

## L'ALLARME VIRUS W32.Opaserv.E.Worm Massima attenzione !

### **WORM\_BUGBEAR**

Fascia di rischio:	<b>Media</b>
Virus tipo:	<b>Worm</b>
Distruttivo:	<b>Sì</b>
Diffusione:	<b>e-mail/Workgroup di rete non protetto.</b>

### **Descrizione:**

Il worm **W32.Opaserv.E.Worm** attacca i sistemi operativi Microsoft Windows 95, 98, 98 SE, ME, NT, 2000 e XP. Agisce sulle cartelle condivise in maniera da forzare la password con la quale sono state protette ed installarsi sul pc. Il virus inizia poi una scansione della rete cercando ed infettando le altre macchine Win9X e Win ME. Una patch per evitare tale problema è stata rilasciata da Microsoft (vedi <http://www.microsoft.com/technet/security/bulletin/MS00-072.asp>) e deve essere installata per prevenire future infezioni.

### **Come riconoscere il PC infetto:**

Se sul vostro PC esistono dei files chiamati Brasil.exe o Brasil.pif e se il file WIN.INI contiene il lancio di questi file (sotto la chiave [windows] esiste il comando run=c:\%windows%\brasil.exe o run=c:\%windows%\brasil.pif), il vostro PC è infetto.

### **Cosa fare:**

La prima cosa da fare è comunque sconnettere il PC infetto dalla rete e da Internet. I produttori di software antivirus hanno prodotto dei tools o istruzioni dettagliate per la rimozione si veda:

- Da Symantec:  
[http://securityresponse.symantec.com/avcenter/venc/data/w32.opaserv.worm.removal\\_tool.html](http://securityresponse.symantec.com/avcenter/venc/data/w32.opaserv.worm.removal_tool.html)
- Da Trend Micro:  
[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM\\_OPASERV\\_E](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_OPASERV_E)

*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.*