

Benign, limitiamo lo spam

(i tutorial di Alessandro de Simone)

Copyright Alessandro de Simone 2003 – 2004 – 2005 (www.alessandrodesimone.net) - È vietato trascrivere, copiare, stampare, tradurre, riprodurre o divulgare il presente documento, anche parzialmente, senza l'autorizzazione scritta dell'autore. I siti Internet, le case editrici e le pubblicazioni di settore che intendano utilizzare questo documento possono contattare l'autore (benign@alessandrodesimone.net) per gli accordi del caso.

Copyright Alessandro de Simone 2003 – 2004 – 2005 (www.alessandrodesimone.net) – No transcribing, no copyng, no reproducing, no translating, no printing, no publishing this document – even if partially – without author's written authorization. Websites and publishing house who wish to employ this document must write the author (benign@alessandrodesimone.net).

Premessa

A causa della complessità dell'argomento è necessario aver ben compreso il fenomeno dello spam e come limitarlo. Per consultare la documentazione disponibile clicca sul collegamento relativo ad altri Tutorial attinenti al medesimo argomento:

"**Spam, la posta spazzatura**" - Considerazioni generali sulle e-mail, non richieste, che riceviamo quotidianamente.

"**MailWasher**" - Primi passi sull'uso del programma MailWasher prendendo come riferimento la versione gratuita.

"**MailWasher Pro 3.3**" - Impostazione dei parametri più importanti della versione MailWasher Pro 3.3

"**MailWasher - Uso del programma**" - Caratteristiche più importanti di MailWasher prendendo come riferimento la versione Pro 3.3

"**MailWasher - I messaggi e gli avvisi**" - Descrizione dei messaggi che compaiono usando MailWasher

"**Benign, limitiamo lo spam**" (questo Tutorial) - Il programma che previene i danni provocati da e-mail contenenti codici dannosi.

Come funziona Benign

Per comprendere come agisce **Benign** bisogna dapprima rendersi conto di come funziona un client di posta elettronica. Prenderò ovviamente come riferimento *Outlook Express* perché – nostro malgrado(?) – è il client più usato al mondo. Ma prima ancora di comprendere come funziona *Outlook Express*, occorre sapere come funziona lo stesso browser *Microsoft Internet Explorer* (e qualsiasi altro browser). Eh già: forse non tutti sanno che c'è una stretta e sistematica interconnessione tra un browser per Internet e il computer sul quale viene usato. Ma cominciamo con ordine.

Come funziona un browser

Nel momento esatto in cui ci connettiamo a Internet non facciamo altro che collocare il nostro PC in un nuovo punto della "ragnatela" mondiale. In pratica un filo invisibile (invisibile mica tanto: il modem, comprensivo del filo della rete telefonica, rappresenta a tutti gli effetti un tangibile esempio di connessione hardware) un invisibile filo, dicevo, viene creato tra il nostro PC e la Rete delle Reti, costringendolo a diventare un nuovo nodo del caotico web. Ma anche "caotico" è un termine improprio: in realtà la connessione è ordinatissima, guai se non lo fosse! In un qualunque istante di qualsiasi giornata, ciascun computer del nostro pianeta è infatti caratterizzato da un indirizzo estremamente preciso, fornito da quattro numeri separati da un punto, come per esempio...
189.43.67.123

Dal momento che ognuna delle quattro parti può essere numerata da 0 a 255, ne

conseguenze che sono possibili...

$255 \times 255 \times 255 \times 255 = 4.294.967.296$

...cioè oltre quattro miliardi di PC connessi contemporaneamente. In realtà il totale non è così elevato perché alcuni valori non sono ammessi. Tuttavia, siccome sulla Terra vi sono sei miliardi (e passa) di persone, immaginate che cosa accadrebbe se ognuno di loro decidesse di connettersi a Internet nel medesimo momento! È questo il motivo, infatti, per cui ci si sta attrezzando – a livello internazionale – per individuare una diversa numerazione che tenga conto del limite accennato.

Ma torniamo a noi: la numerazione deve essere univoca e valida sia dall'interno sia dall'esterno del PC. Ciò significa che un qualsiasi PC si auto-identifica sempre con la quaterna di numeri **127.0.0.1** denominata, in gergo, **localhost** (letteralmente: *computer locale*). Oltre a 127.0.0.1 il PC assume anche uno dei 4.294.967.296 numeri possibili, proprio per essere individuato univocamente dai PC che possono “vederlo” dall'esterno. Riepilogando: tutti i PC del mondo, quando sono connessi a Internet, per distinguersi da tutti gli altri si auto-denominano 127.0.0.1 e – contemporaneamente – assumono un numero identificativo univoco, sempre diverso, che lo distingue da tutti gli altri. Se, per esempio, in un certo istante ci connettiamo al web, il sistema mondiale (al quale fa riferimento il nostro provider) assegna al nostro PC un certo numero (supponiamo: 201.234.0.45) che – a seconda del nostro contratto – può essere sempre lo stesso, oppure cambia dinamicamente di volta in volta. In ogni caso, quando siamo connessi, il nostro PC vede se stesso sempre con il numero 127.0.0.1 mentre gli altri computer, connessi al web in quel momento, lo individuano con il numero 201.234.0.45. In conclusione, se in questo momento il mio sito (www.alessandrodesimone.net) è individuato dal numero 201.234.0.45, dall'interno del vostro browser – qualunque esso sia – potete digitare, indifferentemente *www.alessandrodesimone.net* oppure *201.234.0.45* per visitarlo.

Ma a che cosa può servire sapere tutto ciò? Semplice: qualunque sistema operativo deve necessariamente conoscere, in qualsiasi momento, in che modo identificare il computer sul quale risulta installato. Il valore 127.0.0.1 è quindi memorizzato all'interno di un file particolare, denominato semplicemente **hosts** (privo di suffisso) che, per ciò che riguarda *Windows XP*, è collocato nella cartella *C:\WINDOWS\system32\drivers\etc* mentre, per individuarne la collocazione nelle altre versioni di Windows, basterà effettuare una ricerca, appunto, del file *hosts*.

Dal momento che un PC che si connette a Internet deve sempre gestire il file *Hosts*, ne consegue che l'eventuale manipolazione di questo file può provocare effetti collaterali, alcuni dei quali di sicuro interesse per quanto riguarda la sicurezza. Anzitutto, se manipoliamo il file *hosts* in modo tale che alla semplice riga originale...

```
127.0.0.1 localhost
```

...aggiungiamo la seguente...

```
127.0.0.1 www.alessandrodesimone.net
```

...ogni volta che cercheremo di connetterci al sito digitando l'indirizzo *www.alessandrodesimone.net* nel campo specifico, il sistema operativo dirotterà la ricerca verso... se stesso (o meglio, verso il PC sul quale il sistema operativo stesso risulta installato) con il risultato che la connessione al sito risulterà in pratica impedita. Analogamente, se aggiungiamo il rigo...

```
237.34.50.211 www.alessandrodesimone.net
```

...tutte le volte che tenteremo di visitare il sito *www.alessandrodesimone.net* la navigazione verrà inevitabilmente dirottata verso il sito 237.34.50.211 (numero preso a caso: chissà a quale sito corrisponde...).

Questo modo di operare è sfruttato in tutte quelle procedure di sicurezza che dirottano eventuali richieste di connessioni verso i cosiddetti siti *proibiti* o *inadatti*.

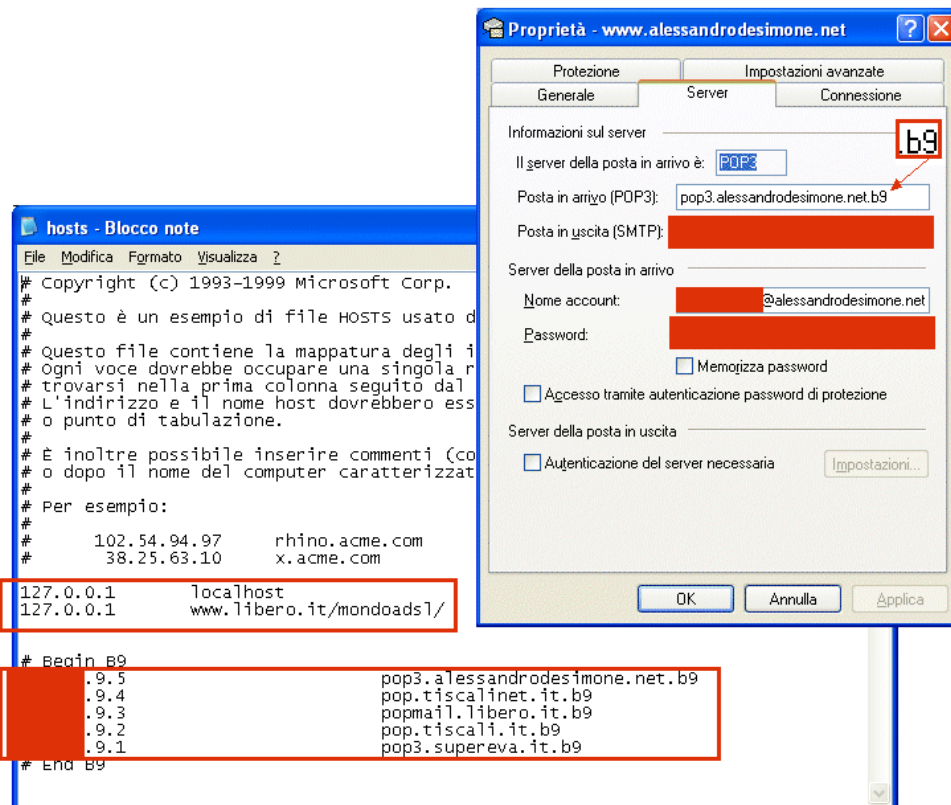


Figura 1. Manipolazioni compiute da Benign sul file Hosts e sulla cartella "Server" di Outlook Express. Sullo sfondo il contenuto del file Hosts di Windows XP dopo l'installazione di Benign.

Benign e il file Hosts

Anche Benign sfrutta la particolare gestione del file *Hosts* per controllare la posta in arrivo: il PC in uso, quando riceve l'ordine di connettersi a un sito, esamina dapprima eventuali "dirottamenti" verso i siti elencati nel file Hosts. Se il sito da visitare non fa parte dell'elenco qui contenuto, effettivamente consente al browser di visitarlo; se, invece, il sito fa parte dell'elenco, lo dirotterà verso il suo sostituto. Il fatto è che il sistema operativo esamina sempre il contenuto del file Hosts, anche se l'ordine proviene da programmi diversi dal solito browser. Ciò significa che l'ordine può essere ricevuto anche dal client di posta elettronica, ed esattamente dal parametro di configurazione per la connessione al server mail della posta in arrivo, il famoso **POP3**. Come si può vedere in figura 1, infatti, la cartella *Server* delle *Proprietà* di *Outlook Express* deve necessariamente contenere la stringa che rappresenta l'indirizzo del server di posta (potrebbe anche essere un nome di pura fantasia). È proprio il caso di Benign: se avete la pazienza di controllare il contenuto della cartella "*Proprietà/Server*" (e contemporaneamente del file Hosts), prima e dopo l'installazione di Benign, vi accorgete che sono state introdotte delle modifiche. Nel campo "*Posta in arrivo (POP3)*" noterete che è stato aggiunto un particolare suffisso (**b9**) che rappresenta il logo di Benign; nel file Hosts, invece, ad ogni account controllato corrisponde un particolare valore, necessario per dirottare la richiesta di lettura della posta. In altre parole, ogni volta che tenterete di scaricare la posta, Benign dirotterà la richiesta verso quel particolare sito al quale è stato affidato il compito di filtrarla prima che venga realmente scaricata sul PC in uso. Lo dimostra, se non altro, la richiesta del firewall eventualmente installato sul PC in uso.

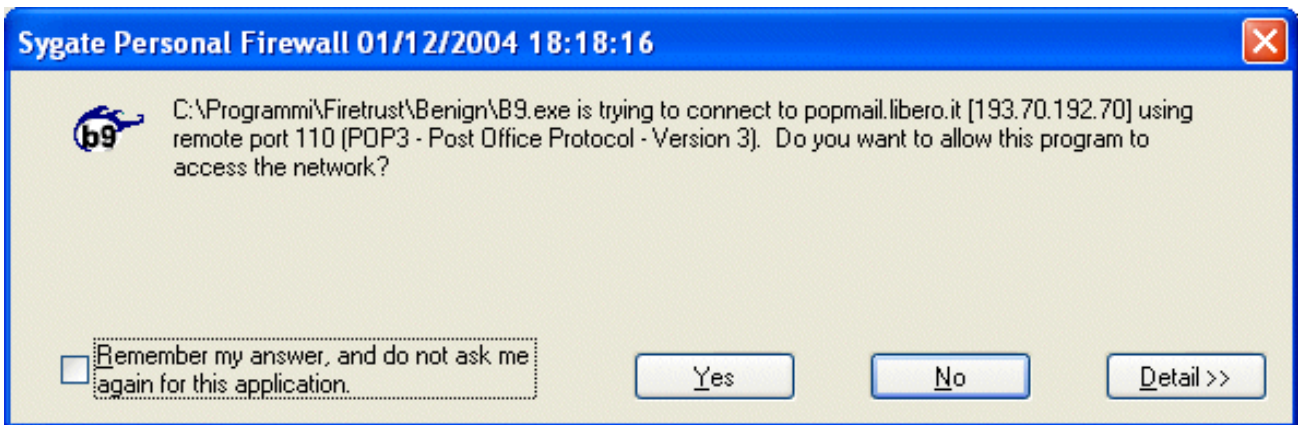


Figura 2. L'azione di Benign è monitorata da un eventuale firewall (in figura, Sygate Personal Firewall).

Caricamento / Installazione / Cookies / Etc.:

Benign è disponibile presso il sito www.firetrust.com sotto forma di un file compresso autoestraente di nome *benign.exe*, lungo 1.295 KB. Dopo una prima verifica (effettuata in data 2 dicembre 2003) il programma *non* manifestava la presenza di trojan, né di spyware (scansione compiuta nella stessa data con il programma "*Spybot - Search & Destroy*" aggiornato alla stessa data). Non sono stati individuati *cookies* né in fase di download del programma, né in seguito alla connessione a Internet per la registrazione. Il programma è garantito funzionante con i sistemi operativi Windows 95, 98, NT4, Millennium, 2000, e XP. È possibile gestire solo gli account che seguono il protocollo POP3: ciò significa che è possibile gestire le e-mail che di solito scarichiamo sul nostro PC con i client specifici (per esempio: *Outlook Express*). **Non** è quindi possibile gestire la posta elettronica se questa viene consultata direttamente sul server del provider (collegandosi, per esempio, alla sezione posta dei siti di *Virgilio.it*, *Libero.it*, *Tin.it* e altri).

Come funziona il programma

Per limitare il fenomeno dello spam, ma soprattutto per evitare la diffusione di pericolosi allegati, **Benign** agisce direttamente sul server della posta elettronica, prima ancora che le e-mail vengano scaricate con il client (per esempio: *Outlook Express*) che abitualmente usiamo per tale funzione. In altre parole, il programma Benign viene aperto non appena si accende il PC (lo dimostra la presenza della sua icona nella *sys tray*, vedi figura 3) e si predispone ad intercettare il momento in cui l'utente apre il client di posta. Appena ciò accade, Benign si connette al server ed attiva tutte le procedure di sicurezza che l'utente ha a suo tempo impostato (e di cui parleremo tra breve): solo dopo aver compiuto tali verifiche, i vari messaggi di posta (comprensivi di eventuali allegati) verranno finalmente scaricati nel PC.

Da quanto detto finora si deduce facilmente che è di fondamentale importanza impostare adeguatamente i parametri di configurazione, in quanto il programma agirà rispettandoli rigorosamente. È ovvio che l'utente può, in qualsiasi momento, intervenire per apportare qualunque modifica.

Primi parametri di installazione

Per facilitare al massimo l'installazione del programma, Benign visualizza un *wizard* (figura 3). La prima finestra (**A**) avverte che le impostazioni che verranno assegnate agiranno solo sugli account che stanno per essere indicati. L'individuazione di questi è infatti automatica in quanto il programma è in grado di individuare tutti gli account presenti sul PC in uso, anche se appartenenti a client di posta differenti. Premendo il pulsante *Next* (non visibile in A) compare una seconda finestra (**B**) che contiene già selezionati, per default, tutti gli account individuati: se si desidera escludere dal controllo qualcuno di questi basterà rimuovere il segno di spunta presente alla loro sinistra. Da notare che gli account vengono indicati con due parametri: il primo (a sinistra, per esempio "*Microsoft Outlook*" or "*Outlook Express*") indica il client sul quale risulta registrato l'account, mentre a destra (per esempio "*Pippo*") il *nickname* con il quale l'utente ha registrato l'account stesso. Da sottolineare che l'utente potrebbe utilizzare il medesimo account (per esempio *pippo@nome_dominio.com*) con due client diversi di posta elettronica (per esempio *Outlook Express* e *Mozilla*). La presenza di un "doppione", apparentemente inutile, indica invece la possibilità di attivare la protezione di Benign solo con uno dei due client che l'utente utilizza. Va da sé che è molto meglio assicurarsi la protezione in qualunque caso, vale a dire qualunque sia il client di posta elettronica che si userà durante le normali connessioni al web. La quarta finestra che compare (**D**, sempre di figura 3), visualizza – a scanso di equivoci – l'elenco di tutti gli account che verranno gestiti dal programma a partire da questo momento.

La terza finestra che compare (**C**, di figura 3) contiene il parametro "*Security profile*" impostato per default sul valore "*Medium*". Nei primi esperimenti, tuttavia (come verrà del resto precisato più avanti) vi consiglio di impostare il valore "*Low*" per evitare la perdita di allegati importanti. Anche questo parametro – come tutti gli altri – può comunque essere modificato in qualunque momento.

Questo spazio è disponibile per il tuo messaggio pubblicitario.

Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.

[Click here](#) for details or [Contacts](#)

Espace puor votre annonce.

[Clic ici](#) pour détail ou [Contact](#)

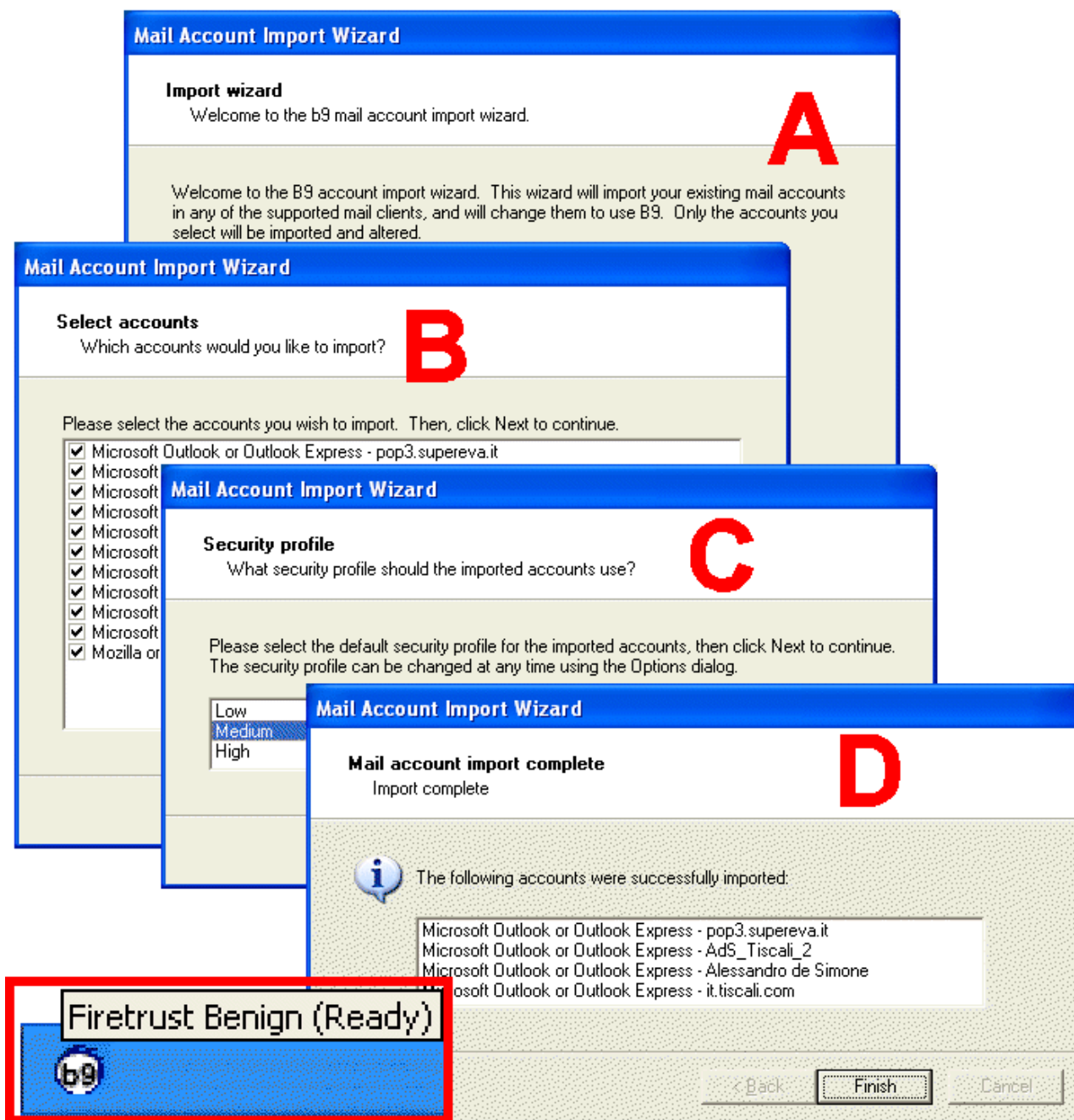


Figura 3. Le quattro finestre dell'installazione guidata (nel riquadro in basso, la presenza di Benign nella systray).

La prima volta di Benign

Dopo aver seguito i quattro passi del wizard di configurazione (figura 3) compare la finestra principale del programma, apparentemente piuttosto scarna (figura 4, in primo piano): oltre alla barra dei menu (*File, Tools, Register, Help*) la barra degli strumenti presenta tre soli pulsanti in grigio (*Summary, Options, Register*) che però diventano verdi sovrapponendo il mouse. Più in basso due barre orizzontali, inizialmente poste a zero, serviranno per visualizzare la quantità di mail processate dal programma (figura 4, sullo sfondo) fino a quel momento (prima barra) e nella giornata odierna (seconda barra).

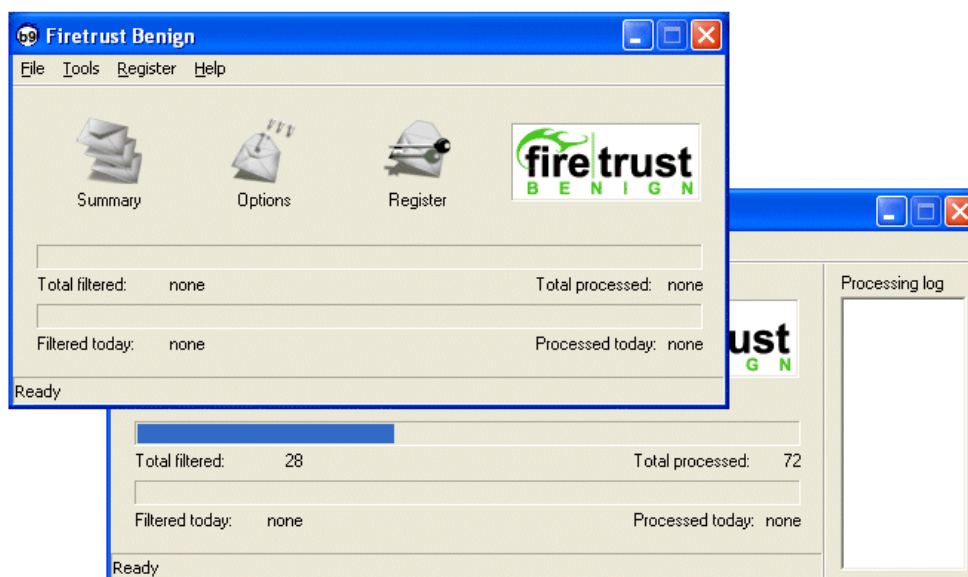


Figura 4. La finestra principale di Benign subito dopo l'installazione (primo piano) e dopo qualche giorno di utilizzo (sullo sfondo).

Summary

Premendo il pulsante “*Summary*” compare una finestra che contiene due cartelle (“*Summary*” e “*Message log*”, vedi figure 5, 6 e 7). La prima di queste (“*Summary*”), a sua volta, permette di consultare i report dettagliati sulla posta scaricata, in modo da individuare con precisione tutte le azioni intraprese dal programma in base ai parametri impostati. La casella di spunta “*Show explanations*” visualizza (oppure nasconde, se deselezionata) una breve descrizione del significato.

Summary/Message (figura 5). Rimandando al Tutorial specifico sullo spam ([clicca qui](#) per consultarlo) mi limiterò a dire che i messaggi di posta elettronica possono contenere codice maligno. Il primo parametro (“*Messeges processed*”) si limita a indicare il numero di messaggi elaborati dal programma. Il secondo parametro (“*Messeges filtred*”) indica il numero di messaggi che *Benign* ha filtrato attenendosi alle indicazioni fornite. Se alcuni messaggi sono stati bloccati dal programma, perché ritenuti pericolosi (sempre in base alle indicazioni fornite dall'utente) “*Read receipts blocked*” ne indica il numero. Analogamente gli ultimi due parametri “*Attachments blocked*” e “*Attachment renamed*” indicano, rispettivamente, il numero degli allegati distrutti (prima che venissero scaricati sul PC) e di quelli che invece sono stati rinominati con un suffisso speciale, per evitare che qualche procedura automatica li attivasse.

Questo spazio è disponibile per il tuo messaggio pubblicitario.
Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.
[Click here](#) for details or [Contacts](#)

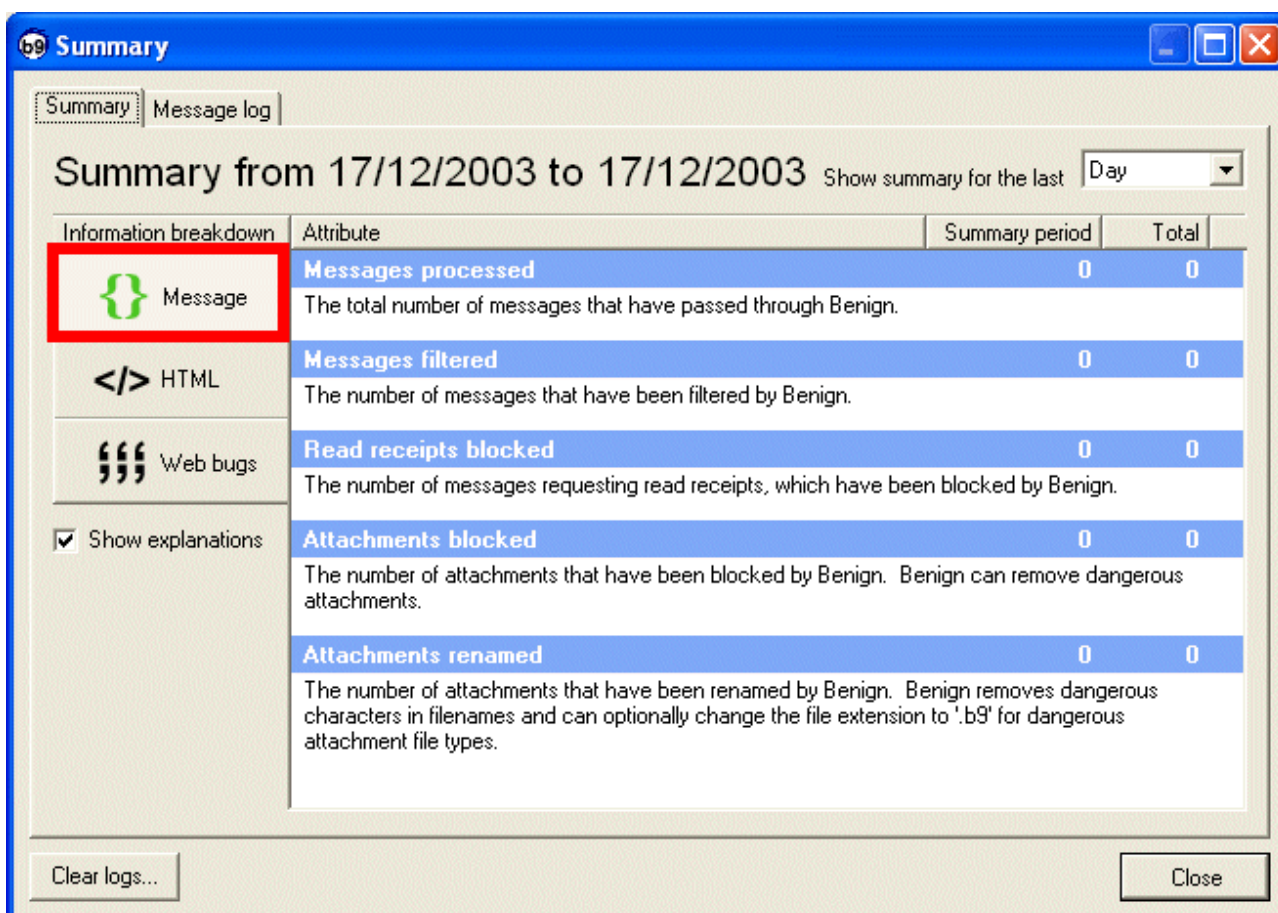


Figura 5. Elenco delle informazioni sulla gestione dei messaggi ricevuti.

A questo punto è bene fare qualche considerazione in proposito: come già specificato nel Tutorial sullo spam ([clicca qui](#) per consultare la documentazione completa) un allegato di posta elettronica potrebbe essere un programma (suffisso *.com*, *.bat* oppure *.exe*) oppure un file di altro genere (suffisso *.doc*, *.xls*) potenzialmente capaci di attivare una procedura dannosa per il PC. Benign permette di eliminare allegati di questo genere *prima* che vengano scaricati sul PC, oppure di *rinominarli* in modo da consentire all'utente di compiere, in seguito, la scelta più opportuna. Anche se torneremo ancora su questo argomento, è ovvio che la cancellazione – ma sarebbe meglio dire “distruzione” – degli allegati è una soluzione certamente sicura, ma drastica: la procedura viene infatti applicata indistintamente a tutti gli allegati, anche a quelli che provengono da mittenti sicuri. Nel caso in cui ci si accorge che un allegato è stato distrutto, l'unico modo per riaverlo è quello di chiederlo nuovamente al mittente! Ecco perché conviene limitarsi a impostare l'aggiunta di un suffisso agli eventuali allegati che corredano le e-mail (vedremo tra breve come fare) piuttosto che distruggerli per “eccesso di prudenza”. Il fatto è che l'impostazione “*Medium*” (al momento della prima installazione, vedi figura 3, C) comporta per default la soluzione drastica: ecco perché, come ho detto in precedenza, conviene impostare il parametro “*Low*”, che si limita ad aggiungere un suffisso agli allegati.

Summary / HTML (figura 6). Una e-mail potrebbe *non* essere stata scritta in puro testo, ma ricorrendo ai cosiddetti *tag* del linguaggio HTML, vale a dire una particolare formattazione del testo che consente di abbellire il messaggio stesso (applicazione di neretto, sottolineato, grandezze diverse dei caratteri, applicazione di colori, inserimento di collegamenti, figure e così via). Purtroppo il linguaggio HTML permette anche la gestione

di file di *scripting* che, invisibili all'utente, potrebbero contenere codice maligno in grado di provocare danni di vario genere.

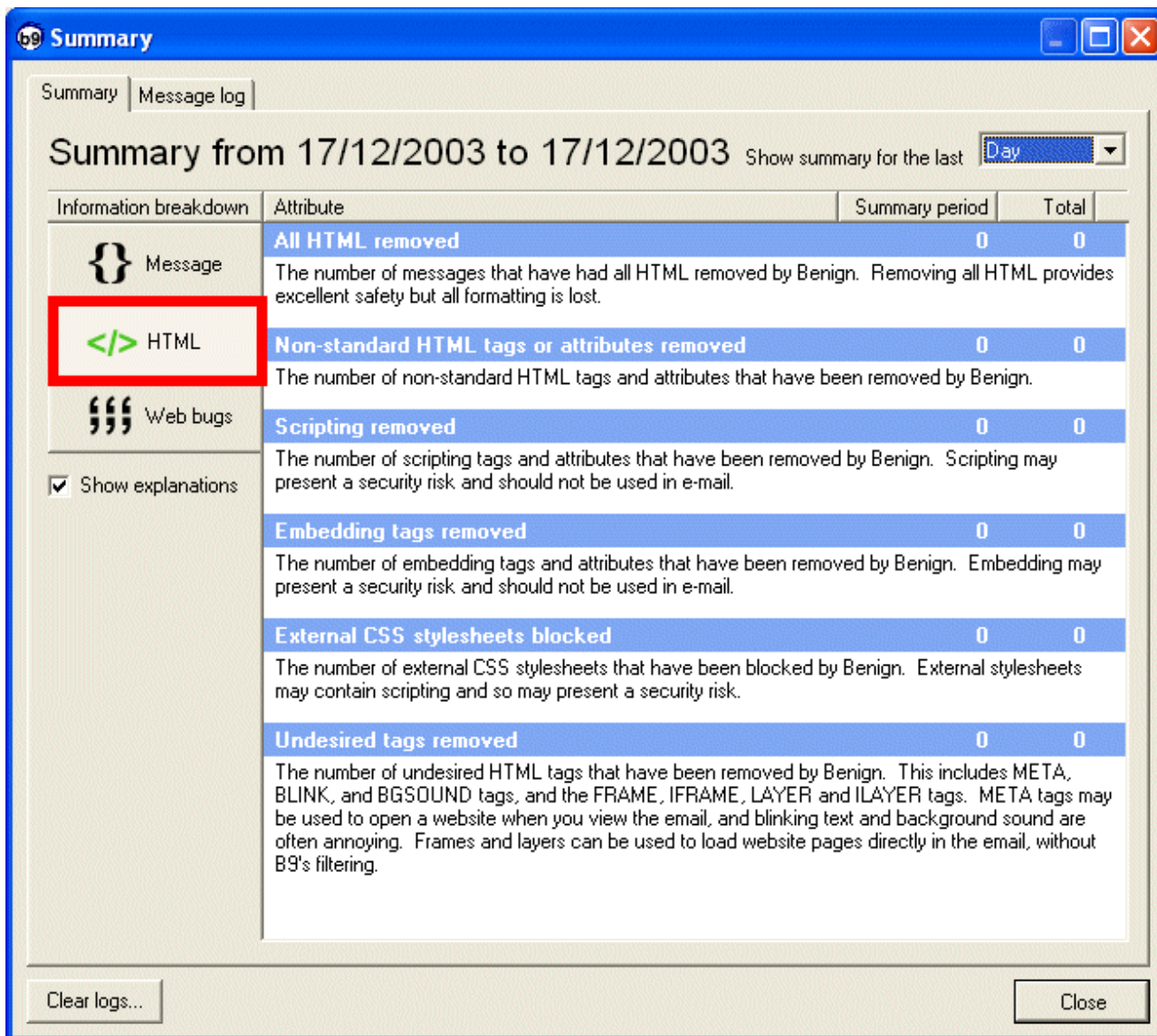


Figura 6. Elenco delle informazioni sulla gestione dei messaggi in formato HTML.

Anche in questo caso la suddivisione in varie sezioni (“All HTML removed”, “Non-standard HTML tags or attributes removed” ... “Undesired tags removed”) fornisce un accurato elenco delle operazioni compiute.

Summary / Web bugs (figura 7). Un'immagine, inserita in una e-mail, potrebbe contenere collegamenti invisibili a siti non affidabili (tra cui quelli che impongono l'uso di costosi prefissi telefonici per la connessione al web): un involontario clic su di esse costringerebbe il browser a connettersi a detti siti, con le conseguenze che è facile immaginare. Analogamente, un'immagine potrebbe fornire informazioni servendosi dei famigerati “cookie”, piccoli file che vengono inseriti sul PC dell'utente a sua insaputa. Anche in questo caso *Benign* mostra l'elenco completo di tutte le azioni effettuate nei vari casi contemplati (“Images from external servers blocked” ... “1x1 images blocked”).

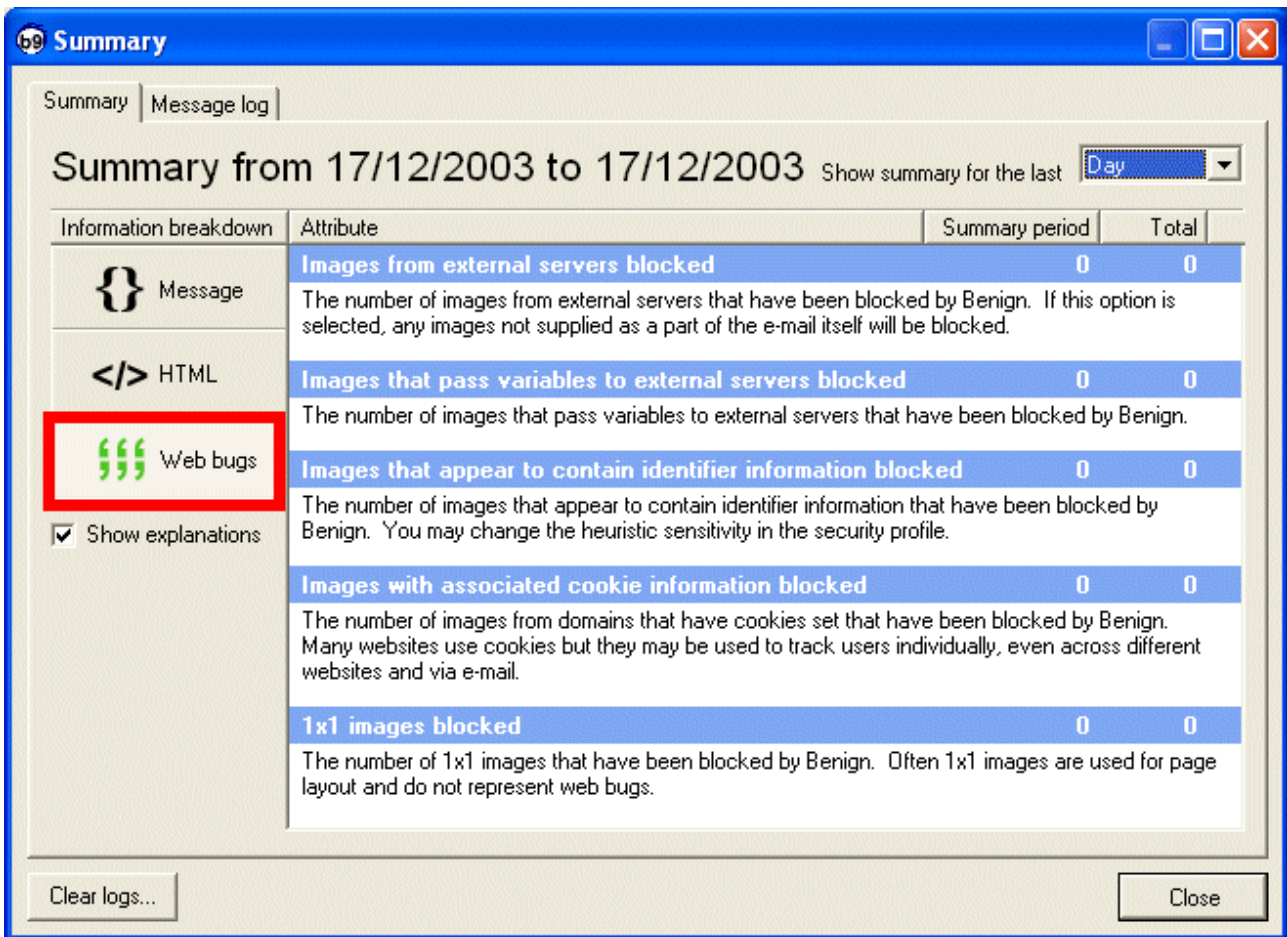


Figura 7. Elenco delle informazioni sulla gestione dei web bugs legati alle immagini eventualmente presenti nelle e-mail a noi destinate.

Questo spazio è disponibile per il tuo messaggio pubblicitario.
 Per informazioni, [clicca qui](#) o invia un [messaggio](#)

This space is for your advertisement.
[Click here](#) for details or [Contacts](#)

Espace puor votre annonce.
[Clic ici](#) pour détail ou [Contact](#)

Il presente Tutorial è stato modificato il giorno 22 settembre 2005
 Per ulteriori aggiornamenti consultare il sito www.alessandrosimone.net