PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 599 di martedì 16 luglio 2002

Allarme virus!

Crescente diffusione delle varianti del worm Frethem. Conosciamone le caratteristiche.

E' partito in sordina il worm Frethem, la prima variante è stata infatti rilevata l'11 giugno, ma nella giornata di ieri, con le varianti Frethem.K e Frethem.L, è stata segnalata una crescente diffusione dell'infezione.

Come illustrato da Symbolic, società di sicurezza informatica, il worm, contenuto nell'allegato di un messaggio di posta elettronica, è in grado di catturare gli indirizzi presenti nel Windows Address Book e nei file con estensione *.dbx e utilizza un proprio motore SMTP per diffondersi.

Di seguito riportiamo la descrizione delle varianti del worm fornitaci da Symbolic.

VARIANTE: Frethem.A
Questa variante si diffonde attraverso messaggi con il seguente contenuto:

Soggetto: Re: Do your Windows looks like Windows XP? I have found very nice desktop themes!

Testo: Hello!
Do you like modern design of new Windows XP?! I have found FREE and easy to use desktop themes! You can open attach with web site and samples! Enjoy it!!!

Attachment: www.freethemes.com

VARIANTE: Frethem.E
Il messaggio tramite il quale si diffonde questa variante è il seguente:

Soggetto: Re: Your password!
Testo: Hello!
ATTENTION!
You can access
very important
information by
this password
DO NOT SAVE
password to disk
use your mind
now press
cancel
Attachment: decrypt-password.exe

Questa variante utilizza una vulnerabilità di Internet Explorer che consente l'esecuzione automatica degli allegati non appena il messaggio di posta viene aperto.Tale vulnerabilita' puo' essere eliminata applicando la patch disponibile sul sito Microsoft.

VARIANTE: Frethem.K
Questa variante del worm si diffonde come file in formato PE oppure UPX di circa 47 Kb. Il worm spedisce se stesso con un

allegato dal nome DECRYPT-PASSWORD.EXE (come la variante Frethem.E).
Questa variante si diffonde attraverso messaggi con il seguente contenuto:
Soggetto: Re: Your password!

Testo: ATTENTION!
You can access
very important
information by
this password
DO NOT SAVE
password to disk
use your mind
now press
cancel
()
Attachment: decrypt-password.exe, password.txt

ll file 'password.txt' contiene il seguente testo: Your password is W8dqwq8q918213.
Symbolic precisa che tutti i file infetti devono essere eliminati e allo stesso modo le mail che contengono gli allegati infetti.

VARIANTE: Frethem.L
Questa variante del worm è molto simile alla precedente ed utilizza un file in formato PE oppure UPX di circa 48 Kb. Il worm utilizza un allegato dal nome DECRYPT-PASSWORD.EXE per diffondersi (come la variante Frethem.E e Frethem.K).

Rimozione del worm (per le varianti: Frethem.M e Frethem.L)
Il worm Frethem copia se stesso nella cartella "Esecuzione Automatica" dell'utente e non introduce altri cambiamenti alla configurazione del sistema. Per rimuovere questo worm è sufficiente terminare dal Task Manager il processo "Setup" ed eliminarlo dall'esecuzione automatica.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.