PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 2 - numero 243 di giovedì 14 dicembre 2000

Attenzione: virus in agguato!

E' stata segnalata la diffusione di due nuovi virus, pronti ad attaccare gli utenti incauti.

Una nota rivista on-line di informatica ha riportato la notizia della diffusione, in questi giorni, di due virus assai pericolosi.

Si tratta di XTC e della nuova versione del visus Blebla, denominato Blebla.B.
Entrambi colpiscono sistemi Windows e giungono come attachment di messaggi di posta elettronica, ma hanno modalita' di attacco differenti.

XTC e' in grado di aprire le porte di accesso del computer infettato; tale operazione consente all'autore del virus di aggiornarlo e di controllarne il comportamento. Non e' escluso che tra i vari danni che questo virus e' in grado di apportare vi sia anche quello di cancellare determinati file presenti sul PC.

Come riconoscere la pericolosa email portatrice del virus?
Il suo subject e' "AVX update notification" ed il file allegato ha dimensione 20480 byte.

Per eliminare il virus e' necessario cancellare tutti i riferimenti a XTCUpdate dal file di registro, riavviare il PC e cancellare il programma Services.exe dalla directory di Windows.

Per quanto riguarda invece il virus Blebla.B, una volta installatosi sul computer, si auto invia a tutti gli utenti presenti nella rubrica di Outlook, ma non solo...
Blebla.B infatti agisce sui file di registro in modo tale che qualsiasi file con estensione .exe, .jpg, .gif, mp3 sia inviato nel cestino con nome modificato; il file originale sara' rimpiazzato dal virus stesso con estensione ".exe".
Attenzione: i file cancellati non saranno piu' utilizzabili.

Come giunge Blebla.B?
Questo virus si diffonde tramite una email costruita in HTML che, una volta aperta, salva sul computer ed attiva i due allegati "Romeo.exe" e "Juliet.chm".
Tra i subject dell'email infetta segnalati vi sono:
"Romeo&Juliet", "where is my juliet ?", "where is my romeo ?", "hi", "last wish ???", "lol:)", ",,...", "!!!", "newborn", "merry christmas!", "surprise !", "Caution: NEW VIRUS !", "scandal !", "^_^".

Per eliminare Blebla non solo e' necessario rimuovere tutti i file"W32.Blebla.B.Worm", ma anche recuperare le impostazioni del file di registro originale.
E' bene inoltre aggiornare l'antivirus ed impostarlo in modo tale che scansioni le email in arrivo e disattivi l'HTML in tali messaggi.

---

www.puntosicuro.it