PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 463 di venerdì 14 dicembre 2001

Nuovo worm in Rete: Gokar

Il messaggio infettante ha soggetti, contenuti e allegati variabili.

Symbolic ha rilevato in data 13 dicembre 2001 la diffusione di un nuovo virus denominato Gokar.
Per diffondersi Gokar utilizza la posta elettronica: la linea soggetto, il contenuto del messaggio e l'allegato sono variabili. Gli allegati in particolare possono avere estensione PIF, SCR, COM, EXE, BAT e il loro nome viene generato combinando in modo casuale alcune parti contenute nel worm.

E' possibile verificare se una macchina è infetta controllando se all'interno della cartella Windows è presente il file KAREN.EXE. Una volta effettuata questa copia di se stesso come KAREN.EXE, Gokar è in grado di modificare il registry per essere eseguito al riavvio di Windows.

Il soggetto dei messaggi può essere uno dei seguenti:
"If I were God and didn't belive in myself would it be blasphemy
The A-Team VS KnightRider ... who would win
Just one kiss, will make it better. just one kiss, and we will be alright.
I can't help this longing, comfort me.
And I miss you most of all, my darling ...
... When autumn leaves start to fall
It's dark in here, you can feel it all around. The underground.
I will always be with you sometimes black sometimes white ...
.. and there's no need to be scared, you re always on my mind.
You just take a giant step, one step higher.
The air will hold you if you try, trust my wings of desire. Glory, Glorified.....
The horizons lean forward, offering us space to place new steps of change.
I like this calm, moments before the storm
Darling, when did you fall..when was it over ?
Will you meet me .... and we'll fly away ?!"

Il testo inviato può contenere una delle seguenti frasi:
"You should like this, it could have been made for you
speak to you later
Hey
They say love is blind ... well, the attachment probably proves it.
Pretty good either way though, isn't it ?
Happy Birthday
Yeah ok, so it's not yours it's mine :)
still cause for a celebration though, check out the details I attached
This made me laugh
Got some more stuff to tell you later but I can't stop right now
so I'll email you later or give you a ring if thats ok ?!
Speak to you later."

Gokar è anche in grado di diffondersi attraverso le chat modificando i client mIRC e inviando il file KAREN.EXE a tutti gli utenti collegati a un canale IRC dove e' presente un utente infetto.

Il virus è anche in grado di fermare i processi dei seguenti prodotti antivirus:
VSHWIN32.EXE (McAfee)
NAVAPW32.EXE (Norton)
_avpm.exe (Kaspersky)
avpm.exe (Kaspersky)
ICLOAD95.EXE (Sophos)
ICMON.EXE (Sophos)
IOMon98.exe (Trend)
VetTray.exe (CA)
Claw95.exe (Norman)
f-stopw.exe (F-PROT)

Per ulteriori informazioni e per le istruzioni relative alla rimozione di Gokar è possibile consultare il sito di Symbolic.

---

www.puntosicuro.it