ASSOCIAZIONE PICCOLE E MEDIE INDUSTRIE
ADERENTE ALLA CONFAPI

ALLARME VIRUS W32.SQLExp.Worm

Massima attenzione per chi usa SQL Server e MSDE.

WORM_GONE.A

Fascia di rischio:	**Alta**
Virus tipo:	**Worm**
Distruttivo:	**Sì**
Diffusione:	**e-mail**

Descrizione:

Dopo il black-out informatico che ha colpito la Rete mondiale (250 mila server) sabato scorso rallentando le comunicazioni (soprattutto di posta elettronica), il virus SQ Hell, partito dalla Corea del Sud e paragonato al "Codice rosso" del 2001, minaccia di fare altri danni, sebbene di minore intensità. Così dicono gli esperti sudcoreani: il "bug" non è sconfitto, si è solo nascosto. E anche il ministero dell'informazione e della comunicazioni di Seul comunica dei disagi: ''Ci sono ancora forti irregolarità di traffico nel server 'KT' (Korea Telecom)". 'Kt' detiene circa il 54% del mercato sudcoreano trasmissione dati via Internet. Il virus che ha colpito il server "MS SQL 2000" prodotto dalla Microsoft sfrutta le debolezze del sistema. La propagazione avviene attraverso la ricezione su porta UDP 1434 di 376 Byte e dal 24/01/2003 si è notato un incremento esponenziale di chiamate a indirizzi IP random su porta UDP 1434.
Si consiglia di visitare i seguenti link Microsoft:

Microsoft Security Bulletin MS02-039
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp

Microsoft Security Bulletin MS02-061
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp

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 ***– Fonte TrenD Micro e PCSELF Osservatorio Virus*** www.pcself.com ***– SYMANTECH security response.***

VIA F. LIPPI, 30
25134 BRESCIA
TEL. 030/23076 – FAX 030/2304108
segreteria@api.bs.it

C.F. 80017870173
P.IVA 01548020179