Malware

Definizione e funzione

Cos’è un Malware

Il termine *Malware* è l'abbreviazione di "malicious software", software dannoso. Malware è un qualsiasi tipo di software indesiderato che viene installato senza un adeguato consenso. Lo scopo di un malware è creare danni al software (e hardware) del computer o ai dati dell’utente del pc: rovinare un sistema operativo, compromettere funzioni del computer, compiere, all’insaputa dell’utente, azioni illegittime con il computer (ad esempio, inviare e-mail dall’account di posta del pc o attaccare altri computer), prelevare o danneggiare i dati, modificare le connessioni, raccogliere vari tipi d’informazioni personali, installare software all’insaputa, e reindirizzare ad altre pagine internet indesiderate, ecc.
Spesso si confonde il termine malware con *virus*. Per malware si intende l’intera tipologia dei software dannosi. Un virus è un *tipo di malware* che, come vedremo, ha la caratteristica di *replicarsi* infettando l'intero computer e quelli a cui sono collegati: un virus, per infettare il pc, *necessita dell’intervento umano* come il doppio clic di mouse su un file o su un’immagine in internet. Da quel momento darà inizio al contagio.
Un malware si può introdurre in un computer in vari modi. In generale i malware si diffondono tra i pc sfruttando i metodi di comunicazione esistenti. Ogni sistema adatto a trasportare informazioni da un pc a un altro è candidato a diventare sistema di infezione. È possibile infettare un computer attraverso una chiave USB, un cd o ogni altro strumento di memorizzazione rimovibile, oppure utilizzando le reti informatiche.
Attualmente i malware si diffondono soprattutto utilizzando le reti di computer, prima tra tutti internet, e la posta elettronica, sfruttando anche l'inesperienza di molti utenti e, nel caso delle mail, la curiosità. Gli utenti devono prestare attenzione soprattutto quando scaricano file e programmi da internet, soprattutto da siti poco conosciuti, e alle e-mail con allegati. Proprio le e-mail sono il metodo di diffusione principale dei malware, sfruttando "buchi" dei software di posta e la curiosità degli utenti che aprono qualsiasi messaggio arrivi sul PC, anche da indirizzi sconosciuti.

Diversi modi con cui si può nascondere il malware

Abbiamo visto che un malware si può introdurre in un computer in diversi modi. A seconda dei casi si può distinguere in:
Trojan: chiamato anche Trojan Horse, consiste in un file nascosto all'interno di programmi di utilizzo comune e largo utilizzo. Per esempio, si potrebbe trovare un gioco gratuito disponibile in rete che, una volta scaricato ed eseguito, senza che l’utente stesso ne sia a conoscenza, avvia e installa il codice trojan nascosto nel programma: questo codice lavora in background nel sistema con lo scopo di danneggiarlo oppure di rubare informazioni. È

chiamato “Cavallo di Troia” proprio perché nasconde secondi fini, dove apparentemente non vi è nessun rischio.
Rootkit: il termine si può tradurre come “equipaggiamento per amministratore”. È un insieme o un singolo software capace di controllare un computer locale o remoto, nascondendosi. In questo modo un hacker può accedere e impossessarsi del computer di un utente e usarlo per i suoi scopi: rubare i dati, utilizzare il computer per attaccare altri sistemi, ecc.
I rootkit attaccano i moduli più interni del sistema operativo, spesso per nascondere delle *backdoors* (porte di servizio, vedi definizione successiva) per scavalcare le porte di sicurezza attivate da un sistema informatico o da un pc, entrando nel sistema.
Non sempre un rootkit è un software maligno. Può essere “regolare” come parte di un software legittimo, ad esempio per il controllo remoto di un pc da parte di un centro di assistenza.
Backdoor: le backdoor (letteralmente”porta sul retro”) consentono di superare le procedure di sicurezza, attivate dal sistema informatico o computer, per entrare nel sistema. Queste porte possono essere create per agevolare la manutenzione o il controllo remoto del pc da utenti autorizzati. Si pensi al caso di un centro assistenza di una software house che opera in remoto per adeguare on line un programma acquistato presso di loro. In questo caso le backdoors sono usufruite in maniera corretta. Invece, se sono installate automaticamente da malware, permettono l’ingresso di utenti malintenzionati che possono utilizzare il pc con il controllo remoto senza che il proprietario ne sappia nulla.

Malware infettivo

Un malware infettivo è composto da poche righe di codice che si attaccano a un programma, infettandolo. Si installa automaticamente e lavora in background.
Il malware infettivo consiste, in linea di massima, di virus e worm.
Virus: un virus è un programma che si attiva e si diffonde in modo totalmente indipendente dalla volontà dell'utente.
L'obiettivo è quello di danneggiare i dati o i programmi dei destinatari, oppure infettare altre applicazioni, modificandole e includendovi una copia di se stessi. Si usa il termine "virus" in quanto il suo comportamento può essere paragonato a quello biologico, per la similitudine del modo di propagarsi dell'infezione.
In genere i virus si “nascondono” per un certo tempo e durante questo periodo, chiamato “letargo”, controllano tutti gli eventi del sistema operativo o quelli legati all'utente. Quando si verifica l'evento atteso, per esempio viene aperto un determinato file, il virus inizia la sua azione.
La “vita” di un virus informatico si svolge in tre fasi: trasmissione, riproduzione e alterazione.

1. Nella fase di trasmissione il virus “infetta” uno o più file del computer;
2. nella fase di riproduzione il virus copia se stesso nel sistema, all'interno del singolo PC o nella rete.
3. Nella fase di alterazione il virus svolge il suo compito, che spesso significa danneggiare dati e programmi.

Worm: tradotto in lingua italiana “Verme“. Questo tipo di malware modifica il sistema operativo in modo da essere eseguito automaticamente ogni volta che viene acceso il

sistema, rimanendo attivo per tutta la durata di tempo, fin quando non si spegne il computer. Si muove quindi senza bisogno di intervento esterno. È in grado di replicarsi come fa un virus, ma non ha bisogno di "attaccarsi" ad altri file eseguibili dato che usa internet per potersi riprodurre rapidamente. Uno dei mezzi per il contagio è la posta elettronica: il worm invia email ai contatti memorizzati allegando un file infetto (Attachment).

Malware usati per furto di dati, profitto/estorsione

Abbiamo visto che un malware può essere progettato con lo scopo di creare danni alle componenti software e hardware del computer su cui viene eseguito. Ma ci sono malware creati per avere un profitto in modo più o meno illecito. Tra questi ci sono:

Adware: (abbreviazione di *advertising-supported software*, "Software sovvenzionato da pubblicità"). È un programma che propone messaggi pubblicitari, non richiesti dall'utente, attraverso finestre popup o durante il processo di installazione di un software. L'apertura di continui popup pubblicitari può rallentare le prestazioni del computer. Altri adware modificano le pagine html proposte dal browser per includere link e messaggi pubblicitari propri. Molti adware inoltre comunicano le abitudini di navigazione dell'utente a server remoti, violando la privacy.

Spyware: ("software spia"). Uno spyware non attacca il computer per danneggiarli, ma, durante l'attività al pc, raccoglie e trasferisce dati e informazioni dell'utente del pc. Questi dati possono essere strettamente personali e riservati, come password, numero di carta di credito, ecc., ma anche indicazioni sull'attività del proprietario del computer: ad esempio, acquisti online, siti visitati, chiaramente senza il consenso. Le informazioni sono vendute ad aziende per effettuare della pubblicità mirata.

Botnet: letteralmente tradotto significa "rete di bot". *Bot* è un'abbreviazione di "robot", ma il termine che rende più l'idea di questo tipo di infezione è "zombie". Attraverso falle nella sicurezza o per mancanza di attenzione da parte dell'utente, il dispositivo viene infettato per consentire ad hacker malintenzionati (*botmaster*) di controllare il sistema da remoto: in questo modo il computer può iniziare a svolgere operazioni a insaputa del proprietario: si può far parte di una botnet senza neanche saperlo. Più computer infettati e controllati formano una *botnet*: se un computer diventa parte di una botnet, potrebbe rallentare ed essere completamente in balia di hacker.

Chi è in possesso di una botnet può far svolgere qualsiasi azione ad ogni singolo computer infetto: inviare messaggi email indesiderati, diffondere virus, attaccare "in massa" computer e server. Infatti, una botnet è formata da un numero elevato di computer, addirittura milioni di pc. Con un tale "esercito" si può sferrare un attacco in sincronia (*DDos*, Distributed Denial Of Service) contro server di enti, società governative, aziende e multinazionali.

Keylogger: un keylogger è uno strumento capace di registrare tutto quello che un utente digita sul suo computer. Dispositivi di keylogger possono essere presenti anche nei bancomat per intercettare il codice PIN. I keylogger possono essere di tipo hardware, inserito dentro la tastiera o collegato al cavo tra tastiera e pc, o software.

Dialer: è un programma che si auto installa nel computer e modifica i parametri della connessione internet e impostarla verso numeri telefonici molto costosi. L'utente si troverà di fronte a inspiegabili aumenti delle bollette telefoniche. Chi utilizza una linea ADSL non corre alcun rischio dato che non è prevista la connessione remota.

Proteggersi dai malware

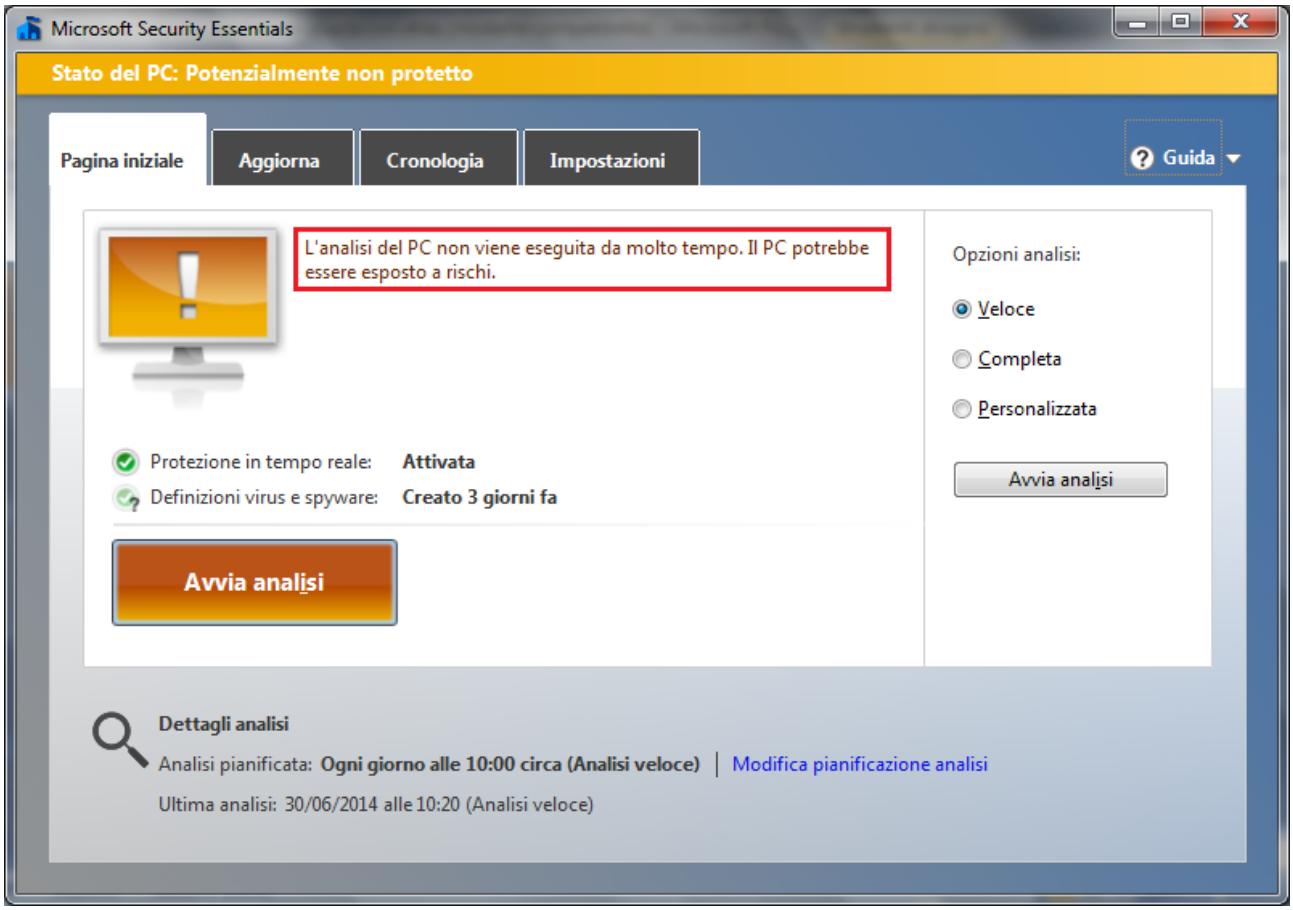
Antivirus e antimalware

Un antivirus è anche antimalware?

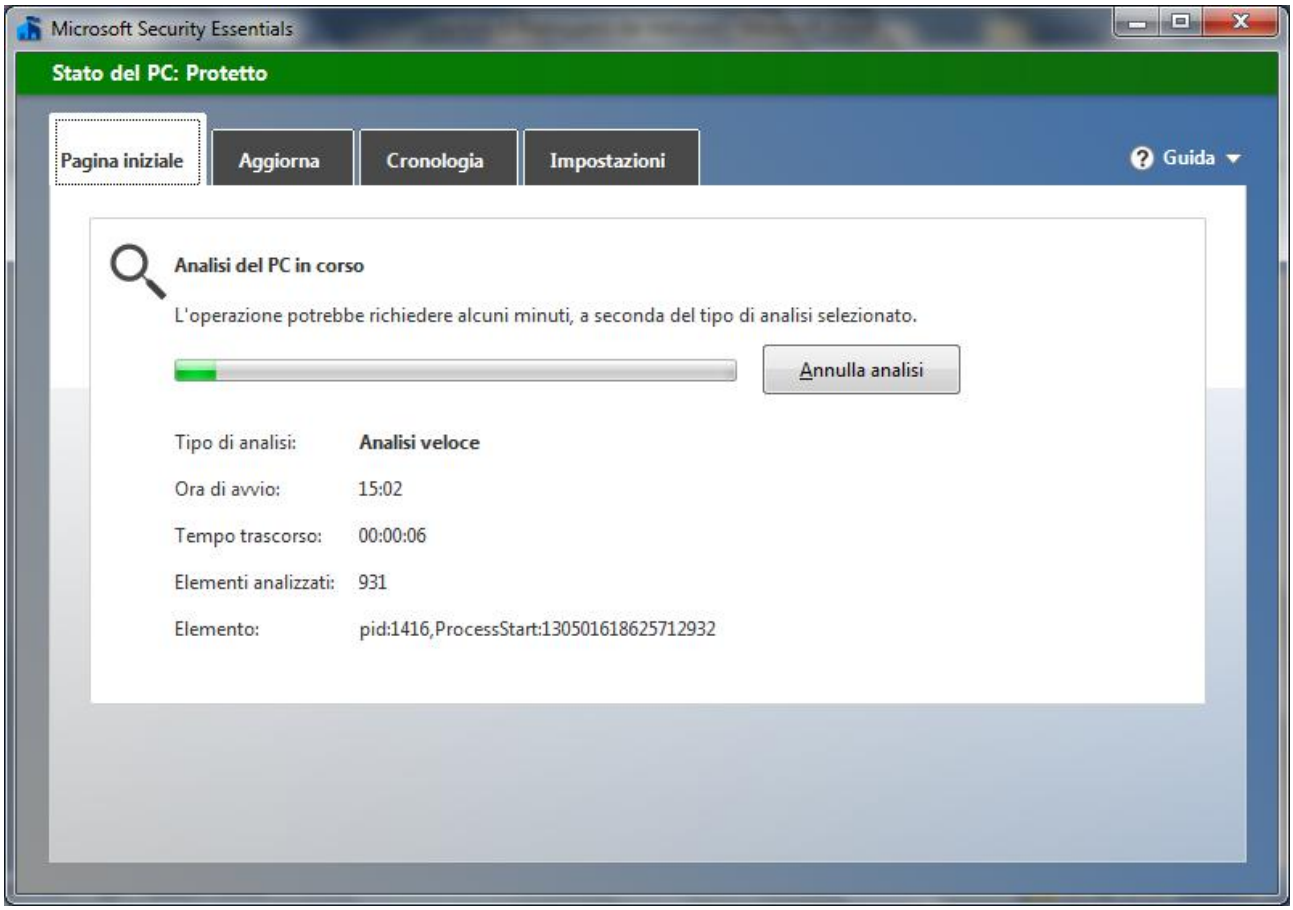
Nel capitolo precedente abbiamo visto come nel computer si può introdurre, all'insaputa dell'utente, del software con lo scopo di provocare un danno. Questi programmi sono detti malware e un virus è una delle tipologie di malware. La caratteristica che contraddistingue un virus è la capacità di replicarsi automaticamente e diffondersi nel computer proprio come un virus biologico.
Dato che i virus, e i danni che hanno creato, hanno fatto molto clamore, spesso si identificano i due termini.
Per combattere il software maligno le aziende produttrici di software per la sicurezza hanno creato dei programmi appositi: gli *antivirus* e *antimalware*. Diciamo subito che ora come ora non c'è una distinzione tra i due prodotti. Normalmente è sottointeso che un programma antivirus è anche antimalware: nella descrizione del prodotto è indicato da quali tipologie di intrusione protegge. Per la maggior "fama" del termine virus si usa genericamente il termine antivirus.
Non si può avere una protezione totale contro i virus, per la continua evoluzione del software maligno, ma è possibile limitare al minimo il rischio di infezione con un buon programma antivirus. A volte può capitare che, per "eccesso di zelo", un antivirus segnali come pericoloso un file totalmente innocuo ("falsi positivi"), ad esempio per la presenza di macro costruite dall'utente.
In generale gli antivirus hanno un sistema di protezione *real time*: operano una *scansione* continua mentre si naviga nel web, quando si installano delle applicazioni e quando si apre un file. Ma, come vedremo, può essere avviata una scansione manuale o periodica per assicurarsi che nulla sia trascurato.

Fare una scansione con un software antivirus

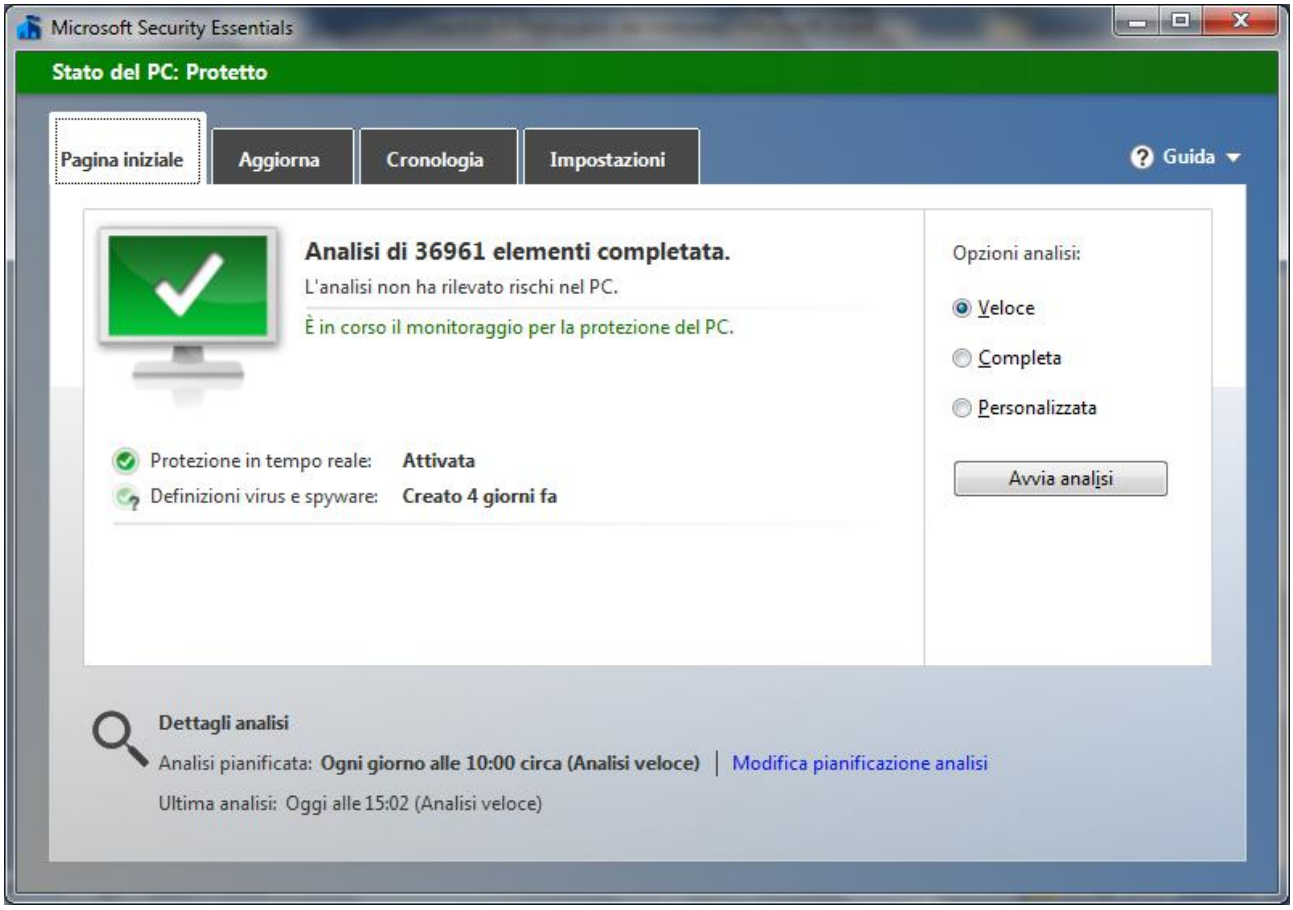
Esistono tanti antivirus, gratuiti o a pagamento, con diversi livelli di sicurezza e affidabilità. A volte è offerta una versione base gratuita con la possibilità di ottenere, a pagamento, il programma completo di tutte le potenzialità. Tutti prevedono la possibilità di effettuare una scansione manuale del software presente nel computer per la ricerca di virus.
In questo manuale utilizziamo il software Microsoft Security Essential (MSE). I comandi per gli altri tipi di antivirus sono comunque molto simili.
Una volta avviato il programma, appare la finestra principale di MSE.



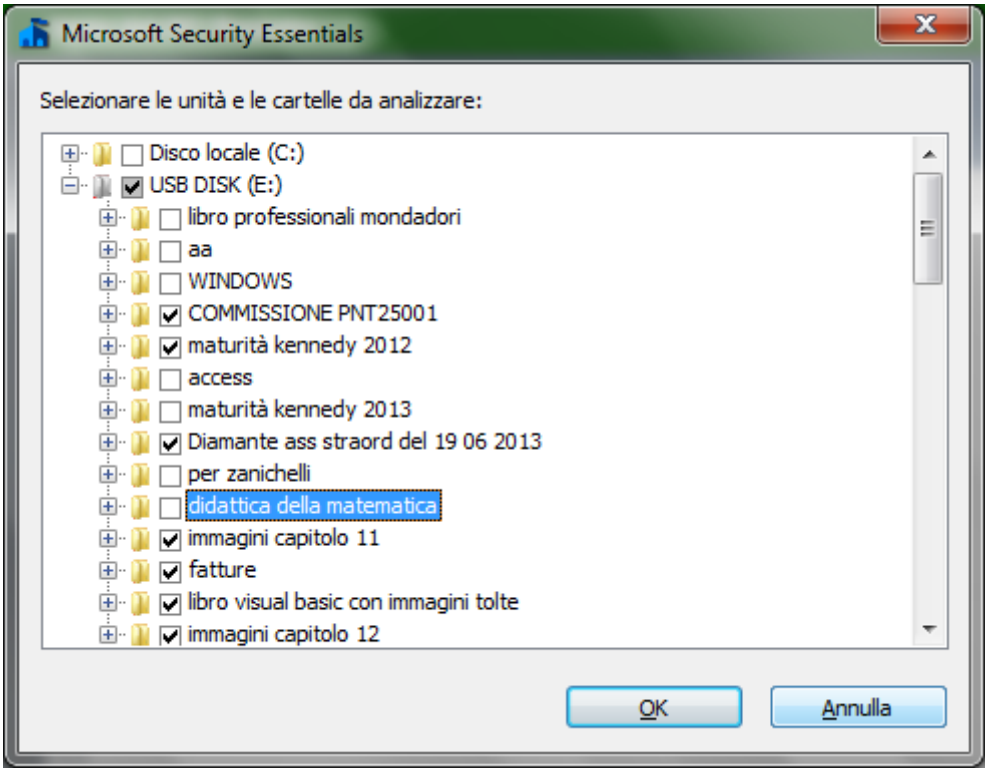
Da qui si possono avviare tutte le operazioni. In figura, il programma segnala che è da molto tempo che non viene effettuata una scansione manuale.
Per avviare la scansione premere il pulsante **Avvia analisi**.



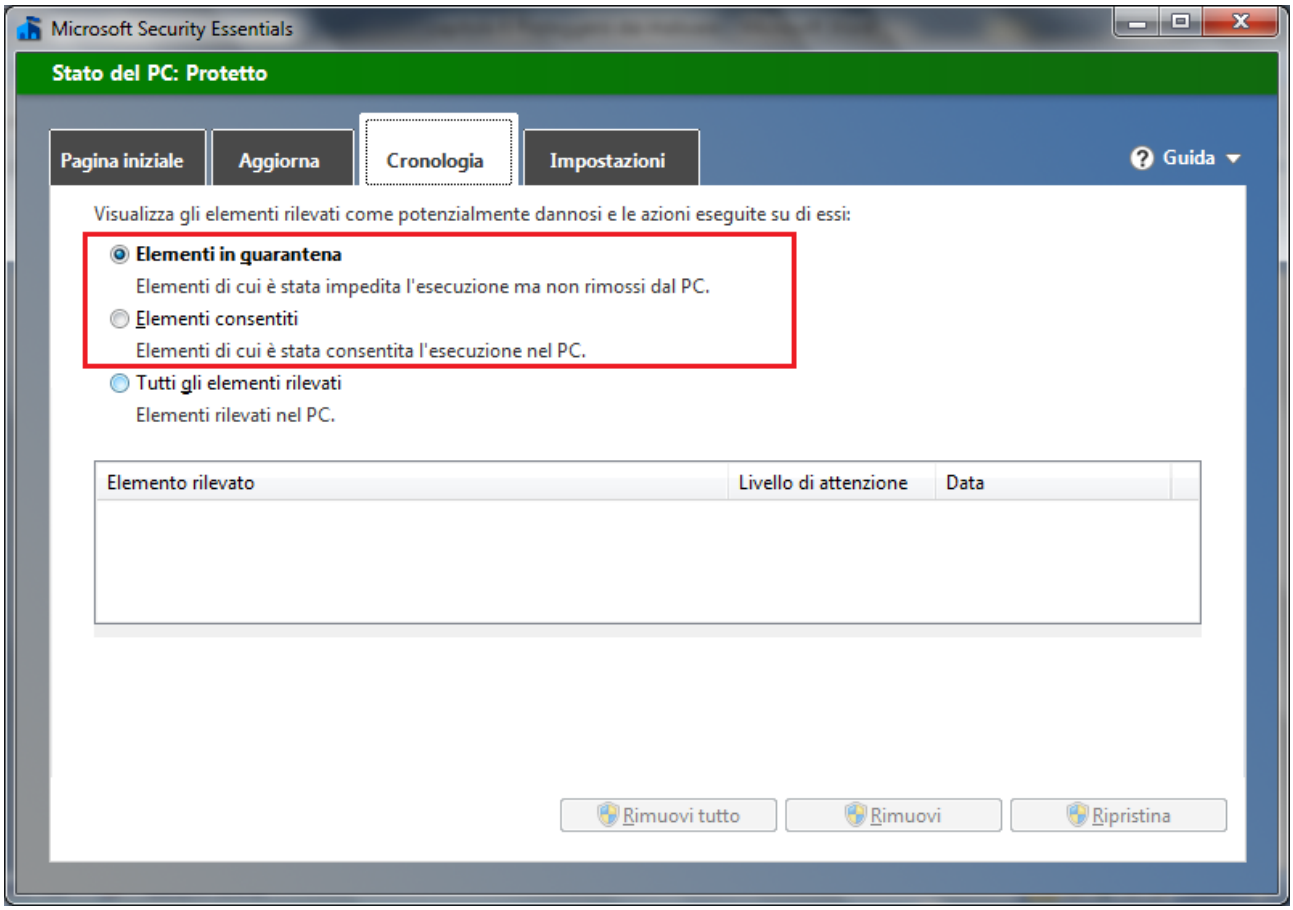
Al termine del processo, se non sono stati rilevati malware, appare il riepilogo degli elementi controllati.



Ci sono tre tipi di scansione: con la scansione **Veloce** i virus sono cercati nei punti dove si nascondono più di frequente. Se si pensa che il computer sia infetto, nonostante la scansione veloce non abbia dato esito, si può eseguire la scansione **Completa**. In questo caso verranno controllati tutti i file del disco rigido e i programmi in esecuzione. Questo processo può durare alcune ore e le prestazioni del computer saranno rallentate. La scansione **Personalizzata** permette all'utente di scegliere i file da esaminare.

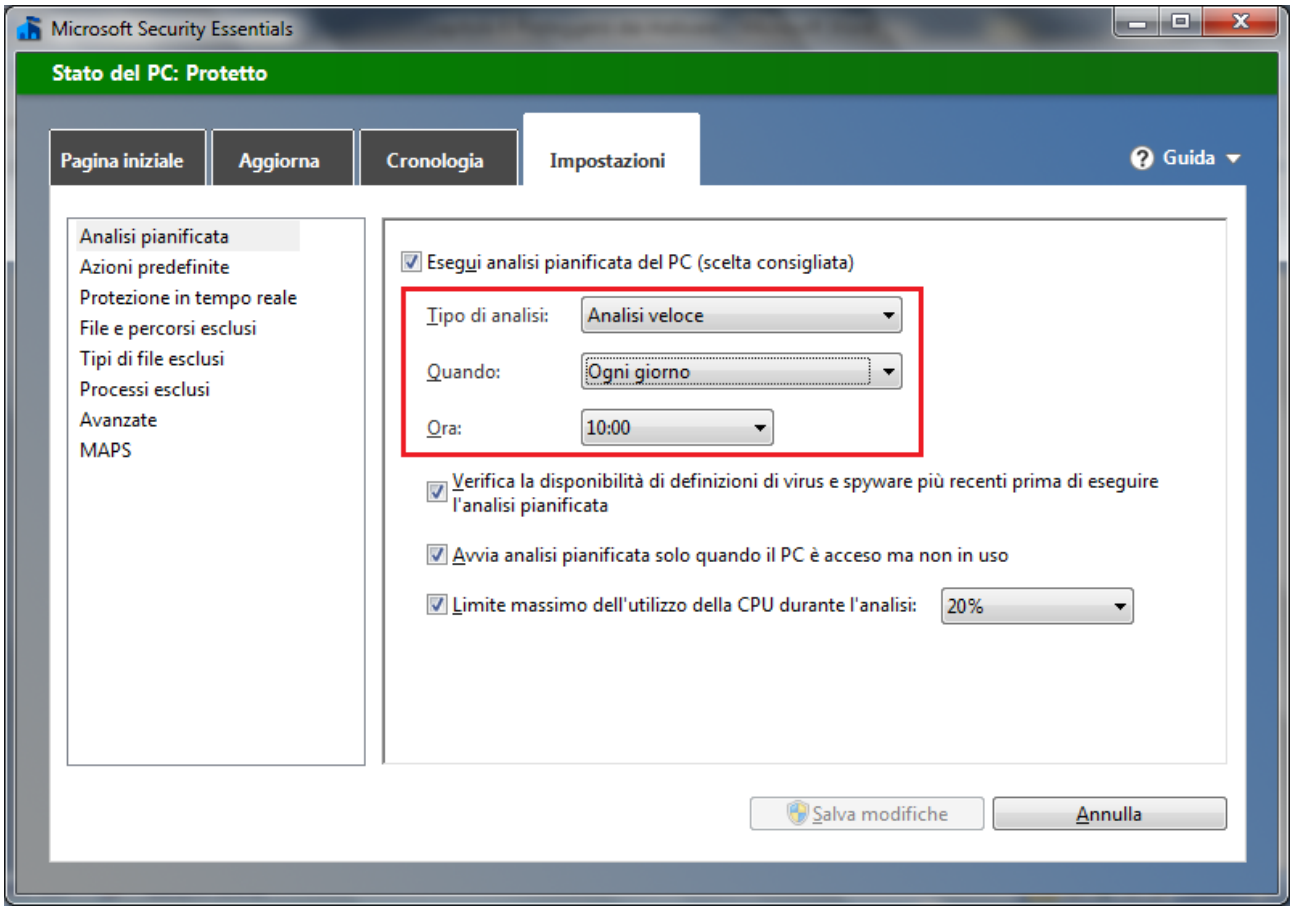


Se l'antivirus rileva del software dannoso, il più delle volte, interviene automaticamente per rimuoverlo e invia un messaggio di notifica all'utente. In altri casi MSE segnala la presenza di software potenzialmente pericoloso e lascia all'utente la scelta dell'azione da intraprendere.
L'utente può *rimuovere* il file o *consentire* la sua presenza. Può, in alternativa, mettere l'elemento in **quarantena**. Il file viene spostato in un'altra posizione nel computer e non verrà eseguito fino a quando non verrà consentito o rimosso. I file in quarantena e consentiti, per MSE, sono visibili nella scheda **Cronologia**.



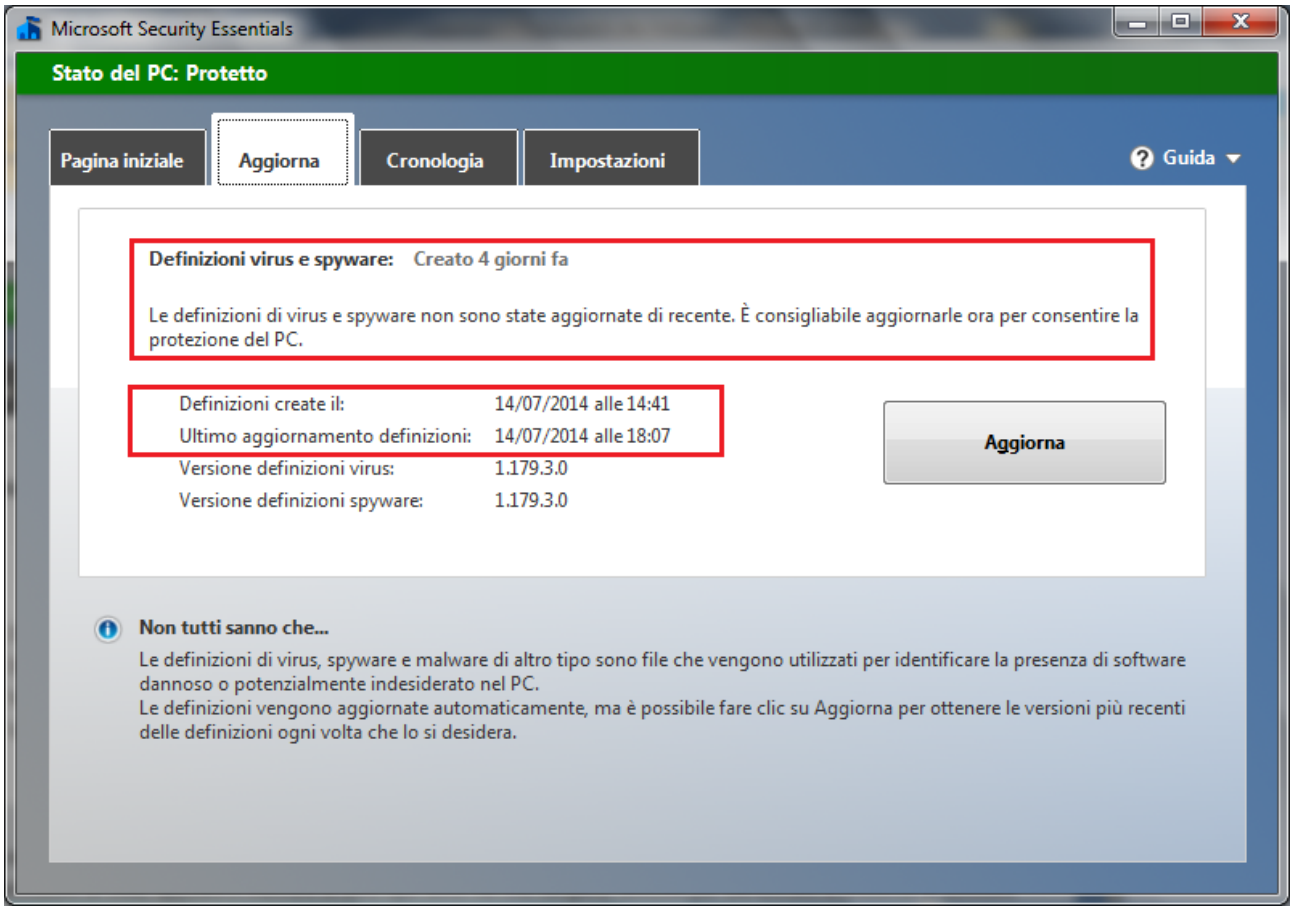
Pianificare le scansioni

La scansione dei file può essere impostata in modo che sia eseguita automaticamente nelle date e nell'orario stabiliti dall'utente. In MSE, nella scheda **Impostazioni**, si può scegliere il tipo di analisi, la giornata e l'orario.



Aggiornare l'antivirus

Ogni giorno vengono creati nuovi malware. Di conseguenza i produttori di software antivirus *aggiornano* le *definizioni* di questi programmi dannosi. Le definizioni di virus, spyware e altri tipi di malware non sono altro che dei file che sono utilizzati dal programma antivirus per rilevare il software dannoso.
MSE, nella finestra iniziale e nella scheda **Aggiorna**, segnala all'utente da quanto tempo non procede con gli aggiornamenti e permette di scaricarli con un clic su **Aggiorna**.



È importantissimo aggiornare con una certa frequenza l'antivirus per avere il computer protetto dalle nuove minacce. Per questo motivo, gli antivirus attuali prevedono l'aggiornamento in automatico.