PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1237 di mercoledì 04 maggio 2005

Allerta worm

Segnalata la diffusione di una pericolosa variante del worm Sober.

Ha fatto la sua comparsa in questi giorni in rete una nuova variante del worm Sober, Sober.P, per il quale Trend Micro ha stimato un grado complessivo di rischio medio, ma che potrebbe arrecare gravi danni.

Secondo quanto riferito da Symbolic, il worm si diffonde via e-mail, tramite un messaggio di posta elettronica scritto in lingua inglese o in lingua tedesca.
Se il dominio al quale viene inviata l'e-mail appartiene a uno dei seguenti ".de",".ch", ".at", ".li", '"gmx." la mail spedita sarà in tedesco, altrimenti è in lingua inglese.

Il messaggio è variabile e può avere uno dei seguenti soggetti:
Re: Your Password
Re: Registration Confirmation
Re: Your email was blocked
Re: mailing error
FwD: Ihr Passwort
FwD: Ihre E-Mail wurde verweigert
FwD: Ich bin's, was zum lachen ;)
FwD: Glueckwunsch: Ihr WM Ticket
FwD: WM Ticket Verlosung
FwD: WM-Ticket-Auslosung

Il testo del messaggio è variabile; tra quelli più diffusi vi è la forma seguente:
Account and Password Information are attached!
Visit: http://www..com
This is an automatically generated E-Mail Delivery Status Notification.
Mail-Header, Mail-Body and Error Description are attached
Attachment-Scanner: Status OK,AntiVirus: No Virus found,Server-AntiVirus: No Virus (Clean)

Passwort und Benutzer-Informationen befinden sich in der beigefuegten Anlage.

- http://www.< nome di dominio >
- MailTo: PasswordHelp@< nome di dominio >

**** AntiVirus: Kein Virus gefunden
**** "GMX" AntiVirus Service
**** WebSite: http://www.gmx.de

Al messaggio sarà allegato un file, in formato ZIP, che contiene al suo interno il file eseguibile di tipo PE, con dimensione 52

KBytes compresso con UPX. L'attach ha uno dei seguenti nomi:
mail_info.zip
our_secret.zip
Fifa_Info-Text.zip
okTicket-info.zip
free_PassWort-Info.zip
LOL.zip

Una volta eseguito l'allegato, nel sistema viene visualizzato il messaggio di errore: "Error: CRC not complete".

Successivamente crea nuovi file, che saranno eseguiti al successivo riavvio del sistema e consentono la diffusione del worm. Prima di diffondersi il worm esamina, in tutti i dischi rigidi, i file con determinate estensioni al fine di raccogliere indirizzi E-mail, ignorando indirizzi e-mail che contengono particolari stringhe, tra le quali. Abuse, antivir, virus.
