PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 916 di martedì 13 gennaio 2004

Virus...mascherati

Segnalate nuove e-mail contenenti falsi aggiornamenti di Windows.

Nei giorni scorsi sono state inviate a numerosi indirizzi, da ignoti, e-mail alle quali era allegato un file contenente un "trojan"; cioè un virus celato in un software che si introduce nel sistema ed esegue in modo nascosto operazioni che danneggiano il computer dell'utente.
Secondo Symbolic che ha riferito la notizia, il trojan in questione, denominato Xombe, è contenuto in una e-mail che si vuol far passare come proveniente da Microsoft. Infatti il messaggio indica come mittente "windowsupdate@microsoft.com" e come oggetto "Windows XP Service Pack 1 (Express) - Critical Update".
L'utente è invitato a scaricare un falso aggiornamento contenuto nel file winxp_sp1.exe.

Se l'utente apre il file, viene aperta una connessione ad internet e viene scaricato un file che si installa sul computer della vittima.

E' bene prestare la massima attenzione a questi falsi aggiornamenti.
Già altri virus e worm, come Swen, hanno utilizzato il nome "Microsoft" per indurre gli utenti ad aprire file allegati a messaggi di posta elettronica.
In quell'occasione Microsoft aveva precisato le modalità con le quali i suoi software vengono aggiornati; modalità che vale la pena ricordare.
"Per la sicurezza dei sistemi, è estremamente importante evitare di utilizzare software ricevuto da fonti sconosciute. [...]
Benché nei messaggi sia indicato che gli allegati contengono aggiornamenti per prodotti software di Microsoft o altri fornitori, in realtà si tratta di software pericolosi che al momento dell'esecuzione possono danneggiare i programmi e i file sul computer.

Il software Microsoft non viene mai distribuito direttamente tramite posta elettronica.
-Il software è distribuito su supporti fisici come CD-ROM e dischi floppy.
-Gli aggiornamenti sono distribuiti via Internet, dal sito Web di Microsoft (http://www.microsoft.com) o dal Download Center (http://www.microsoft.com/downloads/search.asp?).
-Talvolta Microsoft invia comunicazioni tramite posta elettronica per segnalare ai clienti la disponibilità degli aggiornamenti. Questi messaggi tuttavia contengono solo i collegamenti ai siti di download: in nessun caso il software viene allegato al messaggio di posta elettronica. I collegamenti inoltre puntano sempre al sito Web o FTP di Microsoft, non a siti di terze parti.
-Microsoft utilizza costantemente la tecnologia Authenticode per certificare con firma digitale i propri prodotti e assicurare che non siano stati alterati.
Se ricevete un messaggio di posta elettronica che indica che il software allegato è inviato da Microsoft, non eseguite l'allegato ed eliminate il messaggio.
