PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 514 di martedì 12 marzo 2002

Attenzione virus!

Segnalata la diffusione di due worm, uno dei quali si propaga tramite un falso aggiornamento Microsoft...

E' stata segnalata nei giorni scorsi la diffusione di due virus informatici che si propagano via e-mail.
Il primo, denominato MyLife (W32.MyLife@mm), si cela nel file "My Life.scr" allegato ad un messaggio di posta elettronica con oggetto: " my life ohhhhhhhhhhhh".
Nel testo del messaggio e' riportata invece la seguente frase:
" Hiiiii
How are youuuuuuuu? look to the digital picture it's my love
vvvery verrrry ffffunny:-)
my life = my car
my car = my house".

Secondo il quotidiano di informatica che ha dato notizia della diffusione del worm, una volta installatosi sul computer MyLife tenta di cancellare i file con determinate estensioni (".com", ".sys", ".ini", ".exe", ".vxd" e ".dll") e si autoinvia a tutti gli indirizzi di posta elettronica presenti nella rubrica.

Il secondo virus, segnalato da Symbolic -azienda produttrice di antivirus-, e' nominato Gibe e si spedisce per email fingendosi un aggiornamento proveniente da Microsoft. Allegato al messaggio vi e' il file "Q216309.exe".

Il testo del messaggio, del quale riportiamo un estratto al termine dell'articolo, descrive una vulnerabilita' nei sistemi Microsoft e induce l'utente ad eseguire l'allegato.
Se l'utente segue questo "consiglio" e apre l'allegato viene visualizza una finestra di dialogo che chiede se si vuole installare il "security update".
Se si conferma, il worm mostra una finestra e al termine dell'"operazione" informa l'utente che l'aggiornamento e' stato installato con successo.

Se l'utente non conferma, il worm si installa comunque, ma senza mostrare finestre di dialogo.
Gibe imposta un controllo sul sistema infetto, in modo che a una successiva esecuzione venga visualizzato il messaggio: "This update does non need to be installed on this system".

Durante l'esecuzione il worm crea alcuni file nel sistema e si autoinvia a tutti gli indirizzi e-mail trovati sul PC.

Di seguito riportiamo parte del testo dell'e-mail con la quale si diffonde "Gibe":

From: Microsoft Corporation Security Center
mailto:rdquest12@microsoft.com]
To: Microsoft Customer
Subject: Internet Security Update
Attachment: q216309.exe

Microsoft Customer,
this is the latest version of security update, the "5 Mar 2002 Cumulative Patch" update which eliminates all known security vulnerabilities affecting Internet Explorer and MS Outlook/Express as well as six new vulnerabilities, and is discussed in Microsoft Security Bulletin MS02-005. Install now to protect your computer from these vulnerabilities, the most serious of

which could allow an attacker to run code on your computer.

Description of several well-know vulnerabilities:
[.....]

System requirements:
Versions of Windows no earlier than Windows 95.

This update applies to:
[.....]

How to install
Run attached file q216309.exe

How to use
You don't need to do anything after installing this item.

For more information about these issues, read Microsoft Security Bulletin MS02-005, or visit link below.
http://www.microsoft.com/windows/ie/downloads/critical/default.asp
If you have some questions about this article contact us at rdquest12@microsoft.com

Thank you for using Microsoft products.

With friendly greetings,
MS Internet Security Center.
