruttati per ricercare anche in alcuni Black Market oltre a tutte le altre fonti, come ad esempio nei forum.

Not Evil

Ha un'interfaccia molto semplice che permette un facile utilizzo; per effettuare una ricerca basta inserire le keyword dell'argomento desiderato. La pagina che mostrerà i risultati è disordinata e con un font poco gradevole ma i link spesso sono funzionanti.

Candle

È uno dei più semplici motori di ricerca da utilizzare poiché la sua interfaccia assomiglia molto a quella di Google. Vengono visualizzati soltanto i risultati ".onion" e può essere usato per trovare link del Deep Web se si è a conoscenza delle keyword giuste.

[1] Parole chiave

HayStack

Ha più di 1.5 miliardi di pagine indicizzate e più di 300.000 ricerche giornaliere; si può considerare HayStack come uno dei migliori motori di ricerca per il Deep Web.
Mostra soltanto risultati ".onion" e nella versione a pagamento del servizio oltre al link del sito Web vengono mostrate anche informazioni avanzate come la versione cache, Datapoints ecc. Sulla piattaforma è possibile a volte trovare degli annunci ma sono molto occasionali e per la maggior parte ne è priva.

Abiko

È un motore di ricerca molto semplice poiché nella sua interfaccia è presente soltanto la barra di ricerca ed i risultati provenienti dalle ricerche che vengono effettuate, i quali comprendono solo siti ".onion" senza nessun altro elemento. È un motore di ricerca ad-free, cioè privo di annunci pubblicitari.

Onion Land

Viene sponsorizzato da Tor, Tor2web ed ha una homepage molto semplice da utilizzare la quale presenta una barra della ricerca e qualche termine di ricerca generale nel caso non si sappiano o non si vogliano inserire delle keyword; visualizza soltanto i risultati ".onion". La pagina di ricerca non è molto user-friendly poiché vengono visualizzati gli URL in un formato poco gradevole. Ha la funzione di poter visualizzare le pagine memorizzate nella cache nel caso gli utenti ne abbiano in bisogno.

Pipl

Questo motore di ricerca fornisce l'accesso a più di 6 miliardi di risultati provenienti dal Deep e dal Dark Web ed ha un indice di identità delle persone. L'utilizzo principale per cui viene utilizzato è la ricerca di profili di persone; possono essere applicati diversi filtri alla ricerca, come il nome, il numero di telefono o anche l'indirizzo email.

Grams

È un motore di ricerca costruito per i Black market; non è un effettivo Black market ma è molto utile poiché rende semplice trovarne uno. I risultati che vengono forniti corrispondono a parole chiave presenti nei titoli, descrizioni o fornitori. Vengono indicizzate soltanto pagine presenti nella rete Tor perciò è accessibile soltanto attraverso l'utilizzo di un Dark Web browser; ha un'interfaccia molto simile a quella di Google.

Torch

È un buon motore di ricerca da utilizzare nelle Darknet e viene considerato come uno dei più grandi dato che ha indicizzato circa 1 milione di pagine Web. È attivo dal 1996 e questo può dare un'idea sul quanto possa essere efficiente ed affidabile; gode di un'interfaccia molto semplice che rende facile l'utilizzo.
Nell'interfaccia iniziale sono presenti molte pubblicità riguardanti i più svariati contenuti.

5.2 Tools

Il Deep ed il Dark Web sono ambienti incredibilmente vasti nei quali non è molto facile cercare qualcosa o proteggere i propri dati; gli utenti possono utilizzare dei tool per semplificare il proprio lavoro. I tool sono software che possono essere utilizzati per effettuare determinati tipi di azioni sul Web.

5.2.1 Monitoring tools

Nel Deep e nel Dark Web è molto comune trovare siti dove vengono venduti o condivisi i dati personali degli utenti, le informazioni riservate delle aziende e molti altri generi di dati privati; i Monitoring tools sono servizi che permettono di scansionare il Web, anche il Deep ed il Dark, così da accertarsi se determinati dati sono presenti in qualche sito dove non dovrebbero essere; ecco alcuni esempi:

Alert Logic Dark Web Scanner

Offre un servizio di prevenzione per l'acquisizione degli account; viene fatta una scansione del Web e se viene trovato qualche riscontro verrà compilato un elenco di tutti gli account compromessi. Un problema è che il report contenente tali informazioni viene inviato una volta al mese.

SpyCloud ATO Prevention

Offre due servizi per la prevenzione contro l'acquisizione di account(ATO): uno per coprire i dipendenti delle aziende e l'altro per proteggere i clienti dei servizi online. La protezione ATO si concentra sulla protezione degli account creati dalle aziende per l'accesso alle loro risorse; una parte importante del servizio riguarda anche l'individuazione degli account che sono già stati compromessi.
Il servizio ATO include anche un database di informazioni sulle minacce basato sul cloud, che avverte i clienti nel caso ci siano account compromessi; le informazioni sulle credenziali divulgate vengono trovate attraverso uno strumento di scansione del Dark Web. Il servizio inoltre monitora in modo proattivo Active Directory e stabilisce politiche di password più forti, come la rotazione delle password e la complessità di esse.

DigitalStakeout Scout

Offre un servizio di informazione per le minacce del Dark Web; il sistema include flussi di lavoro e di machine learning per poter rilevare comportamenti anomali all'interno di una rete. Attraverso l'utilizzo di uno scanner che lavora sul Dark Web e del servizio di informazioni sulle minacce si riesce ad identificare l'attore dannoso che sta partecipando o ha partecipato all'attività ritenuta sospetta.
Scout è un sistema di prevenzione della perdita di dati e di protezione dalla minacce; una volta identificata una minaccia spetta poi all'amministratore risolvere il problema. Viene offerto anche un servizio di salvaguardia del marchio e della reputazione delle aziende attraverso una scansione dei siti Web che potrebbero avere contenuti dannosi per le aziende; una volta trovato un riscontro verrà reso noto attraverso una notifica sulla dashboard di Scout.

5.2.2 FireEye Digital Threat Monitoring

Questo tool, creato dall'azienda FireEye, è in grado di raccogliere automaticamente contenuti in tutto il Web, così che gli utilizzatori vengano puntualmente avvisati quando viene rilevata una possibile minaccia.
FireEye Digital Threat Monitoring permette agli utenti che lo utilizzano di avere un'ampia visibilità sulle minacce dirette alla propria organizzazione o ai propri dati fornendo un resoconto che permetterà di conoscerle e di conseguenza capire tempestivamente come affrontarle. Il servizio offerto permette di combattere in modo efficace diversi rischi come la perdita di dati, le minacce alle attività o anche furti monetari; la visibilità che verrà fornita comprende aspetti difficilmente accessibili nel Web insieme ad un'analisi focalizzata da parte degli esperti di FireEye, i quali hanno la possibilità di utilizzare l'intera organizzazione di FireEye Threat Intelligence.
Il Digital Threat Monitoring sfrutta una tecnologia di ricognizione Web proprietaria la quale raccoglie dati nel Deep, Dark e Surface Web; questo lavoro si rivolge in particolar modo ai siti utilizzati per le comunicazioni che vengono usati da utenti considerati "dannosi". Utilizzando le keywords[2] query[3], che l'utente può specificare, viene effettuata un'analisi e di conseguenza vengono generati degli alerts di minaccia se vengono trovati dei riscontri potenzialmente significativi. Gli alerts sono visibili dalla dashboard alerts all'interno del FireEye Intelligence Portal; ogni alerts include lo stato di allerta, la fonte e la gravità degli attributi oltre ad informazioni importanti per aiutare l'utente a gestire le attività monitorate. Attraverso la dashboard alerts è possibile comunicare con un analista FireEye o fare segnalazioni individuali o multiple.
Le caratteristiche principali offerte dal Digital Threat Monitoring di FireEye sono:

- Monitoraggio in tempo reale delle minacce digitale dirette alle proprie attività;
- Invia un avviso immediato nel caso in cui le proprie attività o i propri dati vengano menzionati o presi di mira;
- Invia un avviso nel caso in cui i propri dati o le proprie attività sono esposte a minacce o se sono compromesse;
- Fornisce una ricognizione adatta alle esigenze dell'utente.

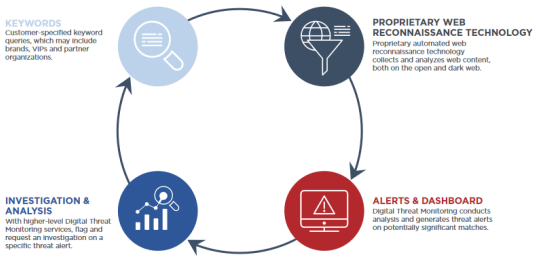

Figura 5.1: Fonte: "https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/ds-digital-threat-monitoring.pdf"

[2]Parole chiave
[3]Interrogazione di un database per estrarre o aggiornare i dati che soddisfano un certo criterio di ricerca

Il FireEye Digital Threat Monitoring fornisce agli utenti quattro diversi tipi di servizi, tra i quali soltanto la prima non è a pagamento:

- Digital Threat Assessment: una sola volta viene effettuata una valutazione point-in-time su un periodo di 30 giorni usando le keywords query scelte dall'utente; al termine di questo periodo verrà fornito un singolo report che valute le minacce identificate con eventuali approfondimenti;
- Digital Threat Monitoring Standard: fornisce un continuo monitoraggio utilizzando le keywords query scelte dall'utente attraverso il Deep, Dark e Surface Web; gli eventuali alerts verranno notificati all'interno del FireEye Intelligence Portal;
- Digital Threat Monitoring Advanced: fornisce gli stessi servizi della versione Standard ma aggiunge 40 indagini che verranno svolte da analisti intelligence di FireEye;
- Digital Threat Monitoring Enterprise: fornisce gli stessi servizi della versione Standard ma aggiunge 80 indagini che verranno svolte da analisti intelligence di FireEye.

Di seguito vi è una tabella che mette a confronto le caratteristiche dei quattro tipi di servizi offerti:

Table 2. Comparison of Digital Threat Monitoring service capabilities.

Entitlements	Digital Threat Assessment	Digital Threat Monitoring Standard	Digital Threat Monitoring Advanced	Digital Threat Monitoring Enterprise
Onboarding	Yes	Yes	Yes	Yes
Unlimited Keywords	Yes	Yes	Yes	Yes
Unlimited Users	–	Yes	Yes	Yes
Threat Alerts	–	Yes	Yes	Yes
Keyword Categories	All	All	All	All
Investigations	–	via Expertise On Demand	40 per year / 10 per quarter	80 per year / 20 per quarter
FireEye Intelligence Portal Access	–	Yes	Yes	Yes
Digital Threat Alert Summaries	–	Yes	Yes	Yes
Self-Serve Keyword Management	–	Yes	Yes	Yes

Figura 5.2: Fonte: "https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/ds-digital-threat-monitoring.pdf"

5.2.3 Research tools

I research tool possono venir utilizzati dagli utenti per cercare informazioni effettuando una ricerca più approfondita e completa.

Zotero

E' un plug-in di Firefox, progettato per aiutare l'utente a salvare le informazioni di citazione per una tesi o un altro documento accademico; è facilmente adattabile alla ricerca nel Deep Web.

Maltego

Maltego è un tool che permette di raccogliere informazioni tramite la consultazione di dati pubblicamente accessibili e raggrupparle in formato grafico. Tramite questo strumento si è in grado di raccogliere informazioni da:

- Siti Web;
- Comunicazioni Web, come nei social network o nei blog;
- Dati pubblici, ad esempio conferenze stampa;
- Osservazioni dirette come foto satellitari o conversazioni radio;
- Professionisti ed accademici, ad esempio conferenze o pubblicazioni scientifiche.

5.3 Strumenti di ricerca

Nel Deep e Dark Web molto spesso non basta effettuare una ricerca dal browser per riuscire a trovare ciò che si vuole; i link sono difficili da ricordare per via della loro complessa sintassi, ad esempio "msydqstlz2kzerdg.onion" è il link per accedere al motore di ricerca Ahmia, e magari l'utente una volta entrato in questo ambiente non conosce i siti nei quali trovare ciò che cerca. Un utente può trovare nella Hidden Wiki, una sorta di Wikipedia ma per i siti del Deep e Dark Web, i link di molti siti di ogni categoria; la versione ufficiale della Hidden Wiki ha un dominio ".onion" e per trovarlo si può utilizzare Pastebin, un'applicazione Web dove chiunque può caricare ciò che vuole sotto forma di testo, ad esempio anche i link di vari siti ".onion". Questi due siti sono la base per un utente alle prime armi che vuole esplorare il Deep Web senza conoscere i link dei vari siti, ma comunque ci sono molti altri strumenti da utilizzare, come ad esempio lo script OnionSearch.

5.3.1 Hidden Wiki

La Hidden Wiki è un sito Web, molto simile a Wikipedia, che fornisce agli utenti i link dei vari servizi nascosti disponibili nella rete Tor; il sito principale è una Web directory di altri siti ".onion". Come servizio nascosto, la Hidden Wiki originale, lavora esclusivamente attraverso lo pseudo-dominio[4] di primo livello ".onion" che può essere raggiunto solo con Tor, ma comunque sono disponibili altre copie non ufficiali del sito nel Surface Web.
E' possibile trovare vari tipi di servizi nascosti, dalla vendita di credenziali delle carte di credito rubate al commercio di armi e droghe, ma ci sono anche servizi nascosti che forniscono servizi non illegali, come ad esempio blog, forum, servizi email e librerie.
Il sito non si assume nessuna responsabilità per ciò che gli utenti caricano al suo interno, per la validità delle informazioni o per il contenuto dei siti esterni alla ad esso.
Ogni utente che carica qualcosa sul sito si prende personalmente la responsabilità del contenuto che inserisce; la Hidden Wiki non verifica o contrassegna i servizi in nessun modo. Qualsiasi utente può contribuire al Wiki, perciò quello che si trova al suo interno non è da considerare veritiero e sicuro al 100%.
La Hidden Wiki è un servizio gratuito, non accetta nessun tipo di pagamento. Se ci si imbatte in un utente che richiede un pagamento per un qualsiasi servizio che riguarda la Hidden Wiki molto probabilmente si tratta di un truffatore.
Dalla sua prima creazione nel 2006 è stata chiusa diverse volte per poi essere sempre rimessa online; attualmente funziona con il semplice scopo di essere una Web directory.

5.3.2 Pastebin

È un'applicazione Web che permette agli utenti di caricare e condividere testi on-line, sia pubblicamente che privatamente, potendo scegliere anche la durata dell'effettiva esistenza del file stesso; l'uso più comune è quello di condividere codice sorgente o informazioni, come ad esempio anche i link dei siti del Deep e Dark Web, che sennò sarebbero difficilmente reperibili.

[4] E' un'etichetta o un nome per una rete di computer che non partecipa al sistema di nomi di dominio ufficiale in tutto il mondo e può anche non partecipare ad Internet, ma può utilizzare una gerarchia di nomi di dominio simile.

Una volta che un file è stato caricato su Pastebin poi potrà essere modificato dagli altri utenti; ogni upload ha un proprio URL che può essere condiviso tramite IRC, forum, o anche nei social.
Ci sono dei simili di Pastebin nel Deep Web, ma bisogna fare molta attenzione quando si visitano questi siti cercando di assicurarsi di essere anonimi e ben protetti. Ad esempio:

DeepPaste

È un sito molto semplice che permette di condividere testi; non verrà mai rimosso o censurato un caricamento ed ogni file pubblico è visibile in un database pubblico. I file invece che sono privati non sono presenti in questo database ma sono visualizzabili solo tramite la ricerca del corretto URL/MD5.
Non è possibile rimuovere un testo pubblico a meno che esso non sia auto-distruttivo, cioè una volta che verrà visualizzato il testo si eliminerà da solo senza lasciare nessuna traccia di esso o del suo contenuto.

5.3.3 OnionSearch

OnionSearch è uno script realizzato in Python3 che ricerca informazioni sul Web attraverso più motori di ricerca ".onion" contemporaneamente. E' possibile installarlo in due modi:

- Con PyPI[5] utilizzando da terminale il comando "pip3 install onionsearch";
- Con GitHub utilizzando da terminale i comandi:

```
git clone https://github.com/megadose/OnionSearch.git
cd OnionSearch/
python3 setup.py install
```

Per poterlo utilizzare è necessario avere Python3, cioè una nuova versione del linguaggio Python; vengono utilizzati 16 motori di ricerca i quali possono trovare informazioni dai domini ".onion", tra questi ci sono anche Ahmia, OnionLand, Not Evil ed HayStack.
È possibile effettuare una ricerca inserendo una stringa ed i possibili comandi messi a disposizione dallo script nel caso li si vogliano utilizzare, sfruttando tutti i motori di ricerca contemporaneamente, ma c'è anche la possibilità di escluderne alcuni dalla ricerca oppure di utilizzarne solamente qualcuno in particolare; oltre alla scelta dei motori di ricerca è possibile mettere un limite alle pagine che ogni motore di ricerca potrà caricare con il comando "–limit" seguito dal numero di pagine.
Di default i risultati delle ricerche verranno scritti in un file CSV alla fine del processo, il quale conterrà determinate colonne: motore di ricerca; nome del link; URL. È possibile personalizzare i dati che verranno scritti nel file di output utilizzando i comandi " –files" e "–field_delimeter". Con il comando "–fields" si possono aggiungere, rimuovere o ordinare diversamente i campi che comporranno il file di output, ad esempio scrivendo "–fields engine link" si avrà un file CSV contenente soltanto i motori di ricerca e gli URL. Mentre con il comando "–fields_delimeter" si può modificare la delimitazione tra i dati nel CSV, che di default è la virgola.

[5]The Python Package Index

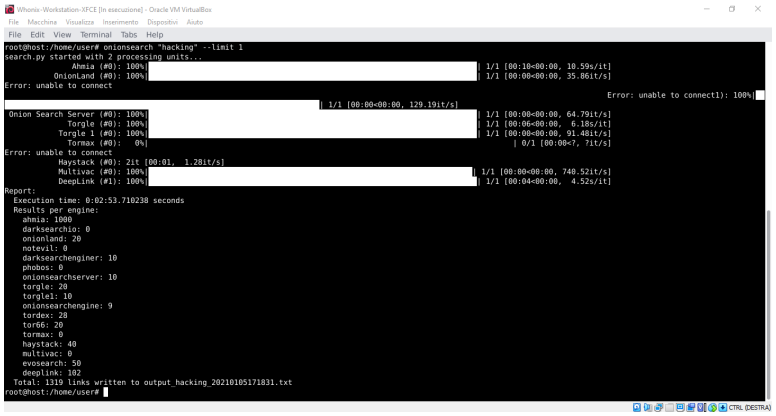

Figura 5.3: Ricerca effettuata con il sistema Operativo Whonix

Il filename di output avrà come titolo di default "output_$DATE_$SEARCH.txt" dove al posto di $DATE ci sarà il tempo corrente ed al posto di $SEARCH ci sarà il primo carattere della stringa utilizzata per la ricerca. Con il comando "–output" è possibile modificare il filename.
Lo script viene avviato con il parametro "mp_units= cpu_count() -1", cioè se la macchina sulla quale viene utilizzato dispone di 4 core, verranno azionate tre scraping functions in parallelo; è possibile forzare il processo e modificare il valore di mp_units e nel caso lo si metta uguale ad uno, di fatto disabilitando la funzione multi-processing, le richieste verranno elaborate in sequenza.

6. Esempi pratici

6.1 Ricerche di determinati oggetti o informazioni

Come visto nel capitolo 5 esistono vari strumenti di ricerca; la ricerca effettuata può essere manuale, cercando personalmente tra i vari siti, oppure può essere effettuata sfruttando un tool o uno script, come OnionSearch, per avere più riscontri in un tempo minore.

Prendiamo come esempio un utente che decide di voler comprare una carta di credito clonata nella rete Tor senza sapere già dove reperirla. Come prima cosa dovrà aprire Tor Browser e cercare dei servizi segreti che forniscano prodotti simili, ad esempio utilizzando Pastebin per conoscere il link Onion della Hidden Wiki, dove può trovare i link di molti servizi segreti tra i quali potrebbero essere presenti alcuni utili alla ricerca dell'utente.
Nel caso l'utente nella Hidden Wiki non trovasse un servizio segreto che disponga di ciò che cerca, un altro metodo sarebbe quello di utilizzare un motore di ricerca del Deep e Dark Web. Ogni motore di ricerca in base ai siti che indicizza può dare un diverso risultato e non sempre si ottengono informazioni adatte a trovare quel che si cerca. Cercare un preciso oggetto, come in questo caso una carta di credito clonata, attraverso varie ricerche in diversi motori di ricerca richiederebbe del tempo poiché Tor browser non fornisce un'elevata velocità di navigazione.
L'utente sfruttando un tool o uno script potrebbe rendere la ricerca meno impegnativa, più breve e godere di un risultato più efficiente; ad esempio utilizzando lo script OnionSearch, del quale è spiegato il funzionamento nel paragrafo 5.3.3, in poco tempo avrebbe un file txt nel quale sono presenti moltissimi link di vari siti che fanno riferimento all'argomento usato per la ricerca.

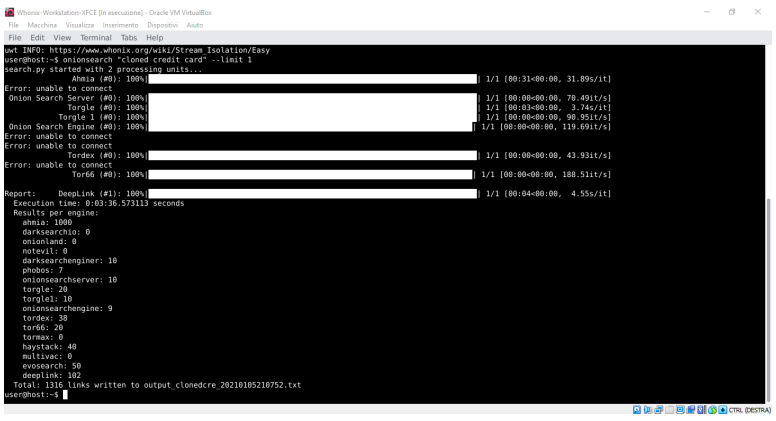

Figura 6.1: Esempio dello script OnionSearch

Come visibile nella figura 6.1 con un tempo di attesa inferiore a 4 minuti si ha come risultato un file contenente 1316 link i quali hanno un riscontro con le keywords specificate. Sfruttando questo script in poco tempo si ottengono una grande quantità di informazioni utili alla ricerca ma poi è compito dell'utente riuscire a trovare un servizio nascosto che effettivamente venda ciò che cerca tra tutti quelli elencati nel file di output.

All'utente dopo aver trovato un servizio nascosto che permette di acquistare ciò che cerca non rimarrà altro che effettuare l'acquisto ed il modo in cui farlo verrà trattato nel prossimo sottocapitolo.

6.2 Come effettuare un acquisto nel Dark Web

Una volta entrati nel mondo del Dark Web è possibile anche effettuare acquisti nei vari siti o Black market presenti in esso.
Come prima cosa l'utente deve creare un proprio wallet[1] di criptovalute poiché tutti le transazioni monetarie vengono effettuate attraverso il loro utilizzo. E' possibile crearlo attraverso delle applicazioni scaricabili nel proprio computer come Electrum Bitcoin Wallet o Monero Wallet, dove Electrum è già presente all'interno dei sistemi operativi Tails e Whonix mentre Monero Wallet è già preinstallato soltanto in Whonix; con questi

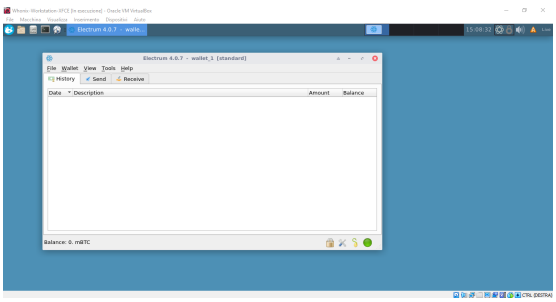

Figura 6.2: Interfaccia iniziale Electrum Wallet Bitcoin su Whonix

due client la creazione e la gestione del proprio wallet sono semplici poiché richiedono pochi dati da inserire e le loro interfacce non sono complicate.
Quando viene creato il wallet viene dato all'utente un Seed, cioè una sequenza di parole, che rappresenta l'unico modo per recuperare il portafoglio nel caso vengano smarrite le credenziali di accesso; viene consigliato di conservarlo in forma cartacea e non in forma digitale poiché se un utente si impossessa del Seed avrà la possibilità di accedere al portafoglio e di conseguenza anche ai fondi monetari presenti in esso.
Un altro modo per creare e gestire il proprio wallet personale è quello di sfruttare i servizi segreti presenti nella rete Tor, come Hidden Wallet o EasyCoin, dove è necessario registrarsi per poter creare il portafoglio ma comunque è una procedura molto rapida e semplice; alcuni di questi servizi segreti offrono anche la possibilità di sfruttare un Bitcoin Mixer. E' possibile comunque creare wallet di criptovalute anche nel Surface Web ma se l'obiettivo è effettuare acquisti nel Dark Web è consigliabile farlo attraverso determinati client o servizi come detto precedentemente.

Dopo aver creato il proprio wallet è necessario comprare delle criptovalute per poter poi effettuare un acquisto; non tutte le criptovalute sono accettate per i pagamenti

[1] Portafoglio

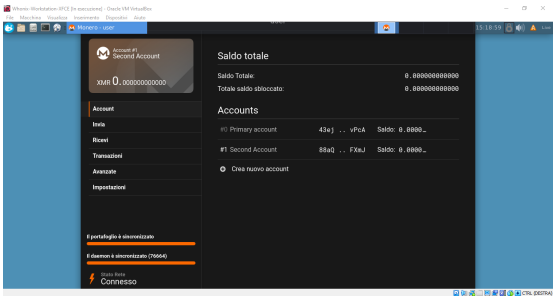

Figura 6.3: Interfaccia Monero Wallet in modalità avanzata su Whonix

e nel caso si compri una valuta che non viene accettata per l'acquisto che si vuole fare non sarà possibile procedere. Il Bitcoin è la valuta più accettata ma anche i Monero spesso e volentieri possono essere usati; in alcuni casi si può ricevere una piccola percentuale di sconto nei Black market se si decide si pagare con i Monero vista la loro predisposizione all'anonimato. Per acquistare criptovalute non è necessario cercare un servizio della rete Onion ma lo si può tranquillamente fare nel Surface Web in quanto è una valuta legale; ad esempio per comprare Bitcoin si può andare nel sito "Bitcoin.org".
Una volta comprata la quantità desiderata l'utente può sfruttare un Bitcoin Mixer per togliere ogni legame tra le criptovalute e se stesso; non è obbligatorio farlo ma garantisce una maggiore sicurezza e quando si vuole comprare qualcosa nel Dark Web è sempre meglio essere il più protetti possibile, considerando il fatto che se si vuole effettuare un acquisto in questo ambiente molto probabilmente si tratta di qualcosa di illegale.
Una volta creato il proprio wallet e comprato la quantità di criptovaluta desiderata l'utente dovrà trovare dove comprare ciò che desidera come spiegato nel capitolo 6.1.
Prendendo come esempio due Black market, Aurora Market e World Market, prima di connettersi alla pagina iniziale è presente una schermata con un captcha[2] che li protegge da attacchi DDoS ed una volta completato si arriva alla schermata dove viene richiesto di effettuare il login per poter entrare nel sito; la registrazione è molto veloce e richiede soltanto di inserire il nome dell'account, la password e di completare un captcha. Una volta registrati si può tornare alla pagina iniziale, effettuare il login ed entrare a tutti gli effetti nel market; l'interfaccia di Aurora Market e di World Market sono differenti ma sono entrambe semplici ed al loro interno sono presenti varie categorie con relative sotto-categorie che differenziano i tipi di prodotti, come ad esempio droghe o servizi di hacking, oppure è possibile ricercare un determinato prodotto se l'utente ha le idee chiare sul ciò che vuole.
Una volta scelto il prodotto è possibile aggiungerlo al carrello per poi procedere all'effettivo ordine; tutte le specifiche dell'ordine come il tipo di pagamento, le valute accettate, i metodi ed i tempi di spedizione variano a seconda del market, del venditore e del tipo di prodotto che si compra.

Effettuare un acquisto in un Black Market è un'azione illegale, poiché lo è anche solo accedere ad essi, e comunque bisogna far molta attenzione dato che il Dark Web è pieno di utenti che non aspettano altro che truffare un utente poco esperto.

[2]Test effettuato per capire se si tratta di un utente o un computer

7. Conclusioni

7.1 Confronto tra Tor, I2P e Freenet

Le tre reti di anonimizzazione più conosciute ed utilizzate sono la rete Tor, I2P e Freenet.
Mettendole a confronto, quali sono i pregi ed i difetti che potrebbero portare un utente a scegliere di usarne una invece di un'altra?

Tor

La rete Tor è una rete di anonimizzazione che ha come scopo quello di garantire ai suoi utenti di navigare in maniera anonima e sicura. Il suo funzionamento è abbastanza semplice, cioè un utente non si collega direttamente al server ma le informazioni passano prima per un circuito composto da alcuni nodi della rete sparsi per tutto il mondo. I nodi conoscono solo determinate informazioni e questo rende più sicura la comunicazione; tutto ciò che passa all'interno del circuito viene crittografato ad eccezione del traffico tra l'ultimo nodo, l'Exit node, ed il server.
Un utente quando decide di utilizzare Tor deve tenere conto dei pro e dei contro riguardanti questa rete.

- Pro:
  - Rispetto ad ogni altra rete dispone della maggior quantità di informazioni e servizi disponibili;
  - Configurazione ed installazione molto semplici;
  - Dispone di un'ottima documentazione e del supporto della community di Tor e da distribuzioni GNU/Linux;
  - Dà agli utenti la possibilità di navigare nel Surface Web;
  - Garantisce basse latenze che aiutano la fluidità della navigazione.

- Contro:
  - Se non si utilizzano contromisure adeguate, la risoluzione dei DNS viene effettuata direttamente dal client, esponendo l'utente a dei rischi;
  - Sono molti i tipi di attacchi che possono essere effettuati verso i client, i server e la rete Tor;
  - E' limitato ai soli protocolli TCP;
  - Usando il protocollo SMTP si corre il rischio di esser presi di mira da spammers.

I2P

I2P nasce come un software libero ed open source con l'obiettivo di offrire una serie di servizi, già configurati e presenti al suo interno, per lo scambio di dati e messaggi, per la navigazione e molto altro. E' interamente strutturato sul peer-to-peer ed è stato creato per garantire anonimato e per combattere la censura.
Similmente a come lavora la rete Tor anche I2P anonimizza la connessione offrendo una navigazione a bassa latenza, ma la differenza principale è la struttura utilizzata per memorizzare le informazioni della rete. Il database del network in I2P è distribuito tra i vari client che compongono la rete e questo permette di offrire un sistema sicuro dagli attacchi provenienti dall'interno del network e da abusi da parte dei gestori.
Come per Tor anche I2P ha i suoi pro ed i suoi contro:

- Pro:
  - E' possibile creare una propria applicazione o piattaforma nel caso non ne sia già disponibile una simile nella rete;
  - Parzialmente distribuito;
  - Fornisce un supporto ai protocolli TCP e UDP;
  - Offre la possibilità di navigare nel Surface Web.
- Contro:
  - Esiste una minore documentazione rispetto alle altre reti;
  - Offre una quantità di contenuti ridotta.

Freenet

La rete Freenet è nata per essere utilizzata come una rete privata a differenza di Tor e I2P, infatti non offre la possibilità di navigare nel Surface Web e questo limita notevolmente la quantità di informazioni di cui dispone, ma comunque al suo interno è possibile trovare vari tipi di servizi come siti Web, forum, blog, chat e tutto il necessario per condividere file e materiali tra gli utenti.
Come I2P anche Freenet utilizza datastore condivisi e permette la condivisione soltanto con client "sicuri" rendendo impossibile accedere al network agli esterni. Come detto precedentemente per I2P e Tor anche Freenet ha i suoi pro e contro:

- Pro:
  - La rete è molto sicura;
  - Sfrutta una tecnologia distribuita;
  - L'utente può scegliere se utilizzare la modalità Opennet o Darknet in base ai propri interessi;
  - La modalità Darknet permette di creare una rete sicura composta soltanto da utenti che si conoscono tra di loro.

- Contro:
  - Non permette di navigare e accedere ai contenuti nel Surface Web;
  - Vista la distribuzione P2P, se un utente è offline nessun altro utente della rete può vedere cosa sta hostando;
  - La navigazione non è molto veloce;
  - Nel caso si utilizzi la modalità Opennet si è vulnerabili a vari attacchi;
  - Utilizzando la modalità Darknet, a discapito di una maggiore sicurezza, si disporrà di una quantità di informazioni e servizi limitati a quelli offerti dagli utenti che ne fanno parte.

7.2 Quale sistema operativo offre le migliori prestazioni?

Come già detto nel capitolo 4 è possibile entrare e navigare nel Deep e Dark Web con i sistemi operativi più comunemente utilizzati, da Windows ad Android, ma oltre a questi sono stati creati dei sistemi orientati al mantenimento della privacy e della sicurezza, il che li rende adatti ad entrare in questo ambiente.
I due sistemi che verranno messi a confronto sono Tails e Whonix, lasciando da parte Subgraph OS poiché non è ancora possibile utilizzare la versione ufficiale essendo in fase di sviluppo.
Sia Tails che Whonix sono Debian-based[1] ed entrambi sfruttano la rete Tor per nascondere l'identità degli utenti, ma forniscono servizi e prestazioni differenti.

Whonix permette di ottenere un'ottima protezione per il proprio indirizzo IP e rende difficile che venga compromesso il DNS; anonimizza anche le sequenze di tasti, le quali rappresentano uno dei modi in cui gli utenti vengono monitorati online.
E' possibile eseguire altre applicazioni in modo anonimo utilizzando Whonix.
Può essere utilizzato come sistema operativo principale ma anche essere avviato tramite l'utilizzo congiunto di due VM[2], con una che lavora come gateway e l'altra come workstation. Con questo metodo la workstation comunica soltanto con il gateway, il quale passa tutte le informazioni ricevute attraverso al rete Tor.
Utilizzare questo sistema operativo presenta alcuni vantaggi e svantaggi:

- Vantaggi:
  - Offre un'eccellente protezione all'identità degli utenti;
  - Permette agli utenti di modificare le impostazioni di sicurezza in base alle loro preferenze;
  - Dispone di molti software tool già configurati.

- Svantaggi:
  - Necessita di un hardware robusto per funzionare al meglio;
  - Il tempo di accensione del sistema e di connessione alla rete Tor è un pò più lungo rispetto a Tails;
  - Utilizzare supporti esterni come USB non è molto semplice;

[1] Basati sulla distribuzione Linux Debian
[2] Virtual Machine

  - Nel caso non si vogliano utilizzare le VM ma si voglia mettere Whonix come sistema operativo principale del computer, l'utente dovrà effettuare una configurazione più complicata.

Tails è stato progettato per proteggere l'identità degli utenti ed aiutarli a rimanere anonimi. A differenza di Whonix non necessita di utilizzare due VM contemporaneamente ma essendo una live distro può essere messo su una chiavetta USB o su un DVD scrivibile ed essere avviato direttamente da lì collegando la chiavetta/DVD ad un qualsiasi computer.
Di default Tails è progettato per proteggere l'anonimato degli utenti anche nel caso venga rubata la chiavetta o il DVD dov'è installato il sistema operativo o se il computer è compromesso poiché non lascia nessuna traccia. Come Whonix anche Tails ha i suoi vantaggi e svantaggi:

- Vantaggi:
  - Può essere avviato da ogni computer essendo compatibile con Windows, Linux e macOS;
  - E' molto semplice da utilizzare;
  - Non richiede un hardware particolarmente potente;
  - Non lascia nessuna traccia di qualsiasi attività poiché non utilizza il disco fisso del computer per memorizzare le informazioni ma la RAM[3]. I dati salvati nella RAM vengono totalmente eliminati quando il computer viene spento.
  - Permette la creazione di un volume persistente nel caso l'utente decida di non voler far cancellare alcune informazioni, configurazioni o file installati.

- Svantaggi:
  - Non è adatto ad essere utilizzato come sistema operativo permanente;
  - Limitate possibilità di personalizzazione delle impostazione a differenza di Whonix;
  - Per essere installato in una chiavetta USB o su un DVD scrivile necessita dell'utilizzo di un altro software;
  - Il computer dove si vuole avviare Tails deve avere la possibilità di utilizzare una chiavetta USB o un DVD ed avere un processore compatibile con l'architettura 64-bit x86-64;
  - Nel caso venga rubato il dispositivo dov'è installato il sistema e che l'utente aveva creato un volume persistente, quest'ultimo sarà visibile;
  - L'installazione di nuovi programmi non è semplice.

Le differenze principali tra questi due sistemi operativi è che Whonix può essere installato sul computer e funzionare con il sistema operativo corrente oppure essere avviato tramite l'utilizzo di due VM insieme, mentre Tails funziona principalmente come live distro e quindi non viene installato sul computer.
Con Tails si perde tutto ciò che viene fatto in ogni sessione, come ad esempio la cronologia di navigazione o i file scaricati, poiché una volta terminata viene tutto eliminato a

[3]Memoria volatile

meno che non si utilizzi un volume persistente che però potrebbe rivelarsi un problema per la sicurezza dell'utente; con Whonix non si perde ciò che viene fatto durante una sessione, a meno che non si utilizzi la live mode, e questo può essere un vantaggio ma rende anche possibile ad un utente esterno di conoscere senza difficoltà le attività svolte se riesce ad accedere al sistema.
Un utente se ha come interesse quello di avere un sistema operativo per l'anonimato a lungo termine la scelta migliore è Whonix, mentre se vuole una soluzione a breve termine la scelta migliore è Tails.

Caratteristiche	Tails	Whonix
Facile da usare	✓	
Sicurezza fisica migliore	✓	
Sicurezza e privacy più avanzata		✓
Velocità di avvio	✓	
Portabilità	✓	
Anonimato a lungo termine		✓
Anonimato a breve termine	✓	

Tabella 7.1: Fonte: "https://consumergearguide.com/whonix-vs-tails/"

Si possono considerare entrambi ottimi sistemi operativi per quanto riguarda la sicurezza e l'anonimato.
Tails è più veloce, fornisce una sicurezza più robusta nel caso di infrazioni fisiche del sistema e lo si può avviare anche quando ci si sposta essendo possibile utilizzare un qualsiasi computer; Whonix non è semplicissimo da utilizzare, sia che si usino le VM sia che venga utilizzato come sistema operativo principale, ma offre una protezione per l'utente più sofisticata.
Questi due sistemi operativi con i loro pregi ed i loro difetti hanno lo stesso obiettivo, cioè garantire all'utente un sistema sicuro.
La scelta sul quale utilizzare tra i due varia in base alle esigenze ed alle preferenze di chi li utilizza in un determinato momento.

7.3 Sviluppi futuri

Il Deep Web è un mondo estremamente ampio ed occupa circa il 90% di tutto Internet. Vista la sua natura e le sue caratteristiche che lo rendono completamente diverso dalla porzione di Web che tutti comunemente usiamo, i contenuti ed i servizi che possono essere trovati al suo interno sono privi di censura e possono variare da qualsiasi genere, dalle cose legali come ad esempio un forum dove si parla di pubblicazioni scientifiche o un servizio di posta elettronica a quelle illegali tipo la vendita di droghe o la vendita di informazioni riservate di un'azienda.
Considerati i mezzi ed il tempo a disposizione limitato non sarebbe stato possibile effettuare una ricerca molto più approfondita o prove più concrete e consistenti.
Alcuni tra i possibili lavori o miglioramenti da effettuare sono:

- Utilizzare tool più potenti anche nelle loro versioni a pagamento visto il fatto che nelle versioni gratuite i servizi offerti sono minori e meno approfonditi;
- Effettuare una ricerca più approfondita riguardante i vari aspetti del Dark Web ricavando una quantità di informazioni e di riscontri maggiore;
- Creare un servizio segreto nella rete Tor, un sito in Freenet ed un'applicazione in I2P e confrontare tutti gli aspetti riguardanti la creazione e la gestione di essi;
- Diventare un nodo della rete Tor così da poter studiare più da vicino le meccaniche della rete stessa.

Bibliografia

[Acc] *Accedere a Freenet*. URL: http://www.astropatrol2450dc.it/pagineguida/freenet.html.

[Adm] Admin. *Sistema operativo Subgraph: un nuovo sistema operativo incentrato su sicurezza e privacy*. URL: https://it.boxxweb.com/subgraph-os-un-nuevo-sistema-operativo-enfocado-la-seguridad-y-privacidad.

[Aie18] Enrico_Cambiaso-Ivan_Vaccari-Luca_Patti-Maurizio Aiello. «Darknet Security: A Categorization of Attacks to the Tor Network». In: (2018).

[Ake] Feranmi Akeredolu. *Top 10 Best Deep Web, Dark Web and Darknet Search Engines in 2020*. URL: https://darkwebjournal.com/best-deep-web-dark-web-and-darknet-search-engines/.

[Ano] AnoNet. *AnoNet*. URL: http://anonet.org/.

[Ant] Antonio. *Le criptovalute sono anonime? Facciamo un po' di chiarezza sull'anonimato di bitcoin e delle principali altcoin*. URL: https://valutevirtuali.com/le-criptovalute-sono-anonime-facciamo-un-po-di-chiarezza-sullanonimato-di-bitcoin-e-delle-principali-altcoin/.

[Ara] Salvatore Aranzulla. *Come usare Tor*. URL: https://www.aranzulla.it/come-usare-tor-1026046.html#chapter1.

[buc] bucap.it. *SaaS: ecco cosa significa software as a service e quali sono i vantaggi*. URL: https://www.bucap.it/news/approfondimenti-tematici/software-gestione-documentale-aziendale/saas-ecco-cosa-significa-software-as-a-service-quali-sono-vantaggi.htm#:~:text=Con\%20Software\%20as\%20a\%20Service,alcun\%20download\%20applicativo\%20o\%20istallazione..

[Bug] *Che cos'è un programma bounty bug e perchè ogni organizzazione ne ha bisogno*. URL: https://security.stilidivita.com/2765/che-cose-un-programma-bounty-bug-e-perche-ogni-organizzazione-ne-ha-bisogno.html.

[Coo] Stephen Cooper. *10 Best Dark Web Monitoring Tools for Network Admins*. URL: https://www.comparitech.com/net-admin/best-dark-web-monitoring-tools/.

[Dea] Dean. *Dark Markets: How to Buy Things from the Deep Web's Black Markets*. URL: https://cryptorials.io/dark-markets-how-to-buy-things-from-the-deep-webs-black-markets/.

[Fai] Andrea Faion. *Come installare Tor in Windonws 10*. URL: https://www.andreafaion.com/come-installare-tor-windows-10/.

[Fir] FireEye. *Digital Threat Monitoring*. URL: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/ds-digital-threat-monitoring.pdf.

[Fre] Freenet. *Cos'è Freenet*. URL: https://freenetproject.org/#whatsfreenet.

[Gag] Cristina Gagliarducci. *Criptovalute: cosa sono e come funzionano?* URL: https://www.money.it/Criptovalute-cosa-sono-come-funzionano.

[htta] https://deepweblinks.net. *Deep Web Pastebin (Onion Links 2020)*. URL: https://deepweblinks.net/pastebin/.

[httb] https://deepweblinks.net. *The hidden wiki (Link 2020)*. URL: https://deepweblinks.net/the-hidden-wiki/.

[httc] https://subgraph.com/. *Subgraph*. URL: https://subgraph.com/.

[httd] https://tails.boum.org/index.it.html. *Tails*. URL: https://tails.boum.org/index.it.html.

[htte] https://www.grsecurity.com/. *grsecurity*. URL: https://www.grsecurity.com/.

[httf] https://www.whonix.org/. *Whonix*. URL: https://www.whonix.org/.

[I2p] URL: https://geti2p.net/.

[Ita] AnoNet Italia. *Cos'è AnoNet*. URL: https://anonetitalia.wordpress.com/2009/04/01/what/.

[ItB] ItBookMac. *Come usare TOR su iPhone e iPad con Onion Browser*. URL: https://itbookmac.com/come-usare-tor-su-iphone-e-ipad-con-onion-browser/.

[Izz] Stefano Izzo. *Pastebin : a cosa serve e come funziona*. URL: https://www.guide-informatica.com/pastebin-cosa-serve-e-come-funziona/.

[Lor] Marco Maria Lorusso. *Deep Web cos'è, come entrare e cosa si rischia*. URL: https://www.techcompany360.it/tech-lab/deep-web-cose-come-entrare-e-cosa-si-rischia/.

[McK] Dave McKay. *How to Install and Use the Tor Browser on Linux*. URL: https://www.howtogeek.com/423866/how-to-install-and-use-the-tor-browser-on-linux/.

[Meg] Megadose. *OnionSearch*. URL: https://github.com/megadose/OnionSearch.

[Mys] Myshadow.org. *Trackography*. URL: https://trackography.org/.

[Nor] NormShield. *Deep Web and Black Market*. URL: https://normshield.com/deep-web-and-black-market/.

[Nova] Matteo Novelli. *Dark Web: cosa si rischia a navigare nell'internet sommerso*. URL: https://www.money.it/Dark-Web-cosa-si-rischia-pericoli-internet-segreto.

[Novb] Stefano Novelli. *TOR vs I2P vs Freenet: Qual è il miglior network per navigare anonimi?* URL: https://www.inforge.net/forum/threads/tor-vs-i2p-vs-freenet-qual-\%C3\%A8-il-miglior-network-per-navigare-anonimi.439605/.

[Pin] Delwyn Pinto. *What's the difference between surface web, deep web and dark web?* URL: https://www.techworm.net/2017/06/whats-difference-surface-web-deep-web-dark-web.html.

[Pip] Vito Pipitone. *Come funziona I2P.* URL: https://wizblog.it/come-funziona-i2p.

[Proa] The Tor Project. URL: https://gitlab.torproject.org/.

[Prob] The Tor Project. URL: https://community.torproject.org/relay/community-resources/.

[Proc] Tor Project. *In che modo Tor differisce da altri proxy?* URL: https://support.torproject.org/it/#how-is-tor-different-from-other-proxies.

[Q] Simone Q. *Tutorial Maltego con OSINT os.* URL: https://www.html.it/articoli/osint-con-maltego/#:~:text=Maltego\%20\%C3\%A8\%20un\%20tool\%20sviluppato,Siti\%20web.

[R.] Claudio R. *Come Accedere Al Dark (Deep Web) Guida Completa.* URL: https://anonymster.com/it/come-accedere-dark-deep-web-guida/.

[Raf] Dan Rafter. *Is the dark web illegal?* URL: https://us.norton.com/internetsecurity-privacy-is-the-dark-web-illegal.html.

[Res] *Deep Web Research Tools.* URL: http://deep-web.org/how-to-research/deep-web-research-tools/.

[Sar] Chris Sar. *What is a High Anonymity Proxy or Elite Proxy?* URL: https://hide-ip-proxy.com/what-is-high-anonymity-proxy-elite/.

[Sjo] Stu Sjouwerman. *What is the difference between the Surface Web, The Deep Web and the Dark Web?* URL: https://blog.knowbe4.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web.

[Smi] Chris Smith. *The best VPN for the deep web.* URL: https://knowtechie.com/the-best-vpn-for-the-deep-web/.

[Sto] Alexander Stone. *8 Best Deep Web, Dark Web hidden Search Engines of 2020.* URL: https://medium.com/@alexanderstonec/8-best-deep-web-dark-web-hidden-search-engines-of-2020-9b528419f2a2.

[Tea] Editorial Team. *Whonix vs. Tails: Which is Better?* URL: https://consumergearguide.com/whonix-vs-tails/.

[Tec] Techlazy.com. *10 Deep Web Browsers for Access the Deep Web.* URL: https://www.techlazy.com/deep-web-browsers/.

[The] TheDarkWebLInks. *Darknet Market List 2020 – World Market — Dark Market — Torrez Market.* URL: https://www.thedarkweblinks.com/darknet-market-list/.

[Tor] .

[tor] torproject.org. *Posso usare Tor su un dispositivo Android?* URL: https://support.torproject.org/it/tormobile/tormobile-1/.

[Wal] Jack Wallen. *How to use the Whonix advanced security and privacy distribution.* URL: https://www.techrepublic.com/article/how-to-use-the-whonix-advanced-security-and-privacy-distribution/.

[Who] Whonix. *Frequently Asked Questions - Whonix ™ FAQ*. URL: https://www.whonix.org/wiki/FAQ.

[Wika] Wikimedia. URL: https://upload.wikimedia.org/wikipedia/commons/thumb/1/1f/Deepweb_graphical_representation.svg/1200px-Deepweb_graphical_representation.svg.png.

[Wikb] Wikipedia. *AnoNet*. URL: https://en.wikipedia.org/wiki/AnoNet.

[Wikc] Wikipedia. *AppArmor*. URL: https://it.wikipedia.org/wiki/AppArmor.

[Wikd] Wikipedia. *Border Gateway Procotol*. URL: https://it.wikipedia.org/wiki/Border_Gateway_Protocol.

[Wike] Wikipedia. *Darknet*. URL: https://it.wikipedia.org/wiki/Darknet.

[Wikf] Wikipedia. *Distribuzione Linux*. URL: https://it.wikipedia.org/wiki/Distribuzione_Linux.

[Wikg] Wikipedia. *GNUnet*. URL: https://it.wikipedia.org/wiki/GNUnet#cite_note-3.

[Wikh] Wikipedia. *PaX*. URL: https://en.wikipedia.org/wiki/PaX.

[Wiki] Wikipedia. *Proxy*. URL: https://it.wikipedia.org/wiki/Proxy.

[Wikj] Wikipedia. *StealthNet*. URL: https://it.wikipedia.org/wiki/StealthNet.

[Wikk] Wikipedia. *The Hidden Wiki*. URL: https://it.wikipedia.org/wiki/The_Hidden_Wiki.

[Wikl] Wikipedia. *Tor(software*. URL: https://it.wikipedia.org/wiki/Tor_\%28software\%29.

[Wikm] Wikipedia. *Whonix*. URL: https://it.wikipedia.org/wiki/Whonix.

Ringraziamenti

Ringrazio il Prof. Fausto Marcantoni che mi ha seguito ed aiutato durante tutto lo sviluppo della tesi.
Un ringraziamento speciale va alla mia famiglia ed ai miei amici che mi hanno sostenuto e mi sono stati accanto durante tutto questo percorso, sia dal punto di vista accademico sia nella vita di tutti i giorni, permettendomi di arrivare a questo prezioso traguardo.