

Ad-Aware Free

Dieci anni di protezione da spyware

► Il problema

Protezione del sistema operativo da spyware, trojan, keylogger e rootkit in tempo reale



► La soluzione

Nella versione del decennale, Ad-Aware ha aggiunto alla sua nota affidabilità la protezione in tempo reale e da vari tipi di malware oltre che da spyware

Quando si parla di un antispyware affidabile, Ad-Aware è uno dei programmi citati più spesso. Da anni viene apprezzato per la capacità di individuare lo spyware, segnalarlo ed eliminarlo. Utilizzandolo, si protegge il sistema operativo e si riducono i rischi per i dati personali degli utenti.

Versione del decennale

Nella versione 8 del 2009, l'aggiunta di *Anniversary Edition* al nome del programma ricorda il fatto che sono trascorsi dieci anni da quando l'applicazione è stata rilasciata la prima volta. Nell'occasione sono state aggiunte nuove caratteristiche e nuove funzionalità che migliorano di molto l'efficacia del prodotto.

Fino a tutto il 2008, per esempio, nelle versioni gratuite la scansione del disco e l'aggiornamento del file delle firme sono stati gestiti dagli utenti in modalità manuale. Ora, invece, con *Ad-Watch Live!* il controllo della presenza di eventuale malware avviene in tempo reale. Il traffico di dati in transito nel sistema

viene intercettato automaticamente per verificare se ci sono elementi maligni che possono compromettere la riservatezza dei dati dell'utente.

Oltre allo spyware, la nuova versione è in grado di combattere altri tipi di malware, ancora più pericolosi. Viene verificata l'eventuale presenza di trojan, di keylogger, di rootkit e di hijacker. I primi possono installare anche *backdoor*, applicazioni che permettono di prendere possesso a distanza del computer, quando è collegato in Rete.

I *keylogger* catturano sequenze di tasti premuti dall'utente per trasferire nomi utente e password ad altre persone che possono utilizzarle per finalità maligne.

I *rootkit* permettono a un utente remoto di prendere possesso del computer. Un *hijacker*, infine, dirotta la visualizzazione di una pagina Web verso un'altra pagina creata ad arte per tentare di fargli installare trojan o altro malware.

Nella versione del decennale, Ad-Aware offre protezione da questi e da altri elementi ancora, pur rimanendo gratuito per l'utilizzo personale.

Altre caratteristiche

L'aggiornamento del file delle firme ora è automatico e, nelle opzio-

Una barriera contro i malware

► Il riavvio completa l'installazione

L'installazione avviene in italiano, selezionando nella finestra *Select Setup Language*. Al termine della sequenza delle finestre dell'installazione guidata, è opportuno selezionare la casella *Riavvia adesso* per provocare la chiusura e la ripartenza di Windows. Solo poi viene attivato correttamente il servizio di protezione di Ad-Aware.

► Interfaccia a icone

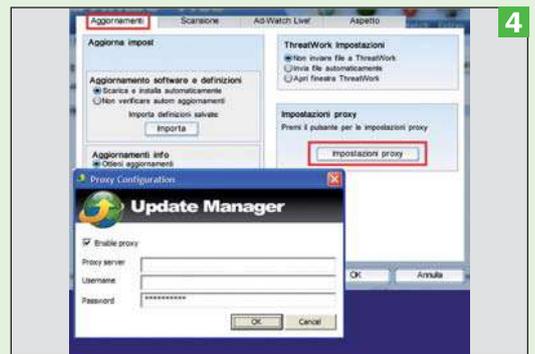
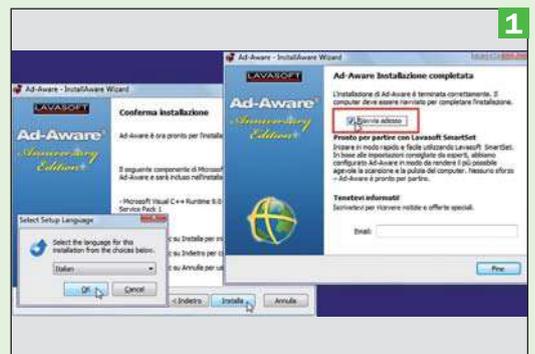
La finestra di lavoro del programma mostra tre grandi icone al centro. Facendo clic sulla prima, si avvia la ricerca degli aggiornamenti del file delle firme. Un clic sul *Sistema di scansione* conduce nell'area in cui si può lanciare la scansione dei dischi. Un clic su *Ad-Watch Live!* apre la pagina con lo stato della protezione in tempo reale.

► Lancio della scansione

Per verificare se sia presente spyware o altro malware, si fa clic sull'icona *Sistema di scansione*. Per lanciare la scansione, si fa clic sul pulsante *Scansione ora* nella pagina *Scansione Intelligente* o in *Scansione completa*. Al termine, il pulsante diventa *Esegui azioni adesso* per attivare le funzioni di pulizia degli elementi individuati.

► Impostazione del proxy in rete

Se il computer è in rete, occorre superare il blocco imposto dal proxy fornendo i dati del server e dell'account. Con la sequenza *Impostazioni, Aggiornamenti, Impostazioni proxy* si apre la finestra *Proxy configuration*. Dopo aver attivato la casella *Enable proxy*, si inseriscono l'URL del proxy, il nome utente e la password e si conferma su OK.



Ad-Aware Free Anniversary Edition
Categoria: sicurezza
Versione: freeware
Sito: www.lavasoft.it
Richiede installazione: si
S.O.: Windows Vista, XP 2003

ni, si può scegliere tra più lingue tra cui l'italiano.

Nella sezione *Extras* si possono pulire le tracce della navigazione in Internet lasciate nella

cache, nei cookie e nella cronologia dei principali browser. Con l'installazione, nel menu contestuale viene aggiunta una voce per verificare l'integrità di un certo fi-

le o di una cartella. Se si lavora in rete, si possono impostare i dati del server *proxy* e dell'account per superare il blocco del traffico verso Internet.

Chi lo desidera può inviare direttamente file sospetti a *ThreatWork*, un'associazione di volontari che combattono minacce che insidiano macchine e dati degli utenti.

Le funzionalità di Ad-Aware si integrano nel *Centro Sicurezza PC*, attraverso il quale si visualizzano anche notizie sul livello di protezione.

Le caratteristiche hardware richieste per il funzionamento equivalgono a quelle di un computer di diversi anni fa. Infatti è sufficiente avere un Pentium a 600 MHz e 100 MB di spazio libero su disco.

Il sistema operativo può essere Vista a 32 e a 64 bit, Windows XP a 32 bit e Windows 2000 Professional.

la ricerca avviene in tutti gli archivi e non solo nei file eseguibili.

Nella scansione completa, inoltre, viene eseguita la ricerca anche nel file *hosts*, nei file aperti di recente dalle varie applicazioni (MRA: *Most Recent Used*) e negli ADS (*Alternate Data Streams*). A questo proposito, va rimarcato che Ad-Aware *Anniversary Edition* è uno dei pochi programmi che controlla anche negli ADS, i flussi di dati alternativi che affiancano i file in NTFS.

Per gli amministratori di Rete e i responsabili della sicurezza è utile sapere che si può lavorare con il programma anche da linea di comando. Il comando da eseguire può essere aggiunto in un file *batch* con parametri che ne determinano la modalità di funzionamento. Le principali opzioni riguardano il livello di "profondità" della scansione e le azioni da eseguire nel caso di rilevamento di malware.

Da linea di comando, poi, si può lanciare anche l'aggiornamento del programma e del file delle firme.

Documentazione e aiuto in linea

Nelsito del produttore, <http://www.lavasoft.it>, è disponibile un manuale PDF in inglese di quasi cinquanta pagine. Il testo illustra in dettaglio le caratteristiche e le funzionalità del programma. Le funzioni sono riportate in modo da evidenziare le differenze tra quelle della versione gratuita di Ad-Aware e quelle disponibili a pagamento.

Analoghe informazioni sono riportate nell'aiuto in linea, attivabile con un clic sulla scritta *Help*. Anche qui viene evidenziata la differenza tra le varie versioni del programma riportando tra parentesi e in tre diversi colori le scritte *Free*, *Plus* e *Pro*.

Saverio Rubini



► Modifica dell'interfaccia

Colori e aspetto della finestra di lavoro possono essere modificati nella pagina *Impostazioni, Aspetto*. A destra c'è un elenco a discesa nella sezione *Interfaccia*. Un clic sulla riga apre l'elenco a discesa delle interfacce disponibili. Per completare l'operazione si deve confermare su *OK*, chiudere e riavviare la visualizzazione della finestra.



► Ad-Aware da linea di comando

Con la sequenza *Start, Esegui, CMD, OK*, si apre la finestra in cui lanciare le funzioni scrivendole accanto al prompt. La sintassi è "Ad-Awarecommand.exe <parametri>". L'elenco dei <parametri> è in *Using Command Line Parameters* del manuale o dell'*help*. Riportando i comandi all'interno di file *.BAT*, l'esecuzione può avvenire in modalità *batch*.

Interfaccia e funzionalità

L'interfaccia di *Ad-Aware Anniversary Edition* è completamente diversa rispetto a quella delle versioni precedenti e può essere modificata per aspetto e colori.

Nella finestra di lavoro appaiono tre icone per gestire le tre principali attività che si possono gestire: l'aggiornamento manuale del file delle firme, l'avvio della scansione e la visualizzazione degli eventi che sono stati rilevati da *Ad-Watch Live!*.

I comandi e le funzioni del programma sono divisi in quattro aree alle quali si accede facendo clic sulle icone in alto a destra. All'interno di ogni area, le attività sono raggruppate in singole pagine, da aprire facendo clic su apposite linguette.

Nell'area *Scansione*, la differenza tra la modalità "intelligente" e quella "completa" viene resa evidente da una tabella che elenca gli elementi sui quali avviene il controllo nei due casi. Per esempio, passando nella pagina della scansione completa si vede che



► Aggiornamento manuale delle firme

Chi lo desidera può eseguire l'aggiornamento manuale del file delle firme. In questo caso occorre prelevare prima il file compresso da Internet, per esempio dall'indirizzo <http://www.lavasoft.com/mylavasoft/securitycenter/blog>. Successivamente si esegue *Impostazioni, Aggiornamenti, Importa*, si seleziona il file e si conferma.



► Modalità di scansione

Con la sequenza *Impostazioni, Scansione*, si giunge nella pagina *Impostazione profili*, dove si scelgono le modalità con cui deve avvenire la ricerca del malware nei supporti memoria. In *Scansione file* si scelgono i tipi di file tra cui indagare. In *Sezioni da analizzare*, invece, si selezionano le aree di sistema in cui eseguire la scansione.