PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 389 di giovedì 26 luglio 2001

Virus SirCam: stato di allarme ai massimi livelli

Colpisce i sistemi Windows intasando le infrastrutture di rete. Utili indicazioni per contrastare l'infezione.

In Europa e negli Stati Uniti sono in continuo aumento le segnalazioni di infezione da parte del virus SirCam.
Questo worm, come avevamo già illustrato nel numero 387 del nostro quotidiano, si diffonde in modo tradizionale, ovvero all'apertura degli allegati di alcuni messaggi di posta elettronica, e si autoinvia a tutti gli indirizzi della rubrica, contagiando altri PC.

SirCam ha la capacità di scegliere liberamente, negli archivi elettronici della macchina infettata, il file da allegare, con il risultato di spedire attach file del peso di alcuni megabyte, che possono rallentare o addirittura intasare le infrastrutture di rete, e di diffondere documenti segreti delle aziende.
La particolarità del suo funzionamento riguarda, però, il collocamento di alcuni file nel cestino di Windows, che in genere non viene scansionato dai tradizionali antivirus, grazie ai quali il virus riesce a ri-infettare il PC.

Lo stato di allarme è in progressiva crescita, infatti, il Symantec Antivirus Research Center, che in Usa sviluppa antivirus elettronici, ha classificato SirCam al quarto livello di pericolosità, in una scala che si estende da 1 a 5.

Ma come è possibile limitare la diffusione del virus?
Una pagina web predisposta da Tiscali, fornisce utilissime indicazioni per riconoscere le e-mail "pericolose" e per intervenire adeguatamente nel caso l'infezione sia già avvenuta.
Il messaggio di posta elettronica riconosciuto come "infettante" è simile al seguente:
" Da: [indirizzo e-mail]
A: [indirizzo e-mail]
Oggetto: [nome del documento senza estensione]
Hi! How are you?
I send you this file in order to have your advice
o
I hope you can help me with this file that I send
o
I hope you like the file that I sendo you
o
This is the file with the information that you ask for
See you later. Thanks "

Il file in allegato ha il nome del documento che il virus ha scelto con l'aggiunta di un' estensione di tipo .EXE, .PIF, .COM, .BAT, .LNK, .DOC, .XLS o .ZIP.

Tutti i maggiori produttori di antivirus hanno già predisposto opportuni aggiornamenti per bloccare la diffusione di SirCam, che pare abbia colto alla sprovvista soprattutto i singoli utenti privati.