VIRUS INFORMATICI: NATURA E RIMEDI

Giorgio MESSI

Si parla spesso di protezione delle informazioni da attacchi ispirati da interessi economici. La minaccia costituita dai virus, essendo il risultato di motivazioni diverse, merita una trattazione a sé stante. Si inizierà con il delineare uno scenario generale per arrivare, in conclusione, a consigliare alcuni metodi di protezione.

1. Introduzione

L'impiego di personal computer per lo svolgimento delle più svariate attività (commerciali, di ricerca, industriali, etc.) si allarga ogni giorno ad un nuovo settore. Questo diffondersi della cultura informatica comporta un flusso continuo di nuovi utenti; come ben ricorda chiunque usi un computer, l'approccio iniziale con la macchina ha aspetti traumatici; domina la paura (dopo i primi inevitabili errori) di perdere i dati, di "toccare il tasto sbagliato". Via via che si apprendono le nozioni basilari questa paura si ridimensiona, salvo riemergere quando si è di fronte a qualcosa che non si conosce.

I virus informatici hanno tutte le caratteristiche necessarie per suscitare timore, anzi direi quasi terrore, in coloro che fanno uso di personal computer.

Viene spontaneo il parallelismo con l'AIDS, come un qualcosa di cui non si sa cos'è, come si diffonde, cosa fa di preciso.

Succede allora che se il monitor video si surriscalda qualcuno pensa possa essere colpa di un virus.

Fino a pochi anni fa se un computer non funzionava le possibilità erano due: o la macchina era guasta, o c'era un errore umano nell'immissione dei dati. Adesso invece viene spontanea in mente una terza possibilità: il virus.

2 La storia

Si può risalire alle origini del termine "virus" in campo informatico: esso fu attribuito per primo nel 1983 da Fred Cohen, ricercatore americano, ad un tipo di software capace di autoriprodursi senza alcun comando da parte dell'utilizzatore.

Nell'agosto dell'anno successivo, alla National Computer Security Conference, Cohen illustrò le proprie intuizioni ed insistette perché fosse aperto un pubblico dibattito sulla materia.

Non tutti i partecipanti alla conferenza erano però d'accordo riguardo questa pubblicità: si temeva la diffusione di idee pericolose. Purtroppo però queste idee erano già nell'aria, e di lì a breve si iniziarono a registrare i primi casi di "infezione" (è un termine che useremo anche in seguito) da virus informatico.

La definizione di Cohen si basava su concetti conosciuti già da tempo, anche se con canoni diversi. Infatti già intorno ai primi anni 70 Victor Vyssotsky, impiegato nei Laboratori Bell, aveva inventato un gioco di nome Darwin, dal nome dello scienziato della teoria dell'evoluzione. Questo gioco simulava l'evoluzione di programmi in un ambiente ostile; vinceva il concorrente capace di continuare a riprodursi sbaragliando i suoi avversari.

Nel 1984 A.K. Dewdney ha introdotto un gioco basato sullo stesso principio con un nuovo nome "CORE WARS" ed esiste tuttora un'associazione internazionale che organizza tornei annuali tra programmi "gladiatori" che si affrontano all'ultimo bit.

Purtroppo la facile adattabilità di queste idee dal campo ludico a quello del normale impiego professionale, assieme alla diffusione di massa del personal computer, hanno portato, in breve tempo, al verificarsi di numerosi casi di crimine informatico. In una società in cui atti di esibizionismo e fenomeni vandalici fanno parte della cronaca di tutti i giorni, i virus altro non sono che l'equivalente in campo informatico.

3 Elementi fondamentali di un virus

Scendiamo per un momento nei dettagli tecnici, per spiegare COS'E' un virus. Per virus si intende, in senso stretto, un programma con due caratteristiche fondamentali: la prima è la capacità di *riprodursi*, ossia di attaccarsi ad un altro programma e propagarsi da esso; la seconda è relativa all'*azione* attraverso cui il virus si manifesta, azione che comporta di solito un danno.

Esistono programmi che difettano di una di queste due proprietà, ma che vengono comunemente definiti virus: programmi che compiono danni senza però sapersi riprodurre (Cavalli di Troia, Catene di lettere, Bombe a tempo), o all'inverso programmi (worms = vermi) che si riproducono soltanto senza compiere alcuna azione dannosa (in effetti poi il danno deriva dalle risorse del sistema progressivamente saturate da questa riproduzione).

Analizziamo ora COSA FA un virus. Va' premesso che data la grande varietà di virus esistenti (diverse centinaia) non tutti compiono esattamente le stesse azioni; è però possibile schematizzare alcune linee di comportamento comuni.

Un virus arriva solitamente attraverso un supporto magnetico: può trattarsi di un dischetto contenente programmi acquistato da terzi, oppure dato in prestito da un nostro amico che non sa di essere già "infetto" : può inoltre essere trasmesso direttamente se il computer fa parte di una rete locale, o si collega ad altri computer attraverso le linee telefoniche mediante un modem.

La prima fondamentale attività di un virus è la stessa di ogni programma al momento di andare in esecuzione: **caricarsi nella RAM.**

Perché ciò avvenga il virus deve essere letto o all'inizio di un programma che lo contiene (che viene normalmente definito infetto) o in particolari zone (BOOT SECTOR) del disco usato per caricare i files di sistema al momento dell'accensione.

Una volta caricato in memoria il virus può restarvi fino allo spegnimento della macchina come un qualsiasi programma TSR[1] oppure restarvi solo fino al compimento delle azioni descritte in seguito.

La seconda caratteristica è la **diffusione**: alcune istruzioni del programma indicano le modalità di duplicazione, che interessano -come già detto- alcune zone fisiche dei supporti magnetici oppure i files eseguibili (COM EXE); in casi più rari anche i file di Overlay (OVL) i SYS (drivers) e particolari tipi di dati (DBF)(DB3)[2].

Non si hanno notizie di files di dati diversi da quelli nominati che siano stati oggetto di "infezione" (ad esempio documenti redatti con un word processor).

Terza caratteristica è la verifica di una **condizione** (di solito controllo della data o contatore incrementato ad ogni utilizzo). Ciò permette al virus di esistere in un sistema, senza manifestarsi, per un certo periodo di tempo, durante il quale ne approfitta per diffondersi.

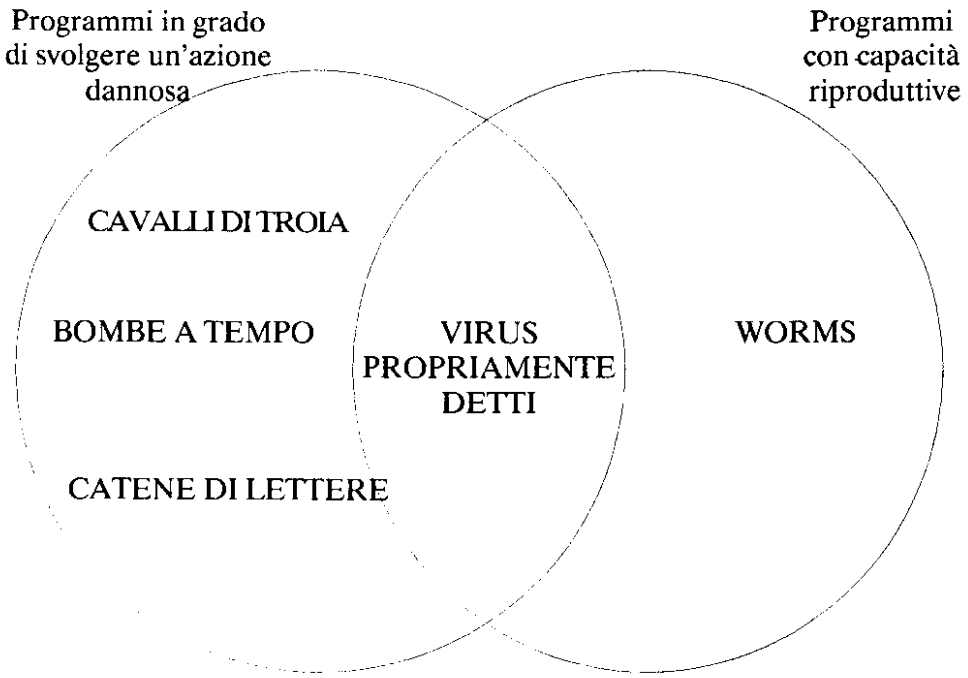
Soddisfatta la condizione di cui si è parlato il virus compie un'**azione**, di solito distruttiva e comunque dannosa: fastidiosi messaggi che vanno e vengono, blocco di programmi durante l'esecuzione, perdita di dati e, in alcuni casi, la cancellazione totale: ciò equivale a dire che il massimo danno di un virus equivale al comando "FORMAT" del DOS.

Finora si è descritto il problema: una volta compreso appieno, è possibile studiarne le soluzioni. Lo schema che segue riassumerà sinteticamente quanto detto :

(1) Sono così definiti i programmi che, una volta eseguiti e terminato il loro impiego, lasciano nella memoria volatile una porzione di sé stessi che non può essere eliminata. Ad esempio: il file di configurazione della tastiera (keybit.com), il Sidekick, etc.

(2) In questo contesto si attribuisce alla voce "dati" il significato più ristretto, cioè il risultato del lavoro di un utente, mentre ove non altrimenti specificato si intenderà per "dati" tutto ciò che è contenuto nell'elaboratore

Classificazione dei programmi "virali"



4 Prevenzione e rimedi

Il primo consiglio non è una novità: effettuare backup dei dati a diversi livelli (su scala mensile; su scala settimanale; su scala giornaliera; naturalmente a seconda dei ritmi di lavoro) ed inoltre non usare, se si lavora su dati di una certa importanza, software non originale o di provenienza sconosciuta.

Un altro metodo di prevenzione, in presenza di ambienti multiutente (reti), può essere l'attenta scelta dei diritti di accesso (di ogni singolo utente) alle risorse comuni. Le reti di comunicazione sono organizzate di solito in maniera gerarchica ed è perciò facoltà del supervisore prevenire "infezioni" più o meno dolose: in un'azienda ad esempio, in cui sia installata una rete di PC, si possono regolamentare i diritti del singolo utilizzatore, impedendogli di usare floppy disk personali che potrebbero contenere virus. Tipicamente ciò avviene non consentendo l'esecuzione di programmi da dischetto, permettendo soltanto la lettura-scrittura di dati[3]. Nelle reti collegate via modem, dove si scambiano quotidianamente programmi di libero dominio, si pone in atto un accorgimento: i programmi che i singoli "scaricano" sull'elaboratore centrale subiscono una quarantena, un periodo in cui vengono testati per verificarne l'"immunità".

Si è già detto che il virus, nelle diverse fasi della sua "vita", modifica in qualche modo i dati contenuti nel computer. Un modo per scoprirlo può essere quindi confrontare, ad intervalli periodici, il contenuto del disco rigido (in particolare i file eseguibili) con copie di riserva effettuate al momento dell'installazione, per questo sicuramente immuni. Tale confronto dovrebbe riguardare sia le dimensioni -e ciò risulta relativamente facile- sia il contenuto dei file, visto che alcuni virus evoluti riescono a conservare immutata la lunghezza dei file da loro infetti. Quest'ultimo tipo di controllo risulta meno agevole; è però possibile, per accelerare entrambi, l'impiego della crittografia. Per chi non conosca il significato di tale termine, si esporranno in breve i chiarimenti necessari alla comprensione di quanto segue, tralasciando una trattazione più completa dell'argomento che esula dagli scopi del presente lavoro.

(3) Per il significato del termine "dati" vedere la nota (2) al paragrafo 3

Crittografia deriva da due termini greci, criptos (nascosto) e grafia (scrittura), significa quindi scrittura segreta, incomprensibile a chi non abbia la chiave per decifrarla. La crittografia nel corso dei secoli ha avuto importanza soprattutto in ambito militare, o come passatempo per una ristretta elite; dalla fine della seconda guerra mondiale ad oggi si è invece sviluppata come una scienza, che cammina di pari passo con la matematica. Agli originali metodi di impiego, che consistevano nel "camuffare" un messaggio per non permetterne la comprensione se non al destinatario, se ne sono aggiunti di nuovi ed è di questi che ci interesseremo.

L'innovazione sta nel poter "marchiare" un messaggio, in modo che non sia possibile a terzi cambiarne un solo bit a nostra insaputa. Operando su di un programma, in questo modo, delle operazioni crittografiche otteniamo come risultato una stringa alfanumerica di controllo. E' assai facile a questo punto memorizzarla per un successivo riscontro .

La prevenzione dai virus si ottiene perciò controllando il più frequentemente possibile (l'ideale sarebbe perdere qualche minuto ad ogni accensione) l'hard disk; in caso di "infezione" viene subito ravvisata la modifica del file (o BOOT SECTOR) ed è possibile limitare al massimo i danni, eliminando la fase di diffusione latente del virus. Esiste già in commercio software che effettua controlli di questo tipo: produce per ogni file, al momento dell'installazione, una chiave di identificazione che viene confrontata, ogni volta, con un valore calcolato in quel momento con uguale procedura.

Anche il tradizionale uso della crittografia può essere d'aiuto nel difendersi dall'attacco di virus. E'necessario però a tale fine conservare i propri dati sotto forma cifrata: quando il virus tenta di "infettare" il programma, cercando di aggiungersi alle istruzioni in esso contenute, non riesce a leggere tali istruzioni e fallisce perciò nel suo intento. Ai vantaggi che un simile sistema di protezione può comportare si contrappongono però degli svantaggi, soprattutto in termini di tempo: per ogni operazione di lettura-scrittura di dati è necessaria infatti la relativa cifratura; procedure di questo tipo risultano perciò proponibili solo in caso si lavori con informazioni di carattere altamente riservato.

La ricerca dei virus può avvenire anche attraverso particolari programmi che ricercano, in ogni file, le istruzioni che contraddistinguono i virus già conosciuti. Tale ricerca non ha naturalmente esito, se il programma non conosce il virus in questione perchè "nuovo di zecca" (per questo vengono rilasciate nuove versioni del programma su scala mensile). Occorre inoltre fare attenzione: sono già due volte che versioni del programma devirus più

diffuso si rivelano "infette".

Al termine di questa trattazione è giunto il momento di parlare dei rimedi: se esistono dei dubbi sulla presenza di virus è opportuno cercare di identificarlo con appositi software (magari non usando l'ultimissima versione appena arrivata da una BBS americana per non correre i rischi di cui si è appena detto), quindi usare un software di rimozione virus per eliminare il problema.

Nella maggioranza dei casi, qualsiasi utente che abbia una discreta conoscenza dell'MS-DOS è in grado, utilizzando tali programmi con le accluse istruzioni, di cavarsela da solo. E' comunque buona norma, se possibile, la creazione di un backup prima dello svolgimento di un tale lavoro, ed è inoltre opportuno rivolgersi a personale specializzato se i dati compromessi sono di valore e l'utente ha scarsa esperienza.

BIBLIOGRAFIA

Estratto da: "La crittografia: aspetti teorici ed applicativi della matematica per il trattamento di dati riservati" Tesi di Laurea, 1991.