Attualità

I virus, dieci anni dopo

di Stefano Toria

Nell'ottobre 1990, sul numero 100 di MCmicrocomputer, uscì il mio primo articolo sui virus informatici, che fu seguito da una serie che per qualche tempo tenne l'attenzione dei lettori centrata su quello che all'epoca non si sapeva ancora se trattare come un problema serio, o come l'ennesima leggenda metropolitana.

Avevo cominciato a interessarmi ai virus due anni prima, quando il mio 286 (sembra di stare a parlare del Triassico) si infettò con il "PingPong", uno dei pochissimi virus che circolavano all'epoca. Trovandomi il PC bloccato senza capirne il perché, mi misi a studiare un po', tirai giù un editor di disco e andai a dare un'occhiata al disco fisso, dove scoprii che "qualcosa" aveva modificato il master boot record che aveva un aspetto decisamente diverso da quello che avrebbe dovuto avere. Una rapida scorsa alle conferenze internazionali (già allora seguivo Internet, nonché la Fidonet e un paio di altri gruppi di conferenze) concentrò la mia attenzione su un termine che allora mi sembrò bizzarro: "computer virus". Che idea, che un PC possa prendersi l'influenza o l'epatite come noi umani. E in effetti molti di questi messaggi avevano un tono scanzonato, buffonesco; eravamo tutti piuttosto divertiti all'idea di un PC con la febbre.

Da allora sono successe tante cose. Abbiamo avuto, l'uno dopo l'altro, almeno tre allarmi planetari in stile "fine del mondo", di cui forse quello che tutti ricordano meglio fu quello del virus "Michelangelo" nel febbraio 1992; ci siamo ritrovati con alcune decine di milioni di dischetti infettati dal "Form" in giro per tutto il mondo; poi il problema è finito piano piano nel dimenticatoio, ma tutti hanno continuato a infettarsi freneticamente a vicenda senza rendersene conto; e alla fine tutto si è ridimensionato in quello che già dall'inizio era palese che fosse: una grossa, noiosissima rogna, che chiunque è in grado di affrontare e risolvere brillantemente dotandosi di un programma antivirus e utilizzandolo nel modo corretto. Vediamo un po' meglio come sono andate le cose e qual è la situazione oggi per l'utente di personal computer.

"Ping-Pong" fu per molti utenti di PC, dodici anni fa, il primo incontro con un virus.

Nel 1983 un giovane e brillante "graduate student" di una università statunitense preparava la propria tesi di dottorato. Ci aveva lavorato per un certo tempo, nell'ambito di un progetto per l'automazione della distribuzione degli aggiornamenti del software di base; più di quindici anni fa, infatti, questo era già un problema ben conosciuto ai sistemisti, un problema che faceva sprecare un sacco di tempo e di soldi alle aziende, e che tutti avrebbero voluto vedere risolto in qualche modo.

Frederick Cohen, così si chiamava il giovane dottorando, aveva fatto una serie di brillanti ragionamenti, ed era arrivato alla conclusione che il software, se opportunamente progettato e gestito, avrebbe potuto "aggiornarsi da sé" senza l'intervento dei sistemisti che dovevano mettere i sistemi fuori linea, fare i backup, caricare uno dopo l'altro una serie di nastri (chi se le ricorda più le vecchie "pizze" a 6250 bpi?), rimettere su i sistemi, fare decine di prove, incavolarsi quando qualcosa non andava per il suo verso, eccetera.

Cohen argomentava: solitamente gli aggiornamenti al software di base consistono in una serie di aggiunte, di moduli aggiuntivi e di estensioni di quelli esistenti; tutte cose che possono essere svolte automaticamente da un programma che vada in giro per le reti a "depositare" nei vari computer degli oggetti che poi vengano eseguiti localmente e provvedano alle opportune modifiche. I programmi così aggiornati avrebbero modificato il loro comportamento secondo quanto previsto.

Un modello logico di questo genere era già ben conosciuto alla scienza: la biologia da alcuni decenni aveva compreso il meccanismo di funzionamento dei virus, che sono dei pezzi di materiale genetico (il "software" delle creature viventi) che si introducono nelle sequenze genetiche degli organismi ospiti, modificandone il comportamento. Quindi Cohen chiamò "computer virus" la propria creatura dietro suggerimento del suo docente Len Adleman, già altrimenti famoso per suo conto per aver ideato nel 1977, assieme a Ron Rivest e Adi Shamir, l'algoritmo crittografico RSA.

Pubblicato sulla prestigiosa rivista "Communications of the ACM", l'articolo di Cohen risvegliò l'interesse degli informatici, che ne discussero a lungo su Internet e altrove. Ma per un paio di anni tutto rimase a livello di curiosità

scientifica per addetti ai lavori.

Nelle sue previsioni, Cohen andava oltre, ipotizzando un mondo in cui questi "virus dei computer" sarebbero potuti diventare una minaccia per la sicurezza del patrimonio informativo di aziende, enti e privati. Come si è puntualmente verificato all'inizio del 1986, alla comparsa del primo virus in ambiente MS-DOS.

Cinque anni prima, la IBM aveva presentato il proprio personal computer, che in breve tempo aveva conseguito un successo commerciale enorme; in tutte le città in tutto il mondo erano nati come funghi i computer shop, un tipo di esercizio commerciale sconosciuto fino a pochi anni prima.

Uno di questi computer shop, gestito da due fratelli, fu la culla del primo virus, che fu chiamato "Brain" dal nome del negozio, che compariva all'interno del virus medesimo. Questo virus, di per sé assai poco pericoloso (si replicava soltanto sui dischetti da 5.25", 360 kb), conseguì una serie di primati: fu il primo virus in ambiente MS-DOS; fu il primo a adottare una tecnologia che poi sarebbe stata definita "stealth", per mezzo della quale tentava di nascondersi all'identificazione da parte dell'utente del PC; fu anche il primo, e per quanto se ne sa anche l'unico, a essere sviluppato dal produttore di un antivirus, per consentire la vendita dell'antivirus. Quest'ultima è un'idea dura a morire, che moltissimi utenti tuttora hanno: sicuramente sono i produttori di antivirus a sviluppare i virus, argomentano molti, senza rendersi conto che chi fa antivirus già è sufficientemente impegnato a studiare e contrastare quelli realizzati dagli altri, e non ha certo bisogno di aumentare il proprio carico di lavoro mettendosi anche a scrivere virus in proprio.

Nel caso del "Brain", invece, accadde proprio così: due fratelli, titolari di un negozio di computer a Lahore, Pakistan, scrissero il virus e il relativo antivirus. La creatura sfuggì ben presto di mano al creatore, e "Brain" fece rapidamente il giro del mondo.

Fu seguito, poco dopo, da una rapida successione di nuovi virus: "Cascade", "PingPong", "Jerusalem", "Lehigh". Tutti nomi che hanno ormai un sapore di antico per chi da dieci anni segue l'evoluzione del fenomeno; sono passati certamente diversi anni da quando ho visto l'ultima infezione da "Cascade", tanto per dirne uno.

E in ogni caso il termine "rapida successione" va inteso in senso relativo: passarono settimane, forse mesi tra la comparsa di un virus e il successivo. I primi antivirus venivano aggiornati ogni due-quattro mesi, perché non era necessaria una frequenza maggiore.

Caratteristiche tecniche dei primi virus

Queste primitive "creature" si suddividevano in due grandi categorie: i virus da boot sector, che si trasmettevano servendosi del settore di avvio dei dischetti; e i virus parassiti, che invece si attaccavano ai programmi eseguibili, in formato COM o EXE.

Anche tra i virus da boot sector si poteva, e si può tuttora, stabilire una distinzione, legata a una caratteristica della strutturazione dei dischi fissi. Mentre i dischetti dispongono di un solo boot sector, i dischi fissi ne hanno almeno due: un boot sector principale, o Master Boot Record (MBR), che installa e definisce la gestione del partizionamento del disco; e almeno un Partition Boot Record, che determina l'avvio del sistema operativo installato nella partizione.

Suddividere il disco fisso in più partizioni è un'operazione che ormai non è più necessaria; molti utenti di lunga esperienza ricorderanno come a un certo punto si cominciò a dover "fare a pezzi" il disco C, ottenendo un disco C, un disco D, un disco E, eccetera, per poter gestire sotto MS-DOS i dischi superiori a 33 Mb circa, per via di una limitazione del modello di file system adottato all'epoca. Successivamente la Microsoft allargò il modello di file system, fino alla situazione attuale, in cui il limite è un valore elevatissimo che si suppone possa essere sufficiente per molti anni a venire.

All'epoca tuttavia era prassi comune partizionare il disco; e se quasi tutti gli utenti avevano dimestichezza con l'operazione, che richiedeva l'uso di FDISK, erano pochi quelli che avevano ben compreso tutto il meccanismo, e purtroppo, va detto anche questo, molti tecnici (o sedicenti tali) non erano abbastanza informati sull'argomento.

Fu così che nacque uno degli equivoci più resistenti, più duri a morire di tutta la storia dell'informatica personale. Ignorando l'esistenza di un Master Boot Record, e non riuscendo a comprendere dove potesse essersi annidato un virus, qualcuno se ne uscì con l'idea (DEL TUTTO ERRATA) che per eliminare un virus occorresse formattare "a basso livello" l'hard disk. Sono dieci anni che lo vado ripetendo, e non credo di aver ancora finito di doverlo ripetere: nessun virus, mai, per essere eliminato ha bisogno che venga formattato a basso livello il disco fisso. Probabilmente nessuno sarà mai in grado di determinare quanti miliardi di ore siano state inutilmente perdute, da quando esistono i virus, con inutili formattazioni di dischi.

Una caratteristica non essenziale dei virus, ma presente nella maggior parte di essi, consiste negli "effetti collaterali". Oltre a infettare e trasmettersi, molti virus fanno qualche altra cosa: presentano scritte, fanno suonare musiche o altro nell'altoparlante del PC, oppure vanno a modificare o distruggere i dati: questi ultimi sono senz'altro i più pericolosi.

Virus, antivirus e contorno: nasce il business

La cultura dei virus intanto si diffondeva, più o meno con la diffusione del personal computer. Alla fine degli anni '80 trovare un personal computer in ufficio aveva smesso di essere un'eccezione; anche in molte case ce n'era uno, e il mondo era praticamente pronto per la rivoluzione degli anni '90, con Windows e le interfacce grafiche per tutti (la Apple c'era arrivata parecchi anni prima con il Macintosh, ma la sua posizione di mercato era ed è tuttora assai più debole rispetto a quella dei sistemi Intel-Microsoft).

Accanto a molti computer si cominciavano a veder spuntare i primi modem, all'epoca ancora rigorosamente a 1200 bit per secondo, perché i 2400 sarebbero arrivati un paio di anni dopo. Internet ancora non c'era, o meglio esisteva da vent'anni ma limitatamente al rarefatto mondo accademico.

In questo contesto molti utenti di PC cominciarono a guardarsi intorno, preoccupati da questo problema dei virus di cui sentivano parlare sempre più spesso; e fu così che da semplice fenomeno di attualità i virus informatici diventarono un business. C'erano i prodotti antivirus per aiutare gli utenti a

scovare le infezioni, e c'erano gli esperti che ti "annusavano" il PC fino a stanare le infide creaturine; nacquero riviste, seminari, corsi, libri, tutta una serie di prodotti legati in qualche modo alla lotta contro i virus.

John McAfee fu uno dei primi a legare il proprio nome a un prodotto antivirus. Fu lui a adottare la struttura che attualmente quasi tutti gli antivirus hanno ripreso: un motore di ricerca e un database di identificazione dei virus. Il motore confronta tutti gli oggetti potenzialmente infetti, contenuti nello spazio in esame, con i criteri di identificazione di ciascuno dei virus conosciuti al momento del rilascio del database; se un oggetto soddisfa i criteri, vuol dire che è infetto, e allora si passa alla fase due: la "disinfezione", o rimozione del virus, per ripristinare per quanto possibile le condizioni precedenti all'infezione.

Le variazioni sul tema sono state numerose, ma in ultima analisi tutti i prodotti attualmente sul mercato funzionano in questo modo; tutti, compreso lo stesso "McAfee", che gli utenti continuano a chiamare col nome del suo ideatore sebbene egli sia uscito ormai cinque anni fa dall'azienda, cedendo la sua partecipazione e passando ad altre attività. La McAfee Associates inoltre è recentemente confluita nella Network Associates International, un gruppo di considerevoli dimensioni che produce e distribuisce software di sicurezza per utenti di PC.

E questa è stata soltanto una delle vicende che hanno animato, negli anni, il mercato degli antivirus. Inizialmente questo tipo di prodotti fu realizzato quasi esclusivamente da singoli programmatori o da piccole aziende; per varie ragioni, i virus informatici sono degli oggetti piuttosto fuori dell'ordinario, difficili da studiare nei termini in cui si studia qualsiasi altro pezzo di software. E così nacque la figura del "ricercatore antivirus", un personaggio un po' allucinato, forse il massimo che il mondo dell'informatica abbia saputo esprimere in termini di esperti "verticali".

"Flu Shot+" di Ross Greenberg, "F-PROT" di Fridrik Skulason, "Thunderbyte Antivirus" di Frans Veldman, "AVP" di Eugene Kaspersky sono soltanto alcuni dei nomi del centinaio e passa di prodotti di maggiore o minore pregio, successo e durata che comparvero sul mercato nella prima metà degli anni '90. I loro autori, estremamente popolari nel loro milieu ma assolutamente sconosciuti fuori di esso, ebbero il pregio di realizzare programmi di basso costo, spesso diffusi con la formula dello shareware o del tutto gratuiti, sviluppando sovente idee di grande pregio come ad esempio la ricerca "euristica", introdotta da F-PROT intorno al 1991, che consiste nella capacità di un antivirus di identificare un programma infetto da un virus anche se quel particolare virus non è mai stato analizzato in laboratorio, cioè se si tratta di un virus nuovo.

Poi arrivarono i "grandi": Central Point, Peter Norton, IBM sono solo alcuni dei nomi di prodotti di grande successo commerciale, realizzati da grandi produttori di software che in alcuni casi peraltro non riuscirono ad essere perfettamente all'altezza dell'esigenza, determinando situazioni a volte acutamente imbarazzanti: fu il caso del CPAV, l'antivirus prodotto da Central Point, che fu acquistato dalla Microsoft per essere distribuito unitamente alla versione 6 di MS-DOS. Non starò a ricordare nei dettagli le circostanze, basti ricordare che la stessa Microsoft fece rapidamente macchina indietro, smise di distribuire il prodotto e da quel momento si rifiutò di includere un antivirus nel proprio catalogo.

E così si presentava la situazione fino a un paio di anni fa, quando iniziò la "campagna acquisti". La IBM decise di accordarsi con la Symantec, produttrice del Norton Antivirus; la S&S, che aveva al proprio attivo il "Dr. Solomon's Antivirus ToolKit", un prodotto di grande successo, lo cedette alla NAI. Attualmente sul mercato è rimasta una gamma piuttosto ridotta di prodotti, e in particolare in Italia la scelta si è ristretta a non più di cinque-sei.

"Den Zuko" fu oggetto di una brillante investigazione da parte di Fridrik Skulason, un ricercatore antivirus islandese, che ne riuscì a scovare l'autore in Indonesia

Chi scrive i virus?

A questa domanda hanno cercato di rispondere in tanti. Se ne è parlato ai convegni, se lo chiedono gli esperti, le polizie, l'uomo della strada.

La risposta è semplice: "non si sa". I virus di cui siano stati identificati con certezza gli autori sono pochissimi; forse non si arriva a una dozzina, su quasi ventisettemila virus conosciuti (comprese le varianti).

Tutti gli altri virus sono frutto del lavoro di perfetti sconosciuti. Nella migliore delle ipotesi si riesce a venire a conoscenza di un soprannome dell'autore o del gruppo di persone che hanno realizzato un virus; ad esempio, "Dark Avenger" è un bulgaro estremamente abile come programmatore, che ha sviluppato due o tre tra i virus che hanno dato più filo da torcere ai ricercatori; a un certo punto ha smesso di scrivere virus, ma non è mai stato identificato.

Tutto ciò che si sa degli autori dei virus è un loro profilo psico-caratteriale, dedotto dal loro stile di programmazione. Infatti un programma, come qualsiasi altra opera dell'ingegno umano, riceve l'impronta della personalità di chi

Il virus "Assassin": chiaramente ispirato alla cultura dark molto popolare tra adolescenti e giovani, la fascia di età da cui proviene la quasi totalità degli autori dei virus

lo realizza; e ci sono dei criteri precisi per capire che tipo è l'autore di un programma, proprio come – a titolo di esempio – avviene con la scrittura, nella grafologia.

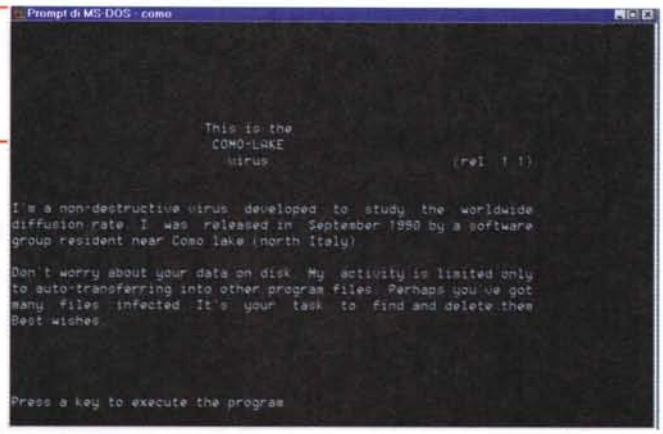
L'autore di virus solitamente è uno studente. Gli studenti, al di là degli impegni di preparazione di esami o interrogazioni, hanno parecchio tempo a disposizione; molto più di un adulto impegnato in una attività professionale, e magari sposato con figli. La fascia di età quindi è quella tra i dieci-dodici e i ventidue-ventisette anni; al di sotto, è difficile che un bambino abbia la preparazione sufficiente a scrivere un virus, e al di sopra solitamente un bravo programmatore riesce in qualche modo a tenersi occupato lavorando, magari part-time in subappalto, ma certamente non ha più tempo da dedicare ai virus

La fascia di età è confermata anche dal tipo di immagini e di testi scelti nel preparare gli effetti collaterali dei virus, che dimostrano interesse per un tipo di cultura tipica dell'età adolescenziale e giovanile, come nelle due illustrazioni qui a fianco. Immagini e testi forti, spesso con legami con la musica heavy metal e la letteratura noir.

Le capacità di programmazione degli autori di virus quasi sempre sono piuttosto scarse. La gente immagina che per scrivere un virus si debba essere dei bravi programmatori; e invece l'analisi dei virus rivela una programmazione sciatta, quasi sempre senza idee brillanti, spesso ottenuta collezionando pezzi qua e là; non è insolito trovare virus che, al di là del replicarsi, non funzionano, oppure che non riescono nemmeno a replicarsi. Inoltre traspare dai virus che i loro autori sovente non hanno una conoscenza approfondita dei sistemi su cui dovranno funzionare le loro creazioni; DOS, Windows, Word sono sistemi complessi, con mille sfaccettature che il programmatore deve conoscere a fondo, e i programmatori dei virus semplicemente non le conoscono.

"Lucifer" è un altro esempio, graficamente più ..."ripulito", di legame tra la cultura dark e i virus

Il virus "Como": l'Italia è uno dei paesi in cui maggiormente ferve l'attività clandestina degli autori di virus



Un'altra domanda a cui si cerca di rispondere nell'analizzare un virus è la sua provenienza. Spesso lo stesso autore la dichiara in un testo contenuto nel virus, ammesso che si possa prestar fede a ciò che dice una persona che nasconde la propria identità. E' il caso del virus "Plovdiv", apparentemente creato nella omonima città bulgara, del "Voronezh" russo e del "Como" italiano. In altri casi si riesce a speculare sulla possibile provenienza del virus risalendo al luogo di originaria infezione, quando ci si riesce; e ad ogni modo, nell'era di Internet e della telematica è perfettamente plausibile che un virus venga scritto, ad esempio, in Canada ma appaia per la prima volta in Nuova Zelanda.

Come ci si difende dai virus

A conclusione di questo articolo la domanda più importante per gli utenti dei PC. Sparita la minaccia della fine del mondo, spuntata la lancia di Michelangelo e anche di Melissa, resta il rischio che tutti gli utenti oggi corrono, di infettarsi con un programma che arriva magari per posta elettronica dal più fidato collaboratore che, a sua volta e a sua insaputa, si è infettato.

La prima norma è anche la più semplice: comprare un antivirus di qualità e mantenerlo aggiornato. Gli antivirus si trovano in tutti i negozi e ormai tutti i prodotti di maggior livello possono essere aggiornati tramite Internet. Non c'è nessuna scusa per non avere un antivirus o per lasciarne scadere il database.

Oltre a comprare un antivirus e tenerlo aggiornato, bisogna ovviamente usarlo. Non è sufficiente installarlo, attivare il monitor residente (che tutti i prodotti di qualità offrono) e dimenticarsene: ad esempio, prima di utilizzare qualsiasi cosa che proviene dalla posta elettronica è fondamentale passarla all'antivirus; anche prima di spedire qualcosa per posta elettronica è bene controllare ciò che si sta per inviare.

Dischetti, CD-ROM, tutto va controllato prima dell'uso. Qualche anno fa stupiva l'idea che un CD-ROM potesse contenere un virus, oggi che i masterizzatori sono largamente diffusi risulta più facile comprendere come un CD in qualche punto della sua vita debba essere riempito con dei file, e che se uno di questi file è infetto, voilà, il virus si trasferisce sul CD.

E poi sono sempre valide le norme fondamentali di "igiene informatica": evitare di prelevare software e documenti da fonti non sicure, non trascurare eventuali stranezze nel comportamento del proprio PC (ma nemmeno correre a gridare "al fuoco" per delle sciocchezze), e soprattutto, fare regolarmente il backup dei propri dati per evitare che il prezioso frutto del proprio lavoro vada perduto.

Stefano Toria si occupa di virus da oltre dieci anni, e da alcuni anni è socio di una azienda che distribuisce in Italia "AntiViral Toolkit Pro" (AVP), un software antivirus, oltre ad altri prodotti di sicurezza informatica. Per questa ragione, e per correttezza nei confronti di prodotti concorrenti, Toria si è astenuto da qualsiasi riferimento, esplicito o implicito, a funzionalità e valutazioni di prodotti antivirus.