Malwarebytes' Anti-Malware

Malwarebytes' Anti-Malware è un programma per la protezione del personal computer che si è guadagnato, soprattutto nel corso del 2008, un'ottima fama come strumento per l'eliminazione dei componenti dannosi eventualmente presenti sul personal computer. Uno dei vantaggi principali derivanti dall'utilizzo di Malwarebytes' Anti-Malware è certamente la velocità di scansione.

Il prodotto viene distribuito in due versioni: la prima, freeware, completamente gratuita; la seconda a pagamento. Se la release freeware permette di riconoscere e rimuovere le minacce già presenti sul sistema, la versione a pagamento aggiunge la possibilità di fruire di un modulo residente in memoria in grado di bloccare le infezioni e di una funzionalità per la pianificazione dell'analisi dei dischi fissi e delle altre unità di memorizzazione.

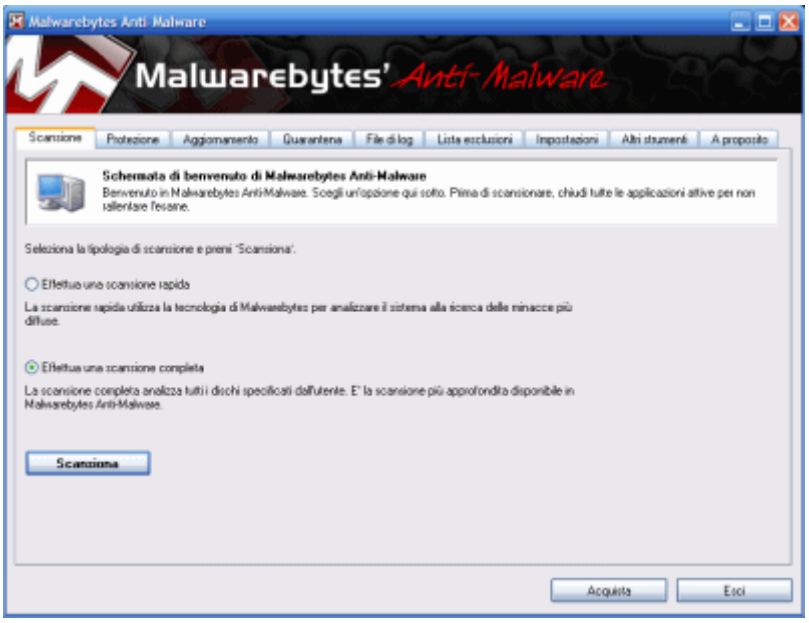
Se, all'atto dell'avvio della procedura d'installazione, il programma sembra non avviarsi, è altamente probabile che sul sistema in uso sia presente un malware in grado di monitorare l'attività del sistema e bloccare automaticamente l'esecuzione di programmi per la sicurezza. Di solito il problema è risolvibile semplicemente rinominando il file `mbam-setup.exe`, ad esempio, in `m.exe`, già all'atto dell'avvio del download.

Una volta avviata l'installazione di Malwarebytes' Anti-Malware, scelta la lingua italiana, accettato il contratto di licenza d'uso e specificata la cartella di destinazione, il programma richiederà se debba essere avviata anche la procedura di aggiornamento (suggeriamo di lasciare attivate sia *Aggiorna Malwarebytes' Anti-Malware* che *Avvia Malwarebytes' Anti-Malware*).

Qualora l'aggiornamento del software sembri non aver luogo (la barra di avanzamento non visualizza il messaggio *Updating*), suggeriamo di eliminare completamente il file HOSTS contenuto, nel caso di Windows XP, nella cartella `\windows\system32\drivers\etc`.

Se anche dopo aver effettuato questo intervento, Malwarebytes' Anti-Malware non fosse in grado di scaricare da Internet alcun aggiornamento, l'unica cosa da fare è proseguire senza applicare gli update (almeno per il momento).

Alla comparsa della finestra principale del programma, è bene scegliere *Effettua una scansione completa* e premere il pulsante *Scansiona*.



Una volta completata questa fase, è bene provvedere alla cancellazione delle minacce eventualmente rilevate da parte di Malwarebytes' Anti-Malware. Pur essendo estremamente abile nell'individuazione dei componenti nocivi, talvolta Malwarebytes' Anti-Malware presenta dei “falsi positivi” ossia indica come pericolosi elementi che in realtà non lo sono veramente.

Se si nutrono dei dubbi sull'effettiva pericolosità dei file indicati come nocivi da parte di Malwarebytes' Anti-Malware, è bene effettuare qualche ricerca in Rete in modo da stabilire l'identità dei componenti segnalati. A tal proposito, si potrebbero sottoporre i file indicati come nocivi ad un'analisi sul sito web VirusTotal. Anche un servizio come SystemLookup si rivela spesso molto utile.

I più esperti possono segnalare gli eventuali “falsi positivi” servendosi dell'apposito pulsante (scheda *Altri strumenti, Segnala falso positivo*): in questo modo, grazie alla collaborazione degli utenti, il team di sviluppo di Malwarebytes' Anti-Malware potrà correggere opportunamente il database contenente le informazioni sulle minacce in circolazione. La scheda *Lista esclusioni* consente di specificare un elenco di file da non prendere in considerazione nel corso delle successive attività di scansione: è questa la sezione ideale per indicare file che sono certamente riconducibili a “falsi positivi”.

Eliminate le minacce individuate sul personal computer, è bene operare un riavvio del sistema operativo quindi eseguire nuovamente Malwarebytes' Anti-Malware.

A questo punto, nel caso in cui ciò non fosse stato in precedenza fattibile, si provi ad aggiornare manualmente il prodotto (scheda *Aggiornamento*, pulsante *Controlla aggiornamenti*) quindi ad effettuare una nuova scansione completa del sistema.

Ricorrendo alla scheda *Altri strumenti*, gli utenti più smaliziati possono ricorrere anche all'uso di *FileAssassin*: si tratta di una speciale funzionalità, disponibile anche sotto forma di software a sé stante, che consente di eliminare file specifici che dovessero risultare “bloccati” da parte del sistema operativo o di altre applicazioni (anche malware).

Per individuare eventuali minacce passate inosservate a Malwarebytes' Anti-Malware, consigliamo, successivamente, di installare il software **SuperAntiSpyware** (ved. anche questa pagina), anch'esso disponibile in versione gratuita, lanciare un aggiornamento delle firme virali ed avviare una scansione completa con le impostazioni di default.

Anche in questo caso, suggeriamo di porre in quarantena le minacce rilevate effettuando un riavvio del personal computer al termine della procedura di analisi.

Infine, sarebbe opportuno avviare una scansione dell'intero sistema con **Avira AntiVir.** Prima di procedere con l'installazione di Avira AntiVir, è bene provvedere alla rimozione dell'antivirus eventualmente già presente sul sistema: se avete rilevato gravi infezioni malware sul personal computer, appare chiaro come l'antivirus installato non abbia fatto il suo dovere (in molti casi il suo corretto funzionamento viene addirittura impedito dal malware stesso, insediatosi sul sistema).

Rimozione delle restrizioni eventualmente imposte dai malware

Non è cosa infrequente avere a che fare con sistemi che, in seguito ad un'infezione da malware, si rifiutano di consentire all'utente l'accesso ad aree chiave del sistema. Ad esempio, anche dopo aver rimosso un malware, può capitare di non riuscire più ad accedere alle proprietà del sistema, alla finestra "Risorse del computer" e così via.

Dopo essersi accertati di aver eliminato tutte le minacce, per eliminare le restrizioni imposte dal malware, è possibile ricorrere ai comandi seguenti:
Per Windows XP: `secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose`
Per Windows Vista: `secedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose`

Nel caso in cui non si riuscisse più ad accedere al prompt dei comandi, è possibile – sempre cliccando su *Start, Esegui...* - ricorrere al comando seguente:
`REG add HKCU\Software\Policies\Microsoft\Windows\System /v DisableCMD /t REG_DWORD /d 0 /f`

Se è il "task manager" di Windows che non si apre, il comando da utilizzare è quello che segue:
`REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG_DWORD /d 0 /f`

Talvolta alcuni malware impostano una restrizione che impedisce il caricamento dell'Editor del registro di sistema (REGEDIT). Per sanare la situazione e riprendere il controllo anche su tale applicazione, si può eseguire questo comando:

```
REG add
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Sys
tem /v DisableRegistryTools /t REG_DWORD /d 0 /f
```

In tutti tre i casi, viene utilizzato il comando REG, basato su riga di comando, abbinato all'opzione “ADD”. L'indicazione finale “ /f ” richiede la sovrascrittura del valore del registro specificato dopo “ /v ”, senza richiedere conferma da parte dell'utente. Il valore DWORD viene impostato a zero (“ /d ”).

Il programma freeware *XP Security Console*, prelevabile da questa pagina, aiuta spesso a risolvere molte problematiche correlate all'applicazione di restrizioni da parte dei malware. Per rimuovere le limitazioni, è sufficiente avviare l'applicazione e cliccare sul pulsante *Apply*. Il software è compatibile solo ed esclusivamente con i sistemi Windows XP.