

# Guida veloce alla sicurezza del pc per sistemi Windows

Nicola Moretti

June 8, 2007

Questo documento e' sotto la licenza Creative Commons BY-NC-SA.

**V 1.3**

## 1 Introduzione

Un computer con sistema operativo Windows XP, se non aggiornato alla versione Service Pack 2 (ma anche dopo averlo fatto), e' letteralmente un colabrodo. Perche' virus come *Blaster* o *Sasser* infettino il vostro pc, ad esempio, basta che sia collegato ad Internet.

Per proteggere il vostro pc avete anzitutto bisogno di alcuni programmi. In questa breve guida cercher di dividere attentamente ed analizzare le differenze tra software gratuito e a pagamento.

Successivamente spieghero' come controllare rapidamente ed efficacemente lo stato di benessere del vostro computer.

Anzitutto per proteggere un pc avete bisogno di

- un buon antivirus;
- un buon firewall;
- un buon software antyspyware o malware generale;

Con i consigli presenti in questa guida non posso garantire la totale sicurezza del vostro pc. Potrete per contare su un livello davvero elevato.

Se avete tempo consiglio inoltre la lettura de "L'acchiappavirus" di Paolo Attivissimo. E un libro semplice, chiaro e molto utile. Potete ordinarlo (costa 7,20 Euro) oppure scaricarlo **gratuitamente** dal sito ufficiale Il documento e' disponibile qui.

## 2 L'antivirus

**Cos'e'** Un antivirus e' un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi come worm, trojan e dialer.<sup>1</sup>

**Funzionamento** Il suo funzionamento si basa principalmente sulla ricerca nella memoria RAM o all'interno dei file presenti in un computer di uno schema tipico di ogni virus (in pratica ogni virus e' composto da un numero ben preciso di istruzioni (codice) che possono essere viste come una stringa di byte, il programma non fa altro che cercare se questa sequenza e' presente all'interno dei file o in memoria). Il successo di questa tecnica di ricerca si basa sul costante aggiornamento degli schemi che l'antivirus e' in grado di riconoscere effettuato solitamente da un gruppo di persone in seguito alle segnalazioni degli utenti e da gruppi specializzati nell'individuazione di nuovi virus.

Esiste anche un'altra tecnica di riconoscimento detta "**ricerca euristica**" che consiste nell'analizzare il comportamento dei vari programmi alla ricerca di istruzioni sospette perche' tipiche del comportamento dei virus (come la ricerca di file o routine di inserimento all'interno di un altro file) o ricercare piccole varianti di virus gia' conosciuti (variando una o pi istruzioni e' possibile ottenere lo stesso risultato con un programma leggermente differente).

<sup>1</sup>Citazione da wikipedia, assieme a "Funzionamento".

**Scelta** La scelta dell'antivirus adatto non e' mai facile. La prime domande da farci sono: siamo disposti a spendere? Quanto?

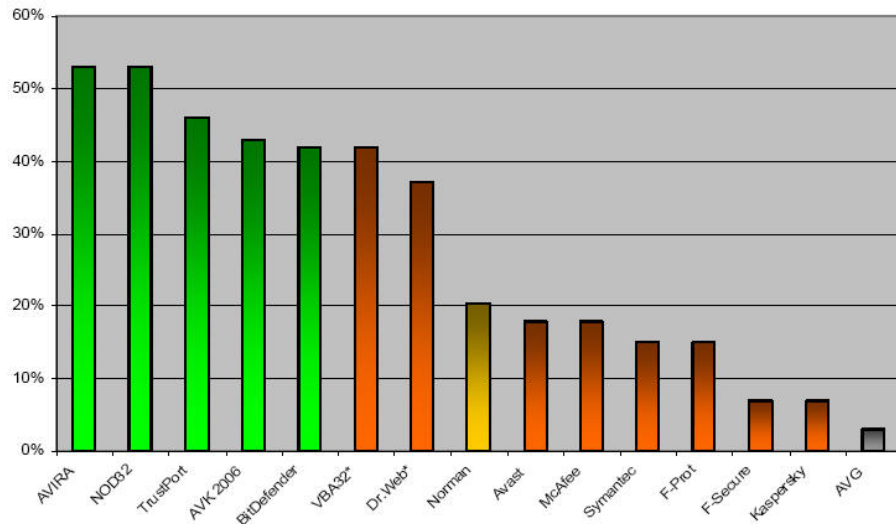
Iniziamo con le soluzioni gratuite.

I software gratuiti che vi consiglio sono Avast e Antivir. Entrambi offrono allincirca le stesse prestazioni (forse preferibile Antivir). Uniche lacune: Antivir non permette il controllo delle email, Avast sembra permeabile ai trojan.

Se invece preferite (come me, in parte) delle soluzioni a pagamento, tutto dipende dalle vostre conoscenze informatiche. Se vi sentite pronti a tutto per la vostra sicurezza correte a comprare Nod32.

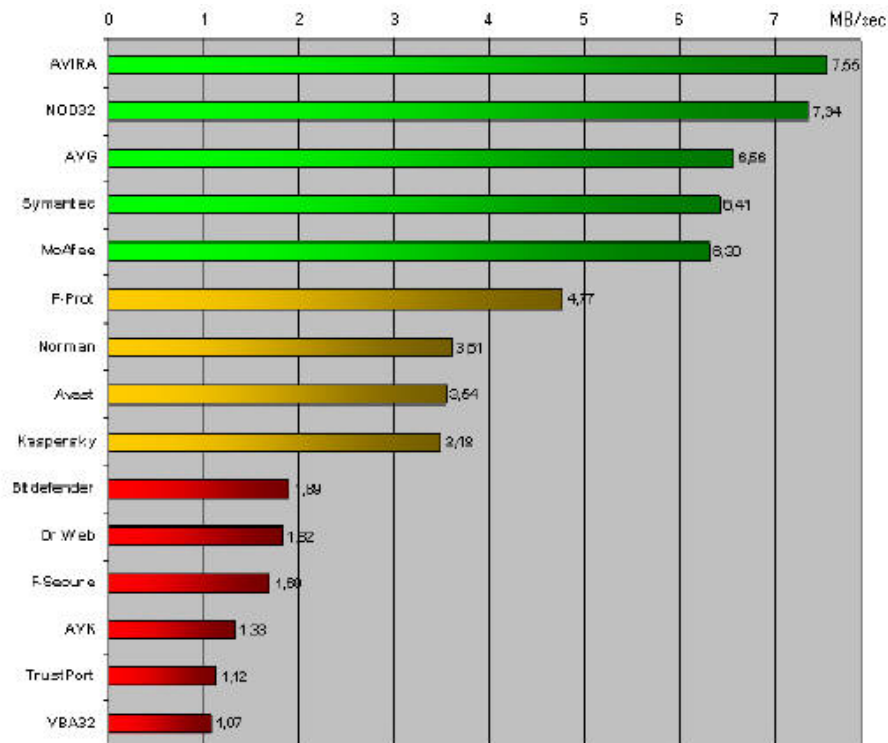
E' un software davvero ottimo. Di recente sembra (soprattutto per quanto riguarda la rilevazione euristica) avere di molto superato Kaspersky.

Riporto una comparativa (da Av-comparatives di novembre 2006 riguardante la rilevazione virus "a richiesta" (richiesta dell'utente di scansione per un file, per capirci).



AVIRA e' Antivir, per versione Premium a pagamento.

Per quanto riguarda la velocita' di scansione:



Se preferite qualcosa di pi semplice, allora potete fidarvi di: Norton Antivirus (molto pesante), McAfee (anche questo molto pesante), F-Secure Antivirus. Mi sono dimenticato di segnalare le soluzioni proposte da Zone Alarm o G-data. Pero' secondo me c'e' gia' abbastanza carne sul fuoco.

Un sito molto interessante che mostra delle comparative affidabili tra gli antivirus e' Av-comparatives.

### 3 Il Firewall

**Cos'e'** Essenzialmente questo programma controlla il traffico di dati fra il vostro computer e la rete. Blocca i programmi che tentano di entrare e, se e' un buon firewall, anche quelli che tentano di uscire (cioe' di connettersi ad Internet), senza la vostra autorizzazione.

**Funzionamento** La funzionalita' principale in sostanza e' quella di creare un filtro sulle connessioni entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza. Il firewall agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di:

- controllo

- modifica
- monitoraggio

2

**Scelta** La scelta del firewall e' molto varia.

Io, personalmente, consiglio Zone Alarm Free, di Zonelabs, totalmente gratuito (non e' la versione pro ma la free). Una alternativa e' Kerio.

## 4 Antispyware a Antimalware

**Cos'e'** Un antispyware e' un programma il cui scopo e' quello di cercare ed eliminare dal sistema, tramite un'apposita scansione, Spyware, adware, keylogger, trojan e altri malware. Le funzioni di questi programmi sono simili a quelle degli antivirus anche se bisogna stare sempre attenti a non confonderli con essi. Come gli antivirus, anche gli antispyware necessitano di costante aggiornamento del database delle definizioni per trovare anche gli ultimi spyware.<sup>3</sup>

**Scelta** Su questo punto non mi dilungo. Dovete semplicemente scaricare due programmi gratuiti:

- Spybot
- Ad-aware

## 5 Patch e aggiornamenti

Avere un buon antivirus spesso non garantisce il suo corretto funzionamento. E questa regola vale anche per gli altri programmi.

In particolare e' importantissimo mantenere aggiornato il proprio sistema operativo.

Windows offre un servizio automatico di update. Non negategli questa possibilita'. Tappare i buchi dei vostri software e' un'operazione di fondamentale necessita'. Inoltre controllate spesso che il database di virus del vostro antivirus sia aggiornato. Controllate periodicamente che il vostro firewall e i vostri Antimalware siano aggiornati all'ultima versione disponibile.

## 6 Eliminare i programmi "Attiravirus"

Alcuni programmi sono davvero da evitare, se non volete trovarvi immersi da una marea di virus. Usateli raramente o, addirittura, disinstallateli.

Anzitutto questi 2:

---

<sup>2</sup>Citazione da wikipedia.

<sup>3</sup>Citazione da wikipedia.

- Internet Explorer, che vi consiglio di sostituire immediatamente con Firefox (gratuito).
- Outlook Express, che vi consiglio di sostituire immediatamente con Thunderbird (anche questo gratuito).

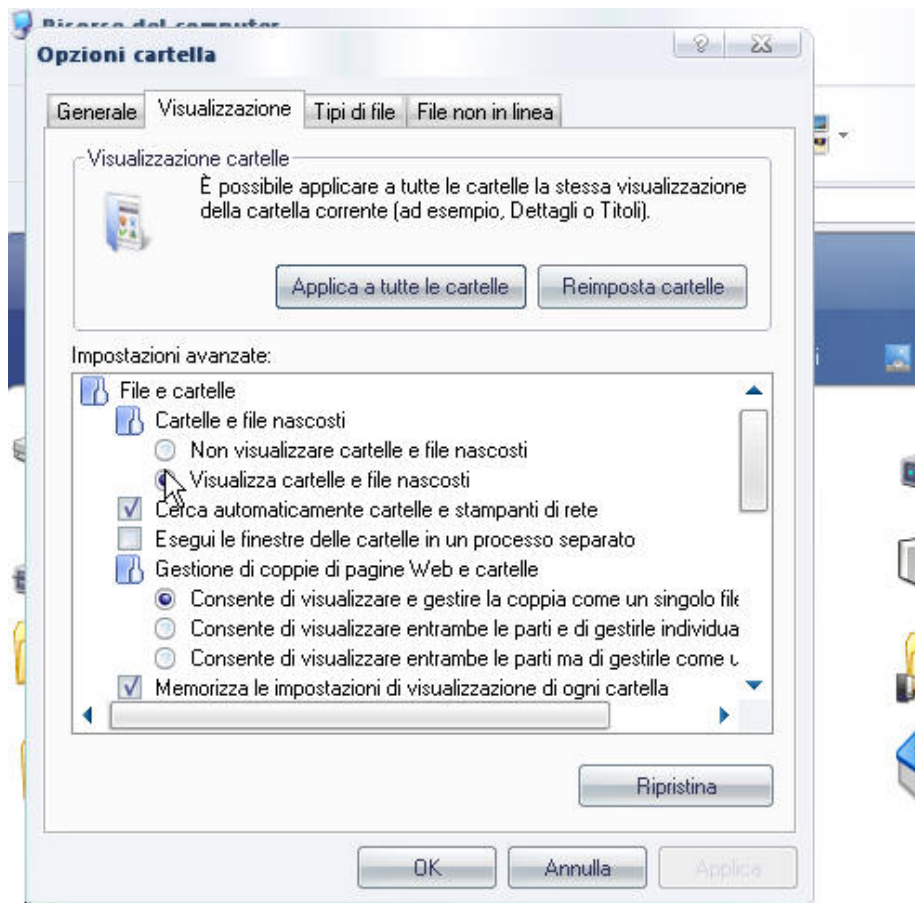
## 7 Eliminare i file temporanei, troppo spesso "Attiravirus"

Eliminare i file temporanei e' molto utile. Si libera spazio (si migliora la velocita' stessa del pc) e, molto spesso, si toglie lo spazio vitale dei virus. Un programma gratuito (potete pero' effettuare donazioni se volete) che ci permette di effettuare velocemente questa operazione e' CCleaner.

## 8 Altre modifiche al sistema operativo

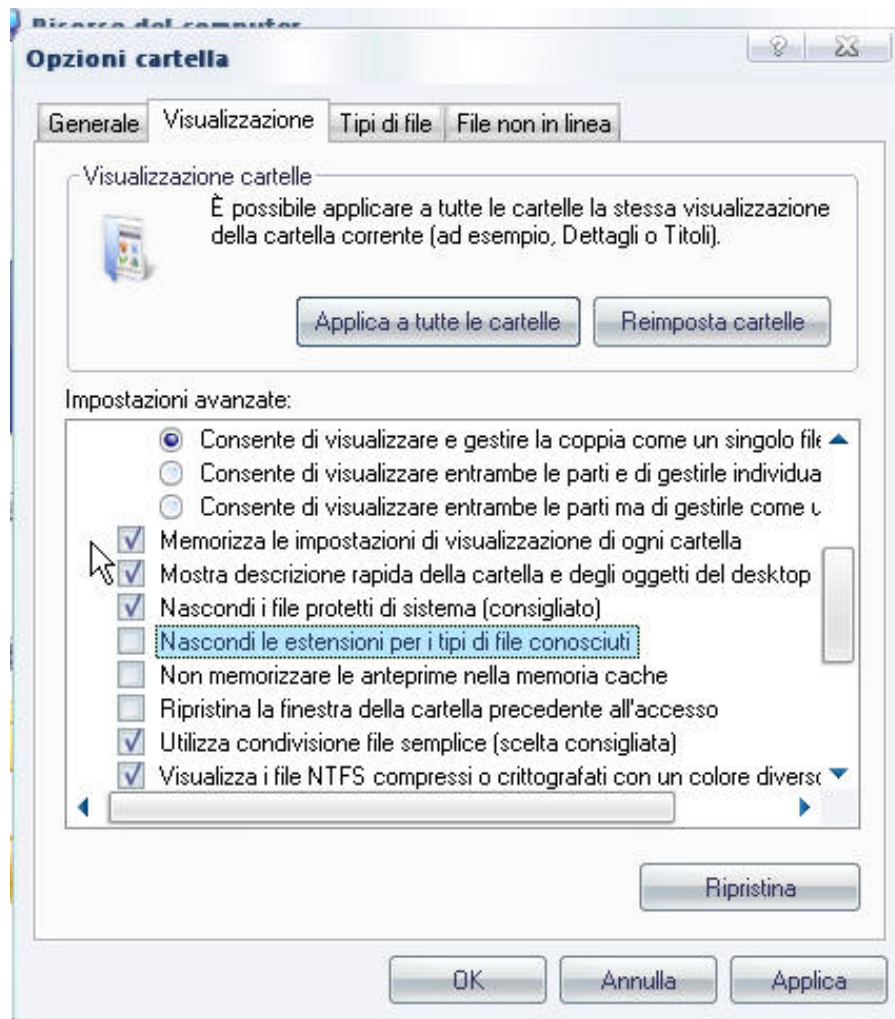
Sotto sistema Windows, esistono altre importanti modifiche da effettuare per aumentare il vostro livello di sicurezza.

**Visualizzare i file nascosti** Per poter visualizzare determinati file e cartelle ("invisibili") e' necessario aprire "Risorse del computer", cliccare "Strumenti", "Opzioni cartella", "Visualizzazione".



Qui cliccate su "Visualizza cartelle e file nascosti" e premete applica.

**Visualizza estensioni dei file comuni** Un'altra importante opzione da abilitare per la vostra sicurezza e' la visualizzazione delle estensioni piu' comuni. Per farlo, sempre nella stessa finestra "Visualizzazione", scorrete piu' giu' fino a trovare e a togliere la spunta da "Nascondi le estensioni per i tipi di file conosciuti". TOEDIT sui CLSID



## 9 La sicurezza dipende da voi

Il 70% della sicurezza del pc non dipende dal software che installate, ma dal vostro comportamento.

Ecco quindi delle regole che fareste bene a rispettare:

- fate spesso il backup (copie di sicurezza) dei vostri dati. Esistono degli ottimi programmi specifici che vi possono aiutare, ma e' spesso sufficiente l'utilita' di backup di windows XP;
- fate attenzione agli allegati che arrivano alla vostra email. L'email e' il principale mezzo di diffusione delle infezioni. Se la provenienza del

messaggio e' dubbia non provate ad aprirli fidandovi del vostro antivirus;

- cercate di evitare l'invio (e bloccare la ricezione) di email in formato html, appesantiscono i messaggi e sono poco sicure;
- state molto attenti agli indirizzi a cui vi collegate! Ultimamente e' nata una nuova tecnica di frode in Internet chiamata phishing, che permette di raccogliere informazioni come il numero della carta di credito con estrema facilità. Vedi la relativa sottosezione 9.1 a pagina 9.
- attenti alle estensioni dei file. Spesso un virus ha un nome del tipo 'fotoxx.jpg.exe', cioè una doppia estensione (ma e' l'estensione finale a contare!).<sup>4</sup>

## 9.1 Il phishing

**Cos'e'** In ambito informatico il phishing e' una attivita' truffaldina che sfrutta una tecnica di ingegneria sociale, ed e' utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalita' del furto di identita' mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a questi messaggi, l'utente e' ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.<sup>5</sup>

**Metodologia di attacco** Il processo standard delle metodologie di attacco di phishing puo' riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (phisher) spedisce al malcapitato ed ignaro utente un messaggio e-mail che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui e' iscritto).
2. l'e-mail contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account ecc.).
3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la societa' di cui il messaggio simula la grafica e l'impostazione.
4. il link fornito, tuttavia, non porta in realta' al sito web ufficiale, ma ad una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere ed ottenere dal destinatario

---

<sup>4</sup>In particolare per i pi esperti consiglio di cercare in internet articoli sulle estensioni tipo js-pif. Un altro interessante articolo sui problemi delle estensioni nascoste e' quello relativo ai CLSID.

<sup>5</sup>Citazione da wikipedia, assieme a "Metodologie di attacco"

dati personali particolari, normalmente con la scusa di una conferma o la necessita' di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.

5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

**Come difendersi** Per difendersi dal phishing la cosa migliore e' stare bene attenti alla barra indirizzi. Ad esempio se cliccate qui: <http://www.ebay.com> pensereste di entrare nel sito di ebay. Invece vi ritrovate a vedere google.it. Purtroppo un phisher esperto riuscirebbe a creare una pagina **identica** a quella di ebay. Come difendersi dunque?

**Anzitutto dobbiamo essere attenti noi** Infatti, se apriamo la pagina di un phisher (un elenco aggiornato e' disponibile qui, ma fate attenzione) ci accorgiamo di due dettagli. Nell'esempio che mi appresto a riportare la pagina incriminata e': <http://www.paypal.com.cgi-bin.jfkasbf.gq.nu/> Esaminiamo l'indirizzo. Il dominio sembra essere paypal.com, ma **fate attenzione**. Quello che davvero ci dice a chi appartiene un sito internet sono gli ultimi due gruppi: gq.nu . Essi corrispondono a microsoft.com, o google.it, o hanicker.it.. gq.nu in particolare e' un servizio di freehosting, un servizio appetitoso per i phisher. Un'altra informazione importante la troviamo guardando la barra di stato in basso a sinistra. Questa e' davvero difficile da falsificare (a differenza di certi attacchi nella barra di indirizzo).

**Lettura di [www.paypal.com.cgi-bin.jfkasbf.gq.nu](http://www.paypal.com.cgi-bin.jfkasbf.gq.nu)**

**Altre armi potenti** Altre armi interessanti sono fornite da particolari toolbar che ci avvisano quando stiamo visitando "siti contraffatti". Attenzione pero', questi avvisi si basano su database aggiornati costantemente, ma non per questo aggiornati agli ultimissimi siti di phishing.

La mia scelta cade in particolare sull'ottima barra di google. Molto utile per fare ricerche veloci, ma anche per la protezione. Ecco un esempio di avviso mentre provo a visitare un sito contraffatto:



## 10 Testare velocemente (e senza rischi) firewall ed antivirus

### 10.1 Testare il proprio antivirus

Per testare il vostro antivirus il modo pi semplice e' scaricare un finto virus che per convenzione viene rilevato dalla maggior parte degli antivirus. Questo finto virus non e' altro che un file contenente:

```
X5O!P%@AP[4  
PZX54(P^7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

cioe' un codice che, salvato all'interno di un file .bat, stamperebbe "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". Potete scaricarli alla home page eicar.

### 10.2 Testare il proprio firewall

Per testare il proprio firewall esistono numerosi test online. Cito i piu' affidabili:

- hackerwatch - McAfee;
- Sygate - Symantec;
- Audity.

## 11 Controllare un singolo file

Mettiamo che un amico ci spedisca un file "inaspettato" per posta e il nostro antivirus non ci avvisi di niente. Per aumentare la probabilita' che un file non sia infetto possiamo effettuare una scansione online **contemporaneamente** con molti antivirus.

Ci sono vari siti che permettono di effettuare questa operazione. Tra i migliori segnalo:

- Virus Total;
- Virus Scan Jotty.

## 12 Come capire che qualcosa non va

A volte, sebbene siano state prese tutte le precauzioni, ma soprattutto se non e' cosi', si notano degli strani comportamenti del pc. In particolare:

- riavvii spontanei (schermate blu);
- **antivirus disattivati**;
- **programmi che, senza motivo, smettono di funzionare**;
- computer molto lento;
- connessione lenta;
- spazio su disco esaurito (senza motivazioni valide).

<sup>6</sup> Questi "sintomi" (soprattutto quelli in grassetto) spesso (**ma non sempre**) indicano la presenza di un virus. Per avere delle conferme abbiamo bisogno di un programma passato per troppo tempo all'ombra: hijackthis.

### 12.1 Hijackthis

**Cos'e'** Hijackthis, spesso abbreviato HJT, un tool gratuito per la rimozione di spyware su sistemi operativi Windows creato da Merijn Bellekom. Il programma famoso per l'approccio intelligente nell'individuazione di codice maligno. Infatti al posto di affidarsi a un database di spyware conosciuti HJT effettua una scansione veloce nel computer dell'utente, creando una lista di differenze tra il pc in cui e' avviato e un modello di computer libero da malware. Quindi spetta all'utente decidere cosa togliere o lasciare.<sup>7</sup>

---

<sup>6</sup>Punti ripresi (e **modificati**) dal libro di Paolo Attivissimo, gia' citato nell'introduzione, che consente solo la riproduzione integrale.

<sup>7</sup>Citazione tradotta liberamente da wikipedia, assieme a "Metodologie di attacco"

**Guida all'uso** Anzitutto e' necessario scaricare il programma dal sito del produttore. Questo software non necessita di installazione. Semplicemente decomprimete il file (anche sul desktop va bene) e fate doppio click sul file "HijackThis.exe". Nella finestra che vi appare scegliete "Do a system scan and save a log file". Dopo qualche secondo vi si aprir una finestra di blocco note. Salvate il file ed inviatelo allegandolo ad un messaggio nella sezione apposita del sito [blog.hanicker.it](http://blog.hanicker.it). Aspettate quindi una risposta.

In questo modo saprete con precisione se il vostro sistema e' infetto oppure no. Inoltre riceverete istruzioni precise sulla rimozione del codice dannoso, eventualmente.

## 13 Proteggere i dati importanti da occhi indiscreti

Spesso alcuni pensano che per proteggere i propri dati da occhi indiscreti sia sufficiente rendere le cartelle invisibili. Oppure qualche altro programma poco professionale. Altri addirittura stimano che un rename dal dos sia sufficiente<sup>8</sup>. Il modo migliore per proteggere i vostri dati, invece, e' la vera e propria crittografia. Vi consiglio il facile e gratuito True Crypt.

### 13.1 Attenzione: cancellare e' una cosa, svuotare il cestino un'altra

Una cosa che non tutti sanno e' che svuotare il cestino non vuol dire eliminare effettivamente il file. Il file infatti viene semplicemente "deindicizzato". Un modo sicuro per cancellare effettivamente i file e' sovrascriverli in memoria con dei dati casuali per almeno 3 volte (consiglio 7 volte). Un programma gratuito che vi permette di farlo automaticamente e' Eraser.

## 14 Prossimi updates della guida

- Sfruttare la modalita' provvisoria;
- Qualcosa dui Dialer e la pubblicita';
- Proteggere il piu' possibile le connessioni wireless;
- Programmi antispam;
- Utilizzare le scansioni online.

---

<sup>8</sup>Provate da dos 'ren [nomecartella] xxxx.{21EC2020-3AEA-1069-A2DD-08002B30309D}'

## Contents

<b>1</b>	<b>Introduzione</b>	<b>2</b>
<b>2</b>	<b>L'antivirus</b>	<b>2</b>
<b>3</b>	<b>Il Firewall</b>	<b>4</b>
<b>4</b>	<b>Antispyware a Antimalware</b>	<b>5</b>
<b>5</b>	<b>Patch e aggiornamenti</b>	<b>5</b>
<b>6</b>	<b>Eliminare i programmi "Attiravirus"</b>	<b>5</b>
<b>7</b>	<b>Eliminare i file temporanei, troppo spesso "Attiravirus"</b>	<b>6</b>
<b>8</b>	<b>Altre modifiche al sistema operativo</b>	<b>6</b>
<b>9</b>	<b>La sicurezza dipende da voi</b>	<b>8</b>
9.1	Il phishing . . . . .	9
<b>10</b>	<b>Testare velocemente (e senza rischi) firewall ed antivirus</b>	<b>11</b>
10.1	Testare il proprio antivirus . . . . .	11
10.2	Testare il proprio firewall . . . . .	11
<b>11</b>	<b>Controllare un singolo file</b>	<b>12</b>
<b>12</b>	<b>Come capire che qualcosa non va</b>	<b>12</b>
12.1	Hijackthis . . . . .	12
<b>13</b>	<b>Proteggere i dati importanti da occhi indiscreti</b>	<b>13</b>
13.1	Attenzione: cancellare e' una cosa, svuotare il cestino un'altra . .	13
<b>14</b>	<b>Prossimi updates</b>	<b>13</b>