

## Breve storia dei Virus

Nel 1948 Jhon Von Neumann dimostra matematicamente la possibilità di costruire una macchina o un programma in grado di replicarsi autonomamente. Nel 1959, il concetto di programma auto-replicante viene per la prima volta implementato in un gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T. Il velo di omertà che ricopre i programmi auto-replicanti venne rimosso nel 1983 da Ken Thompson, autore del sistema operativo UNIX. Nel frattempo (novembre 1983) il primo esempio di virus viene mostrato nel corso di un seminario sulla sicurezza dei computer. La teoria dei programmi auto-replicanti è ormai di dominio pubblico. Nel gennaio del 1986, due fratelli gestori di un computer shop in Lahore (Pakistan) si resero conto che il settore di boot di un floppy disk contiene del codice eseguibile eseguito ogni volta che il computer viene avviato da un dischetto inserito nel drive A. In seguito a ciò i due fratelli scrissero un programma TSR e lo sostituirono al codice normalmente presente nel settore di boot. Il programma è scritto in modo da riprodursi ricopiando se stesso nel settore di boot di ogni floppy disk utilizzato. Nel frattempo un programmatore di nome Ralf Burger sperimentò la possibilità che ha un programma di replicarsi attaccando una sua copia a un altro file e le sue simulazioni suscitarono un interesse tale da convincerlo alla pubblicazione di un libro. Contemporaneamente in diverse parti del mondo la produzione di virus era in continua crescita. A Tel Aviv, Israele (altre fonti dicono in Italia) un programmatore sperimentò e creò uno dopo l'altro Suriv-01 (virus al contrario), Suriv-02, Suriv-03. Il quarto virus di questa serie, conosciuto come Jerusalem, si diffuse rapidamente al di fuori dei confini di Israele. Nell'altro emisfero, in Nuova Zelanda, un giovane programmatore creò un virus che si diffuse molto rapidamente. Il virus denominato Stoned, visualizza sullo schermo il messaggio 'Your PC is Stoned' quando il computer viene avviato da un dischetto infetto. In Italia, all'università di Torino, un programmatore (probabilmente un docente) creò un nuovo virus che si sostituì al settore di boot. Questo virus visualizza sullo schermo una pallina che rimbalza ogni qual volta raggiunge il bordo, se viene effettuato un accesso al disco alla mezzora esatta. Per questo suo effetto a tale virus venne assegnato il nome di virus italiano o Ping Pong virus. Simpatico e per fortuna innoquo!!! Nel 1987, un programmatore tedesco scrisse un virus complesso, Cascade, a causa dell'effetto che provoca sul testo presente sullo schermo. Cascade incorpora una nuova idea: la maggior parte del codice del virus è crittografato. Stoned, Cascade e Jerusalem sono tuttora i tre virus più diffusi nel mondo. Nel 1988 apparvero sul mercato i primi prodotti anti-virus a basso prezzo se non freeware, perché il problema non era ancora così sentito. Nel 1989 sia la produzione dei virus che la ricerca di efficaci prodotti anti-virus vennero guidate dalla Gran Bretagna. Nello stesso anno anche Bulgaria e Unione Sovietica cominciarono a produrre virus. A seguito della comparsa di un nuovo virus, denominato Datacrime, IBM decise di commercializzare un programma anti-virus scritto inizialmente per uso interno. Datacrime, ridenominato Columbus day virus, si dimostra un virus poco pericoloso, tanto da essere praticamente scomparso. Il 1990 segna la comparsa, ad opera di Mark Washburn, di un nuovo virus: l'intero codice è crittografato in modo variabile, la parte del virus che si incarica della de-crittografia può assumere diverse forme, per questo detto virus polimorfico. Sempre nel 1990 si ha in circolazione un gran numero di virus di produzione Bulgara. Il loro produttore, che si identifica come Dark Avenger, introduce i propri virus sui BBS di numerose nazioni, infettando anche i programmi anti-virus shareware. Nel dicembre dello stesso anno vi sono in circolazione circa 150 virus, e la Bulgaria è ormai il leader nella produzione di virus. Nel 1991, il problema diventò commercialmente interessante: nuovi prodotti anti-virus entrano nel mercato. Ma la vera novità del 1991 fu la comparsa di un grande numero di variazioni, ovvero un virus ottenuto modificando alcune istruzioni di un virus già esistente, in modo da renderlo irriconoscibile da parte dei prodotti anti-virus in commercio. Per questo il numero di virus in circolazione aumentò enormemente e i piccoli produttori di anti-virus scomparvero. Nel gennaio del 1992 Dark Avenger rilascia il suo Self Mutation Engine (MtE): un file oggetto (.OBJ) e il codice sorgente di un semplice virus. MtE costituisce un vero e proprio ambiente di sviluppo per virus polimorfi che diviene così accessibile al grande pubblico. Inoltre commercianti senza scrupoli vendono interi CD-ROM pieni di virus già pronti o in formato sorgente. Il resto è storia recente e troppo densa per essere sintetizzata e raccontata.