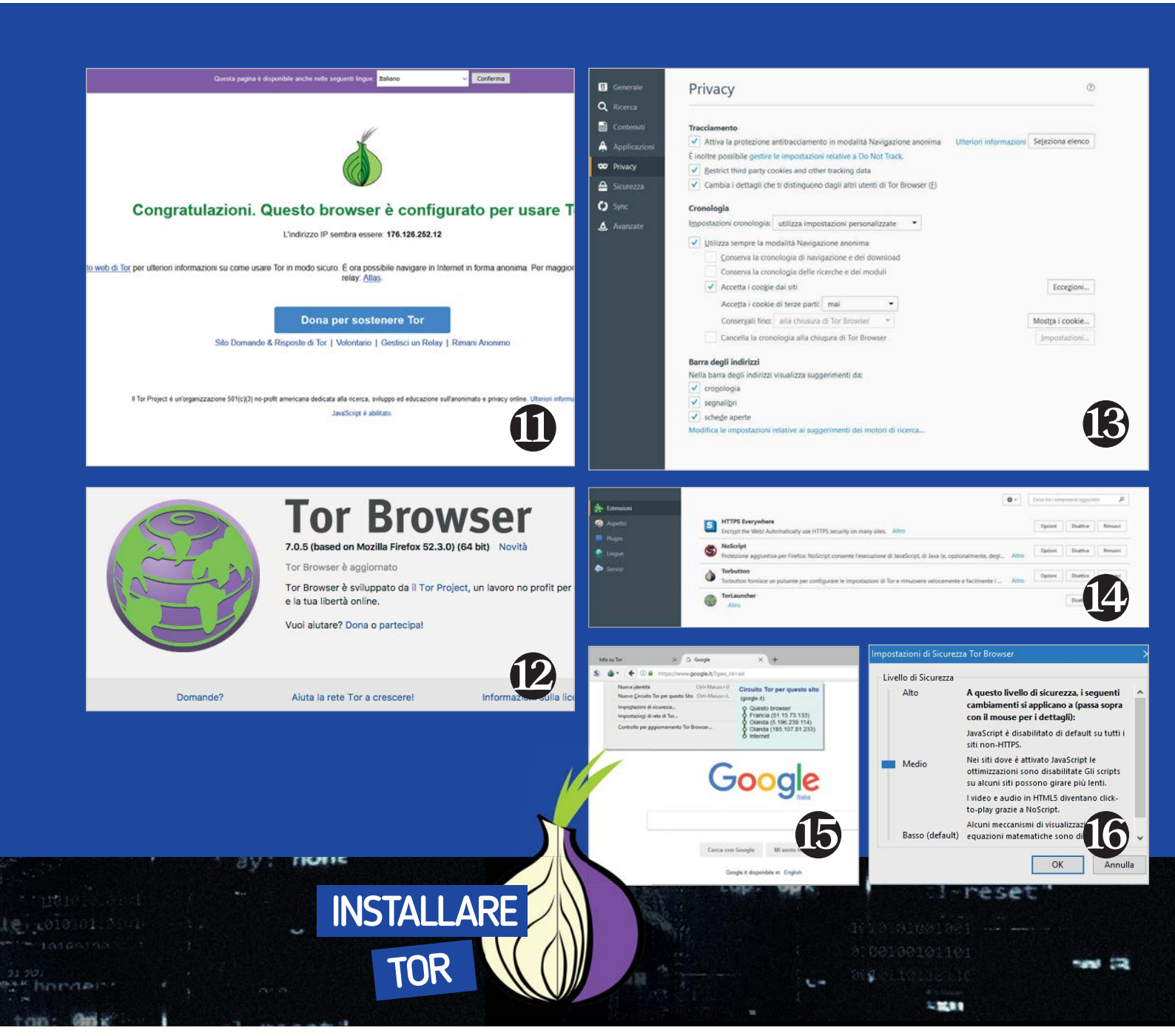


sicurezza riducendo al minimo la superficie di attacco e quindi la possibilità che l'indirizzo IP reale dell'utente venga smascherato, il team di Tor suggerisce tra l'altro di non usare un client BitTorrent facendolo passare dalla darknet, non installare o abilitare plug-in esterni sul Tor Browser, usare sempre la versione https di un sito Web laddove disponibile e di non aprire documenti scaricati tramite Tor (specialmente file *.doc* e *.pdf*) mentre si è ancora online.

Tor non è una rete ottimizzata per le prestazioni, quindi l'esperienza di navigazione può variare anche molto e magari richiedere la selezione di un nuovo circuito se un sito (pubblico o nascosto che sia) non vuole proprio saperne di caricarsi. La darknet di Tor supporta tutti i flussi di rete basati su protocolli Tcp e socks, quindi la navigazione Web è solo uno degli strumenti di comunicazione anonima a disposizione del pubblico. Fra i tool progettati per sfruttare Tor segnaliamo *OnionShare* (condivisione file), *Tor Messenger*, *TorChat*, *Ricochet* (messaggistica istantanea), *Mailpile* (client di posta elettronica), *ProtonMail* (Webmail). *Tails*, sistema operativo open source basato su kernel Linux, è preconfigurato per ridirigere tutto il traffico di rete attraverso la rete di Tor. In tutti questi casi lasciamo all'utente il piacere della scoperta e della sperimentazione.

Sicurezza: il team di Tor suggerisce di non usare un client BitTorrent facendolo passare dalla darknet

PER COSA È UTILE TOR

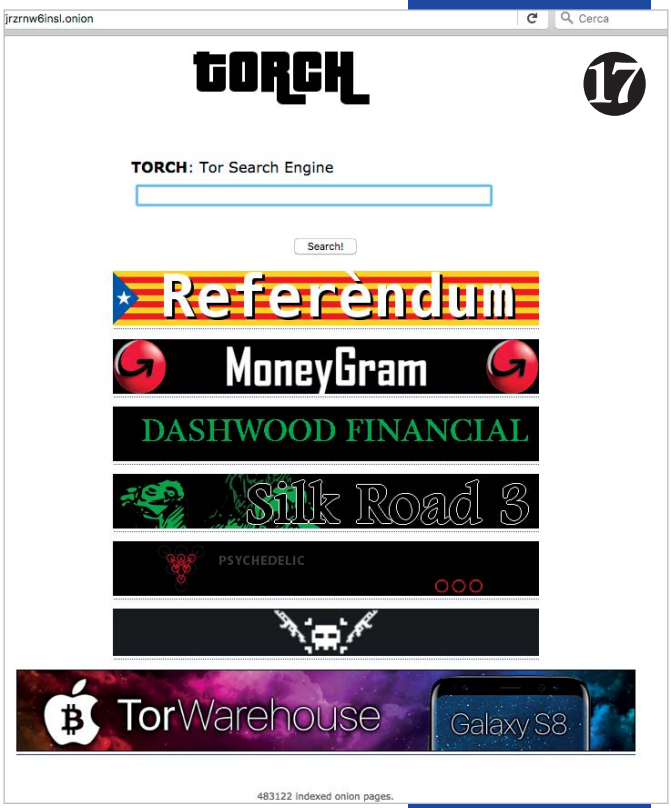
Come spiegato nei paragrafi precedenti, Tor è una rete pensata prima di tutto per difendere l'anonimato dei sistemi client connessi a Internet, mentre la darknet è utile a difendere anche l'anonimato dei server nascosti dietro un dominio .onion. La ragionevole garanzia di accesso anonimo al Web in chiaro che Tor offre è ovviamente utilissima per gli utenti più interessati alla privacy in rete, ma può anche essere uno strumento importante se ci si vuole difendere dall'advertising più invasivo, dai provider di rete e servizi Web impegnati a raccogliere dati sulle nostri abitudini di navigazione da rivendere alle società di marketing, dai siti Web che tengono accuratamente traccia di quello che l'utente fa on-line per vendergli prodotti o tracciarne un profilo da archiviare a uso futuro.
La darknet può essere uno strumento utilissimo nelle mani dei genitori più coscienziosi e tecnologicamente consapevoli, perché l'indirizzo di rete (IP) è sempre più importante nella vita dei giovani connessi a Internet e può essere usato da malintenzionati per esporre anche l'indirizzo di casa o quantomeno la zona di residenza: camuffare efficacemente il primo permette di tenere al sicuro le informazioni sul secondo. Tor può essere un compagno di viaggio indispensabile se si decide di visitare uno di quei paesi attivi nella censura delle comunicazioni telematiche come l'Egitto, dove l'uso della darknet – magari tramite un relay ponte nel caso in cui la directory pubblica dei nodi di entrata fosse bloccata dall'Internet service provider locale – garantisce un accesso a Internet trasparente e non soggetto ai controlli di un regime poco sensibile ai diritti umani.
La privacy della darknet può rappresentare uno scudo per la serenità mentale prima che per la difesa dell'identità digitale di quegli utenti interessati, per qualsivoglia motivo di natura personale, professionale o altro, ad approfondire e a fare ricerche su argomenti scabrosi, imbarazzanti o poco allineati con la morale comune come l'AIDS e le altre malattie infettive trasmesse per via sessuale, metodi contraccettivi o di interruzione della gravidanza, sette religiose o millenariste, droghe ricreative o allucinogene e via elencando. La fantasia e le esigenze personali di ciascuno sono davvero l'unico limite imposto alle possibilità di utilizzo della rete anonimizzatrice di Tor.

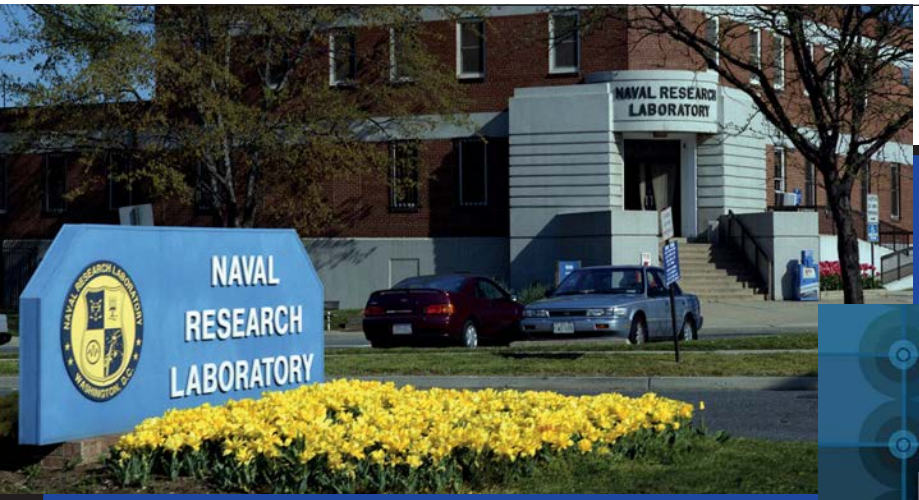
Quando si passa dalla clearnet ai siti .onion la questione si complica, e non solo perché la darknet o il dark Web vengono costantemente additati come il luogo in cui si commettono i peggiori crimini informatici e non. Intervenendo all'ultima conferenza *DEF CON* di Las Vegas, Roger Dingledine ha provato a ridimensionare le voci su Tor fornendo un po' di dati aggiornati: gli utenti che ogni giorno accedono alla darknet sono stimabili in più di due milioni, e solo una piccola porzione del traffico totale (1 gigabit o il 3%) è riconducibile ai servizi .onion. La darknet inaccessibile si trova ancora allo stadio di un "giocattolo" tecnologico, sostiene Dingledine, e tra i server controllati da criminali, botnet o malintenzionati una ricerca di *Tiberium labs* e altri ha identificato circa 7.000 siti onion dotati di una qualche utilità per l'utente finale. "Sostanzialmente non esiste alcun dark web", dice Dingledine, o comunque si tratta di poche pagine che per di più (anche se questo lo sviluppatore non lo dice) sono generalmente gestite da amministratori poco professionali e tendono a non reggere il traffico in entrata, esporre le identità degli utenti registrati o peggio

TOR
UN PO' DI STORIA

Come già era successo decenni addietro per Arpanet, l'antesignano di quella che sarebbe poi diventata Internet, Tor è nato come progetto sponsorizzato, finanziato e voluto dalle autorità militari statunitensi. Il principio alla base della darknet, l'*onion routing*, è nato negli anni '90 presso i laboratori di ricerca della Marina Militare americana *(United States Naval Research Laboratory)* a opera del matematico Paul Syverson e degli ingegneri informatici Michael G. Reed e David Goldschlag; come già con Arpanet, anche in questo caso i militari erano alla ricerca di un sistema in grado di proteggere le comunicazioni on-line delle agenzie di intelligence.

Dalla fase progettuale si è poi passati a quella pratica con il coinvolgimento di Roger Dingledine e Nick Mathewson, che hanno rilasciato la versione *alpha* del "*Progetto TOR*" nel settembre del 2002. Due anni dopo Dingledine e Mathewson hanno presentato la "seconda generazione" della rete a cipolla durante il tredicesimo





Il principio alla base della darknet, l'*onion routing*, è nato negli anni '90 presso i laboratori di ricerca della Marina Militare americana (*United States Naval Research Laboratory*)

xxxxxxx A quel punto sono arrivati i finanziamenti pro-bono di Electronic Frontier Foundation xxxx

Simposio sulla sicurezza USENIX, e in quello stesso anno i laboratori della Marina hanno distribuito il codice di Tor sotto licenza gratuita.

A quel punto sono arrivati i finanziamenti pro-bono di *Electronic Frontier Foundation*, mentre Dingledine, Mathewson e altri hanno fondato (nel 2006) l'organizzazione no-profit "The Tor Project". Nei primi anni i finanziamenti sono arrivati da EFF, organizzazioni per i diritti civili (inclusa Human Rights Watch), società private (Google) e governo degli Stati Uniti. In effetti, a tutt'oggi le autorità federali di Washington sono responsabili della stragrande maggioranza dei fondi che tengono in piedi il Progetto Tor accanto ai finanziamenti di organizzazioni non governative (Ong), aziende esterne e donazioni di privati cittadini. Negli ultimi tempi il team di Tor ha passato un momento burrascoso per una brutta storia di abusi sessuali che ha coinvolto Jacob Appelbaum, e a luglio dell'anno scorso il consiglio di gestione si è dimesso in blocco lasciando il posto a una nuova amministrazione composta da esperti legali, informatici e in crittografia come Matt Blaze, Cindy Cohn e Bruce Schneier.

ancora a prestare il fianco allo smascheramento dell'IP reale a causa delle vulnerabilità di sicurezza. Tenendo bene a mente le considerazioni di Dingledine, che di Tor è uno dei creatori originari, quello che segue è un breve elenco di quanto c'è di interessante da fare e da esplorare sulla rete a cipolla senza dover necessariamente infrangere la legge:

➜**Ricerca Web e directory**. 17 Google non indicizza i servizi .onion, ma all'interno di Tor sono comunque disponibili alcuni motori di ricerca in grado di facilitare l'accesso ai server nascosti. Siti come *TORCH* (*http://xmh57jrzrnw6insl.onion/*) e *AHMIA* (*http://msydqstlz2kzerdg.onion/*, o *https://ahmia.fi/* sulla clearnet) scandagliano i contenuti della darknet con i rispettivi crawler, anche se l'esperienza di utilizzo tende a essere molto diversa da quella super-efficiente, personalizzata e performante a cui ci ha abituato l'onnipresente search di Mountain View. Il motore di ricerca sulla clearnet *DuckDuckGo* offre un sito onion (*https://3g2upl4pq6kufc4m.onion/*) come ulteriore strumento di difesa contro il tracciamento, mentre il motore di ricerca torrent *The Pirate Bay* mette a disposizione un sito onion (*http://uj3wazyk5u4hnvtk.onion/*) capace di resistere a qualsiasi tentativo di censura.

Google non indicizza i servizi .onion, ma all'interno di Tor sono comunque disponibili alcuni motori di ricerca

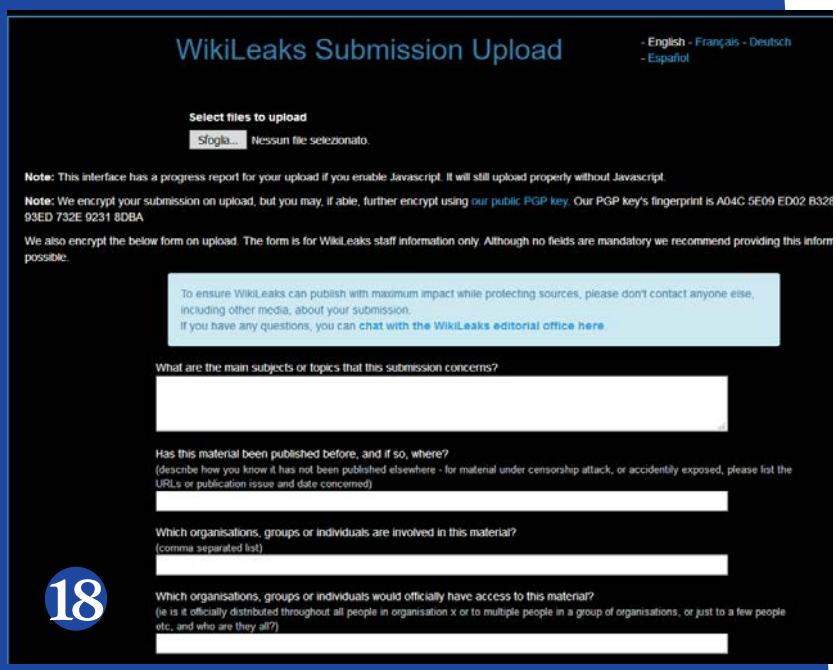
Su Tor esistono anche directory di servizi onion dai contenuti moderati come *The Hidden Wiki* e *TorLinks*, siti che possono agire da punti di accesso ai contenuti meno problematici della darknet. Il lettore è invitato a cercare on-line i rispettivi siti .onion ed è in ogni caso avvisato: la navigazione tra i suddetti link e tutte le eventuali conseguenze legali derivanti sono una sua esclusiva responsabilità.

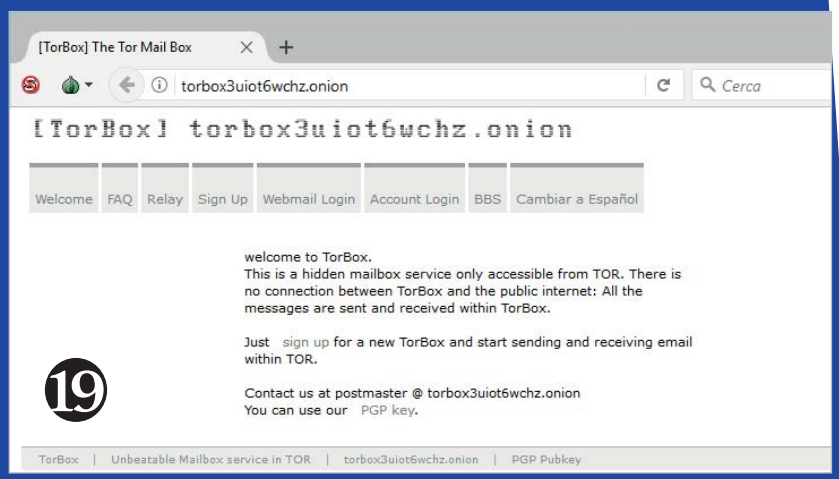
➜**Social networking**. Tre anni fa Facebook ha deciso di aprire un sito .onion sperimentale (*https://facebookcorewwwi.onion/*), sebbene in questo caso "anonimato" sia un concetto del tutto fuori luogo visto che il social network di Mark Zuckerberg è basato sulla corrispondenza tra identità digitale e identità reale dell'utente. Accedere a Facebook da Tor ha però il vantaggio di rendere il sito raggiungibile anche nei paesi in cui esso è ufficialmente censurato. Beninteso, quando tale accesso funziona: le caratteristiche proprie delle comunicazioni sulla rete a cipolla vengono spesso interpretate da Facebook come un tentativo di attacco da parte di malintenzionati, quindi la sola operazione di login via Tor potrebbe risultare fin troppo problematica per l'utente comune. Stando a quanto comunica la società, oggi più di un milione di persone usa Facebook accedendo al sito nascosto di Tor.

➜**Attivismo digitale**. 18 Avete bisogno di contattare in forma anonima i mezzi di comunicazione? Vi è capitato tra le mani del materiale altamente compromettente per un personaggio pubblico e volete farne partecipe l'opinione pubblica senza rischiare conseguenze legali per voi e la vostra famiglia? Tor è in questo senso lo strumento ideale, anche se purtroppo le varie piattaforme disponibili per le "delazioni" (whistleblowing

in inglese) non parlano ancora italiano: *Wikileaks*, l'organizzazione no-profit che ha inguaiato (tra gli altri) Hillary Clinton pubblicando le e-mail del Comitato Democratico durante le ultime elezioni presidenziali, ha a disposizione un sito nascosto (*http://wlupld3ptjvsgwqw.onion/wlupload.en.html*) a cui inviare documenti e altri file di natura confidenziale, mentre la piattaforma *SecureDrop* pubblica una directory degli hidden service (*https://securedrop.org/directory*) a disposizione di testate di informazione internazionali del calibro di The Guardian, ProPublica, Associated Press, Forbes, The Washington Post e molti altri. *Riseup*, un collettivo di attivisti nato a Seattle nel 1999, offre l'accesso a tutti i suoi servizi di comunicazione (e-mail, chat, VPN) tramite hidden service (*https://riseup.net/it/security/network-security/tor#riseups-tor-hidden-services*).

➜Posta elettronica. 19 Spesso e volentieri comunicare in rete significa inviare e ricevere e-mail, e anche in questo senso Tor offre notevoli possibilità di sperimentazione: *ProtonMail* (*https://protonirockerxow.onion*) è una Webmail con cifratura end-to-end e residenza in Svizzera, al riparo delle giurisdizioni europea e americana; il servizio offre





QUANDO TOR LO USANO I CATTIVI

L'anonimato garantito da Tor esercita un'attrattiva quasi fatale sui criminali, e le cronache degli ultimi anni sono piene di casi in cui aspiranti "boss" del cyber-crimine hanno costruito piccoli imperi nella darknet per poi dover fare i conti con le agenzie di investigazione di tutto il mondo e le loro tecniche di indagine più o meno avanzate tecnologicamente. Qualche esempio tra i più eclatanti in ordine cronologico:

2011 ➜ *Freedom Hosting*, allora il servizio di hosting per siti nascosti più esteso di Tor, viene preso di mira dagli *hacktivisti* di Anonymous per aver fornito i server a *Lolita City*, sito contenente milioni di immagini e video di natura pedopornografica. Un attacco di *SQL injection* porta alla pubblicazione della lista dei membri del sito, mentre una vulnerabilità del browser Firefox viene sfruttata dall'FBI per identificare il proprietario dell'hosting (Eric Eoin Marques) e chiederne l'estradizione negli Stati Uniti.

Tor e il Web filtrato non sono tecnologie di per sé "malvagie"

account gratuiti e a pagamento ma richiede la registrazione e il login tramite connessione cifrata (https) sulla Clearnet. *TorBox* (*http://torbox3uiot6wchz.onion/*) è invece una mailbox accessibile esclusivamente tramite Tor, senza passaggi intermedi sul Web pubblico; *TorGuerrillaMail* (*http://www.grrmailb3fxpjbwm.onion/*) è la versione Tor di Guerrilla Mail, servizio di e-mail usa e getta che non richiede registrazione e permette di ricevere messaggi per 60 minuti. È possibile consultare una lista dei tanti servizi e-mail disponibili tramite Tor sulla community di Reddit (*https://www.reddit.com/r/emailprivacy/wiki/index#wiki_tor_accessible_onion_email_providers*).

CONCLUSIONI

In un post pubblicato di recente sul blog corporate ufficiale di *McAfee*, la storica società di sicurezza ha definito il dark Web come "la parte criptata di Internet in cui hanno luogo attività illegali", un "posto spregevole" da cui gli utenti farebbero bene a stare alla larga per non incappare in vendite di droga e armi da fuoco illegali, assassini mercenari, pornografia infantile e video di "persone che vengono ferite o violentate" facilmente accessibili per il download.
La versione del dark Web proposta da McAfee è in effetti molto fedele a quella che viene ripetuta quasi sempre a mena-dito da chi il dark Web non lo ha evidentemente visto molto da vicino. Certo, di contenuti illegali sulla darknet di Tor ce ne sono un bel po', ma se si prova a usare il Tor Browser per più di qualche minuto ci si rende conto che la facilità di accesso di cui parla McAfee è in realtà inesistente. Una parte significativa dei siti "cattivi" del dark Web funzionano male o non funziona affatto per buona parte del tempo, e per quelli che pretendono di offrire un servizio "premium" occorre sborsare un contributo economico in Bitcoin o altre monete virtuali. Persino accedere ai siti della clearnet può essere spesso un'esperienza frustrante.
In pratica la possibilità che l'utente comune si trovi ad avere a che fare con il peggio del (dark) Web in via del tutto accidentale è sostanzialmente inesistente, e chi è alla ricerca di quei tipi di contenuti illegali che secondo McAfee abbondano sulla darknet li cercherebbe (e probabilmente li cerca) attivamente anche fuori dalla rete nascosta. Tor e il Web filtrato dagli strati della rete a cipolla non hanno il potere di "corrompere" alcuno e possono essere tranquillamente usati da chiunque – magari adoperando la stessa prudenza che ormai occorre quando si naviga sul Web in chiaro. Tor non è una tecnologia intrinsecamente "malvagia" e viene usata quotidianamente da giornalisti, attivisti, forze dell'ordine, agenti sotto copertura, servizi di intelligence, dirigenti d'azienda, militari operanti sul campo, professionisti dell'IT, utenti comuni. Nessuno di questi soggetti è o aspira a essere un "cyber-criminale", e come suggerisce Roger Dingledine la "diversità" degli utenti che usano Tor e dei motivi per cui lo usano sono le migliori garanzie per la sicurezza della darknet e il suo sviluppo futuro.

2013 ➜ Ancora l'FBI si muove contro *Silk Road*, uno dei più grandi *marketplace* di prodotti illegali (soprattutto droghe) nascosto nella darknet di Tor. Le vulnerabilità di sicurezza presenti all'interno del codice del sito portano all'individuazione dell'indirizzo IP di Ross William Ulbricht, fondatore e gestore del marketplace anche noto con lo pseudonimo di "Dread Pirate Roberts" (DPR). Ulbricht viene in seguito condannato alla galera a vita senza possibilità di rilascio in libertà vigilata.

2015 ➜ Il sito nascosto *Playpen*, divenuto il forum di condivisione di materiale pedopornografico più esteso della darknet, viene compromesso dall'FBI. L'agenzia statunitense identifica il suo fondatore (Steven Chase, poi condannato a 30 anni di carcere), prende il controllo del sito e continua a fornire l'accesso a immagini e video per altre due settimane, lasso di tempo in cui viene usata una "tecnica di investigazione telematica" (NIT) a base di malware per smascherare l'identità reale degli utenti. Novecento di questi utenti vengono arrestati, ma in almeno un caso l'FBI decide di non procedere in tribunale per evitare di dover svelare i dettagli della tecnica NIT usata per la compromissione dell'IP.

2017 ➜ *AlphaBay*, marketplace di droghe illegali che ha raggiunto una dimensione dieci volte superiore al famigerato Silk Road, viene buttato giù grazie a un'azione di cyber-polizia internazionale assieme all'erede designato *Hansa* e molti altri siti nascosti. Le scarse misure di *opsec* messe in atto dal fondatore Alexandre Cazes (come l'utilizzo di una casella di posta Hotmail e le attività di amministrazione del sito visibili "in chiaro" sul suo laptop appena sequestrato) condannano il business illegale alla sua fine, mentre Cazes viene trovato morto suicida in una cella alcuni giorni dopo il suo arresto in Thailandia.