21/10/2009

Come proteggere la privacy in Rete

di Matteo Cappelli

Livello guida: Principiante-Intermedio

Indice

1 Introduzione

Per comprendere quali e quante siano le potenziali minacce alla privacy su Internet, basta pensare alla navigazione di un utente: forum, siti di informazione, motori di ricerca, webmail, mailing list, newsgroup, e soprattutto in questi ultimi anni social network. In tutti questi luoghi virtuali vengono lasciate tracce del passaggio di una determinata persona. Su "mondomappa" vengono lasciate le indicazioni di un luogo dove si ha intenzione di recarsi. Sul forum viene chiesto quale prodotto acquistare, perché il vecchio magari non ha convinto del tutto. Sul motore di ricerca si cercano informazioni sul proprio lavoro, per vedere se altri hanno già fatto qualcosa di simile, ne hanno già discusso o se già esiste quello che si vuole realizzare. Sicuramente non sono cercate informazioni che non interessano.

Al giorno d'oggi quindi non esiste più privacy [18], ed è necessario attuare opportuni metodi di difesa. Di seguito sono presentate le tecniche più diffuse e pericolose che permettono la raccolta e la profilazione[1] delle informazioni di un individuo, e quindi sono proposti dei metodi per difendersi da queste

[1] Il termine profilazione indica l'analisi dei dati raccolti in riferimento ad un determinato target, quale ad esempio: iscritti ad una mailing list, visitatori di un dato gruppo di pagine web, ecc.

minacce. Dietro alla raccolta dei dati si celano, tipicamente, aziende senza scrupoli che vogliono aumentare i loro profitti e sorpassare la concorrenza.

La guida è rilasciata con licenza CC [2].

1.1 A chi è rivolto il manuale

Questo manuale è rivolto a tutti coloro che hanno una discreta conoscenza del pc, e che vogliono apprendere quali sono le più diffuse minacce alla privacy (da non confondere con le minacce informatiche [16]), in relazione principalmente alla navigazione tramite browser. Ogni minaccia viene prima descritta in dettaglio dal punto di vista teorico, quindi viene presentato un metodo pratico per difendersi da essa. A fine lettura, il lettore sarà in grado di comprendere quali sono le tecniche che minacciano la sua privacy, e sarà in grado di mettere in atto un primo metodo difesa, nei casi in cui si possa agire sulle caratteristiche del browser. Le soluzioni proposte non sono da intendersi come le migliori, in quanto, relativamente alla privacy, la soluzione ideale sarebbe di utilizzare un software per l'anonimato (come Jap/Jondo o Tor), con i relativi plugin (JondoFox e Torbutton). Per maggiori dettagli vedere il paragrafo 6 - La soluzione ideale.

Si presume che il lettore sappia utilizzare correttamente un browser web, cambiarne le impostazioni, installare un add-on (nel caso di Firefox), e sappia eseguire sul web operazioni fondamentali quali usare un motore di ricerca. Da notare infine che quanto segue è da ritenersi valido alla data di rilascio del manuale, data la rapida evoluzione nel settore informatico e delle sue tecnologie.

1.2 Note di produzione

I metodi di difesa proposti sono stati applicati ai seguenti browser:

- Internet Explorer versione 8;
- Mozilla Firefox, versione 3.5.3;
- Opera, versione 10.00.

2 Cookie

Tecnicamente, i cookie rappresentano un sistema che può essere utilizzato da connessioni lato server per memorizzare e recuperare informazioni sul lato client della connessione, ed attraverso questo tipo di meccanismo è possibile mantenere uno stato attraverso più pagine o script. Le possibili applicazioni realizzabili mediante l'utilizzo dei cookie sono diverse. Un esempio viene fornito dai siti su cui si ha la possibilità di personalizzare la pagina visualizzata e di scegliere alcuni parametri preferenziali, come i colori

ed il tipo dei contenuti che più interessano. In tal modo, quando il client accede nuovamente a quella pagina, il server conosce già le informazioni da fornire. Un'altra applicazione tipica è quella di memorizzare determinate informazioni per evitare al navigatore di doverle immettere più di una volta, come nei servizi di webmail, dove si ha la possibilità di essere "riconosciuti" al momento che si accede all'account. Un ulteriore esempio è quello dei "carrelli," componente irrinunciabile dei siti di commercio elettronico.

Dal punto di vista del sito che lo invia, un cookie è utile perché permette al sito stesso di essere più efficiente: può scartare le pagine che non vengono utilizzate, e concentrare gli sforzi sulle informazioni che l'utente desidera.

I cookie non sono altro che semplici file di testo, di dimensioni ridotte, non possono essere in alcun modo dannosi, non riempiono il disco fisso di un utente con file qualunque, non danneggiano il pc, non introducono virus e non possono accedere ad informazioni su memoria locale.

Il funzionamento è basato su due stadi. Al primo, il cookie viene memorizzato sul pc dell'utente senza alcun avvertimento, almeno che non sia impostato diversamente dal browser. Durante il secondo stadio, il cookie viene trasferito clandestinamente ed automaticamente dal pc dell'utente al server web, con all'interno tutte le informazioni memorizzate. Nello specifico esistono due varianti dei cookie:

Cookie di sessione. Sono temporanei, e sono eliminati nel momento in cui il browser viene chiuso e la sessione di navigazione finisce. La successiva volta che l'utente visiterà quello stesso sito apparirà come un nuovo visitatore, e il sito non saprà se l'utente aveva già visitato il sito stesso oppure no.

Cookie persistenti. Questi cookie rimangono in memoria finquando non sono eliminati manualmente, o finquando scadono. In questo scenario, tutte le volte che un utente visiterà uno stesso sito, che ha inviato il cookie, sarà "riconosciuto" dal sito.

I cookie identificano l'utente in base al browser per navigare su Internet, al computer e all'identificatore utente con il quale accede al proprio computer. Rispetto all'indirizzo IP, i cookie forniscono un'informazione in più: l'identificatore utente. Combinando cookie e rilevazione dell'indirizzo IP, aumenta il numero di informazioni che si possono ottenere. Le conseguenze ed i pericoli per quanto riguarda la privacy sono:

- memorizzazione di informazioni sensibili dell'utente all'interno dei cookie (nome, cognome, indirizzo mail, ...), per poi essere recuperate dal server web in un secondo momento (o da persone che possono accedere al pc, e leggere i file testuali dei cookie);

- comparsa di banner pubblicitari ad hoc, e di finestre di pop-up;

- recupero di informazioni sulle precedenti visite all'interno dello stesso sito;
- individuazione del comportamento di un utente, con la creazione di profili personalizzati.

Per approfondimenti sui cookie e sulla loro struttura consultare [22], mentre riguardo i rischi per la sicurezza visitare [20].

2.1 Cookie di terze parti

Esiste anche un particolare tipo di cookie, chiamato *cookie di terze parti*. La differenza è che un cookie di terze parti viene inviato a un sito web diverso da quello visualizzato, mentre un cookie normale viene inviato indietro solamente al server che lo ha impostato, o in alternativa ad un server dello stesso dominio. Nello specifico, viene sfruttata la possibilità di includere elementi appartenenti a siti (e quindi domini) diversi all'interno delle proprie pagine, legando perciò all'invio di questi elementi un cookie. Con questa tecnica è possibile che un server memorizzi su un client informazioni in maniera permanente, senza che esso abbia mai richiesto una pagina del dominio a cui il server è riferito [26].

2.2 Modifica dei cookie

La soluzione "perfetta" sarebbe la disabilitazione totale di tutti i cookie, ma nella pratica questo risulta fin troppo radicale, in quanto risulterebbero inutilizzabili molti siti che fanno largo uso di cookie. Per esempio, qualora tutti cookie fossero disabilitati, non sarebbe possibile utilizzare i seguenti siti:

- `www.ebay.it`;
- `www.facebook.com`;
- `www.paypal.it`;
- gli account per i servizi di `www.google.it`;

e, più in generale, tutti quei siti che richiedono l'autenticazione dell'utente.

Dunque, è necessario trovare un compromesso. La soluzione migliore è quella di disabilitare unicamente i cookie di terze parti, lasciando attivi i cookie inviati dal solo sito che si visita. Inoltre, è opportuno anche cancellare i cookie alla chiusura del browser (cookie persistenti), in modo da limitare la permanenza delle informazioni sul proprio pc troppo a lungo. In questo modo si farà uso unicamente dei cookie di sessione. Queste operazioni possono essere effettuate in modo semplice con qualsiasi browser. Vediamo di seguito.

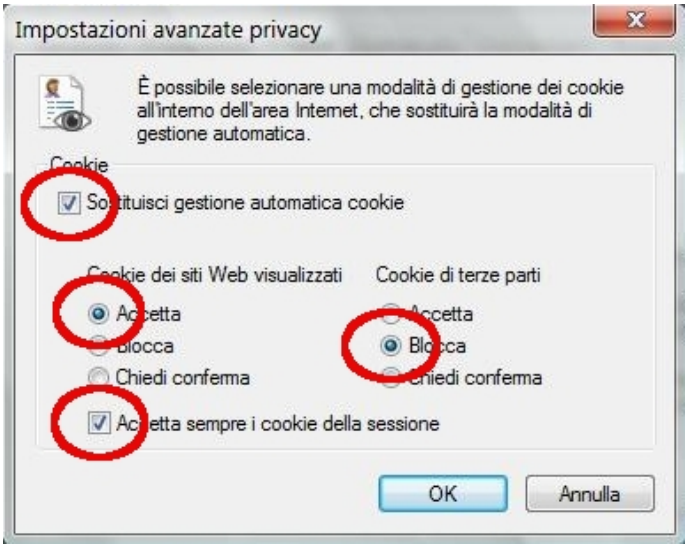

Figura 1: Personalizzazione cookie con Internet Explorer.

Nel caso di Internet Explorer, dalla barra del menù si deve scegliere il sottomenù **Strumenti** → **Opzioni Internet**. Dalla finestra aperta si deve selezionare il tab **Privacy**, quindi premere il pulsante **Avanzate**, e abilitare le voci seguendo la figura 1.

Come secondo passo è necessario procedere all'eliminazione dei cookie persistenti. Il punto di partenza è sempre **Strumenti** → **Opzioni Internet**, da dove poi bisogna selezionare il tab **Generale** e spuntare la voce **eliminare la cronologia delle esplorazioni**, all'interno della sezione **cronologia esplorazioni**. Prima di chiudere la finestra delle opzioni però si deve premere il pulsante **Elimina**, che comporterà l'apertura di una nuova finestra, all'interno della quale si devono spuntare le voci seguendo la figura 2 (anche se non necessario, è consigliabile effettuare una cancellazione di tutti i dati, non solo dei cookie).

Figura 2: Eliminazione cookie persistenti con Internet Explorer.

Nel caso di Firefox è necessario andare a **Modifica** → **Preferenze**, e selezionare il tab **Privacy**. Quindi, osservando la figura 3, si devono abilitare le voci indicate, togliendo la spunta alla voce Accetta i cookie di terze parti.

La navigazione privata è una funzione molto utile di Firefox che permette di cancellare ricerche, pagine visitate, download, pagine in cache e cookie, una volta che viene chiusa la finestra di navigazione.

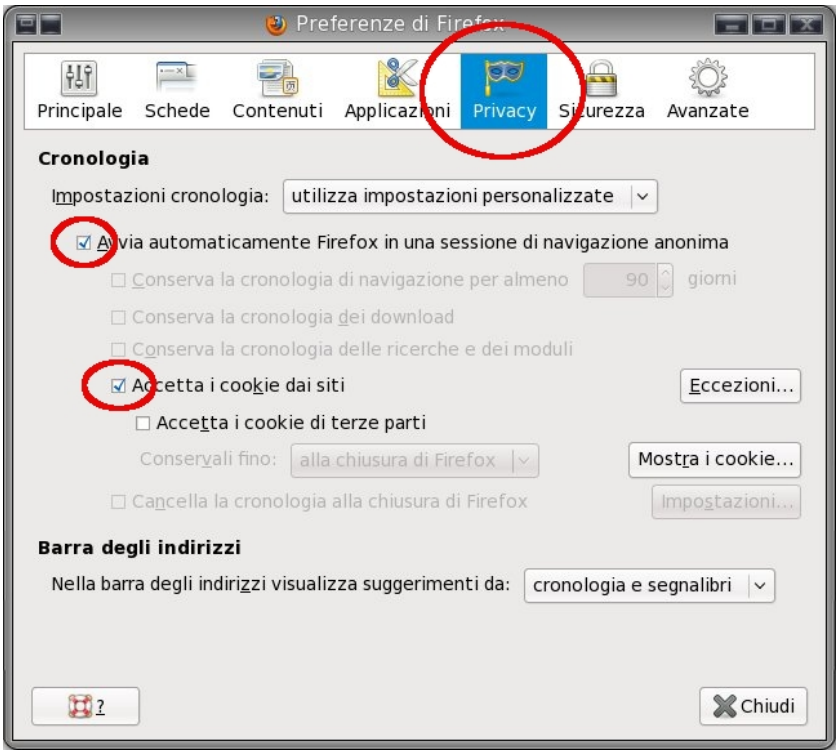

Figura 3: Personalizzazione cookie con Firefox.

Infine per Opera si deve andare alla voce **Strumenti** → **Preferenze**, e abilitare solamente le voci visibili in figura 4.

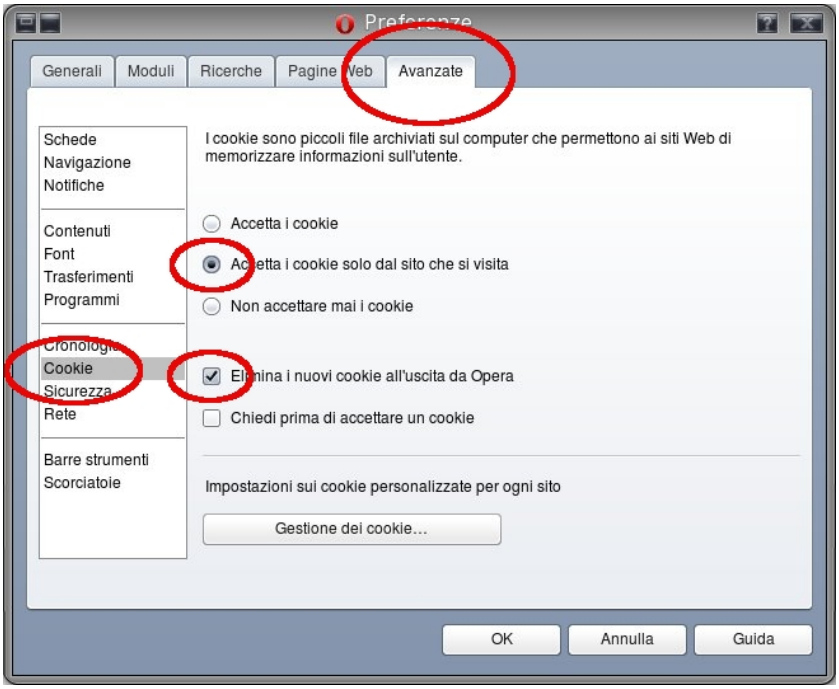

Figura 4: Personalizzazione cookie con Opera.

Fatto ciò, tutti i cookie che verranno da ora in avanti salvati saranno poi eliminati alla chiusura della finestra. Tuttavia qualora, al momento dell'attivazione dell'opzione, fossero già stati salvati sul pc cookie, relativi a sessioni precedenti, è necessario eliminarli manualmente. Per eseguire tale operazione è sufficiente partire dalla finestra mostrata sempre in figura 4, fare click sulla finestra **Gestione dei cookie**, e selezionando ogni cookie presente (una riga rappresenta un cookie), e dunque premere il pulsante **Elimina**.

3 File di log

Tutte le informazioni inviate dal pc di una persona sono memorizzate dai singoli Internet Service Provider (di Alice, Libero, Tele2, ...) e dai server web, e sono organizzate in quelli che vengono denominati file di log, o più semplicemente log. I possibili file di log possono essere diversi:

1. log dei server web (HTTP);
2. log dei server di posta elettronica (SMTP);

3. log degli ISP;

4. file di registro di altro tipo.

In particolare, un log contiene al suo interno i dati relativi ad ogni navigatore web, ad ogni sua mail inviata e/o ricevuta, ad ogni collegamento e ad ogni accesso effettuato sulla Rete. Nel caso del log di un server web, una possibile riga di uno del file potrebbe essere la seguente:

```
122.122.122.122
- -
[26/Apr/2000:00:16:12 -0400]
"GET /curedipendenzadadroga.html HTTP/1.1"
200
15496
"http://www.google.it"
"Mozilla/4.7 [en]C-SYMPA  (Win95; U)"
```

Da notare che ogni campo è stato messo su una linea differente per maggior chiarezza, in realtà in un file di log tutte queste informazioni sono concatenate in una sola riga. Inoltre, in un log ogni riga si riferisce ad una specifica richiesta fatta dall'utente al server web per qualunque oggetto necessario al caricamento della pagina, come le immagini, i download o altri file richiesti, che saranno registrati singolarmente in altre righe.

Di seguito sono analizzati in dettaglio i singoli campi dell'esempio proposto, specificando per ognuno le informazioni contenute.

Indirizzo IP: 122.122.122.122. Questo è l'indirizzo IP della macchina che ha effettuato la richiesta, ed è la principale informazione che minaccia la privacy di un navigatore del web.

LogName e FullName: - -. Questi due campi rappresentano il nome di login ed il nome completo, utilizzati solo quando il contenuto richiesto richiede l'autenticazione. In questo caso il campo è stato disabilitato direttamente dall'host, quindi appare il trattino (-) per entrambi i dati.

Timestamp: [26/Apr/2000:00:16:12 -0400]. Questo campo contiene la data e l'ora in cui è stata effettuata la richiesta.

Richiesta: GET /curedipendenzadadroga.html HTTP/1.1. Questo è il file richiesto dall'utente, e solitamente vengono indicati il percorso ed il nome. Nell'esempio è stata richiesta la visualizzazione (metodo GET) della pagina web /curedipendenzadadroga.html.

Codice di status: 200. Il codice di status indica se la richiesta è andata a buon fine oppure no. In questo caso "200" indica un successo.

Byte trasferiti: 15496. Questo valore indica il numero di byte trasferiti.

Referer[2]**: "http://www.google.it"** . Questo campo indica l'URL da cui l'utente è arrivato, in questo caso dal sito `www.google.it`. Questa è un'informazione molto utile soprattutto per i webmaster, ed è una delle informazioni più confidenziali.

User Agent: "Mozilla/4.7 [en]C-SYMPA (Win95; U)". Questa informazione comprende tutti quei software che l'utente ha utilizzato per richiedere la risorsa, come ad esempio un client FTP, un browser web, o un link checker. In questo caso è stato utilizzato il browser Mozilla versione 4.7, probabilmente in versione inglese ([en]), ed in ambiente Windows 95.

Come abbiamo appena osservato le informazioni salvate nel file di log non sono poche. Spesso questi dati sono anche confidenziali, addirittura, anche se raramente, può essere trasmesso dal pc di una persona l'indirizzo di posta elettronica.

Il prossimo esempio mostra come le informazioni trasmesse possano essere molto private. Consideriamo il seguente file di log:

```
123.123.123.123
- -
[26/Apr/2000:00:23:48 -0400]
"GET /www.cristianifedeli.it HTTP/1.1"
200
6248
"http://www.sessoinvendita.it"
"Mozilla/4.05 (Macintosh; I; PPC)"
```

In questo caso, l'utente tenta di accedere a `http://www.cristianifedeli.it`[3], provenendo dalla pagina `http://www.sessoinvendita.com`[4]: questo dato è memorizzato in chiaro all'interno del log del server!

Molto più completi sono invece i log di un provider, che solitamente mantengono informazioni del tipo:

- utente;
- IP connessione;
- durata connessione;
- MAC address modem/router/scheda di rete;
- cronologia navigazione, download, P2P, ecc.

[2]Il referer è semplicemente l'URL di un elemento che conduce all'elemento corrente. In sostanza, esso rappresenta la fonte dalla quale un utente è venuto a conoscenza di una pagina.

[3]Il sito è puramente di fantasia, e al momento attuale non esiste su nessun dominio.

[4]Anche questo sito è di fantasia.

Il principale rischio è ancora una volta solamente uno: la profilazione dell'utente.

3.1 Limitare le informazioni inviate dal pc

Nel caso dei log, gli unici valori su cui possiamo agire per limitare le informazioni inviate sono tre: l'indirizzo IP, i referer e l'user agent[5]. Per quanto riguarda l'indirizzo IP, l'unico metodo per poterlo "mascherare" è di ricorrere all'utilizzo di un software per l'anonimato (come Jap/Jondo [8] o Tor [15]) o a un proxy, in modo da far apparire ad un server un indirizzo IP differente da quello reale dell'utente. Tuttavia, la configurazione e l'utilizzo di un software per l'anonimato, o di un proxy, è un'operazione troppo lunga per questa guida (si rimanda a guide future). In generale per l'anonimato si rimanda al link [9], per la configurazione/utilizzo di Jap/Jondo si consiglia di consultare la guida [10] (anche se non aggiornatissima), per Tor [11], mentre per i proxy consultare i link [19], [1], e [5] (in inglese).

Di seguito sono mostrate le configurazioni dei browser in relazione ai referer e all'user agent.

Per Internet Explorer, il cambio dell'user agent deve avvenire necessariamente attraverso il registro di sistema[6], alla seguente posizione:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\5.0\UserAgent`

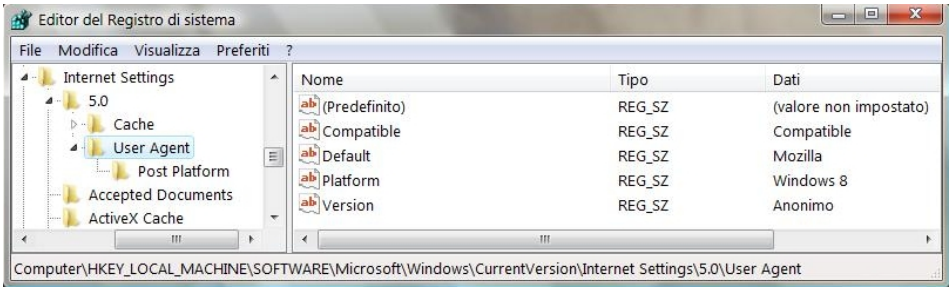

Figura 5: Modifica dell'user agent inviato da Internet Explorer.

Seguendo l'esempio in figura 5, è necessario creare, qualora non siano presenti, le seguenti stringhe e i loro rispettivi valori:

- Compatible = Compatible
- Version = NomeBrowser 1.0

[5]Cambiare l'user agent immettendo dei valori diversi da quelli di default può comportare piccoli problemi con alcuni siti, nel quale caso alcune funzioni del sito potranno essere disabilitate.

[6]Il registro di sistema si avvia dal menù di avvio, selezionando **Esegui** e scrivendo il comando `regedit`.

- Platform = SistemaOperativo2010
- Default = Mozilla/5.0

Per quanto riguarda invece l'invio del referer, non è possibile disattivare in alcun modo tale opzione né dal browser, né agendo sul registro di sistema. Una possibile soluzione sarebbe quella di fare uso di un proxy web, quale ad esempio Fiddler [3], ma la sua configurazione è complessa e non può essere quì trattata.

Nel caso di Firefox, è necessario digitare sulla barra di navigazione `about:config`, ed accettare l'eventuale domanda posta dal browser per motivi di sicurezza ("Questa operazione potrebbe invalidare la garanzia", l'operazione che si sta per eseguire non invaliderà la garanzia!). Quindi il secondo passo è di specificare la parola `referer` come filtro, e modificare la voce `network.http.sendRefererHeader`, cambiando il valore di default 2 in 0: in questo modo non saranno più inviati referer. I dettagli sono visibili in figura 6.

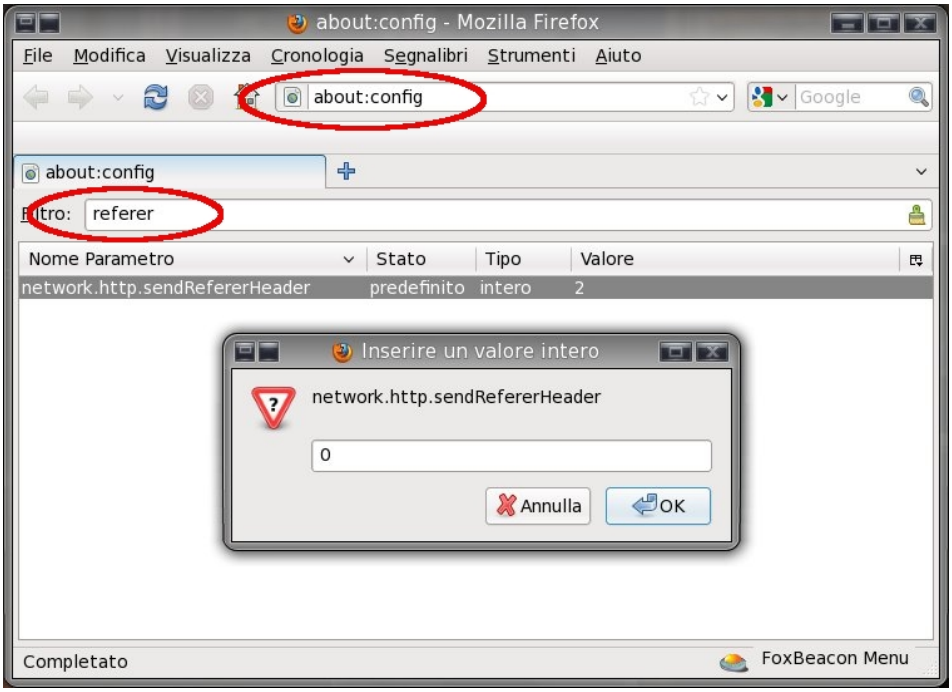

Figura 6: Disabilitazione invio referer con Firefox.

Adesso possiamo passare a nascondere l'user agent inviato da Firefox. Per fare ciò è necessario creare una nuova stringa con il nome `general.useragent.override`, utilizzando il tasto destro e selezionando **Nuovo** → **Stringa**, e impostando come valore una parola qualsiasi ("Anonimo" o "Paolino Paperino"). In figura 7 è visibile la stringa da creare.

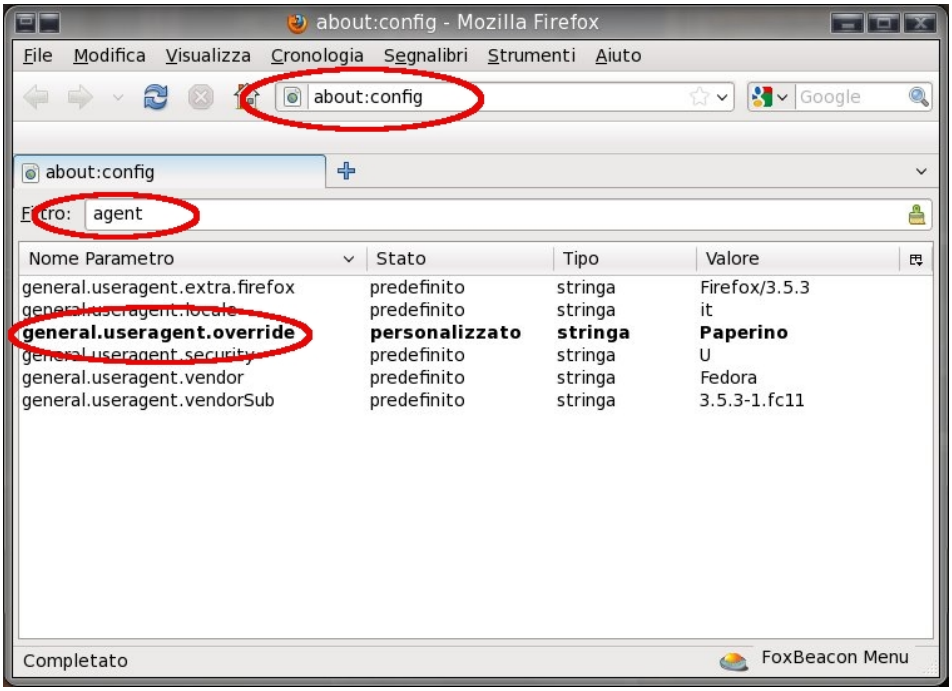

Figura 7: Modifica dell'user agent inviato da Firefox.

In caso di problemi di battitura, o per qualsiasi altro problema, è sempre possibile ripristinare i valori di default delle voci modificate, semplicemente selezionando **Ripristina** dal menù a tendine visualizzabile con il tasto destro.

Infine in Opera, per disabilitare i referer, bisogna andare alla voce **Strumenti → Preferenze**, selezionare il tab **Avanzate** e seguire le indicazioni della figura 8.

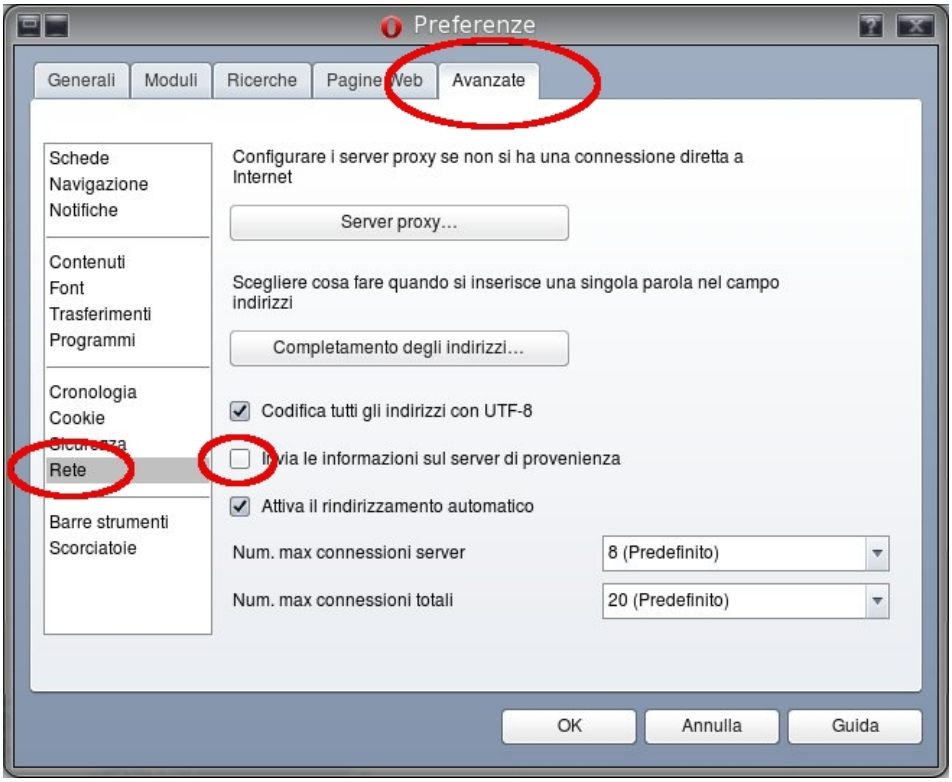

Figura 8: Disabilitazione invio referer con Opera.

Per modificare l'user agent teoricamente esistono due modi, tuttavia i cambiamenti sono piuttosto limitati. Il modo più semplice è di caricare la pagina della configurazione di Opera, digitando sulla barra di navigazione `opera:config`, e quindi impostare come parametro di ricerca `agent`. Nella figura 9 è mostrato il risultato di queste operazioni. A questo punto è possibile scegliere un'opzione tra cinque possibili, indicando il relativo numero per la stringa `SpoofUserAgentID` secondo lo schema seguente:

1. Identificati come Opera (opzione default);
2. Identificati come Firefox;
3. Identificati come Internet Explorer;
4. Mascherati da Firefox;
5. Mascherati da Internet Explorer.

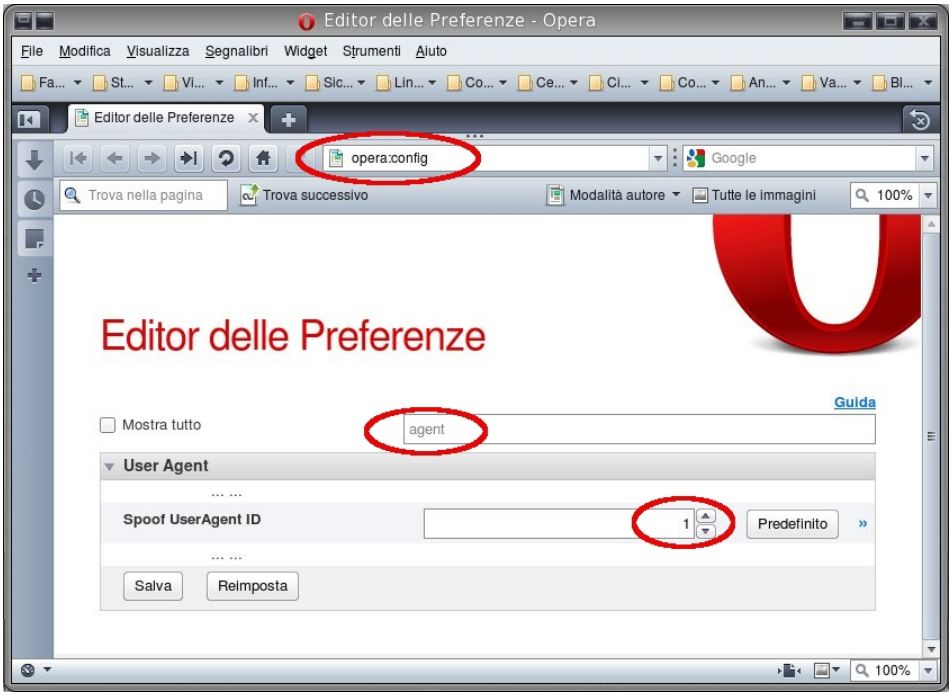

Figura 9: Modifica dell'user agent inviato da Opera (con file config).

Si consiglia di usare una delle ultime due opzioni, in quanto alcune volte il sito target (come [14]) è in grado di rilevare il mascheramento di Opera. Dopo aver scelto un'opzione è necessario selezionare il pulsante **Salva**, e quindi riavviare Opera. Tuttavia i test effettuati (anche con la modifica diretta del file opera6.ini) hanno mostrato che questo procedimento non è efficace, poiché, al riavvio di Opera, il valore viene automaticamente reimpostato ad 1 (forse una scelta consapevole degli sviluppatori, forse un bug).

Il secondo procedimento invece è pienamente funzionante, ma è piuttosto noioso, dal momento che l'impostazione dell'user agent deve essere effettuata per ogni singolo sito visitato. Ecco le operazioni che devono essere seguite:

- inserire nella barra di navigazione il sito target;
- caricare la pagina;
- andare alla voce **Strumenti** → **Preferenze veloci** → **Modifica le preferenze per questo sito...**;
- selezionare il tab **Rete**;
- alla voce **Identificazione del browser** scegliere l'opzione che si ritiene più opportuna (vedere lista di cinque opzioni sopra).

In figura 10 è possibile osservare il mascheramento del browser rispetto al sito `www.libero.it`.

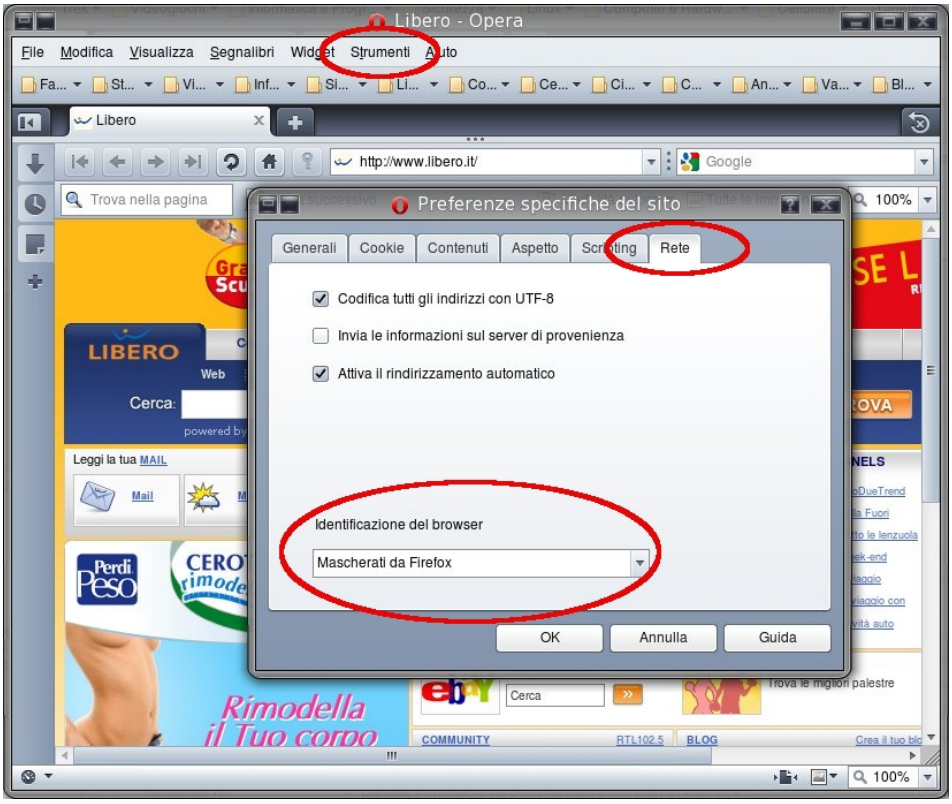

Figura 10: Modifica dell'user agent inviato da Opera (per ogni sito).

4 Motori di ricerca

I motori di ricerca sono gli unici strumenti su Internet davvero insostituibili. Insostituibili perché svolgono una funzione di "unione" tra il bisogno dell'utente di accedere ad un archivio unico e centralizzato, e la necessità della rete di essere decentralizzata e sparsa. Un motore di ricerca è unico, e può essere visto come punto di congiunzione, come nesso in comune attraverso cui tutta la rete di persone passa per raggiungere Internet. Un punto di congiunzione di questo tipo ha la completa visibilità sulle informazioni, su cosa viene cercato, su cosa è stato cercato e visitato ieri, e può dedurre cosa verrà cercato domani. Tutto questo, unito al fatto che la maggior parte delle navigazioni WWW partono proprio da uno dei motori di ricerca, rende questi strumenti una minaccia concreta alla privacy.

Ecco i principali rischi che ne derivano [25]:

- le informazioni sono spesso associate al comportamento dello specifico utente su orizzonti temporali lunghi;
- l'utente, spesso, si registra presso il motore di ricerca per ottenere servizi aggiuntivi (Google prima di tutti, con gmail e la sua immortalità [6]);
- impostazione di cookie a "lunga conservazione" (ancora Google prima di tutti);
- possono essere messe in correlazione informazioni relative a servizi diversi, forniti sempre dal motore di ricerca (ricerche, mail, gruppi di discussione);
- profilazione dell'utente: l'utente che usa il computer ha il suo cookie che consente ad un motore di ricerca di mettere in ordine tutte le sue ricerche effettuate. Cosa saranno mai? Semplicemente le nostre curiosità, passioni, conoscenze che crescono con il tempo, lavori che seguiamo, persone che conosciamo, eventi ai quali partecipiamo, il nostro nome in più di una salsa, e così via. Decisamente sufficiente per essere preoccupati.

4.1 Come difendersi dai motori di ricerca

Le difese che possono essere attuate nel caso dei motori di ricerca sono principalmente riconducibili a quelle utilizzate per i cookie. Infatti la cancellazione dei cookie alla chiusura del browser permette di eliminare le eventuali informazioni, memorizzate all'interno del cookie, sui comportamenti dell'utente (si risolve il problema dei cookie a "lunga conservazione").

Nel caso in cui si utilizzino servizi diversi messi a disposizione dal motore di ricerca, è bene effettuare le operazioni di ricerca mentre siamo disconnessi da tali servizi: in questo modo il motore di ricerca non associerà le ricerche fatte da una persona con alcun account. La figura 11 mostra come google memorizzi le pagine visitate da un utente, nel caso in cui, in quel momento, si sia connessi ad uno dei suoi servizi. Nello specifico, vengono memorizzate dal motore di ricerca:

- le pagine visualizzate;
- il numero di volte che queste pagine sono state visualizzate;
- le date di ogni visualizzazione.

Figura 11: Memorizzazione delle pagine visitate.

5 Web bug

Un web bug, chiamato a volte anche beacon, è una tecnica poco conosciuta che viene usata per tracciare chi legge una pagina web o un messaggio mail, e da quale pc. Generalmente, un web bug è una piccola immagine trasparente di dimensioni praticamente nulle (1x1 pixel), inserita all'interno di una pagina web su un server X. In realtà l'immagine che costituisce il web bug non è presente sullo stesso server X, ma si trova su un secondo server Y. In questo modo, quando un client richiede al server X il sito da visualizzare, viene restituita al cliente la pagina web richiesta con all'interno un link al server Y: se il browser ha abilitata la visualizzazione delle immagini, viene inviata immediatamente una richiesta al server Y. In figura 12 è mostrato il funzionamento di un web bug.

I web bug sono tipicamente usati da terze parti, per controllare l'attività dei clienti di un sito, e permettono di recuperare le seguenti informazioni:

- l'indirizzo IP del client che richiede il web bug;
- l'URL della pagina su cui si trova il web bug, e l'URL dell'immagine stessa;
- la data e l'ora in cui il web bug è stato visualizzato da un utente;
- il tipo di browser che ha richiesto l'immagine;
- il precedente valore del cookie.

Ed ancora [23], una compagnia che usa un web bug può:

- avere il numero di accessi ad una particolare pagina web;

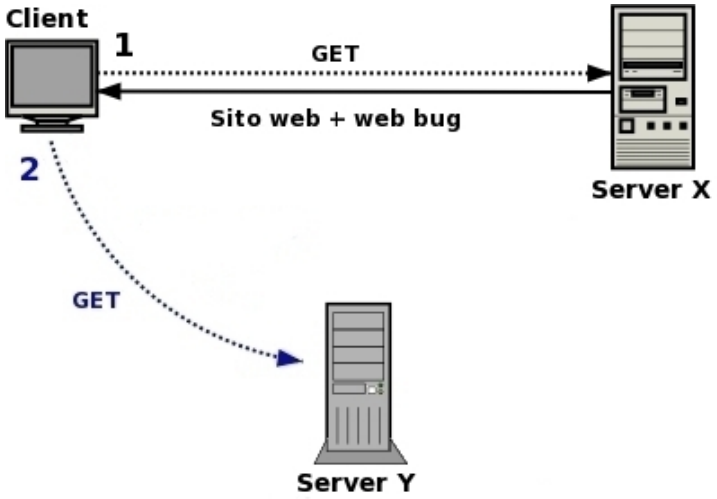

Figura 12: Funzionamento di un web bug.

- tracciare le pagine web visitate da una persona all'interno di un sito, e tracciarle anche attraverso siti differenti;
- contare il numero di volte che un certo banner pubblicitario è apparso;
- associare un acquisto fatto al relativo banner, che una persona ha visualizzato prima di fare l'acquisto. Un sito che mostra i banner tipicamente ottiene una percentuale sul prodotto venduto;
- permettere a terze parti di memorizzare un log con gli accessi al sito, qualora il server non sia in grado di farlo;
- memorizzare il tipo e la configurazione del browser adoperato dall'utente;
- memorizzare le parole cercate con il motore interno al sito, se presente. Questa informazione viene generalmente usata per creare profili sugli utenti;
- trasmettere le informazioni raccolte sui navigatori (nome, età, nazione, sesso, ...) ad una compagnia specifica.

Oltre a questi usi, la tecnica dei web bug spesso viene usata da coloro che inviano spam. Ciò viene fatto inserendo un web bug all'interno delle mail inviate, formattate in HTML. Non appena il messaggio viene aperto, se la persona risulta collegata ad Internet, viene immediatamente attivata una connessione con un server remoto (spesso il server della stessa azienda pubblicitaria) in grado di ottenere tutte le informazioni sopra elencate. Con questa tecnica chi ha inviato il messaggio di spam viene a conoscenza che

l'indirizzo mail è reale, e può registrare anche l'indirizzo IP del PC a cui è stato inviato il web bug.

5.1 Rilevare e bloccare i web bug

La disabilitazione dei cookie può prevenire la tracciatura da parte di certi web bug, tuttavia, come visto precedentemente, questa metodo non è applicabile in teoria. Un'alternativa è utilizzare software specifici che sono in grado di analizzare il traffico in entrata sul proprio pc, e di rilevare se un'immagine è un web bug. Purtroppo, gli unici due software degni di nota non sono al momento più sviluppati: Bugnosis Web bug Detector, appositamente creato per la rilevazione di web bug, e Proxomitron, un proxy web che permette il filtraggio dei pacchetti, e teoricamente in grado di essere utilizzato per bloccare web bug. Questi software potrebbe ancora essere utilizzati, ma se ne sconsiglia l'uso, soprattutto di Proxomitron, il cui ultimo aggiornamento risale al 2003 (è stato sviluppato per Windows 95!). In definitiva, se si utilizza Internet Explorer o Opera, non si avranno protezione reali per i web bug.

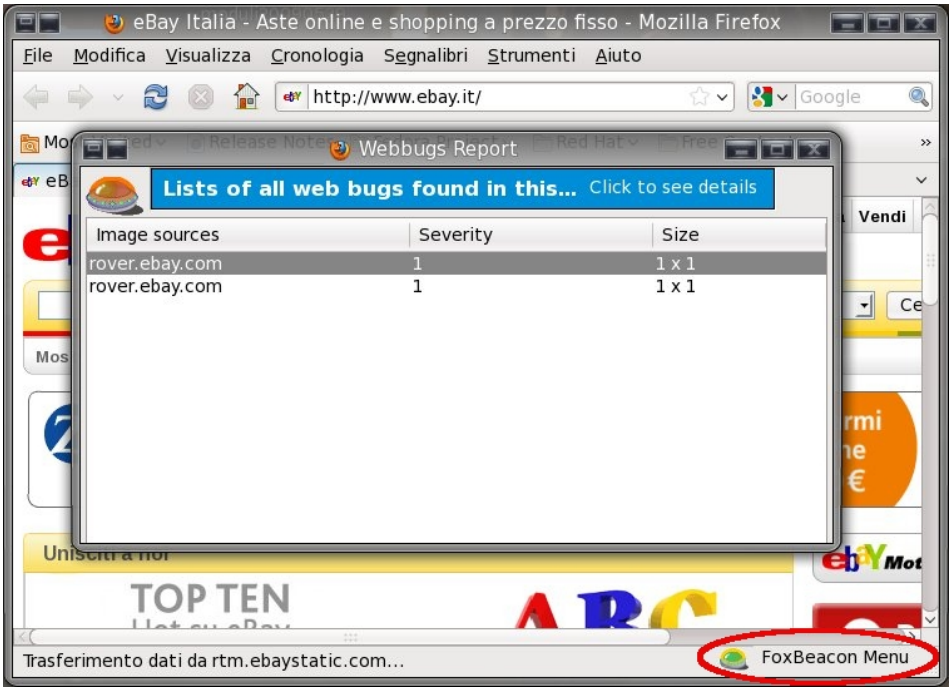

Figura 13: Funzionamento di un web bug.

Diversa è la situazione qualora si utilizzi Firefox, in quanto è possibile installare l'add-on Web Bug Detector 1.0.1, reperibile al link [17]. Questo add-on, una volta installato, viene automaticamente attivato, e automaticamente rileva e blocca tutti i web bug che trova all'interno delle pagine

visualizzate. In figura 13 si può osservare il rilevamento di un web bug sul sito di `www.ebay.it`.

Diverso è nel caso della posta elettronica, in quanto una semplice contromisura attuabile è di bloccare la visualizzazione di tutte le immagini presenti nelle mail, evitando che il web bug entri così "in azione". In particolare ciò deve essere attuato per i messaggi provenienti da fonti sconosciute, ma di norma è meglio bloccare *sempre* la visualizzazione delle immagini nelle mail in formato HTML, e solo se la fonte è affidabile permetterne la visualizzazione. Si ricorda anche che una mail puramente testuale non può contenere nessuna immagine, e quindi *nessun* web bug.

6 La soluzione ideale

La soluzione ideale ai problemi finora esposti è di utilizzare un software per l'anonimato, in grado di nascondere non solamente molte delle informazioni inviate da un browser, ma anche e soprattutto l'indirizzo IP. Gli strumenti oggi disponibili per navigare in completo anonimato sono moltissimi, e brevemente è possibile suddividerli in 4 grandi categorie:

VPN. Una VPN crea una connessione fra un pc ed un server remoto VPN, e tutti i dati in transito attraverso Internet sono così inviati all'interno di un tunnel virtuale, criptato ed inaccessibile da chiunque, garantendo l'anonimato. I software che ricorrono alle VPN spesso sono a pagamento, come GoTrusted e Anonymizer.

Darknet. Una darknet è una rete virtuale privata, del tutto separata da Internet. Nel suo significato più generale, può essere considerata come darknet un qualsiasi gruppo chiuso e privato di persone che comunicano tra loro, ma il nome spesso è usato nello specifico per reti di condivisione di file, dette P2P. Solamente all'interno di questa rete viene garantito anonimato e privacy. Soluzioni di questo tipo sono Freenet ed Anonet.

Server Proxy. Questo gruppo è costituito dai server proxy HTTP e SOCKS. I primi possono essere utilizzati esclusivamente al di sopra del protocollo HTTP, e solo alle volte con FTP o con HTTPS. La particolarità dei server SOCKS invece è quella di poter essere usati con numerosi altri protocolli di livello superiore. Garantiscono un minimo grado di anonimato, rispetto ad altri sistemi.

Mix Network. Questi sistemi creano una catena di proxy, attraverso la quale vengono inviati i messaggi. In aggiunta ogni messaggio viene criptato da ogni proxy, il quale conosce solamente il nodo da cui il messaggio è arrivato, e quello a cui deve essere trasmesso. Le mix network permettono di rendere difficile la tracciatura dei dati inviati,

e, di conseguenza, un buon livello di anonimato. I software di questo tipo più diffusi sono Tor e Jap/Jondo.

La configurazione e l'utilizzo di questi sistemi esula dallo scopo di questa guida.

6.1 Gli svantaggi dei software per l'anonimato

Molti utenti "comuni" potrebbero ritenere superfluo usare uno strumento di questo tipo, o per i costi dovuti all'utilizzo (come le VPN), o per il degrado delle prestazioni (nel caso di Jap/Jondo o Tor), e comunque per il tempo necessario alla corretta configurazione del software. Inoltre, alcuni di essi, sebbene facilmente installabili ed avviabili, richiedono un'attenta e non banale fase di configurazione (ad esempio Tor) per essere utilizzati al meglio, in quanto basta un minimo errore per perdere l'anonimato ottenuto con tanta fatica! Ecco perché applicare dei semplici metodi di difesa può essere una soluzione sufficiente per molte persone, anche se non alternativa (se un software come Tor viene configurato ed utilizzato al meglio permette di ottenere un grado di privacy elevatissimo).

7 Conclusioni

I metodi esposti in questa guida permettono di limitare le informazioni inviate dal pc di una persona, e di proteggere pertanto la sua privacy. Tuttavia, è bene tenere presente che le informazioni sensibili trasmesse da un utente durante la navigazione sono tante, molte più di quanto si possa credere, e questi metodi sono solo il primo passo che qualunque persona dovrebbe fare. La frase *privacy in Rete* viaggia di pari passo a quella di anonimato e sicurezza, entrambe strettamente legate. Se qualcuno fosse interessato ad approfondire gli argomenti, i passi successivi che si potrebbero fare, sono quelli di utilizzare un software quale Tor o Freenet, proteggere la privacy per quanto riguarda la posta elettronica ad esempio con la criptatura (GnuPG) e imparare a riconoscere i messaggi phishing. Insomma, imparare a proteggere la propria privacy non è facile, e soprattutto non si dovrebbe mai dimenticare che navigare in Rete significare uscire di casa lasciando la porta socchiusa. Come ha detto Bart Simpson: "*Io non l'ho fatto, nessuno mi ha visto farlo, e non puoi provarlo in nessun modo!*"

Riferimenti bibliografici

[1] Come nascondere l'indirizzo ip usando http, connect, proxy cgi/php/web e sock.
`http://tools.rosinstrument.com/proxy/howto.htm`.

[2] Creative commons license.
`http://www.creativecommons.it/`.

[3] Fiddler web debugger - a free web debugging tool.
`http://www.fiddler2.com/`.

[4] The free network project.
`http://freenetproject.org`.

[5] Free proxy servers: free proxy lists, programs to work with proxies, proxy faq.
`http://www.freeproxy.info`.

[6] Gmail is too creepy.
`http://www.google-watch.org/gmail.html`.

[7] Guida sicurezza dei pc: Microsoft activex.
`http://sicurezza.html.it/guide/lezione/2417/microsoft-activex`.

[8] Jondonym - servizio commerciale di jap.
`http://www.jondos.de/en`.

[9] Navigazione anonima.
`http://proxoit.altervista.org/jap.html`.

[10] Navigazione anonima-guida di jap/jondo.
`http://proxoit.altervista.org/navigazione-anonima.html`.

[11] Navigazione anonima-guida di tor.
`http://proxoit.altervista.org/tor/tor.html`.

[12] Operator - opera + tor. surf anonymously.
`http://archetwist.com/opera/operator`.

[13] The privacy.net analyzer.
`http://network-tools.com/analyze`.

[14] Rilevazione dell'user agent.
`http://www.useragentstring.com/`.

[15] Tor: anonymity online.
`http://www.torproject.org`.

[16] Virus/cavalli di troia/worm.
`http://it.trendmicro.com/it/threats/enterprise/threats-summary/viruses/index.html`.

[17] Web bug detector 1.0.1.
`https://addons.mozilla.org/en-US/firefox/addon/9202`.

[18] Marco Calamari. Cassandra crossing/ compriamoci la privacy, November 2005.
`http://punto-informatico.it/1349426/PI/Commenti/cassandra-crossing-compriamoci-privacy.aspx`.

[19] Maurizio DelVecchio. Guida di base all'utilizzo dei proxy, December 2007.
`http://forum.zeusnews.com/viewtopic.php?t=27739`.

[20] Seth Fogie. How not to use cookies, December 2006.
`http://www.informit.com/guides/content.aspx?g=security&seqNum=232`.

[21] Gloria Marcoccio. Data retention, la pisanu dovrà fare i conti con l'europa, July 2007.
`http://www.interlex.it/675/marcoccio1.htm`.

[22] Michele Nasi. Cookie: cosa sono, come vengono usati e quando sono pericolosi.
`http://www.ilsoftware.it/articoli.asp?id=894&pag=0`.

[23] Richard M. Smith. The web bug faq, November 1999.
`http://w2.eff.org/Privacy/Marketing/web_bug.html`.

[24] Christopher Soghoian. Blog slight paranoia: The analysis and rantings of a security and privacy researcher, November 2006.
`http://paranoia.dubfire.net/2006/11/good-news-and-bad-news.html`.

[25] team s0ftpr0ject. La minaccia fantasma, privacy e sicurezza, rischi del 2006, October 2006.
`http://www.s0ftpj.org/docs/LMF/LMF.htm`.

[26] Andrea Vit. I cookies di terze parti, November 2007.
`http://andreavit.blogspot.com/2007/02/i-cookies-di-terze-parti.html`.