Allarme virus!!!

Seconda parte

Ed eccoci a riparlare di virus, nella buona e nella cattiva sorte. Ce n'è tanti, da quelli che la mattina di Natale ci fanno gli auguri e di quelli che ci invitano, al boot, a partecipare a una partita , con posta il nostro HD. Continuiamo a conoscerli, per evitare di gridare "... all'untore" a ogni pie' sospinto, senza però mai abbassare la guardia, per non dovercene pentire amaramente in seguito.

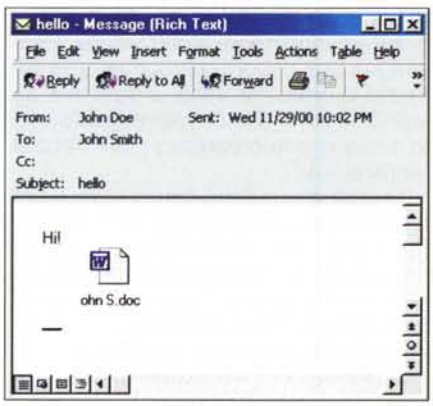
di Raffaello De Masi

Ma cos'è e come funziona un virus del computer? Una spiegazione semplice non esiste e meriterebbe ben altro spazio di quello che possiamo riservare sulle pagine di questa rivista. Probabilmente il sistema migliore per intendere che cosa è e come esso funzioni potrebbe venire proprio da un esempio ricavato dalla vita normale. Per giungere quindi a una vera definizione di virus-non virus abbiamo utilizzato una serie di esempi e di indicazioni ricavate da un pregevolissimo tutorial presente sulle pagine Internet al sito http://www.metro.ch , sito che fortemente ci sentiamo di raccomandare per la completezza dell'esposizione, la chiarezza concettuale e l'assoluta accuratezza delle informazioni in esso contenute.

Il sito è anche altresì consigliabile per contenere una estesa serie di riferimenti, e per consentire il download del programma AVP-Antiviral Toolkit Pro, uno degli antivirus più potenti e raffinati attualmente esistenti in commercio.

Una spiegazione terra terra

Per comprendere la tecnica di funzionamento, di infezione, e di distribuzione di un virus utilizzeremo un esempio, ben noto in letteratura, dovuto a.N. Lozinski.

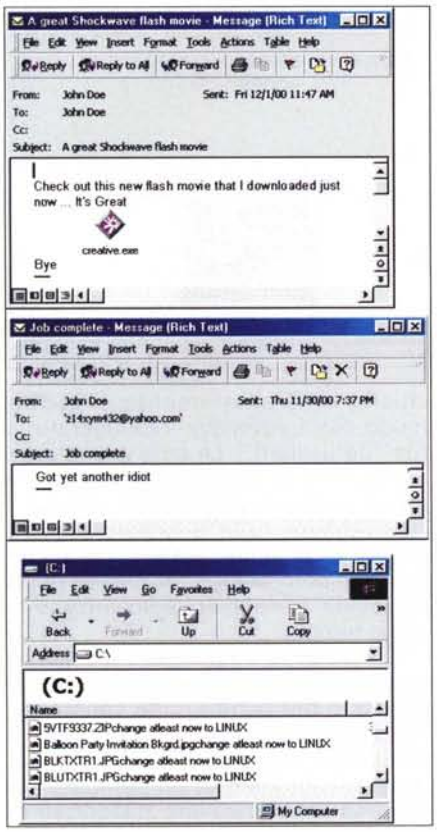


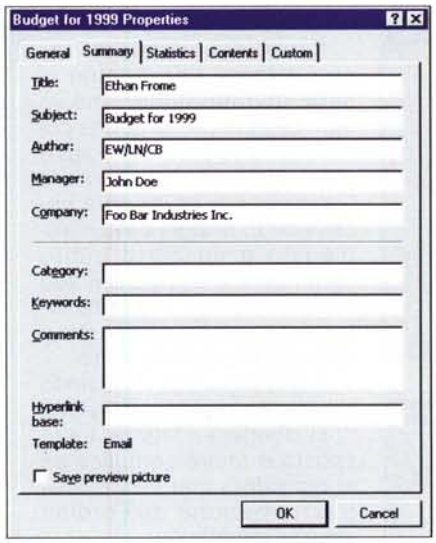
Immaginiamo un impiegato di un ufficio che lavora, in un compito di scrivania, ogni giorno. Ogni mattina egli trova una catasta di fogli sul tavolo, con una lista di cose da fare che devono essere portate a termine durante il lavoro quotidiano. Il suo ruolo consiste nel prelevare il primo foglio dalla catasta, leggere le istruzioni del suo superiore, seguirle accuratamente, e gettare via i fogli delle istruzioni ultimate nel cestino della carta.

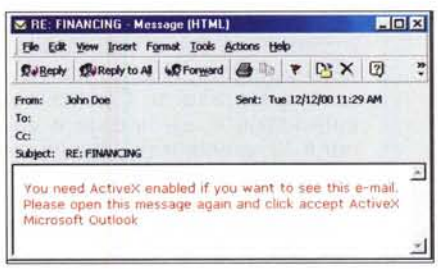
Immaginiamo che un burlone entri in 'ufficio a sua insaputa e inserisca nella catasta un foglio su cui c'è scritto il seguente ordine:

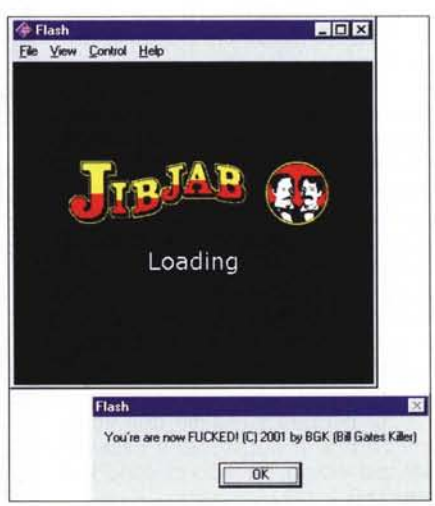
" Copiare questo foglio due volte e mettere le copie nella catasta dell'impiegato accanto. "

Cosa succederà quando impiegato incontrerà quest'ordine? Esso copierà il foglio due volte, distruggerà l'originale, e continuerà con il foglio successivo nella catasta, proseguendo nel suo lavoro abituale. Cosa farà invece impiegato accanto, che, essendo stato istruito ad eseguire gli ordini senza discutere, troverà i fogli con gli ordini? Farà esattamente le stesse cose che ha fatto il primo: copierà il foglio due volte e li trasferirà all'impiegato successivo. In questo modo avremo già









quattro copie del foglio e l'ordine continuerà ad essere copiato e trasferito ad altre persone.

È questo esattamente lo scenario nel quale e secondo cui agisce un virus del computer, dove i programmi prendono il posto dei fogli di carta e le macchine quella degli impiegati.

Un computer, come un impiegato, esegue ordinatamente e correttamente tutti comandi contenuti in un programma (lista degli ordini) cominciando col primo.

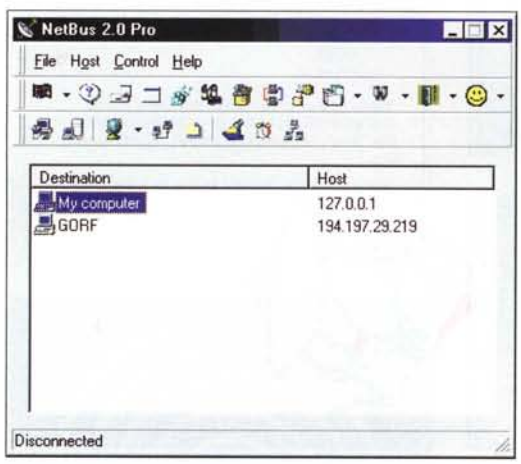
Se il primo comando è del tipo "copia il mio codice su due altri programmi" il computer eseguirà questi ordini, e il comando inserito nel virus sarà presente su altri due programmi. Nel momento in cui il computer lancerà un altro " infetto", il virus continuerà nell'opera di incollaggio sugli altri programmi, fino a saturare completamente il computer.

Nell'esempio precedente riguardante gli impiegati nel loro ufficio il nostro virus di carta non controlla se la catasta su cui è capitata è già infettata oppure no. In questo caso alla fine della giornata di lavoro tutto l'ufficio sarà sommerso da pile di queste copie e gli impiegati non avranno altro da fare che copiare continuamente lo stesso testo e passarne le copie ai vicini.

Facendo un po' di conti alla buona, e considerando che il primo impiegato produrrà due copie del foglio, quello successivo quattro, e successivamente 8, 16, 32, 64 e così via, noteremo facilmente che il numero delle copie si raddoppia ad ogni passaggio.

Immaginando che un impiegato ha bisogno di trenta secondi per copiare un foglio di carta e trenta secondi per passare le copie al suo vicino, si può facilmente calcolare che in un'ora saranno prodotti un miliardo di miliardi di copie del virus cartaceo.

Poiché l'ufficio non può disporre di tanta carta, la propagazione del virus si fermerà un certo punto, per ovvie ragioni.



Buffo vero? Ammesso che gli impiegati siano tanto stupidi da non accorgersi di quello che sta succedendo!

Esattamente la stessa cosa avvenne nel 1988 negli Stati Uniti, quando diversi network di informazione globale furono sommersi da copie di un virus (Morris worm) che trasferiva se stesso da un computer all'altro, con una tecnica abbastanza simile a quella descritta.

I virus un po' più evoluti si comportano in maniera meno stupida e meno evidente. In questo modo il virus viene immediatamente scoperto e perde lo scopo per cui è stato costruito. Il passo successivo per evitare problemi di questo tipo (e ovviamente, per evitare di essere scoperti) è quello di modificare leggermente l'ordine che può essere così nuovamente redatto:

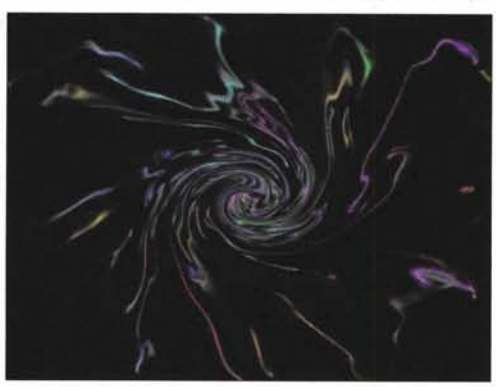
" Copia questo foglio due volte e sistema le copie nella catasta del tuo vicino, se non ci sono già presenti ".

Il problema in questo caso è risolto, perché non ci sarà sovrappopolazione, e ogni catasta conterrà una copia del virus pronta a colpire solo se se ne presenterà l'occasione e ce ne sarà necessità. E, in ogni caso, l'impiegato a un certo punto continuerà a svolgere il suo lavoro, mentre l'agente infettante resterà nascosto e comunque poco evidente.

" Ma cosa c'entra questo con la distruzione dei dati? ", si chiederà il lettore. La risposta è molto semplice se si considera una successiva trasformazione dell'ordine appena modificato:

" copia il foglio due volte e sistema le copie nella catasta dell'impiegato accanto, se non sono già presenti. Controlla il calendario e, se la data è venerdì 13, prendi tutti i documenti e gettali nel cestino ".

A questo punto lo scopo, le funzioni, e le metodologie d'attacco di un virus sono del tutto



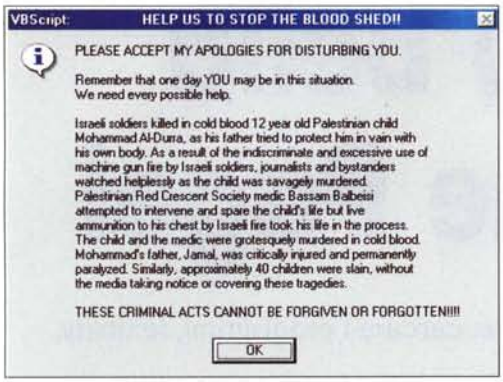
```
2E 68-73 71 00 00      qazwsx.hsq
74 65-2E 63 6F 6D  %s %s   note.com
52 45-5C 4D 69 63     SOFTWARE\Mic
64 6F-77 73 5C 43  rosoft\Windows\C
69 6F-6E 5C 52 75  urrentVersion\Ru
45 00-4E 55 4C 4C  n   startIE NULL
00 00-72 00 00 00     roc *   r
65 00-72 00 00 00  notepad.exe r
00 00-6E 6F 74 65  note.com    note
00 00-25 64 2E 25  .com     ..  %d.%
25 64-2E 25 64 2E  d.%d.%d \\%d.%d.
00 00-5C 5C 00 00  %d.%d   %s  \\
64 2E-65 78 65 00  %s\ notepad.exe
6F 74-65 70 61 64  SOFTWARE\notepad
```

chiare, ed è esattamente in questo modo che funzionava il famigerato virus "Jerusalem". La cosa più interessante, in tutti questi ragionamenti, e da un punto di vista anche ironica, è che, sebbene tutte le cataste degli impiegati siano state infettate, il virus originale (il primo foglio trovato dal primo impiegato e cestinato) è scomparso da lungo tempo.

C'è solo da aggiungere un paio di considerazioni: primo, che i virus non appaiono per generazione spontanea, ma sono costruiti da programmatori e comunque persone, secondo che non possono accedere a un computer da soli, ma devono essere trasportati da qualche intermediario che può essere un dischetto, un CD o, in ogni caso, un agente di trasporto, come accade quando viene accidentalmente scaricato dal network o ci giunge attraverso un messaggio di posta elettronica. Inoltre, il virus infetta solo il computer e nient'altro, e quindi non possono passare attraverso tastiere, mouse, né possono determinare distruzioni meccaniche.

Ad un passo da una definizione completa

Il primo tentativo di esplorare la possibilità dell'esistenza di entità artificiali capaci di moltiplicarsi può fatto negli anni 50 daVon Neumann, Wiener e altri, ma il termine "computer virus", divenuto poi di accezione comune, fu co-



niato, come abbiamo già visto nella puntata precedente, nel 1984, in occasione della settima conferenza sulla sicurezza informatica tenutasi gli Stati Uniti. Ebbene, nonostante che i virus siano da tempo il fardello più grave nella comunità informatica, non è stata ancora stabilita un'esatta definizione di essi, malgrado numerosi tentativi in proposito.

La principale difficoltà nel tentare di creare un'esatta definizione dipende dal fatto che non esiste una caratteristica unica che li possa individuarne in base a una qualunque delle loro caratteristiche. Infatti quelle ritenute dannose - capacità di incorporarsi in altri oggetti, capacità di riprodursi, capacità di trasferirsi senza controllo - possono essere ritrovate in programmi che non sono virus, o almeno non si comportano come tali.

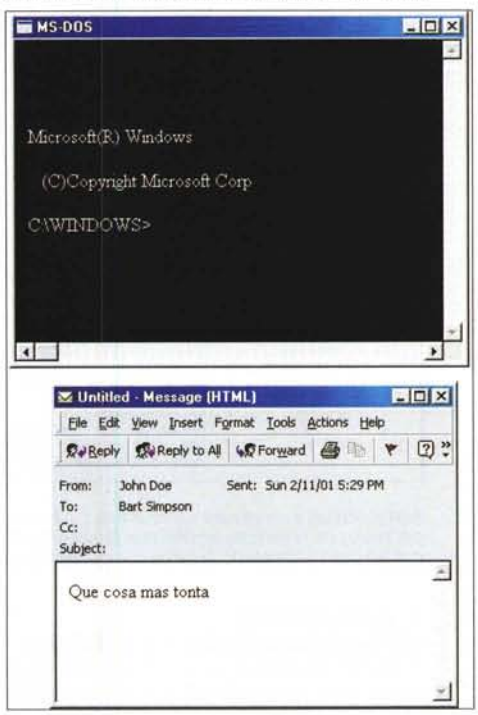
D'altro canto, se consideriamo l'abilità di un programma di distruggere dati su una macchina come caratteristica essenziale del virus, si potrebbero elencare diecine di virus che non producono alcun danno, tranne il fatto di duplicarsi. Ancora, la caratteristica principale del virus, vale a dire la capacità di incorporarsi in oggetti differenti del sistema operativo, può essere ritrovata in molti programmi convenzionali che non sono virus.

Ad esempio, non è certamente un virus l'installer dei normali programmi commerciali, che , però, incorpora nel registro di Windows nuove righe di comando ad ogni installazione. Lo stesso, per esempio, si può dire a proposito dei programmi che modificano il file AUTOEXEC.BAT, e infiniti altri esempi possono essere trovati facilmente durante il lavoro di ogni giorno.

La difficoltà forse più sottile per la definizione di un virus sta nel fatto che la definizione stessa deve essere specifica per il sistema operativo cui si riferisce. Ad esempio, ci possono essere sistemi operativi nei quali lo stesso virus può essere disastroso o senza effetto.

In teoria ancora potrebbe esserci un ipotetico sistema operativo in cui il virus non potrebbe esistere; questo avverrebbe in un ambiente costruito in modo che in esso non possono verificarsi modifica del codice eseguibile. È ovvio che si tratta di una condizione assolutamente ipotetica, visto che in un computer di questo genere non sarebbe neanche possibile costruire dei documenti.

Per giungere, in ogni caso, a una definizione finita potremmo dire che la condizione necessaria perché un virus possa essere considerato tale è la capacità di produrre copie di se stesso, e di incorporarle in un network, in file di sistema o altri oggetti eseguibili, mantenendo la capacità di continuare nella sua opera.



Infine, chi sono i creatori di virus? Ne abbiamo già detto, professionisti, impiegati, programmatori, che conoscono generalmente il linguaggio assembler e che vorrebbero lavorare nel campo della programmazione, ma non riescono a trovare meglio da fare.

Ma si tratta anche di ragazzi, spesso studenti che, non esperti in programmazione, elaborano modifiche di virus classici, o ne producono di loro stessi, contenenti generalmente un grande quantitativo di errori (l'autore delle note cui facciamo riferimento all'inizio li chiama "virus da studente").

Purtroppo la vita di questi produttori è diventata molto più facile da quando sono apparsi in circolazione, e spesso scaricabili gratuitamente, i cosiddetti "virus construction set", che permettono di creare pacchetti virali anche senza la minima conoscenza dei sistemi operativi e del linguaggio assembler. Oltre tutto, nell'ultimo periodo, la vita di questi realizzatori è diventata anche più facile, visto che sono apparsi i macro virus, le macroistruzioni dei programmi evoluti, che non richiedono più neanche la conoscenza del linguaggio assembler.

Esiste infine una terza categoria di produttori, i cosiddetti " professionisti ", che producono "virus professionali ".

Si tratta, in questo caso, di veri e propri capolavori di programmazione, prodotti da gente di talento che spesso hanno concepito algoritmi originali, chiamate non documentate al sistema, e metodi inesplorati per incorporare il loro codice nei punti di obiettivo.

Questi " esperti", in molti casi, utilizzano tecnologie raffinate, e le loro creature sono sovente polimorfiche, infettano non solo i file ma anche i settori di boot, e talvolta intervengono perfino sul BIOS. Alla prossima volta!

MC