PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 847 di lunedì 22 settembre 2003

Usa la firma Microsoft, ma e' una e-mail fasulla

Attenzione! Circola un messaggio, simile ad una comunicazione di Microsoft, che in realtà contiene un worm.

Indica come mittente "MS Technical Support", "Microsoft" "Microsoft Service" (o altri soggetti simili) e invita ad installare al più presto gli allegati, ma in realtà è un messaggio fasullo che contiene il worm Swen.

Affermano gli esperti di Symbolic: "Swen si distingue per un utilizzo estremamente astuto dell'ingegneria sociale.
Infatti, la mail creata dal worm e' fatta in modo da sembrare una informativa proveniente da Microsoft riguardante una fantomatica hotfix da installare al più presto; il linguaggio e l'aspetto del messaggio sono tali da indurre molti utenti ad aprire l'allegato e attivare così il worm.

Swen non e' intenzionalmente distruttivo, ma e' in grado di disattivare alcuni programmi antivirus e soprattutto e' capace di ricavare dal sistema infettato altri indirizzi di posta elettronica a cui spedirsi."

L'e-mail è ben fatta, con tanto di logo Microsoft, indica i sistemi per i quali sarebbe necessaria l'installazione dell'"aggiornamento" ed i riferimenti tecnici. Le caratteristiche del messaggio sono tuttavia variabili.

Il worm, segnalato nei giorni scorsi, si diffonde oltre che via e-mail, anche attraverso le reti locali e sistemi di condivisione (reti IRC, reti Kazaa).

Come riportato da Symbolic, Swen sfrutta una vecchia vulnerabilità di Internet Explorer per eseguirsi direttamente dalla e-mail.

Il file costituente il worm è un eseguibile, non compresso, Windows PE di dimensione 10649 bytes.

Quando il file del worm viene aperto controlla che non sia già stato installato, si copia in una cartella di Windows con un nome casuale (ex: MLMHP.EXE) e modifica una chiave di registro in modo che il worm sia sempre avviato con Windows.

Il worm mostra poi una successione di finestre di dialogo ("This will install Microsoft Security UpDate. Do you wish continue?"), come se si trattasse dell'installazione di un aggiornamento.
Swen cerca di disabilitare i dispositivi di sicurezza, come i firewall e raccoglie informazioni riguardanti il computer infetto..
Una volta installato il worm è in grado di prendere il controllo del sistema ogni qual volta un utente provi a lanciare eseguibili o file di registro.

Riguardo alla diffusione via e-mail, il worm scandisce periodicamente le pagine HTML e ASP sull' hard disk e raccoglie gli indirizzi e-mail nel file GERMSO:DBV nella directory di Windows. Il worm cattura le mail anche da file .EML, .DBX, .WAB e .MBX . Swen non raccoglie mail contenenti le stringhe 'delete' e 'spam'.

Se il worm non riesce a trovare gli indirizzi dei server SMTP per inviarsi, mostra una falsa "MAPI dialog box"chiedendo all'utente di inserire il dato.

Per quanto concerne la diffusione nelle reti IRC, il worm crea il proprio file SCRIPT.INI nella directory di installazione di mIRC. Questo script fa in modo che un IRC client mandi un file chiamato 'WinZip installer.zip' a tutti gli utenti che si uniscono al canale dove è presente un utente infetto.

Per diffondersi invece nelle Kazaa worm modifica il Registro in modo da abilitare la condivisione per i client Kazaa,

successivamente trova le directory condivise e ci si copia utilizzando come nome, ad esempio, una delle seguenti stringhe:Kazaa Lite, WinRar, WinZip, Download Accelerator, key generator, Bugbear, removerv removal tool, AOL hacker, Yahoo hacker, HardPorn, XP update, XXX Video, XXX Pictures, Virus Generator. I file possono avere estensione EXE o ZIP.

---

www.puntosicuro.it