NoScript per Firefox, una guida informale

La versione originale di questa guida è pubblicata presso:
https://chiquadro.blogspot.com/2020/12/noscript-per-firefox-una-guida.html
Eventuali aggiornamenti saranno disponibili allo stesso indirizzo.

Versione 1.2 del 28.12.2020

Questa versione è stata impagina e convertita in PDF con OpenOffice 4,
disponibile gratuitamente presso https://www.openoffice.org/it/

Prologo

In origine l'HTML era stato pensato come puro linguaggio di markup contenente quindi solo istruzioni su come mostrare un dato contenuto. Il Web era ancora in fasce e già qualcuno, lasciamo perdere chi, decise che questo approccio era insufficiente ed eccessivamente limitante. Arrivarono gli script, le applet, i plug-in e tutto divenne maledettamente più complicato. I browser non si limitarono più a mostrare contenuti ma cominciarono a eseguire veri e propri programmi sempre più complessi esponendosi inevitabilmente ai rischi di sicurezza che ciò comporta. Non ancora paghi anche l'HTML venne progressivamente arricchito di contenuto "attivo" che col solito alibi di migliorare l'esperienza degli utenti ha iniziato a trasformarli in merce di scambio. Se pensate che stia esagerando, fatevi un giro sul sito CoverYourTracks della Electronic Frontier Foundation e poi ne riparliamo.

Giusto per darvi un'idea del problema, un qualsiasi sito web può ottenere l'elenco di tutti i font installati sul vostro computer, può conoscere il livello di carica della batteria del vostro dispositivo, può localizzarvi con un errore di pochi metri, può combinare tutte le informazioni che ha su di voi per creare una impronta unica (fingerprint) e riconoscervi ovunque su Internet. E non stiamo ancora neppure parlando di azioni veramente ostili. Se a questo punto pensate che la cosa non vi riguardi e che comunque non avete nulla da nascondere, è il caso che vi fermiate qui con la lettura. Non ho davvero voglia di spiegarvi quanto questa logica sia fallace e a quanti livelli lo sia. A tutti gli altri invece vorrei presentare NoScript, un componente aggiuntivo per Mozilla Firefox che è in grado di attenuare i rischi della navigazione sul Web soprattutto quando si visitano siti sconosciuti. NoScript è opera dell'italiano Giorgio Maone di cui potete trovare un po' di informazioni sul suo sito. Bene, non sarà un percorso breve ma spero che possa interessarvi.

Indice dei contenuti

NoScript in due parole

NoScript permette di bloccare il contenuto attivo sul Web proteggendo la sicurezza e la privacy dell'utente. Permette anche di creare regole personalizzate per i siti di cui si ha fiducia in modo da non limitarne le funzionalità. Per come è costruita, questa estensione richiede un po' di lavoro di personalizzazione prima di poter funzionare al meglio. Nei primi giorni che passerete con l'accoppiata Firefox+NoScript avrete la sensazione che non funzioni quasi più nulla, in realtà si tratterà di ragionare un po' sulla situazione specifica e decidere se un certo sito web meriti la creazione di una eccezione. Nel frattempo però NoScript vi terrà a riparo dai mille tranelli che si incontrano sul Web e in una certa misura renderà più complesso il lavoro di chi prova a tracciare le vostre attività online. Dopo breve tempo, i siti che visitate abitualmente saranno pienamente operativi mentre i pericoli delle aree dubbie della Rete resteranno bloccati. NoScript in altre parole vi restituisce l'enorme potere di decidere di chi fidarvi e di chi no sul Web, e come ogni grande potere che si rispetti sta a voi farne un buon uso.

Per questa guida ho preso a riferimento le versioni 11.1.5/11.1.6 di NoScript installate su Firefox 78 ESR.

In giro con NoScript

Installata l'estensione NoScript, l'unico segnale visibile della sua presenza sarà un nuovo pulsante aggiunto accanto alla barra degli indirizzi di Firefox. Apriamo dunque un sito qualsiasi senza farci prendere dal panico se il suo aspetto sarà molto diverso dal solito. Poi facciamo clic sull'icona di NoScript per aprire la sua finestra di dialogo che avrà un aspetto simile a quello mostrato in Fig. 1.

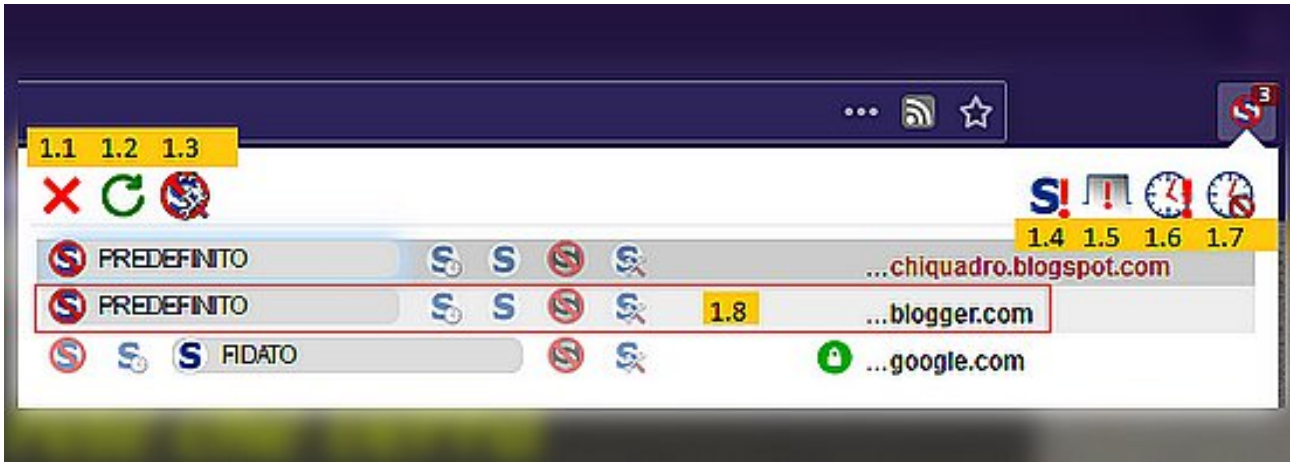

Figura 1: finestra di dialogo di NoScript

Nella riga in alto si trovano sette pulsanti, tre a sinistra e quattro a destra, dei quali vedremo le funzioni tra poco. Ora però è importante soffermare la nostra attenzione sulla parte immediatamente sottostante della finestra. Qui, la prima riga rappresenta il dominio del sito visitato mentre le righe successive indicano tutti i domini che a vario titolo sono richiamati nella pagina. Bisogna infatti tenere conto che ormai la maggior parte dei siti web è un grande patchwork di elementi che si trovano su siti diversi e che vengono richiamati in parallelo quando si apre la pagina. Sia per il dominio visitato che per i domini richiamati, NoScript mostra una riga con cinque possibili condizioni (elemento 1.8 della Fig. 1):

- *Predefinito*: al dominio saranno applicate le impostazioni predefinite di NoScript

- *Temporaneamente Fidato*: al dominio saranno applicate le impostazioni dei siti fidati ma solo per la sessione corrente; riavviato il browser il dominio tornerà nella categoria Predefinito.
- *Fidato*: al dominio saranno applicate sempre le impostazioni dei siti fidati.
- *Non fidato*: al dominio saranno applicate regole più restrittive anche rispetto al profilo Predefinito; tipicamente si utilizzerà questa impostazione solo per siti ritenuti pericolosi.
- *Personalizzato*: al dominio si applicheranno una serie di regole specifiche secondo una logica che vedremo tra breve.

Sempre con riferimento all'esempio di Fig. 1, possiamo osservare che il dominio principale del sito ricade nel profilo Predefinito di Noscript mentre il dominio della terza riga (*google.com*) adotta il profilo Fidato. È questa una situazione molto frequente dal momento che con l'uso tenderemo a impostare come fidati i siti che frequentiamo più spesso e allo stesso tempo alcuni di questi siti (da Google a Facebook ai vari circuiti pubblicitari) sono caricati in un gran numero di pagine.

Ora veniamo alla parte attiva del discorso. Se il sito visitato è di nostra fiducia e se con il profilo predefinito il sito stesso non è usabile, non dovremo far altro che fare clic sul pulsante *Fidato* della prima riga e ricaricare la pagina direttamente dal browser o usando il pulsante *Ricarica* indicato in Fig. 1 come elemento 1.2. Il pulsante 1.1 (*Chiudi*) si limita invece a chiudere la finestra di dialogo.

Se non siamo certi di voler abilitare il livello *Fidato* per un sito, è sempre possibile attivare il livello *Temporaneamente Fidato* e verificare in queste condizioni come si comporta il sito.

Arriva a questo punto la parte un po' noiosa. Abilitare il livello *Fidato* per il dominio principale spesso non è sufficiente a rendere funzionanti tutte le sue caratteristiche. Occorre quindi intervenire sugli altri domini

mostrati da NoScript portandoli a livelli meno restrittivi uno alla volta fino a trovare la combinazione che preserva le funzioni del sito senza concedere privilegi elevati a elementi non necessari o addirittura pericolosi. A complicare ulteriormente le cose concorre il fatto che un dominio impostato su *Fidato* a sua volta acquisisce i diritti per richiamare altri domini per cui a ogni ricaricamento della pagina l'elenco riportato da NoScript potrebbe allungarsi. Può sembrare frustrante, ma in realtà con il tempo si comprende che i domini da ritenere fidati sono in un numero ragionevolmente basso che comprende i siti che frequentiamo, i principali Content Delivery Network (CDN) e poco altro.

La via di fuga: quando NoScript è troppo rigido

Nell'uso di NoScript vi capiterà di tanto in tanto di incontrare qualche sito che nonostante tutti i vostri sforzi continuerà a non funzionare correttamente. In questi casi esistono delle soluzioni che permettono di risolvere il problema rinunciando temporaneamente alla protezione offerta dall'estensione. Va da sé che questi metodi andrebbero utilizzati solo su siti di buona reputazione e come misura transitoria. Se vi ritrovate a utilizzarli continuamente, allora probabilmente NoScript non è adatto al vostro stile di navigazione.

Una prima soluzione consiste nel fare clic sul pulsante *Imposta temporaneamente tutti i contenuti di questa pagina come fidati* indicato come elemento 1.6 nella Fig. 1. Il nome di questo comando è piuttosto esplicativo, in pratica stiamo applicando le impostazioni del livello Fidato a tutti gli elementi caricati nella pagina. Per quel meccanismo "a matrioska" di cui abbiamo parlato sopra, potrebbe essere necessario ripetere la procedura più volte fino ad autorizzare tutti i componenti attivi del sito e ripristinarne la piena funzionalità. Le impostazioni ottenute con il pulsante 1.6 sono temporanee, si annullano quindi chiudendo e riavviando Firefox oppure possono essere annullate facendo clic sul pulsante *Revoca i permessi temporanei*, indicato come elemento 1.7 della Fig. 1.

Una soluzione ancora più sbrigativa consiste nel fare clic sul pulsante *Disattiva le restrizioni per questa scheda*, indicato come elemento 1.5 della Fig. 1. In questo caso la scheda corrente viene svincolata dal controllo di NoScript e si comporta quindi con le impostazioni standard di Firefox; in altre parole gli script e gli altri contenuti attivi verranno eseguiti liberamente in base alla configurazione che avete adottato per Firefox. È il caso di notare che Firefox possiede dei meccanismi propri di protezione degli utenti, per cui alcuni componenti a rischio di una pagina

potrebbero comunque essere bloccati. Utilizzare il pulsante 1.5 già all'apertura di una nuova scheda è inoltre un buon metodo per navigare senza restrizioni in un sito di nostra fiducia. I permessi accordati con il pulsante 1.5 decadono automaticamente chiudendo la scheda a cui sono riferiti.

Lo stesso approccio del "liberi tutti" oltre che alle singole schede può essere applicato all'intera sessione di navigazione. Può essere utile ad esempio quando si intendono visitare siti certamente sicuri per i quali non si ritiene necessaria l'azione di NoScript. Per ottenere questo risultato basta fare clic sul pulsante *Disattiva le restrizioni a livello globale (rischioso)* indicato come elemento 1.4 della Fig. 1. Per ripristinare la situazione precedente è sufficiente fare clic nuovamente sullo stesso tasto che avrà assunto la nuova denominazione di *Attiva le restrizioni a livello globale*. Le medesime impostazioni si trovano anche nel pannello di configurazione di NoScript, come vedremo tra un po'.

Facciamo il punto della situazione: arrivati fin qui sarete in grado di configurare i siti di vostra fiducia in modo che possano funzionare con NoScript. Sarete inoltre in grado di disattivare a vari livelli l'azione di NoScript per poter accedere senza limitazioni a quei siti che non è stato possibile configurare individualmente. Non male direi. Adesso si tratta di fare un ulteriore passo in avanti e andare a sbirciare dentro le impostazioni di NoScript.

Le opzioni di NoScript

Partiamo per l'ennesima volta dalla Fig. 1 e facciamo clic stavolta sul pulsante *Opzioni...* indicato come elemento 1.3. Apriremo in questo modo una nuova scheda di Firefox contenente le impostazioni di NoScript il cui contenuto sarà simile a quello mostrato in Fig. 2.

Figura 2: Opzioni di Noscript

Le opzioni di configurazione sono distribuite su diverse schede. Iniziamo con ordine e partiamo proprio dalla scheda *Generale*. Qui ci sono tre diverse voci che permettono di modificare il comportamento predefinito di NoScript:

- *Disattiva le restrizioni a livello globale (rischioso)*: se spuntata, l'opzione disattiva l'azione di NoScript. Questa voce è associata al pulsante 1.4 di Fig. 1 che può essere utilizzato, come detto sopra, come scorciatoia per modificarne lo stato.
- *Imposta i siti principali temporaneamente come FIDATI*: Come abbiamo visto sopra, NoScrit di base non fa distinzioni tra il sito principale visitato e gli altri domini che vengono richiamati all'interno di una pagina. Questa opzione permette di considerare

temporaneamente fidati i siti principali visitati mantenendo invece un controllo più elevato sugli altri domini. È in sostanza una impostazione che rende meno rigido il funzionamento di NoScript e che può essere utile soprattutto per gli utenti che visitano solo siti affidabili. Ora, mi rendo conto che il concetto di che cosa sia affidabile sul Web è abbastanza effimero, per cui sta a voi decidere entro quali margini muovervi.

- *Applica le restrizioni del documento principale anche ai sotto-documenti*: questa impostazione serve a mitigare il problema dei "siti matrioska" di cui abbiamo discusso sopra. Se attivata fa sì che le impostazioni applicate al sito principale (prima riga) siano estese automaticamente anche agli altri siti richiamati nella pagina (righe successive). Può essere una opzione utile, a patto però di diventare molto più selettivi nel concedere diritti ai siti visitati. Altrimenti si rischia di vanificare le funzioni di NoScript.

La parte inferiore della scheda *Generale* ci permette di andare ancora più in profondità nel funzionamento di NoScript. Qui infatti è possibile stabilire per i livelli *Predefinito*, *Fidato* e *Non fidato* quali azioni sono concesse e quali no, agendo sulle voci del riquadro *Consenti*. Per esempio i siti che ricadono nel livello *Predefinito* non possono eseguire script Javascript né caricare font remoti. Le stesse operazioni sono invece concesse ai siti nella categoria *Fidati*. I siti nella sezione *Non fidati* invece non potranno caricare nessuno degli elementi controllati da NoScript.

Di base non è necessario modificare queste impostazioni. Ciò non toglie che, presa confidenza con l'estensione, non vi verrà voglia di fare un po' di esperimenti. È inoltre interessante notare che se nella finestra di dialogo di Fig. 1 si sceglie il livello *Personalizzato* per un sito si avrà la possibilità di configurare gli stessi elementi visti ora ma specificamente per il singolo sito.

Vediamo a questo punto di capire meglio su cosa interviene

concretamente NoScript partendo proprio dall'elenco di voci del riquadro *Consenti*:

- *script*: Interviene essenzialmente su JavaScript e più astrattamente sul tag script di HTML. È il cuore di NoScript proprio perché all'abuso degli script sono legati quasi tutti i maggiori pericoli che si riscontrano sul Web. D'altro canto il Web moderno non esisterebbe senza JavaScript, da qui la necessità di riportarne il controllo nelle mani dell'utente.
- *oggetto*: indica gli oggetti caricati attraverso plug-in. Con l'imminente fine di Flash questo genere di contenuti diventerà molto più raro. A livello generale, un plug-in può essere più rischioso di uno script perché tipicamente interagisce a un livello più profondo con il sistema operativo.
- *contenuti multimediali*: indica i flussi multimediali audio e video che possono essere inseriti in HTML5. Disattivare questa voce anche per i siti fidati è un buon modo per non ritrovarsi musiche e filmati che partono a tradimento ;)
- *riquadro*: attraverso i tag frame e iframe una pagina HTML può caricarne un'altra anche completamente diversa. Di per sé non è una funzione malvagia, tuttavia può essere utilizzata anche per scopi ostili. Spuntando questa voce questi tag vengono ignorati.
- *font*: come già detto permette di bloccare il caricamento dei font da remoto. Se questa voce è attiva, i font remoti verranno sostituiti con dei font locali e questo è un buon metodo anche per risparmiare banda sulle connessioni con traffico limitato. D'altro canto, utilizzare font sostitutivi potrebbe alterare il modo in cui la pagina si presenta. Personalmente penso che valga la pena provare ad attivare questa voce anche sui siti fidati, ma va a gusti.
- *webgl*: per farla breve WebGL fornisce supporto alla grafica 3D nel browser. Se ne può fare a meno, tranne casi particolari.

- *recupera*: interviene sulle API XMLHttpRequest, ma detto così mi rendo conto che non è di grande chiarezza :) Allora, XMLHttpRequest è un insieme di strumenti che permette lo scambio di dati in formato XML tra due siti. Utilizzata tramite script, questa funzione consente di creare pagine il cui contenuto cambia dinamicamente senza bisogno di ricaricarle. Ovviamente consentire questo scambio espone l'utente a possibili attacchi e violazioni della sua privacy.
- *ping*: l'attributo ping in un link consente di avvisare un altro sito quando si fa clic sul link stesso. Funzione decisamente odiosa oltre che molto discutibile in termini di privacy.
- *altro*: indica genericamente altri tipi di richieste appartenenti per esempio a standard in via di definizione. Difficile valutare quindi come gestire questa voce senza entrare nei dettagli del codice, direi che le impostazioni predefinite sono le più opportune (bloccate solo per i siti Non fidati).

Gestire i permessi di NoScript

Portiamo ora la nostra attenzione sulla seconda scheda delle impostazioni di NoScript, quella denominata *Permessi siti individuali*. In questa sezione è riportato l'elenco di tutti i domini per cui siano stati impostati permessi diversi da quelli predefiniti. Ogni volta che con NoScript si aggiunge un sito tra i fidati, tra i temporaneamente fidati o tra i non fidati, le relative impostazioni vengono aggiunte in questa sezione. Lo stesso accade quando per un sito si definiscono impostazioni personalizzate. In Fig. 3 è mostrato un esempio del tipo di struttura con cui è organizzata la lista.

Figura 3: Permessi in NoScript

Come si può osservare, per ogni dominio configurato sono riportate cinque icone corrispondenti ai livelli di configurazione che abbiamo visto in precedenza: *Predefinito*, *Temporaneamente fidato*, *Fidato*, *Non fidato* e *Personalizzato*. Il preset a cui il dominio appartiene è evidenziato con il relativo nome scritto per esteso.

Lo scopo primario della finestra *Permessi siti individuali* è quello di permettere all'utente di rivedere le impostazioni che ha regolato in

precedenza. Se per esempio abbiamo inserito il dominio example.com tra quelli fidati e in un secondo momento volessimo cambiare questa regola, non dovremmo far altro che trovare il dominio stesso nell'elenco e poi fare clic sul preset a cui vogliamo portarlo. In particolare, applicando il livello *Predefinito* il sito verrà rimosso dalla lista dato che a esso si applicheranno le impostazioni di default. La rimozione non è istantanea per evitare di dover ricaricare la pagina di configurazione, ma riaprendola in un successivo momento si potrà verificare l'assenza dei domini riportati al livello predefinito.

Altra funzione utile in questa scheda di configurazione è la casella *Cerca o aggiungi un sito web*. Scrivendo in questa area il nome di un dominio, lo si potrà isolare facilmente dalla lista globale evitando in questo modo di dover scorrere a mano l'elenco. Se il dominio non è presente nella lista invece, basterà fare clic sul pulsante [+] per aggiungerlo. In questo modo si disporrà di un canale alternativo per configurare un dominio, utilizzabile anche senza visitare il sito stesso. Eseguendo questa operazione il dominio viene aggiunto alla lista fidata e la relativa riga viene evidenziata. Si potrà quindi procedere ad applicare al dominio il livello di preset desiderato.

Scorrendo la lista presente in *Permessi siti individuali* salta subito agli occhi che alcuni domini sono scritti in nero e preceduti dal simbolo di un lucchetto verde chiuso. Altri invece sono scritti in rosso e preceduti dal simbolo di un lucchetto rosso aperto. Probabilmente avrete già intuito di che cosa si tratta. La combinazione lucchetto verde chiuso e sito in nero indica i domini configurati con protocollo sicuro https. La combinazione lucchetto rosso aperto e sito in rosso indica invece i domini configurati su protocollo standard http. Il discorso sarebbe davvero lungo a questo punto, ma semplificando molto le cose possiamo dire che le comunicazioni da e verso un sito https sono cifrate e quindi protette mentre quelle verso un sito http avvengono senza cifratura. È buona

regola trasmettere dati personali o riservati solo attraverso connessioni https.

Attenzione però a non interpretare la presenza del protocollo https come garanzia di serietà del sito che lo adotta. Il protocollo garantisce, entro certi margini, la riservatezza delle informazioni trasmesse ma non dice nulla sul modo in cui poi quelle informazioni saranno utilizzate una volta arrivate a destinazione. Aggiungendo il fatto che i certificati necessari a implementare un sito https sono disponibili anche gratuitamente, si capisce perché da solo questo elemento non deve essere considerato una garanzia assoluta. Trattate https come un test di esclusione: se un sito vi chiede di inviare dati sensibili sul protocollo standard http, allora è sicuramente da scartare se non altro per la scarsa serietà che dimostra. La situazione contraria invece di per sé non è garanzia di affidabilità e sicurezza.

Dopo questa piccola deviazione, torniamo ora a NoScript. In linea di massima sarebbe preferibile inserire tra i domini fidati solo quelli protetti dal protocollo https. Nella pratica prima o poi vi toccherà inserire qualche dominio su protocollo non protetto. Anzi è frequente il caso in cui potreste dover configurare lo stesso dominio sia in https che in http. Niente panico comunque: sarà il browser, nel nostro caso il buon Firefox, ad avvisarci nel caso una pagina web cerchi di inviare dati senza proteggerli.

Visualizzando la sezione *Permessi siti individuali*, subito dopo aver installato NoScript, noterete la presenza di un breve elenco di domini già configurati come fidati. Si tratta di una scelta fatta dall'autore e spiegata nelle FAQ relative all'estensione. In sostanza:

- le pagine di servizio e configurazione di Firefox introdotte da pseudo-protocolli sono sempre considerate fidate per consentirne il corretto funzionamento;

- i domini addons.mozilla.org e mozilla.net da cui si scaricano le estensioni di Firefox sono considerati fidati;
- il dominio noscript.net, casa del progetto NoScript, è considerato fidato;
- alcuni domini per consentire i pagamenti con carte di credito, per vedere video su Internet e per consultare le più diffuse caselle di posta, sono inseriti nella lista dei siti fidati;
- alcuni CDN (Content Delivery Network) per elementi Javascript notoriamente affidabili sono inseriti nella lista dei siti fidati.

A parte gli pseudo-protocolli, per tutti gli altri domini preinseriti nella lista dei siti fidati è possibile intervenire manualmente. Probabilmente potrebbe sembrarvi una buona idea azzerare la lista e partire da un foglio bianco, ma è una soluzione che vi sconsiglio a meno che siate utenti piuttosto esperti o che abbiate esigenze di privacy e sicurezza davvero particolari. La whitelist precaricata in NoScript è stata evidentemente ben ponderata per non pregiudicare alcune funzionalità fondamentali della Rete e non bloccare completamente gli utenti meno esperti. Con il tempo nulla vi vieta di rimuovere alcuni dei siti della whitelist una volta accertato che non sono necessari alle vostre esigenze.

Se invece non aveste resistito alla tentazione di cancellare tutto, avete comunque un salvagente per tornare indietro. Sia in Fig. 2 che in Fig. 3 potete notare in alto il pulsante *Ripristina impostazioni* che non fa altro che riportare NoScript al suo stato iniziale. Attenzione al fatto che l'uso di questo strumento azzererà tutti i permessi impostati a livello utente, pensateci quindi due volte prima di procedere. E soprattutto non fatelo prima di aver letto il successivo capitolo ;)

Backup e ripristino di NoScript

Con il tempo l'elenco delle regole di NoScript conterrà facilmente decine e forse centinaia di voci. Nel loro insieme queste definiranno la nostra "comfort zone" nel Web e sarà quindi importante poterla ricostruire in caso di necessità. Allo stesso modo potremmo voler replicare la stessa configurazione su un computer diverso o in un differente profilo di Firefox.

Per fare un backup della configurazione di NoScript utilizzeremo il pulsante *Esporta* visibile in alto sia in Fig. 2 che in Fig. 3. Questa operazione ci permetterà di salvare un file di testo contenente tutte le nostre impostazioni. Questo file andrebbe sempre inserito nelle nostre procedure di backup in modo da poterlo recuperare facilmente in caso di bisogno. Anche una semplice copia del file archiviata su una chiavetta USB, o inviata come allegato via mail a se stessi, comunque può bastare. Più in generale dovremmo fare un nuovo backup ogni volta che la configurazione di NoScript è cambiata in maniera significativa. Anche qui il concetto di significativo è molto variabile e lasciato alla libera interpretazione di ogni utente.

Il ripristino di NoScript è altrettanto semplice. Si tratterà di utilizzare il pulsante *Importa* (Fig. 2 e Fig. 3) per caricare il backup fatto in precedenza. Attenzione al fatto che qualsiasi impostazione aggiunta dopo la data del backup ovviamente non sarà recuperabile e verrà persa dopo aver effettuato il ripristino.

NoScript è un adblock?

NoScript nasce per portare sotto il controllo dell'utente l'esecuzione degli script e altre funzioni potenzialmente indesiderate. Da questo punto di vista l'estensione è assolutamente neutrale e permette di trattare indistintamente qualsiasi dominio. Effetto indiretto di questo approccio è che anche i domini associati ai grandi circuiti pubblicitari di default si trovano nell'area dei siti predefiniti e non possono quindi caricare script. Il risultato è che gran parte della pubblicità su Internet viene a essere bloccata, pur non essendo questa la funzione primaria di NoScript.

Il discorso sarebbe lungo, ma esula decisamente dagli scopi di questa guida. Mi sembrava il caso di segnalare questa situazione solo per un motivo pratico: alcuni siti confondono l'azione di NoScript con quella di un adblock e potrebbero quindi impedirvi l'accesso. Ricaricare il sito dopo aver disattivato le protezioni di NoScript per la scheda corrente (elemento 1.5 di Fig. 1) permette di solito di risolvere il problema.

Qualche altra impostazione

Oltre alle sezioni *Generale* e *Permessi siti individuali* la pagina delle opzioni di NoScript contiene altre due schede. Ne parlo in coda perché qui si trovano impostazioni certamente utili ma non fondamentali per l'uso dell'estensione.

Nella scheda *Aspetto* è possibile regolare alcune funzioni visuali dell'interfaccia di NoScript. In particolare:

- *Mostra la voce NoScript nel menu contestuale*: se abilitata permette di richiamare la finestra di dialogo di Fig. 1 anche dal menu contestuale abbinato del tasto destro del mouse.
- *Visualizza il badge con il contatore degli script*: se abilitata mostra sull'icona di NoScript il numero di script bloccati nella scheda aperta.
- *Elenca gli indirizzi completi nel popup delle impostazioni*: se abilitata permette di applicare impostazioni differenti tra il dominio principale (example.com) e il sottodominio di default dei siti web (www.example.com). Utile probabilmente solo in pochissimi casi.
- *Alto contrasto*: se abilitato mostra l'interfaccia di NoScript con colori ad alto contrasto che ne migliorano la leggibilità e l'accessibilità tramite uno screen reader.

Nella scheda *Avanzate*, indovinate un po', si trovano alcune opzioni utili per lo più agli utenti esperti. Vale comunque la pena illustrarne brevemente il significato:

- *Purifica le richieste cross-site sospette*: se abilitato offre una protezione aggiuntiva rispetto agli attacchi cross-site scripting (XSS). Anche qui sarebbe necessario un lungo discorso propedeutico ma estraneo agli scopi di questa guida. Semplificando molto la questione, una vulnerabilità cross-site scripting permette di

iniettare un codice ostile nelle pagine di un sito web. Se questo sito è inserito nella lista dei siti fidati di NoScript, allora anche il codice ostile verrebbe eseguito con gli stessi privilegi. La funzione *Purifica le richieste cross-site sospette* controlla la struttura dei link per evitare questo genere di rischio. Potete approfondire la questione nelle FAQ di NoScript e nella descrizione delle sue funzionalità.

- *Attiva l'impostazione di permessi permanenti nelle schede incognito/anonime*: se attiva consente di poter impostare permessi permanenti anche nelle schede anonime di Firefox, una soluzione comunque sconsigliabile in termini di sicurezza. Attenzione inoltre al fatto che, nelle versioni più recenti di Firefox, le estensioni come NoScript di default non sono attive nelle schede anonime. Per utilizzare NoScript anche nelle schede anonime, occorre aprire la finestra di configurazione delle estensioni di Firefox (Menù > Componenti aggiuntivi) e, in corrispondenza della casella di NoScript, occorre impostare su *Consenti* l'opzione *Funzionamento in finestre anonime*.
- *Revoke temporary permissions on NoScript update, even is the browser is not restarted* (questa voce non è tradotta in italiano): se attiva azzera i permessi temporanei dopo ogni aggiornamento di NoScript anche se il browser non viene riavviato.
- *Debug*: se attiva consente l'accesso alla modalità di debug.

Epilogo

Siamo giunti alla fine di questo tour guidato attorno a NoScript. Spero che possa esservi utile nell'uso di questa estensione ma soprattutto che abbia contribuito ad aumentare la vostra consapevolezza sui meccanismi che reggono il Web e sui rischi che ne derivano. Per il resto, come al solito, le richieste di chiarimenti, le osservazioni o le critiche possono essere inviate all'indirizzo mhl *chiocciola* mail *punto* ch.

Risorse utili:

- NoScript.net
- Forum su informaction.com
- NoScript su Mozilla addons

Ringraziamenti: un ringraziamento speciale ai lettori che hanno contribuito a migliorare questo documento ed in particolare a *miki64*, del forum di Mozilla Italia, per aver revisionato il testo snidando molteplici refusi ed errori e per avermi fornito preziosi suggerimenti sulla struttura della guida.