MALWARE

Il termine malware indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito.

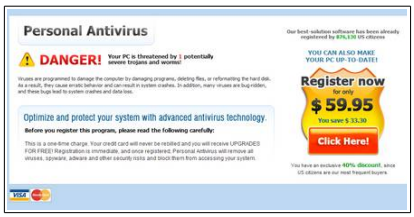
Categorie di malware
Esistono malware di molti tipi differenti, tra cui i più comuni e diffusi sono:
Virus: si diffondono copiandosi all'interno di altri programmi e vengono eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
Worm: modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.
Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Il nome deriva dal famoso cavallo di Troia.
Backdoor: Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione.
Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.
Rootkit: hanno la funzione di nascondere la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.
Scareware: ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware che si spacciano per degli antivirus veri e propri
Keylogger: sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password

Aspetti legali
Esiste un vero e proprio mercato nero legato ai malware: oltre alla compravendita di dati personali, è possibile acquistare l'utilizzo di computer infetti, cioè la possibilità di impiegare, per i propri fini e a insaputa dei legittimi proprietari, una certa quantità (nell'ordine delle migliaia) di computer controllati da remoto tramite una backdoor.
Va da sé che chi utilizza un computer (o un dispositivo mobile) infetto da malware in cui tratta dati non solo propri ma anche di altre persone (indirizzi email, ecc...), è responsabile di non aver saputo proteggere questi dati. La diffusione di questi dati può portare effetti negativi per sé e per altri.

COME DIFENDERSI DAL MALWARE
Il sistema operativo Windows è il più colpito dal malware per diversi motivi:

- è il più diffuso
- è il più vulnerabile a causa della propria architettura interna
- i suoi utenti sono generalmente meno preparati e informati rispetto agli utenti di altri SO (Mac o Linux)

La prima cosa da fare è capire come i malware attaccano i computer, ed **evitare comportamenti a rischio**. La seconda cosa da fare è **tenere aggiornato il sistema operativo**, cosa che avviene attraverso la procedura automatica.
La terza cosa è avere un **software antivirus** e tenerlo **aggiornato**. Esistono efficaci antivirus gratuiti nella versione di uso personale per esempio i seguenti:
AVIRA http://www.avira.com/it/download-start/product/avira-free-antivirus
AVAST http://www.avast.com/it-it/download-thank-you.php?product=FA-AVAST&locale=it-it
AVG http://www.avg.com/it-it/free-antivirus-download
BITDEFENDER http://www.bitdefender.it/solutions/free.html

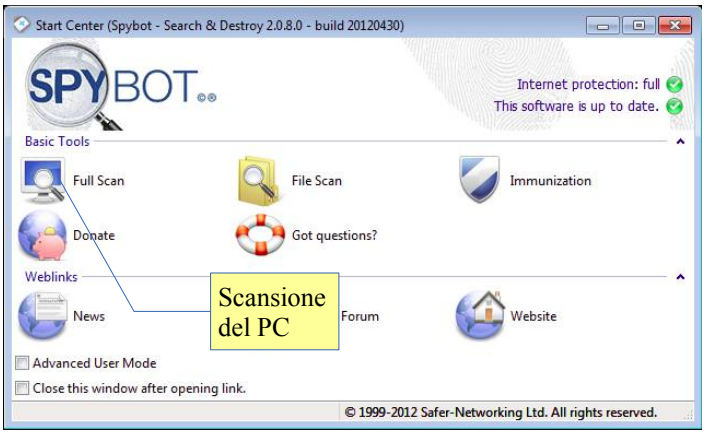


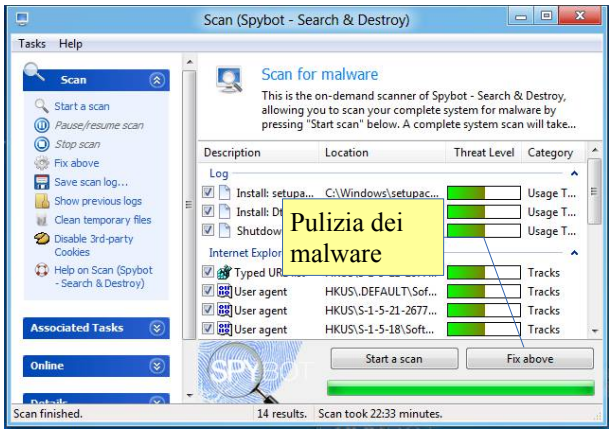
Seguendo i passi precedenti è più difficile che il proprio dispositivo venga infettato, tuttavia a volte può succedere. Capita a molti che il browser modifichi

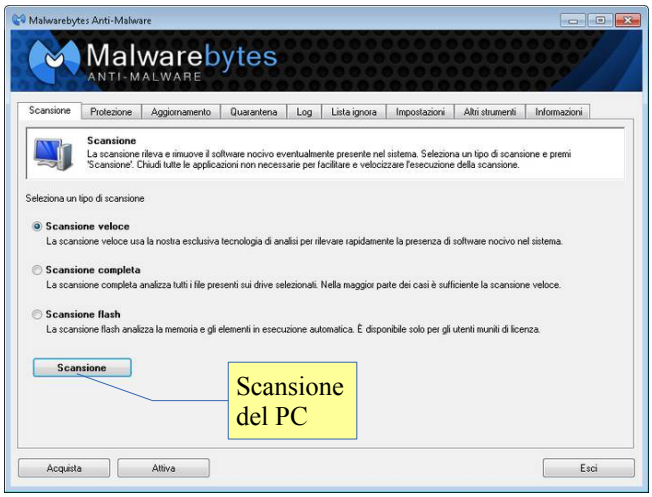
da solo la pagina iniziale, oppure che si aprano finestre su siti indesiderati, o che compaiano banner pubblicitari in pagine web che non dovrebbero contenerne: è un sintomo che qualcosa non va.
Un secondo sintomo è il fatto che l'antivirus non si aggiorna più regolarmente. Se compaiono avvisi di allerta virus diversi da quello installato, il problema è evidente.

RIMUOVERE UN MALWARE DA UN COMPUTER INFETTO
Se il computer si avvia, si possono installare alcuni software gratuiti che generalmente sono in grado di rimuovere il malware.
MALWAREBYTES http://it.malwarebytes.org/products/malwarebytes_free è un software che analizza il computer e rimuove una grande quantità di malware. Esiste anche in versione portable.
SPYBOT SEARCH & DESTROY http://www.safer-networking.org/it/mirrors/ simile al precedente

L'uso di questi programmi è molto semplice: una volta installati presentano un pulsante SCAN che avvia l'analisi del computer. Al termine della scansione si preme il pulsante FIX o CANCELLA TUTTI.



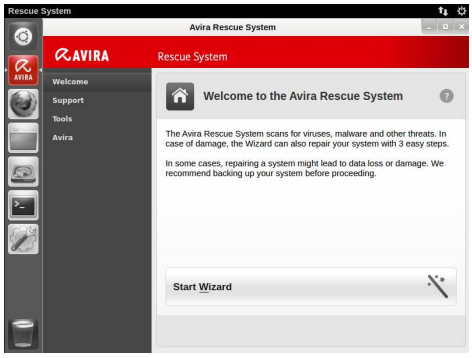




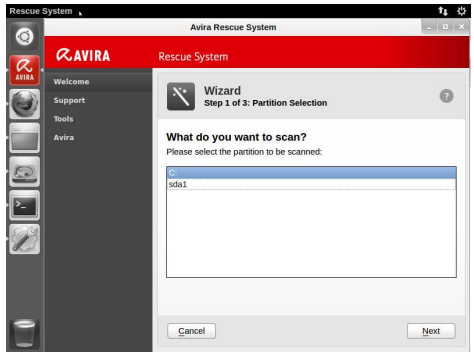
CREARE UN CD DI AVVIO E SALVATAGGIO (rescue)
Se il computer non si avvia più a causa di un malware, è necessario ricorrere a un altro metodo: procurarsi un CD antivirus autoavviante (che avvia il computer).
La procedura è nel complesso non troppo complicata e consiste in alcuni passi:

- utilizzando un algtro computer, scaricare l'immagine ISO del CD di dal sito di Avira e il manuale (in inglese)
- Masterizzare il CD (con l'immagine scaricata) avendo cura di renderlo avviabile (controllare la guida del programma di masterizzazione).
- Se il computer non ha il lettore CD si può usare una chiavetta USB utilizzando il programma UnetBootin
- impostare il BIOS del computer perché cerchi di avviarsi dal CD, se non lo è già
- avviare il pc col CD inserito
- seguire le istruzioni:
  - effettuare l'aggiornamento (update)
  - premere il pulsante Start scanner

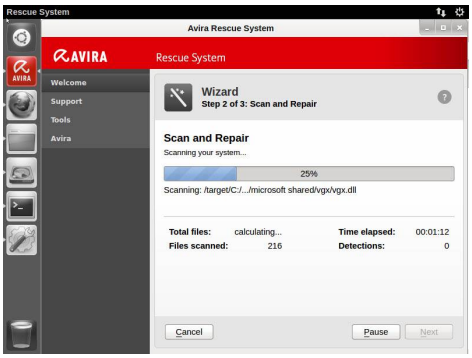
Avvio del PC



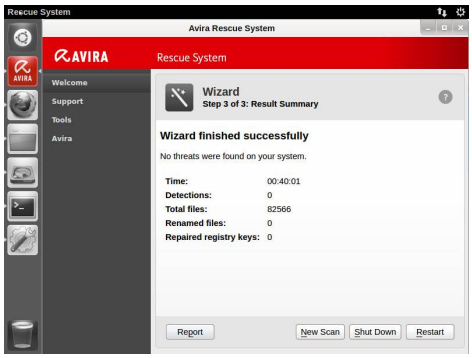
Premere Start Wizard



Selezionare C:



Scansione del disco



Esito della scansione

In Tools è possibile trovare strumenti avanzati, per esempio per modificare il registro di windows (solo per esperti)

PER SAPERNE DI PIÙ

qui di seguito potete trovare dei link a filmati che aiutano a capire più in profondità il fenomeno del malware e le strategie per difendersene, individuarlo ed eliminarlo.

- aspetti tecnici su come agisce un malware e come fare a bloccarlo
  - lezione 1 https://www.youtube.com/watch?v=ZteTui49QgY
  - lezione 2 https://www.youtube.com/watch?v=wTgePzGfPCY
- usare il software Malwarebytes https://www.youtube.com/watch?v=qIan4W52GzE
- usare il software Spybot S&D (in inglese) https://www.youtube.com/watch?v=NC5fE8pn_JE
- usare il software Spybot S&D (in italiano, però una versione vecchia) https://www.youtube.com/watch?v=tXRrcner70k
- usare Avira Rescue Disk (in inglese) https://www.youtube.com/watch?v=-KYi1DJlFj4
- masterizzare immagine ISO su CD/DVD https://www.youtube.com/watch?v=AiA0V0UTg-Y
- usare UNetBootin per creare una chiavetta USB avviabile per usare Avira rescue su pc che non hanno il CD https://www.youtube.com/watch?v=rvsDHM68jM8