

Rilevamento e rimozione Virus avast! 4

Di seguito sono elencate le domande più frequenti riguardo il rilevamento e la rimozione di virus con avast! 4.

- ➔ Come è possibile che avast! trova virus nella sua cartella “C:\Program Files\Alwil Software\Avast4\Data\Moved” ? Significa che avast! è infetto?
- ➔ I virus scoperti sono “Panda Antivirus” (Win95:Matyas and Win32:Kuang2 in PAV.SIG mainly), che cosa sono?
- ➔ Avast! ha trovato un virus sul mio computer. Mi dà diverse opzioni, ma nessuna di esse funziona. Come posso risolvere questo problema?
- ➔ Avast! ha trovato un virus, mi chiede solo di abbandonare la connessione, perché non posso cancellarlo?
- ➔ Ho diversi messaggi di virus trovati nelle mie e-mail, provenienti dai mail server. Ma non appena provo a fare la scansione con avast! non viene trovato nessun virus. Cosa dovrei fare?

D: Come è possibile che avast! trova virus nella sua cartella “C:\ProgramFiles\Alwil Software\Avast4\Data\Moved” ? Significa che avast! è infetto?

R: No, la cartella “C:\Program Files\Alwil Software\Avast4\Data\Moved” , è quella di default in cui vengono messi tutti i file infetti quando si effettua l’azione di MOVE. Per cui, se trovi alcuni virus in questa cartella, è solo perché sono stati trovati da una precedente scansione, e sono stati spostati lì.

D: I virus scoperti sono “Panda Antivirus” (Win95:Matyas and Win32:Kuang2 in PAV.SIG mainly), che cosa sono?

R: Questo è un problema conosciuto. Ogni virus, può essere identificato perché contiene una “signature” univoca. I programmi Antivirali hanno nei propri database delle signature.

Noi chiamiamo questi database “virus definition file”.

Quando un programma Antivirale scandisce un file per i virus, confronta tutte le signature del database, con quella del file. Se c’è un match il file viene marcato come infetto. Per un programma antivirus, è importante nascondere il database delle signature, ad esempio cifrandolo. Panda Antivirus è un database non cifrato, in cui le signature sono in chiaro e visibili a tutti.

Noi non possiamo farci nulla, possiamo solo consigliarti di non usare più antivirus contemporaneamente, o di mettere questi file nella lista delle eccezioni, in modo che non verranno scannerizzati.

Informazioni aggiuntive:

Questa è una lista di Panda Antivirus files che avast! riconosce come infetti:

- **IMSCAN.DLL**
- **PAVDLL.DLL**
- **PAV.SIG**
- **APVXD.VX2**
- **APVXD.VXD**

Questa è una lista virus di file menzionati Panda Antivirus files.

Considera che è una lista non completa, e che nel futuro subirà cambiamenti:

- **Gift-724**
- **VBS:Redlof**
- **Win32:Aliser**
- **Win32:Bolzano-3011**
- **Win32:Bolzano-3223**
- **Win32:Bolzano-3384**
- **Win32:Crypto**
- **Win32:CTX**
- **Win32:Kenston**
- **Win32:Kuang2**
- **Win32:Nimda [Drp]**
- **Win32:Qozah-C**
- **Win32:Small-1700**
- **Win32:Vypne [Trj]**
- **Win95:Boza**
- **Win95:Bumblebee**
- **Win95:CIH 1.x**
- **Win95:CIH-1106**
- **Win95:CIH-1142**
- **Win95:Fabi-B**
- **Win95:Filezz-B**
- **Win95:Hazlo**
- **Win95:Heathen**
- **Win95:Kenston**
- **Win95:Leviathan-3236**
- **Win95:Leviathan-3240**
- **Win95:Leviathan-B**
- **Win95:Matyas**
- **Win95:One-SGWW**
- **Win95:Orochi**
- **Win95:PowerFul**
- **Win95:Sledge-689**
- **Win95:Werther**

D: avast! ha trovato un virus sul mio computer. Mi dà diverse opzioni, ma nessuna di esse funziona. Come posso risolvere questo problema?

R: Prova a seguire i seguenti passi:

1. Se stai usando Windows Millenium Edition (ME) o Windows XP, disabilita la caratteristica **(system restore)**.

Se usi una versione diversa di Windows come XP o ME, salta questo step. Dopo, avrai bisogno di riavviare il tuo computer.

2. Effettua nuovamente la scansione. Non appena avast! mostra la finestra "Virus was found!" , clicca sul bottone **(delete)**.

3. Si aprirà un'altra finestra pop up. Here, seleziona l'opzione "**(if necessary, delete file(s) at next system start)**", come mostrato nella figura sotto:



Riavvia il tuo computer. Dopo il riavvio i file infetti non dovrebbero esserci più.

D: avast! ha trovato un virus, mi chiede solo di abbandonare la connessione, perché non posso cancellarlo?

R: Non puoi cancellare questo virus subito sul tuo computer. Infatti è stato trovato da uno degli "avast! resident providers - Web Shield". Questo provider effettua la scansione di tutti i file scaricati via Internet (HTTP protocol) **prima** che essi vengano salvati sul tuo disco locale. L'unica azione da fare è abbandonare la connessione e non permettere ad altri virus di essere scaricati.

D: Ho diversi messaggi di virus trovati nelle mie e-mail, provenienti dai mail server.

R: Alcuni virus sono falsificati dai "sender's e-mail address", così da sembrare virus ricevuti da e-mail servers come messaggi infetti, anche se non è così.