Combattiamo il Grande Fratello!

Avete mai notato quanto è fastidioso, in tram o al bar, sfogliare un giornale con qualcuno che legge alle spalle? Io una tecnica ce l'ho, per scoraggiare il seccatore! Faccio finta di leggere e faccio invece ondulare il giornale con movimenti piccoli, rapidi e regolari. Vi assicuro che l'effetto è immediato, salvo poi a scansarvi se l'intruso è un po' debole di stomaco.

Il fatto è che, in tram, chi ci spia, fosse pure per un'innocente sbirciata alle notizie di oggi, lo vediamo e ce ne possiamo difendere, fosse pure chiudendo la rivista. E, dagli occhi indiscreti di Web, chi ci difende? Niente paura, amici lettori, con la ricetta seguente andiamo dal farmacista, pardon, dal signor WWW e scarichiamoci il pacchetto di cui parliamo. E' solo funzionante per quindici giorni, un poco come i medicinali formato ridotto che distribuiscono ai medici, ma vi permetterà di rendervi conto di quel che accade quando navigate, senza neppure lontanamente rendervene conto, e di stabilire se è opportuno comprare la cura completa.

di Raffaello De Masi

Assoldiamo un gorilla!

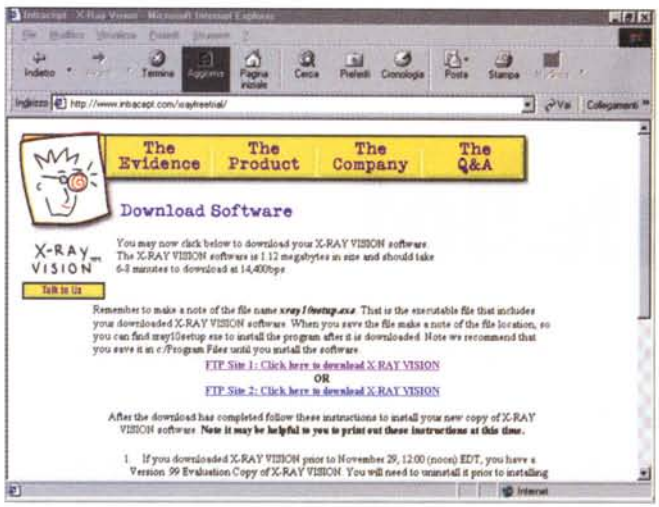
Fate una prova; quando vi collegate a un sito, fosse pure la Startup page, attivate la finestrina della connessione; come mai, se stiamo scaricando una pagina, quindi dati, sulla nostra macchina c'è il contatore dei dati in uscita che si aggiorna continuamente in alto? Certo, si tratta probabilmente di scambio di handshake, controlli di password, verifica e test di parità, e tante altre cose ancora, probabilmente innocue. Probabilmente!

Fatto è che, si può dire giornalmente, la qualità dell'interattività dei siti più moderni e funzionali cresce, senza tregua. Una volta scaricare un sito significava scaricare una pagina statica, i dati circolavano praticamente in un solo senso e, quando questa era completa, il browser si arrestava nelle sue attività e aspettava ulteriori ordini. Oggi si rimarrebbe sbalorditi se si potesse vedere il lavorio di scambio di dati, nei due sensi, che si verificano a ogni passo. Gli agenti segreti di tali scambi si nascondono dietro nomi esotici e suggestivi, come cookie, Java applet, script, plug-in, server-push e client-pull, ma si tratta, inutile nasconderlo, di agenti, depositati nelle viscere della nostra macchina, che stanno lì, se ci pensate bene, non per servire noi, ma chi ci viene in visita. E spesso questi "parassiti" ci vengono attaccati senza che neppure ce n'accorgiamo. E, come dicevamo, potremmo essere davvero sconvolti se riuscissimo, in qualche modo, a vedere la quantità di informazioni riguardanti la nostra macchina che vengono spediti al nostro interlocutore.

X-Ray Vision, versione 1.0

http://www.intracept.com

Prezzo: 39.95 US $
versione trial scaricabile dal sito



La pagina home da cui scaricare il programma.

Beh, non allarmiamoci, la maggior parte di queste attività sono benigne. Immaginate l'esempio più tipico di ospite, il biscotto-cookie. Serve, come è noto, a farci riconoscere dal sito che stiamo visitando, in modo che questo possa, ad esempio, configurarsi od offrirci certe notizie secondo le nostre preferenze (immaginate, giusto per semplificare, un cookie di un motore di ricerca). Ma chi impedisce a un realizzatore di cookie di inserire, nella sua creatura, una routine che trasmetta, al collegamento, anche notizie, da parte nostra, non consentite?

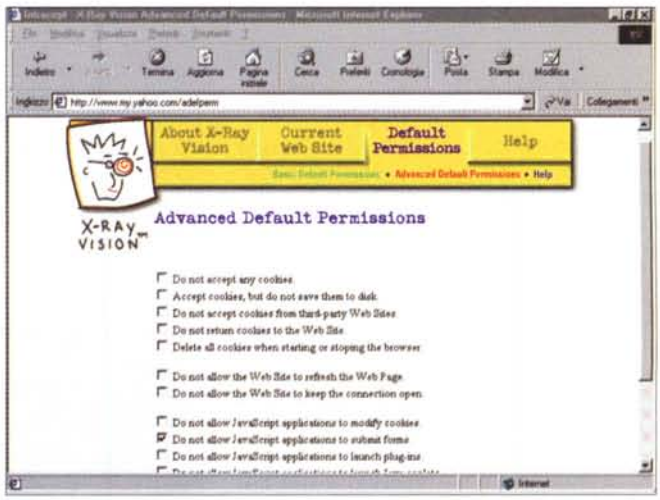
La soluzione è rappresentata da un originale programma di Intracept (http://www.intracept.com), denominato X-Ray Vision, che controlla e dettaglia tutte le attività di entrata e uscita di dati quando ci colleghiamo a WWW. In pratica il programma, che può funzionare in background in maniera trasparente, o viceversa interattivamente con l'utente, permette due livelli principali di filtro e verifica, uno di base e uno avanzato, ambedue ampiamente personalizzabili. Nel primo caso ritroviamo certe opzioni già presenti nei più recenti browser: permesso a siti Web di accedere (in qualunque modo) a dati presenti sulla nostra macchina, permesso di lanciare programmi residenti, messaggistica di allarme quando intervengono tecnologie che consentono scambio di dati.

E se non basta?

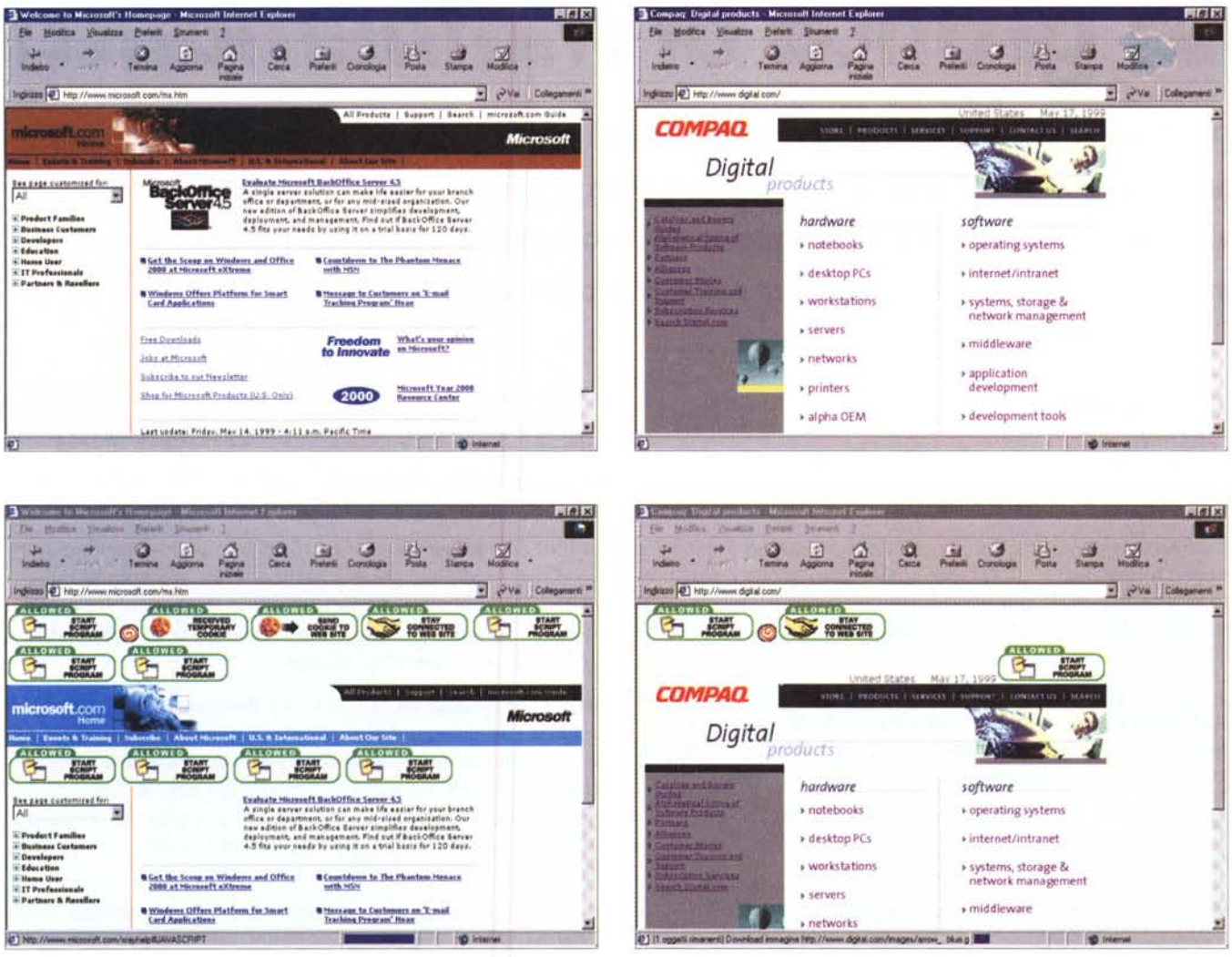
Questo livello è già sufficientemente avanzato, ma si può fare di più e meglio. Se si passa alle autorizzazioni avanzate, si raggiungono livelli di sottigliezza, nelle scelte, di tutto rispetto. Si può scegliere di non accettare nessun cookie, di accettarlo ma di mantenerlo solo in memoria, senza depositarlo sul disco, di cancellare tutti i cookie in presenza di certe attività, di non accettarne se non provenienti da certe locazioni. Si può impedire il refresh della pagina, e si può altrettanto impedire agli JavaScript di eseguire certe attività potenzialmente perniciose, come sottomissione di form, lancio di plug-in e di Java applet, come pure è possibile impedire a pagine Web di lanciare controlli Active-X o eseguire redirection.

Ma perché tante precauzioni? Occorre ricordare che anche siti famosi e di tutto rispetto, specie se continuamente aggiornati, usano le più moderne tecnologie per raggiungere scopi che ben poco riguardano la nostra personale convenienza. Ad esempio le pubblicità sui banner che cambiano anche durante la lettura, le finestrine aggiuntive degli sponsor, la messaggistica più o meno nascosta che si aggiorna continuamente in base alle nostre preferenze, sono cose che fanno molto comodo a chi fa pubblicità ma di cui faremmo volentieri a meno.

Spesso i banner trasmettono di ritorno messaggistica atta a verificare la quantità di eventuali clienti che visi-



Le due tipologie di base d'uso del programma, normale e avanzata.



Un esempio di funzionamento del programma; i siti di Microsoft e Digital, prima e dopo essere stati visti ai raggi X. Attenti agli ospiti invisibili e indesiderati!

ta il sito collegato, o almeno legge il banner o il messaggio; cose certo utili per scopi di marketing, ma di cui facciamo volentieri a meno. Inoltre occorre tenere presente che siti molto più spregiudicati e aggressivi ricuperano spesso, dal nostro browser, l'indirizzo di e-mail per consentire di arricchire mailing list (vi siete mai chiesti come mai quell'organizzazione di cui non avete neppure sentito il nome v'invia la sua pubblicità? Attenzione, anche se v'invitano a inviare una e-mail per cancellarvi dalla lista, evitate di rispondere; è solo un trucco per verificare la correttezza del vostro indirizzo).

C'è una cosa da rimarcare, nell'uso di X-Ray, che lo rende, per così dire, non perfettamente efficiente. Al momento in cui raggiunge un nuovo sito potenzialmente "pericoloso", esso carica dapprima tutta la pagina e poi indica se in questa ci sono annidati "ospiti" pericolosi; talvolta può esser troppo tardi, se l'applet o il cookie contenuto nella pagina ha già svolto la sua funzione di trasmissione dei dati (a meno di non aver insegnato a X-Ray di rifiutare qualunque ingresso). Inoltre, sebbene X-Ray possa evitare di accettare cookie di terze parti (ottenuti, ad esempio, vistando un link da un'altra pagina), non permette di capire, in questi casi, da dove essi provengano in modo da poterli accettare, se ritenuti innocui, al volo.

Conclusioni

X-Ray Vision è un buon cane da guardia, capace di sbarrare efficacemente la porta a intrusi di qualsiasi genere o di consentire l'accesso a soli ospiti desiderati. Necessario per chi ospita dati riservati sul suo computer, va settato in maniera oculata, visto che tra un blocco serrato (e sovente inutile) di ogni attività di scambio e un comportamento tollerante e potenzialmente rischioso ci sono una infinità di passaggi. Ma, ben istruito, fa il proprio dovere, in un'area dove praticamente non ha concorrenti.

MC