PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 792 di lunedì 09 giugno 2003

Allarme worm!

Massiccia diffusione di una variante polimorfica del worm Bugbear, che "ruba" dati e password.

Nello scorso week end è stata segnalata la massiccia diffusione di una nuova variante polimorfica del worm Bugbear (si veda PuntoSicuro 635), denominata Bugbear.B.

Symbolic ha posizionato il worm al livello 1 di allerta (massimo rischio).

Il nuovo worm, dotato di un proprio motore SMTP, si diffonde attraverso messaggi di posta elettronica, oppure si propaga tramite le reti locali.

Le caratteristiche del messaggio sono variabili. Il worm falsifica l'indirizzo del mittente della mail, ad esempio indicando un indirizzo preso casualmente tra gli indirizzi trovati sul computer infetto.

Il soggetto dei messaggi infetti e' preso casualmente da file del computer infetto oppure viene scelto da un elenco predefinito. Tra i soggetti più comuni, e che quindi possono trarre in inganno, vi sono: Greets! ; Hi! ; Re: ; Your Gift, Report; Warning!; update; Hello!; various.

Il corpo del messaggio infetto può essere vuoto oppure può contenere un testo estratto da un file scelto casualmente dal computer infetto.
Questa modalità di composizione dell'e-mail rende il virus particolarmente insidioso, informazioni riservate contenute sul pc infettato potrebbero infatti essere diffuse a migliaia di utenti.

In alcuni casi il testo del messaggio può sfruttare una vulnerabilità di Internet Explorer per eseguirsi automaticamente su alcuni computer quando una e-mail infetta viene aperta.
(Questa vulnerabilità può essere corretta dalla nuova patch reperibile sul sito di Microsoft).

Come riportato da Symbolic "Il file contenente il worm e' un eseguibile Windows PE compresso mediante compressore di file UPX e cifrato con un semplice crittoalgoritmo che cambia in ogni generazione del worm rendendolo così polimorfico."
In alcuni casi il nome dell'allegato è il "tradizionale" SETUP.EXE oppure può contenere, ad esempio, le parole: reame, Card, Docs, news, image, photo, video, music, data.
In altri casi il nome è scelto in modo casuale tra i file presenti sul computer infetto.
L'estensione dell'allegato e' scelta fra le seguenti: exe; scr; pif.
Nel caso in cui il worm usi il nome di un file presente sul computer infetto l'allegato potrebbe avere una doppia estensione, ad esempio DOCUMENT.DOC.EXE. Il worm controlla l'estensione del file e setta il content type dell'allegato in modo appropriato.

Per trovare gli indirizzi e-mail verso cui propagarsi il worm cerca nei file con queste estensioni: .ODS, .MMF, .NCH, .MBX, .EML, .TBB, .DBX, INBOX

Particolarmente pericoloso il fatto che il worm contiene una componente di backdoor , che "ascolta" sulla porta TCP 1080, tramite la quale un assalitore può inviare i seguenti comandi:
-informazioni sul computer infettato
-upload e download di file
-esecuzione di file
-eliminazione di file

-terminazione di processi
-lista dei processi in esecuzione
-avvio del keylogger
-avvio di un server web su una porta a scelta
Gli esperti di Symbolic rilevano che "la backdoor presente in Bugbear.B non usa, a differenza della variante precedente, un sistema di autenticazione e quindi può essere usato da chiunque e non solo dall'autore del worm."

---

www.puntosicuro.it