PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 695 di lunedì 13 gennaio 2003

Invasione di worm

In meno di 48 ore si sono diffusi 4 worm. Elevate la capacità di propagazione di "Lirva". Le caratteristiche delle infezioni.

Symbolic, azienda che opera nell'ambito della sicurezza informatica, ha rilevato in meno di 48 ore la diffusione di quattro diversi worm, due dei quali(Lirva.A, , Lirva.B) proverrebbero dallo stesso autore.

Lirva
Lirva.A e Lirva.B hanno grandi capacità di propagazione, e si possono collocare dopo il noto Klez per diffusione e prevalenza sulle reti di tutto il mondo.
Lirva è in grado di utilizzare diversi meccanismi per replicarsi, sfruttando la posta elettronica, ICQ, Kazaa, mIRC e attraverso le risorse condivise di Windows.

Il worm Lirva, inoltre, e' in grado di disabilitare diversi software antivirus e altri software di sicurezza.
Il worm, una volta attivatosi, cerca di appropriarsi delle password e le invia ad un indirizzo di posta esterno.

Riguardo alla diffusione via e-mail, il messaggio infetto è formattato come pagina HTML contenente la vulnerabilità Exploit IFrame che consente, semplicemente aprendo l'email, di eseguire in automatico l'allegato.

Il subject, il corpo della mail ed il nome del allegato vengono generati in modo casuale utilizzando una lista predefinita.

Tra i subject segnaliamo: Fw: Prohibited customers..., Re: Reply on account for IFRAME-Security breach, Fwd: Re: Reply on account for Incorrect MIME-header, Re: Brigade Ocho Free membership.

Anche i testi dei messaggi sono variabili. Riportiamo due esempi:
Restricted area response team (RART)
Attachment you sent to %s is intended to overwrite start address at 0000:HH4F%s To prevent from the further buffer overflow attacks apply the MSO-patch %s'

oppure

'Microsoft has identified a security vulnerability in Microsoft(r); IIS 4.0 and 5.0 that is eliminated by a previously-released patch.
Customers who have applied that patch are already protected against the vulnerability and do not need to take additional action.
Microsoft strongly urges all customers using IIS 4.0 and 5.0 who have not already done so to apply the patch immediately.
Patch is also provided to subscribed list of Microsoft(r) Tech Support:'

Numerosi i nomi tra i quali il worm sceglie l'allegato; segnaliamo ad esempio: Resume.exe, Download.exe, MSO-Patch-0071.exe, Readme.exe, Sophos.exe, Cogito_Ergo_Sum.exe.

ExploreZip.E
ExploreZip.E è invece una variante di un worm che risale al 1999. La versione attuale non presenta differenze rispetto all'originale, se non un nuovo metodo di compressione dell'eseguibile.
ExploreZip si diffonde mediante un allegato di mail chiamato zipped_files.exe, la cui icona sembra quella di un archivio compresso eseguibile.

Quando il worm viene lanciato per la prima volta, viene visualizzato un finto messaggio di errore:

Error
Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help

Il worm si propaga via e-mail, con il seguente messaggio:
Soggetto:
RE:
Messaggio:
Hi ! I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs. bye.
Allegato:
zipped_files.exe

Sobig
Sobig si diffonde via e-mail e attraverso le condivisioni di rete. Cerca inoltre di scaricare altri file da alcuni indirizzi su geocities.

Riguardo alla diffusione via e-mail, il soggetto del messaggio viene generato in modo casuale utilizzando una lista predefinita: Re: Here is that sample, Re: Document, Re: Sample, Re: Movies

Il testo del messaggio è fisso: "Attached file:".

Allegato al messaggio può essere uno dei seguenti file: Sample.pif, Untitled1.pif, Document003.pif, Movie_0074.mpeg.pif.

Sobig si distingue dai precedenti due worm per il tentativo di installare una backdoor nei sistemi infettati.
Al momento il tentativo non riesce, ma, secondo Symbolic è probabile "che questa prima versione di Sobig costituisca una sorta di test per un attacco più strutturato, oppure che il virus writer progetti di attivare il prelievo della backdoor successivamente alla diffusione del worm."

---

www.puntosicuro.it