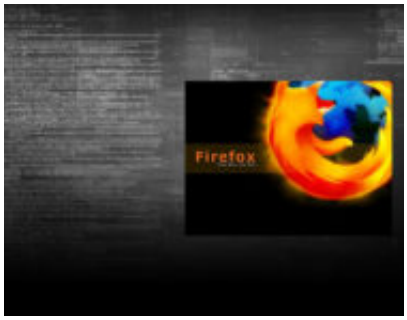
WebAnon con Proxychain e Firefox

Author : Fabio Carletti aka Ryuw

Date : 3 Febbraio 2020



Negli ultimi anni la **profilazione degli utenti** di internet è sempre più invasiva da parte di siti web, e-commerce e social network. I dati degli utenti sono diventati preziosi per creare pubblicità mirate e inserzioni di siti o prodotti pertinenti agli interessi del navigatore. Sarà capitato a tutti di comprare qualcosa su sito web e trovare poi, sui Social Network, pubblicità affini a quel prodotto o banner di Google con stessa tematica durante le nostre ricerche.

Tool OpenSource mirati a questo argomento possono venirci in aiuto per aumentare la nostra **privacy** durante la navigazione. Il primo è un programma multipiattaforma Free-OpenSource che nasconde il nostro reale indirizzo IP ad ogni connessione, il software **ProxyChains**. Il programma ProxyChains reperibile al sito (proxychains.sourceforge.net) è uno strumento per proteggere la propria identità utilizzando una macchina intermedia il cui indirizzo IPv4/IPv6 coprirà il nostro IP originario nel sito da visitare. Tale operazione può essere svolta usando un proxy: esso è un pc che funge da tramite tra un dispositivo finale e la nostra connessione. Collegandosi a internet a un determinato sito usando un proxy il server-web che ospita il sito vedrà l'indirizzo ip del proxy e non l'origine della connessione. Proxychains supporta server proxy, socks5 e socks4. Il programma è **configurabile in diversi modi** usando proxy in modo random, usando tor o una lista personalizzata di indirizzi proxy risolvendo anche indirizzi DNS. Programmi client tcp come il browser FireFox posso essere usati con proxychains per aumentare la nostra privacy durante la navigazione. Il programma - essendo multipiattaforma - è installabile in Macosx usando il sistema Brew, che permette di installare programmi Linux, lanciando da riga di comando "brew install proxychains" oppure da Ubuntu/GnuDebian lanciando l'apposito comando come root in debian e ubuntu "sudo apt-get install proxychains". Nei sistemi Unix con il comando da terminale "curl icanhazip.com" comparirà il nostro indirizzo IP pubblico quando la nostra connessione entra in internet. La parte principale del software è il file di configurazione "proxychains.conf" editabile da qualsiasi editor che si preferisce usare in base al sistema operativo.

In questo file è possibile configurare i serverproxy e la modalità di esecuzione del programma. Usando da terminale il solo comando "proxychains" risponde il proxychains con la versione, il sito di riferimento del progetto e l'indicazione di lanciarlo seguito dal programma che segua la via dei proxy. Per eseguire il programma da terminale basta il comando "proxychan firefox" o

per testare se il software è in esecuzione correttamente con IP diverso, il comando “proxychains curl icanhazip.com” dovrebbe visualizzare un IP di uno dei proxy inseriti precedente. Visualizzando i siti dove vi indicano il vostro indirizzo ip noterete che **non è dal vostro ip pubblico** che risulta la navigazione ma dall’indirizzo IP del proxy. In ProxyChains è possibile, per paranoia, abilitare catene di indirizzi di server diversi per le richieste DNS. Usare IP diversi per navigare ma lo stesso server DNS interrogando “in chiaro” dallo stesso IP sorgente equivale a informare il provider - che visualizza il traffico dati - che anche se gli indirizzi sorgente cambiano, le richieste del dominio a cui stiamo interrogando il servizio DNS è allo stesso sito.

Il browser free e OpenSource **FireFox** ha da poco implementato sulle impostazioni di rete la possibilità di abilitare un proxy interno per le richieste DNS cosi da avere un DNS over HTTPS usando **Cloudflare** come server predefinito. Richiedere le risoluzioni DNS crittografando le richieste da parte del server-DNS permette un certo livello di privacy rispetto al provider di servizi internet, ma il server-DNS conosce il nostro IP pubblico, mentre usando diversi proxy e server-DNS cambiando ogni volta l’indirizzo IP rende molto difficile individuare il profilo della persona. Browser OpenSource multipiattaforma minimali come Chromium - purgato di interazioni con Google - permettono una buona privacy di navigazione ma la comunità di Mozilla, in questo settore, è al top. FireFox ha plug-in che permettono di cambiare lo user-agent del browser cosi da camuffare un browser FireFox eseguito da un pc Linux in un computer con MsWindows che usa Opera come browser. Esistono **diverse estensioni** che permettono di personalizzare e falsificare la stringa user-agent del browser permettendo di cambiare un profilo casuale o personalizzato; quindi per esempio si potrebbe navigare nei siti web con un identità di un pc con MsWindows XP e browser Internet Explorer. I siti cambiano veste in base se identificano se l’utente usa un dispositivo mobile o workstation, con questo tool potremmo mostrarci a internet come dispositivo Android o IOS. Lo spoof sia dell’indirizzo IP che del browser e quindi anche del sistema operativo, ad ogni connessione, che realmente usiamo permette di rendere impossibile, da parte del server e dei siti che stiamo visitando, risalire alla nostra identità digitale. Javascript e plug-in dei CMS di siti possono tuttavia essere invadenti e proporre banner e pubblicità che possano mandare le nostre info sulla connessione a soggetti terzi del sito o tracciare in qualche modo il nostro browser se non ripuliamo la nostra *cache* regolarmente.

Un’altra estensione di FireFox che è tra le più consigliate è **Ublock Origin,** un plug-in gratuito che permettere di bloccare banner e pubblicità anche in base alla nazione tramite le liste da selezionare. I filtri aggiornati automaticamente bloccano tutte quelle interazioni tra browser e sito destinatario per velocizzare la navigazione e impedire che possa cliccare link che potrebbero catturare info sulla vostra attività in rete.

Se volete usare un **motore di ricerca discreto** evitate Google, Yahoo o Bing e passate a Duckduckgo, Startpage o altri motori di ricerca che non salvino le informazioni sulle ricerche degli utenti, che non memorizzino indirizzi IP, l’utilizzo dei cookie e che diano la possibilità di avere ricerche criptate. Più tasselli inseriamo come protezione più alziamo la nostra privacy durante la navigazione, in base alla censura governativa in cui operiamo, al tipo di controllo che subiamo, abbiamo molteplici tool per combattere la censura del web. L’unione di progetti OpenSource che mirano in questa direzione, anche grazie allo sforzo di volontari che si

adoperano nel contribuire a un web più libero, rendono possibile navigare senza la presenza costante del “grande fratello”.

> Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere
> è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire.

È il concetto su cui il perseguitato americano, ora rifugiato in Russia, **Edward Snowden** ha invitato più volte a riflettere, per evitare di essere fuorviati dalle informazioni mirate che siti e social vogliono che noi vediamo.

Articolo a cura di **Fabio Carletti aka Ryuw**