



ASSOCIAZIONE PICCOLE E MEDIE INDUSTRIE  
ADERENTE ALLA CONFAPI

## ALLARME VIRUS SOBIG.E

Fascia di rischio:	<b>Media</b>	Distruttivo:	<b>No</b>
Virus tipo:	<b>Worm</b>	Diffusione:	<b>e-mail</b>

### Descrizione

Una nuova variante del virus Sobig ha iniziato a diffondersi in modo massiccio attraverso Internet. Nel corso del week-end Sobig ha subito una mutazione e ha dato vita a due varianti: "Sobig.C" e "Sobig.B". Ma con una particolarità che li contraddistingue entrambi: si presentano nella casella di posta elettronica come normali e-mail il cui mittente però è...Bill Gates! Il 70% dei messaggi che contengono Sobig.E comunque giunge dagli Stati Uniti.

### Come arriva

arriva via e-mail, Sobig.E giunge in allegato ad un messaggio di posta elettronica con oggetto "Re: Movie" o "Re: Application" e recante il messaggio "Please see the attached ZIP file for details" (Guarda il file ZIP in allegato per maggiori dettagli).

### Con allegato

Il file your\_detail.zip. Il file una volta aperto con WinZip va in esecuzione infettando il computer se non protetto.

### Cosa fa

Il virus è in grado di colpire i computer con sistema operativo Microsoft Windows e utilizza un motore e-mail interno per inviare copie di sé stesso agli indirizzi prelevati dal computer infettato. Contrariamente alle versioni precedenti, Sobig.E è in grado di inviare più messaggi e-mail allo stesso tempo, riducendo così i tempi necessari per diffondersi.

### Come eliminarlo

aggiornare il pattern e l'engine del software antivirus. I grandi produttori di software antivirus hanno già catalogato e distribuito gli antidoti necessari.

**Ricordiamo di prestare sempre la massima cautela nell'aprire file allegati di e-mail della cui origine non si sia certi e di esercitare la massima prudenza anche in presenza di allegati provenienti da conoscenti, ma che non erano attesi.**

### Supporto & Consulenza Informatica

Dr. Gioachino Roccaro

**N.B. Le operazioni consigliate devono essere eseguite da personale esperto. L'associazione non si assume nessuna responsabilità per danni provocati dall'uso delle informazioni fornite. Tratto dal sito [www.antivirus.it](http://www.antivirus.it) – Fonte TrenD Micro e PCSELF Osservatorio Virus [www.pcself.com](http://www.pcself.com) – SYMANTECH security response.**