PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 451 di mercoledì 28 novembre 2001

Attenzione alle e-mail!

Procede a ritmi sostenuti la diffusione del virus informatico "Badtrans". Alcune precisazioni.

Sul numero di ieri del nostro abbiamo dato notizia della diffusione di una variante del virus informatico Badtrans.
Secondo le notizie fornite da Symbolic, azienda che si occupa di antivirus, pare che la diffusione di questo virus proceda a ritmi sostenuti.
Ricordiamo che "Badtrans"e' in grado di inviare allegati con nomi variabili, che al verificarsi di alcune condizioni potrebbero auto-eseguirsi durante la lettura della mail.
Oltre alla diffusione via posta elettronica, il virus e' in grado di installare componenti al fine di sottrarre informazioni dai sistemi infettati.

A completamento di quanto pubblicato ieri, riportiamo di seguito ulteriori informazioni riguardo a Badtrans.B.
Il virus viene trasmesso in un file eseguibile in formato PE (Portable Executable), di circa 29 Kb nella sua forma compressa.
E' composto da due parti - Worm e Trojan. La prima componente si occupa di inviare i messaggi infetti, mentre la seconda invia informazioni sull'utente e sul PC infetto a un indirizzo esterno di posta elettronica.

Il worm si puo' attivare in due modalita' differenti: con la collaborazione dell'utente (se quest'ultimo esegue l'allegato infetto) o autonomamente, sfruttando la vulnerabilita' di Internet Explorer della quale abbiamo accennato nell'articolo di ieri.
In seguito all'attivazione, il worm rilascia nel sistema la sua componente Trojan. Il nome del file che contiene il trojan, la directory in cui viene creato e la chiave di registro in cui viene inserito il riferimento possono essere configurati dall'hacker prima di spedire la mail.

Inoltre, viene installato un file, dal nome variabile, con funzioni di Keylogger (cioe' in grado di memorizzare il testo digitato tramite tastiera). Opzionalmente, Badtrans.B puo' cancellare il file originale infetto dopo l'installazione del trojan.

Per reinviare i messaggi infetti, il worm usa una connessione diretta al server SMTP; gli indirizzi dei destinatari vengono ricavati dalla casella della Posta in Entrata oppure analizzando il contenuto dei file *.HT* e *.ASP.

L'e-mail "infetta" e' in formato HTML.
Il campo "From" della mail puo' contenere il vero indirizzo dell'utente infettato oppure un indirizzo scelto a caso tra i seguenti: " Anna", "JUDY", "Rita Tulliani", "Tina", "Kelly Andersen", " Andy", "Linda", "Mon S", "Joanna", "JESSICA BENAVIDES", " Administrator", " Admin", "Support", 'Monika Prado", "Mary L. Adams"

Il soggetto della mail e' vuoto, oppure "Re:", o "Re:" piu' il soggetto di una mail trovata nella casella della Posta in Entrata; il corpo del messaggio e' vuoto.
L'allegato ha un nome casuale con doppia estensione, secondo le modalita' specificate ieri.

Le aziende produttrici di antivirus sono gia' in grado di fornire gli opportuni aggiornamenti per rilevare ed eliminare il virus.