PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 405 di venerdì 21 settembre 2001

Allarme virus!

Rapidissima la diffusione di un nuovo e complesso worm che colpisce anche attraverso le pagine web. Come riconoscerlo e come difendersi.

Una vera e propria epidemia quella provocata dal nuovo virus Nimda (W32/Nimda.A@mm) in soli due giorni di diffusione.
Le prime segnalazioni sono giunte dal Giappone, ma cresce di ora in ora il numero dei computer e dei web server in America ed Europa colpiti da questa infezione.

Il ministro della giustizia americano, in conferenza stampa, ha dato notizia della diffusione del worm, tuttavia ha affermato che non sono emerse prove di eventuali legami con gli attentati terroristici dell'11 settembre.

Vulnerabili al virus sono i sistemi Windows 95, 98, ME, NT e 2000, ed i server NT/2000.

A tutti gli utenti Internet e' raccomandata la massima attenzione; anche perche' trattandosi di un virus del tutto nuovo, le effettive potenzialita' e conseguenze derivanti dall'infezione sono ancora allo studio degli esperti.

Diversamente dai virus che hanno colpito negli ultimi tempi, il "contagio" puo' avvenire non solo da allegati infetti di messaggi di posta elettronica, ma anche da pagine web e attraverso unita' di rete condivise (nelle reti locali, ad esempio quelle delle aziende).

Nimda si diffonde mediante e-mail contenenti un file chiamato README.exe (sono stati segnalati anche file README.wav e README.com) di dimensione 57.344 byte.
Il virus varia invece il soggetto della mail infetta componendolo con una serie di al massimo 80 caratteri.
Nella posta elettronica il Nimda ha funzioni di "mass mailer", ovvero manda copia di se' stesso agli indirizzi di posta presenti nella rubrica.

Una volta attivo, Nimda cerca di connettersi a indirizzi casuali ed effettua una scansione per appurare la presenza di bachi noti di IIS (Microsoft Internet Information Server) per manipolare il server, ad esempio il baco "Web directory traversal".
I server compromessi possono diventare a loro volta vettori del virus; infatti se un utente visualizza una pagina ospitata dal server infetto, viene avviato automaticamente un codice che scarica ed esegue il virus sul suo disco fisso.
Il worm si diffonde anche attraverso condivisioni gia' presenti sulla rete locale, o creandone di nuove sul computer infetto; diminuendo il livello di sicurezza delle reti.

Come riconoscere se un server e' stato infettato?
Il primo campanello di allarme e' un improvviso ed insostenibile traffico di rete.

Verificare la presenza sui sistemi del file invisibile admin.dll, del file "readme.eml" all'interno delle cartelle condivise o della riga di testo "Shell=explorer.exe load.exe -dontrunold" all'interno del file system.ini.

Le principali aziende produttrici di antivirus hanno gia' approntato strumenti per rilevare la presenza del virus.

Per rendere i sistemi meno vulnerabili e' bene che gli utenti che utilizzano Internet Explorer 5.01 e 5.5 installino la patch per IE 5.5SP1 e precedenti; un'apposita patch e' disponibile sul sito di Microsoft per IIS.

Trend Micro raccomanda "l'uso di meccanismi di blocco per i file eseguibili in modo da raggiungere un veloce livello di sicurezza contro la diffusione di worm, come Nimda, il cui soggetto varia in modo casuale". Per i client di rete, anche quelli non

ancora infetti, Trend Micro consiglia poi di chiudere in scrittura tutte le condivisioni di rete e procedere a ripulire il sistema.

Oltre al pericoloso Nimda segnaliamo anche il virus "WTC" che si diffonde tramite l'allegato di un'e-mail.
Il worm e' nascosto in un file che invita alla lettura di informazioni relative agli avvenimenti dell'11 settembre.
In realta' WTC, se aperto, si autoinvia a tutti i nominativi contenuti nella rubrica del programma di posta elettronica.

---

www.puntosicuro.it