▶ Sicurezza

Virus: tutto quello

Cosa sono, chi li produce e perché. E poi, come difendersi? Ecco il primo di una serie di articoli che introdurrà al tema dei codici maligni

di Raffaello De Masi

Solo dieci anni fa, chi di noi si sarebbe seduto davanti al suo PC, e, in caso di malfunzionamento, avrebbe pensato all'attacco di qualche virus? Probabilmente nessuno. Ai tempi d'oggi, invece, anche in caso di rallentamento della macchina, il primo pensiero corre a una possibile infezione.

Otto anni fa ben difficilmente una persona che utilizzava il suo computer in cicli di lavoro ben definiti poteva temere di essere infettato; i soggetti a rischio allora erano gli utenti che montavano o si scambiavano tra di loro software pirata, passandoselo su dischetti che, a quel tempo, rappresentavano il più importante veicolo di infezione. Oggi, le cose sono profondamente cambiate.

Consistenza numerica del malware

1995	2476
1996	4800
1997	4985
1998	5680
1999	33830
2000	36978
2001	66984

Il numero dei virus *propagatisi a partire dal 1995. È evidente come la diffusione di Internet sia stata fondamentale*

L'utilizzo di Internet e della posta elettronica

L'uso esplosivo della posta elettronica e degli altri servizi Internet ha creato un ambiente di sviluppo di propagazione ideale per i virus; ciò che prima richiedeva una vera e propria operazione manuale (scambio di floppy), con conseguenti tempi lunghi di trasmissione e intrinseche difficoltà di contagio, legate al mezzo fisico, oggi si è trasformato in un'operazione "in tempo reale".

Un virus particolarmente "cattivo" può fare il giro del mondo in poche ore, provocando tanti problemi al suo passaggio, probabilmente anche prima che qualcuno delle vittime si sia accorto di aver subito tali e tanti danni.

Pertanto, la parola d'ordine, è difendersi al meglio.

Molte persone immaginano un'infezione da virus come un'invasione di una macchina da parte di un programma non desiderato.

Perfino la stampa più o meno specializzata tende a far coincidere questo fenomeno con la parola "virus", generalizzando molto il problema. Tecnicamente, invece, il termine virus si riferisce solo ad una della dozzina di categorie di programmi che, in maniera più generale, possono essere definiti *codici maligni*.

Col nome di *malicious code* (altrimenti chiamato *malware*, *pestware*, *vandalware*, *punkware* o altro) viene genericamente definito un qualsiasi programma specificatamente creato per essere ospitato, per così dire senza essere invitato, su un computer ed esercitare operazioni diverse sul suo contenuto. Sotto questa forma, la definizione comprende non solo i virus ma anche una serie di programmi comunque distruttivi o dannosi, tra cui ricorderemo i *cavalli di Troia* e i *worm*.

Ma chi produce questi programmi? Rimandiamo ad un approfondimento sul tema nella pagine che seguono.

Diremo qui solamente che i produttori di codice maligno coprono un'ampia casistica di personaggi, dai cracker, le cui intenzioni possono variare dal semplice divertimento fino al guadagno di accesso su informazioni riservate e importanti, a semplici ragazzi o adulti che creano pacchetti di questo tipo per invadere intenzionalmente computer altrui, o hanno una conoscenza abbastanza buona delle tecniche di programmazione per modificare un virus già esistente o per scaricarne uno da qualche sito disponibile in rete.

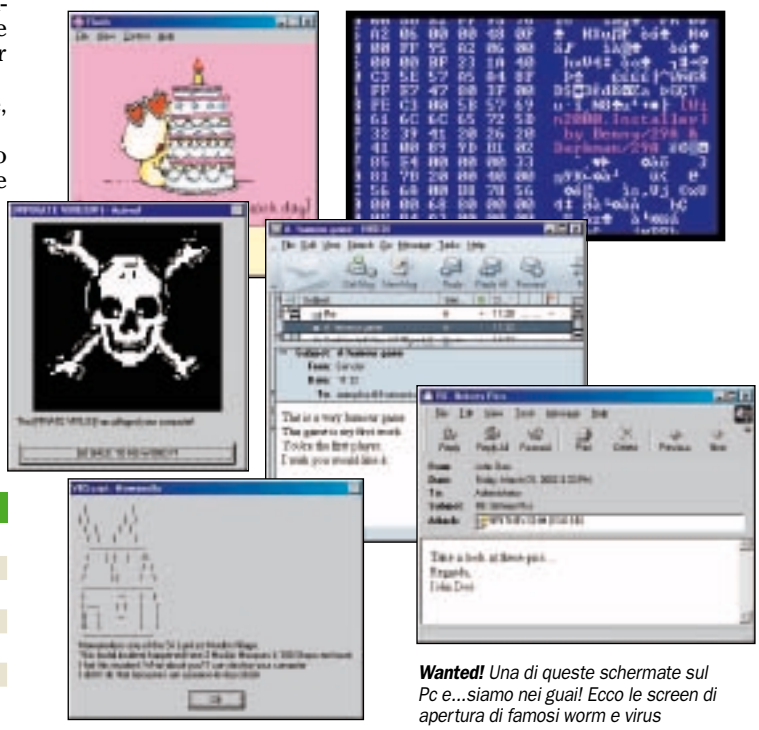
A questo proposito, è possibile trovare di tutto, a ben cercare, dal codice già pronto a programmi capaci di generare, autonomamente, virus (è a una procedura di questo genere che è dovuta la nascita dell'infame virus Anna Kournikova, creato nel febbraio dell'anno passato e divenuto in breve tempo tristemente famoso).

Il codice così realizzato è inquadrato in una delle categorie di cui parlavamo in base al modo in cui agisce e si propaga da macchina a macchina.

Tipi più diffusi di codice

	1995	1996	1997	1998	1999	2000	2001
file	7,5	5	4	9	8	6	2
boot	78	62	40	27	4	14	7
macro	6	24	51	61	76	56	19,5
multifunzione	8,5	9	5	3	1	2	1,5
network worm					11	22	70

L'evoluzione dei tipi di virus *in percentuale dal 1995 al 2001*



Wanted! *Una di queste schermate sul Pc e...siamo nei guai! Ecco le screen di apertura di famosi worm e virus*

Semplificando il problema, è possibile suddividere un attacco in tre categorie, da virus, da worm o da cavallo di Troia. Questa definizione, rimasta valida per molti anni, sta perdendo ultimamente parte del suo significato, in quanto l'evoluzione dei codici ha portato alla creazione di nuovi programmi più complessi, che spesso coprono le modalità di azione dell'uno e dell'altro insieme, generando ancora maggiore confusione sul metodo di classifica e, per numerosi versi, anche sulle tecniche di difesa.

Che cosa è un virus?

A voler mettere insieme una definizione propria, un virus è un programma capace di infettare un PC all'insaputa del proprietario, e da qui, adatto a replicarsi e infettare altre macchine.

Buona parte dei virus include anche un *payload*, vale a dire il "carico" trasportato dal virus e rappresentato da differenti azioni fastidiose o distruttive che si aggiungono all'operazione di replica.

Esistono tre tipi principali di virus, anche se poi, da questi, le successive combinazioni ed evoluzioni permettono di ampliare notevolmente la famiglia delle tipologie.

Sono i *boot sector virus*, i file *virus* e i *macro virus*. Vediamoli da vicino.

Boot sector virus

Si tratta del tipo più datato di virus, che infetta i settori di *boot* di un floppy o di un disco rigido.

Per *boot sector* si intende quella sezione, localizzato su un'unità di massa, che contiene un codice-programma eseguito automaticamente ogni volta che il computer parte o il dischetto viene inserito.

Quando un boot sector è infetto, il virus viene lanciato automaticamente con i programmi di utilizzo comune del sistema, viene caricato in memoria e replica se stesso infettando ogni dischetto successivamente inserito nel drive.

Se lo stesso dischetto viene utilizzato su un'altra macchina (spesso non è neppure necessario lanciare un file) il nuovo computer diviene vittima e riprende la stessa operazione.

Il virus Brain, come già abbiamo accennato, fu il primo boot sector virus della storia, dedicato al mondo MS-DOS, seguito nell'87 da Stoned, e nel 1991 da Michelangelo (che si attivava il 6 marzo di ogni anno, anniversario della nascita dell'artista, e sovrascriveva il disco rigido con caratteri casuali).

File virus

Vengono talora chiamati anche *virus parassiti*. Essi infettano o sostituiscono file con l'estensione *.EXE* o *.COM*. Al momento del lancio dell'eseguibile il virus si replica e si inserisce in altri eseguibili, determinando poi anche alcuni effetti di payload.

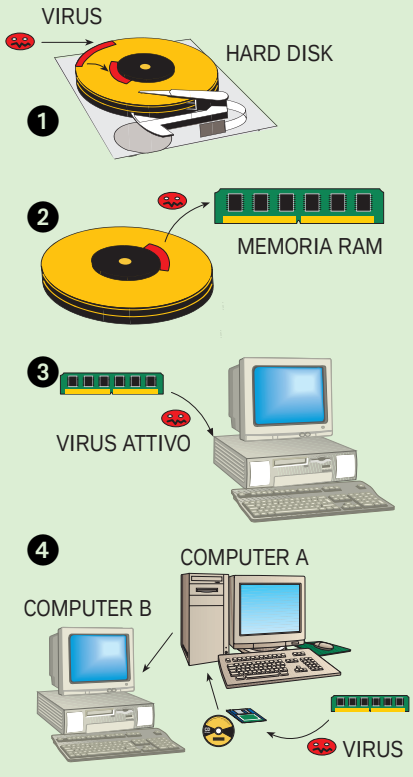
Un classico esempio di file virus è stato Chernobyl (anche noto con la sigla W95/CIH); scoperto nel 1998, segue il tipico scenario di un file virus, in- ▷

Che cosa può fare un virus e da dove arriva

Ecco un elenco dei più comuni effetti *(payload)* provocati dai virus per computer:
Visualizzazione di messaggi offensivi o allarmanti
Azioni a sorpresa senza conseguenze (come suonare un motivetto)
Impedire l'accesso a file o dati nel computer (ad esempio proteggendoli con una password che l'utente non conosce)
Rubare dati
Cancellare dati
Disabilitare il funzionamento di alcune componenti hardware

Le fonti da cui è possibile contrarre l'infezione sono:
Internet, scaricando documenti o programmi
Programmi infetti che installiamo sul computer dopo averli ricevuti da altri
Documenti e fogli elettronici infetti che ci arrivano da altri
Allegati di posta elettronica
Floppy disk e CD infetti all'origine

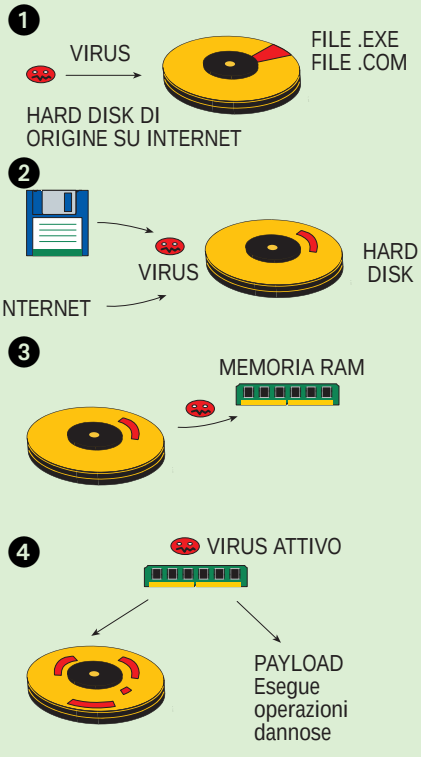
BOOT SECTOR VIRUS



Come avviene l'infezione:
si avvia un computer da un dischetto o CD di sistema operativo infetto
1. Il virus infetta l'hard disk generando un nuovo settore di boot e copiando quello originale in altra porzione del disco
2. Alla partenza del computer il virus si copia in memoria assieme al sistema operativo
3. Esegue operazioni contenute nel "payload" danneggiando il computer in varie forme
4. Quando s'inserisce un floppy nel computer il boot sector virus lo infetta così da propagarsi su altri computer

L'efficacia dei boot sector virus è strettamente legata al sistema operativo per cui è stato creato, non può quindi propagarsi tra macchine dotate di sistemi operativi diversi.
L'unico modo per contrarre l'infezione è avviare la macchina da un disco (floppy e CD) infetto.
È il tipo più vecchio di virus che esista, molto popolare ai tempi del DOS ha perso efficacia col diffondersi di Windows 95 e successivi.
Un vecchio boot virus per DOS comunque blocca l'avvio di una macchina Windows

FILE VIRUS



Come avviene l'infezione:
si riceve da Internet o da disco un file di programma infetto e si esegue il programma sulla propria macchina

1. Il virus si aggiunge al file che contiene il programma

2. Il programma viene installato nell'hard disk dell'utente

3. Quando l'utente attiva il programma il virus parte per primo e si mette al lavoro

4. Infetta altri file di programma sul disco – esegue operazioni dannose

La propagazione dell'infezione dipende dallo scambio e dall'uso di programmi infetti

fettando e propagandosi ad altri eseguibili, ma presenta una caratteristica originale che lo rende interessante.

Programmato per scattare il 26 di ogni mese (giorno del famoso disastro nucleare) il virus sovrascrive il primo megabyte del disco rigido e, subito dopo il BIOS (*Basic Input/Output System*), rendendo il computer praticamente inutilizzabile e imponendo, nella maggior parte dei casi, operazioni di riparazione piuttosto costose.

Macro virus

Una macro è un gruppo di istruzioni che automatizza alcune routine all'interno di un'applicazione. Le macro sono componenti comuni in file, *template*, modelli usati da Microsoft Word ed Excel, ed è proprio a questi popolari programmi che sono mirati la maggior parte degli attacchi di questo tipo di agenti patogeni.

Essenzialmente un macro virus non è altro che una macro contenente un set di istruzioni malicious. È creato utilizzando un linguaggio di programmazione, come Microsoft VBA, abbinato a un documento o un modello. Quando la macro si attiva ed esegue il compito per cui è stata realizzata, infetta gli elementi essenziali del sistema operativo e del programma. In questo modo si crea un ambiente di sviluppo per le successive operazioni di infezione su altre macchine (ad esempio, in Microsoft Word, l'attacco iniziale del virus è diretto al file template *Normal.dot*).

I worm, l'evoluzione della specie

Agli inizi del 1999 un documento Word 97 fu messo a disposizione, come attachment di messaggio, su un NewsGroup Usenet. Coloro che scaricarono e aprirono questo attachment ebbero una sgradevole sorpresa e conquistarono il triste primato: essere stati infettati da un nuovo tipo di virus ibrido che, in tre giorni, si sarebbe propagato su più di 100.000 computer.

Da allora, centinaia di variazioni sul tema di Melissa, questo il nome del neonato, sono state segnalate in tutto il mondo. Melissa è il primo esempio di un nuovo tipo di agente patogeno che, oltre a comportarsi come macro virus, apre la rubrica di Outlook e rispedisce se stesso agli indirizzi che trova memorizzati.

Un worm è un programma *self-contained* che combina insieme un payload, una tecnica di replicazione, una routine di distribuzione, ma non infetta altri file. I worm si propagano ad altre macchine attraverso connessioni di un network, attraverso posta elettronica, IRC (Internet Relay Chat), FTP e più in generale attraverso la Rete. Molti worm si possono attivare senza alcun intervento da parte di un utente.

Anche qui, come con i virus, ci sono differenti tipologie di worm, anche se, in questo campo, la distinzione fra i vari tipi non è sempre chiara e netta. Eccoli.

Script worm

Si tratta di worm creati utilizzando un linguaggio di script come VBSScript (*Visual Basic Script*).

Probabilmente il primo worm di questo tipo è stato BubbleBoy, comparso nel 1999 e immediatamente seguito da esemplari molto più devastanti, come VBS/LoveLetter (detto anche ILoveYou) e Anna Kour-

Da dove nascono i virus? Un po' di storia

La storia dei virus coincide, se vogliamo, con la nascita dei computer. Già nel 1949, in una pubblicazione dell'istituto di calcolo dell'Università di Indianapolis, in Indiana, John von Neumann, pioniere della tecnologia e padre universalmente riconosciuto del calcolo automatico, ipotizzava (e ne dava una dimostrazione puramente analitica) l'idea di un programma per computer capace di autoriprodursi.
La cosa non rimase solo un'intenzione in quanto, nel 1960, lo stesso von Neumann presentò un gioco, Core Wars, in cui alcuni piccoli programmi, fortemente aggressivi, tentavano di attaccarsi l'un l'altro su una macchina, distruggendosi a vicenda.
Il primo vero virus, però, risale a circa 21 anni fa, attraverso una di quelle storie che deliziano i lettori americani nate da avvenimenti realmente accaduti e condite da particolari destinati a rendere più aneddotistico l'effettivo accaduto.
Dicevamo, nel 1981, un gruppo di ragazzi di un istituto superiore a Pittsburgh scoprì, accendendo i computer (per la cronaca degli Apple II) una schermata che recitava:

"It will get on all your disks
It will infiltrate your chips
Yes, it's Cloner!

It will stick to you like glue,
It will modify ram too
Send in the Cloner"

Ovviamente, il programma era ben lungi dalla pericolosità degli attuali virus; non produceva praticamente alcun irreparabile effetto, sebbene avesse qualche piccolo risultato distruttivo. Si scoprì, dopo qualche giorno, essere stato realizzato da Rich Skrenta, un ragazzo di quattordici anni che, con molto tempo a disposizione, si dedicava alla copiatura di giochi piratati, e, per puro diletto, inseriva nei dischetti da lui stesso distribuiti piccoli programmi, come appunto *Elk Cloner*, che per varie strade erano stati poi trasferiti ai computer del laboratorio della scuola.
Skrenta, divenuto poi fondatore di una società prestigiosa come Open Directory, e attualmente programmatore capo in America Online, ammette, in un'intervista di qualche anno fa, di non aver mai avuto alcuno scrupolo morale nell'aver realizzato quei programmi.
Aggiunge anche di non aver mai usato la parola virus per descrivere i suoi prodotti; ciò nonostante, continuando a distribuire i suoi dischetti su aree piuttosto ampie, determinò la distribuzione dei suoi prodotti, sui computer Apple, in maniera diffusa e capillare fin oltre il 1990 (occorre considerare che, a quei tempi, non esisteva affatto una cultura antivirus, per cui la diffusione, in un ambiente del tutto indifeso, di Cloner e derivati fu paragonato, poi, all'effetto della varicella sulle popolazioni Inca e Azteche).
Il primo vero programma antivirus per PC apparve poco dopo la comparsa di Cloner.
Il fatto ha un che di curioso, considerando che fu realizzato da uno studente della A&M University del Texas, Joe Dellinger, che sviluppò un virus, sempre per macchine Apple II; egli stesso, essendo dotato, probabilmente, di senso morale più sviluppato rispetto a Skrenta, forniva contemporaneamente un programma capace di neutralizzare l'azione, un vero e proprio antivirus ante litteram, mettendo poi a disposizione di tutti i sorgenti dell'uno e dell'altro.
Proseguendo in questa avventurosa storia, il primo vero virus per PC, Brain, vide la luce nel 1986, e fu immediatamente seguito da alcune centinaia di nuovi nati.
Fortunatamente, fino al 1995, i virus erano praticamente condizionati da una importantissima limitazione; la velocità con la quale si potevano propagare.
Poiché, all'epoca, il mezzo di diffusione più comune erano i floppy, le infezioni potevano ancora contarsi a migliaia piuttosto che a milioni. Ma mancava poco a che l'allarme diventasse generale!
Un incidente, nel 1988, aveva già messo in guardia sul potenziale potere distruttivo rappresentato dalla miscela esplosiva di Internet e virus.
Uno studente della Cornell University, Robert Morris jr, figlio, guarda caso, di uno dei programmatori di Core Wars, scrisse un worm, un minuscolo programma capace di riprodursi e distribuirsi attraverso la rete Usenet in maniera invisibile, rete che già all'epoca contava circa 60.000 computer.
Lo studente aveva creato il codice dotandolo di una routine che doveva limitare la sua propagazione, legandola alla coincidenza di una serie di parametri (accensione della macchina in uno specifico giorno della settimana e del mese).
Sfortunatamente, un bug determinò il malfunzionamento di questo trigger; il virus sfuggì definitivamente a qualsiasi controllo, infettando un decimo almeno delle macchine allora collegate in rete (facendo un debito rapporto, e basandosi sulle ultime stime riportate nell'Internet Domains Survey

nikova. Nella maggior parte dei casi gli effetti dannosi riportati riguardano la sovrascrittura di file con estensioni, come .JPG, .VBS, .MP3 e così via.

Molto spesso questo tipo di worm incorpora un payload aggiuntivo, che viene eseguito prima dell'apertura della rubrica di posta di Outlook o Outlook Express attraverso cui il messaggio, con il relativo allegato, viene poi ridistribuito agli altri componenti della lista.

Internet worm

Noto anche con il nome di network, loner, hacker o mass-mail worm, si propaga attraverso la posta elettronica ma ha l'abilità di auto attivarsi e di propagarsi attraverso bug del sistema operativo del network o attraverso buchi nella sicurezza di Internet.

Il lato pericoloso della cosa è che la propagazione avviene in maniera assolutamente subdola e non richiede processi di attivazione da parte di alcuno. Nel 2001, i worm Internet hanno rappresentato il tipo più frequente di infezione e l'esemplare più diffuso di codice maligno.

Secondo i laboratori Kaspersky, gli Internet Worm, fin dal 1995, hanno sempre avuto loro rappresentanti in testa alla classifica dei primi dieci agenti pericolosi.

I cavalli di Troia

Il terzo degno rappresentante di cotanta famiglia sono i *cavalli di Troia*. Come i corrispondenti esemplari in legno, un *Trojan* è un programma che nasconde intenzionalmente la sua natura distruttiva, pretendendo di essere qualcos'altro, ad esempio un gioco o una utility. Al contrario dei virus, esso non si copia su un altro file ▷

pubblicato da Network Wizard, è come se oggi rimanessero infettati almeno 50 milioni di PC nel mondo).

Poiché l'utilizzazione commerciale di Internet era ancora di là da venire (i primi timidi tentativi furono fatti un paio d'anni dopo) Morris non subì un grave danno da questa sua azione; l'università gli inflisse una censura verbale insieme all'interdizione dell'uso della rete per un mese.

Oggi Morris è docente al MIT. Col passare del tempo, purtroppo, molte cose sono accadute.

La maggior parte dei personal computer utilizza Windows e Microsoft Office, cosa che crea, per i virus, una diffusa e omogenea piattaforma di sviluppo e riproduzione (è praticamente impossibile, per una buona parte dei virus, trasmettersi tra sistemi operativi diversi, ad esempio tra Windows e MacOS o Linux, questo anche per il fatto che molti virus operano direttamente sui file di sistema operativo che, ovviamente, sono differenti).

Per giunta, alla propagazione contribuisce in maniera devastante, la presenza della posta elettronica. In un'intervista rilasciata gli inizi dell'anno, Steve Gottwals, responsabile marketing di Sigaba, società specializzata nella sicurezza della posta elettronica, definisce l'e-mail come "the true killer application of the Internet"; l'esplosiva diffusione di questa tecnologia ha infatti determinato un salto in avanti nella velocità di propagazione di codice maligno, la cui diffusione è oggi inarrestabile.

Il 26 marzo del 1999, in un solo giorno, il virus Melissa si riprodusse tramite Outlook in maniera talmente impressionante, da poter essere paragonato, come azione, in un solo giorno, all'effetto di qualunque altro virus durante la sua intera esistenza.

Mike Trillings, di Symantec Corporation ebbe a dire, in quell'occasione, che Melissa rappresentava, davvero, un punto di svolta nella storia dei PC.

Dal 1996 al 2001, la percentuale di virus propagatisi via posta elettronica è passata dal 9% a oltre l'80%, secondo quanto riferisce TrueSecure, mentre i metodi di trasmissione attraverso floppy che, cinque anni fa, rappresentavano il 75% di tutte le infezioni, passano, all'inizio di quest'anno, a meno dello 0,5%.

E che le acque non si siano certamente quietate è dimostrato dalla comparsa successiva, sul mercato, di codici come LoveLetter, NewLove, Anna Kournikova, la cui capacità di propagazione non ha niente da invidiare al capostipite.

Roger Thompson, direttore tecnico e capo della ricerca della stessa TrueSecure, afferma che ormai siamo entrati nella quarta generazione dei virus.

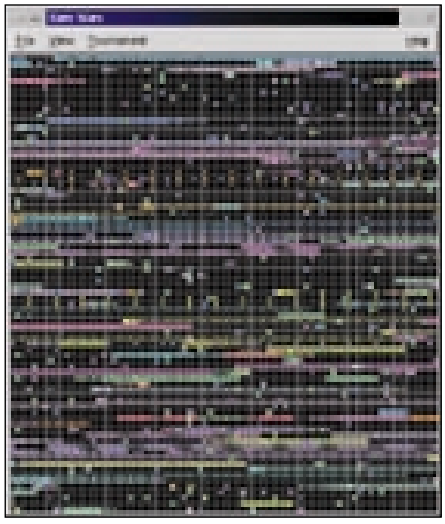
La prima può essere localizzata negli anni tra l'87 il '95, ed era caratterizzata da virus che infettavano applicazioni e settori di boot di dischetti e dischi rigidi; la seconda fase, che va dal '95 al '98, è stata l'epoca dei virus macro e script, come Melissa e Love Bug, che usavano semplici linguaggi di programmazione realizzati da Microsoft per aiutare gli utenti a manipolare pacchetti come Windows ed Office.

La terza generazione ha dato alla luce prodotti ancora più complessi, il cui esemplare più rappresentativo è certamente SirCam, capace di funzionare come uno script ma disegnato in un linguaggio di programmazione avanzato, e per questo più robusto, flessibile, e capace di sfuggire alle tecniche di intercettazione.

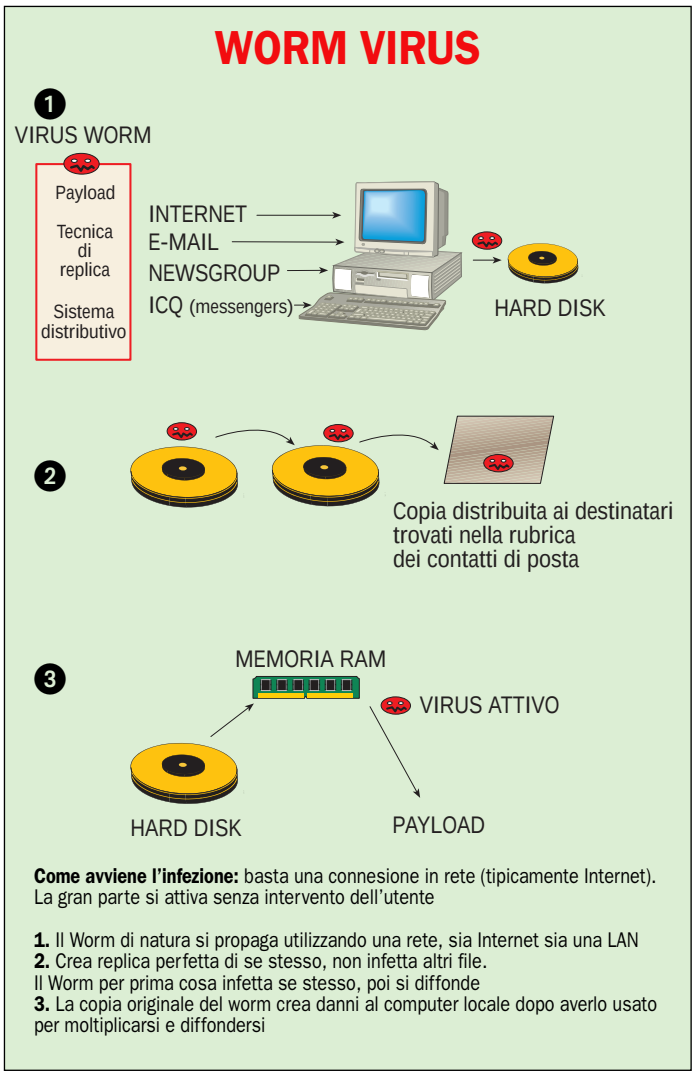
Thompson riferisce che la nuova frontiera dei virus sarà, domani, quella rappresentata da forme di attacco multiple, localizzate ai buchi di sicurezza dei sistemi operativi e dei pacchetti.

"Finora", egli afferma, "il mondo degli hacker si è sempre mantenuto separato da quello degli realizzatori di virus, mentre oggi la cooperazione sta diventando sempre più stretta".

Ad esempio Nimda riesce a trarre vantaggio da un bug di Internet Explorer per autolanciarsi all'interno di un messaggio di posta elettronica, anche se l'utente non apre l'attachment. In altre parole, il futuro ci riserva una terribile battaglia tra gli implementatori di virus e i produttori di antivirus. Con noi nel mezzo...

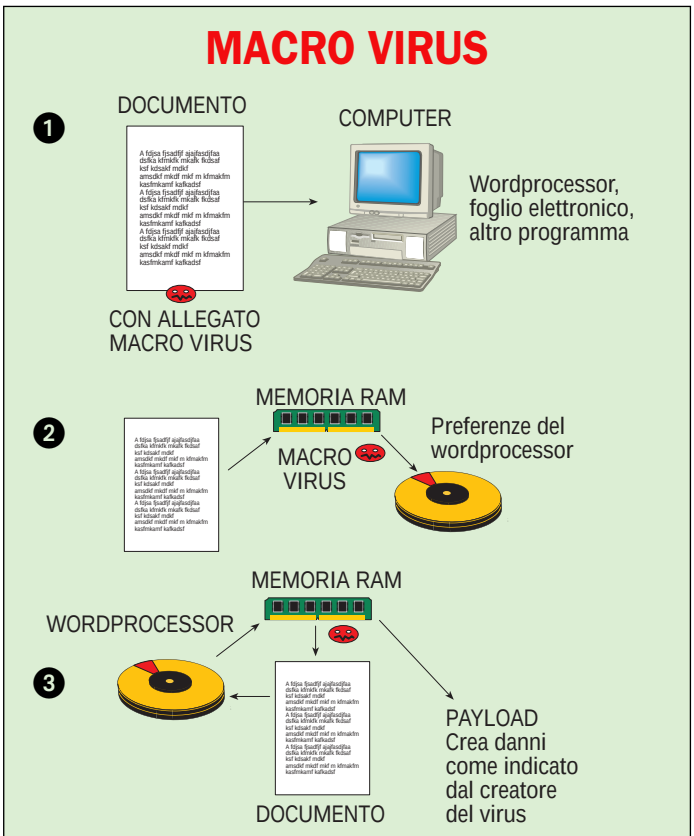


Core Wars, il padre di tutti i virus *era un gioco in cui alcuni piccoli programmi tentavano di attaccarsi l'un l'altro distruggendosi a vicenda. Oggi è ancora giocabile o scaricabile all'indirizzo www.corwars.sourceforge.net*



Come avviene l'infezione: basta una connesione in rete (tipicamente Internet). La gran parte si attiva senza intervento dell'utente

1. Il Worm di natura si propaga utilizzando una rete, sia Internet sia una LAN
2. Crea replica perfetta di se stesso, non infetta altri file.
Il Worm per prima cosa infetta se stesso, poi si diffonde
3. La copia originale del worm crea danni al computer locale dopo averlo usato per moltiplicarsi e diffondersi



Come avviene l'infezione: si apre un documento infetto (solitamente un allegato di posta elettronica
1. Il virus arriva allegato a un normale documento
2. Il documento viene caricato in memoria e la macro si mette in azione copiando il virus nel disco dove sono contenuti i file di preferenza dell'applicazione che ha aperto il documento
3. Ogni successiva volta che il word processor viene avviato, il virus entra in azione e infetta tutti i documenti che l'utente crea poi si trasferisce ad altri, infettando così anche questi ultimi

eseguibile o su un'area di boot, e non ha un suo proprio meccanismo di replica.

Se ne conoscono, essenzialmente, di due tipi.

I backdoor

Il backdoor è un agente che modifica connessioni Internet e/o di un network aggiungendo un servizio nascosto che permette a un cracker remoto di scaricare codice sulla macchina vittima.

Uno degli esemplari più noti di questo genere di pacchetti è tHing Trojan, che si installa sotto forma di file NETLOG1.EXE e modifica i file di sistema in modo che, ogni volta che viene lanciata la macchina, lo stesso trojan possa lanciarsi.

In questo caso, il backdoor invia un messaggio ICQ (*I Seek You*, programma di instant-messaging) al cracker remoto, e apre un gateway che permette al cracker di esplorare la macchina vittima.

Remote Administration Trojans (RAT)

RAT (*Remote Administration Trojans*): si tratta di programmi che, oltre a funzionare come i precedenti, consentono un controllo completo della macchina remota da parte del cracker, che, praticamente, può eseguire sul PC vittima tutto quel che desidera.

Ad esempio, SubSeven avvisa il cracker remoto attraverso un messaggio di IRC (*Internet Relay Chat*), e gli mette a disposizione il completo accesso a più di un centinaio di opzioni riservate all'amministratore del sistema.

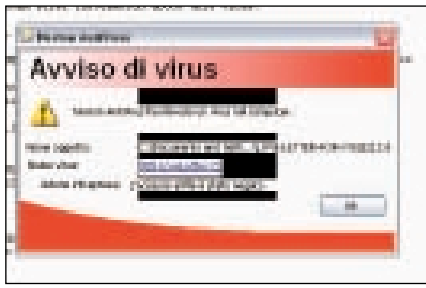
In molti casi, con una tecnica ancora più raffinata, un cracker può utilizzare una macchina vittima per controllare attraverso di essa altre macchine, catturando password, dati personali e sensibili, e/o iniziando un attacco DoS (*Denial of Service*). Sebbene non così diffusi come in virus e worm, alcuni cavalli di Troia, come BackOrifice e SubSeven riappaiono periodicamente sulla rete, sfruttando alcuni canali preferenziali di trasferimento file, come Grokster e Limewire, programmi per condividere i propri file con altri utenti.

Infine, non possiamo completare la trattazione di questo argomento senza parlare degli *hoax*.

Curioso fenomeno ampiamente diffuso, un hoax non è altro che un messaggio di posta elettronica, non nocivo, contenente una richiesta di aiuto, un avviso della scoperta di un virus che nessuno riesce a fermare, la richiesta di inviare a grandi organizzazioni copie del testo contenuto nel messaggio, a fronte di un improbabile contributo da parte di queste per un'opera umanitaria o per un sostegno alla ricerca scientifica.

Talvolta il processo si spinge oltre, consigliando il ricevente di rimuovere dal sistema file poco noti, dichiarati come virus, e che invece assolvono a determinate funzioni del sistema stesso.

Gli hoax sono facilmente riconoscibili in quanto pretendono di utilizzare un linguaggio tecnico di alto livello o dichiarano di distribuire informazioni ricevute direttamente da grosse organizzazioni, come Microsoft, Symantec, Oracle, e via dicendo.



Outlook è la porta principale *di infezioni da virs del tipo worm. Ecco qua ILoveYou, alias VBS/Loveletter in azione!*

Ovviamente nessuna organizzazione di questo tipo si sognerebbe mai di utilizzare un canale di questo genere per distribuire le sue notizie.

In altri termini, si tratta di un fenomeno più fastidioso che nocivo, ma se si considera che anche la più semplice operazione di inoltro richiede qualche secondo, è facile mettere insieme migliaia e migliaia di ore lavorative per una stupidaggine di questo tipo.

Cosa ci riserva il futuro?

Secondo Denis Zenkin, dei laboratori Kaspersky, il numero delle presenze di codice maligno sulla Rete è raddoppiato tra il 2000 e il 2001; l'incremento è stato essenzialmente causato dalla fioritura di worm, grazie alla facile programmabilità e alla presenza di codice ampiamente disponibile sulla Rete. Circa il 60% delle infezioni è dovuto ad agenti di questo tipo, mentre i boot sector virus , che rappresentavano 80% dal 1995, sono scesi a meno dell'8% nel 2001. Vincent Weafer, di Symantec Corporation, prevede per i prossimi due anni l'incremento di virus capaci di utilizzare contemporaneamente diverse strade di infezione. Probabilmente, la migliore previsione l'ha fatta proprio Weafer, ipotizzando un sempre maggior passaggio da virus distruttivi a virus capaci di prelevare, sottrarre, esportare dati sfruttando vulnerabilità e buchi della sicurezza. La frontiera si amplia ancora di più considerando che in tempi recentissimi, un nuovo esemplare di codice ancora più sofisticato ha fatto la sua comparsa sul mercato; si tratta di codici nascosti in file che finora erano considerati esenti dalla possibilità di attacco. Ad esempio, un Internet Worm, chiamato Peach, e scritto in VBS, è capace di attaccarsi a file di tipo PDF. Curiosamente, al lancio del file, il worm invita l'utente a partecipare a un gioco, mascherando, nel frattempo, la sua azione distruttiva e di propagazione attraverso la rubrica degli indirizzi di Outlook.

Allo stesso modo, un codice chiamato SWScript.LFM attacca i file Shockwave, anch'essi finora ritenuti immuni; il virus non provoca alcun danno, ma mostra una nuova strada di attacco che certamente non rimarrà deserta. In conclusione, che fare? Ripetendo un luogo comune, prevenire è meglio che curare. L'unico sistema è adottare un buon antivirus e, ancora di più, provvedere, anche giornalmente, ad eseguire l'upgrade della relativa libreria.

Si tratta di un'operazione che nei pacchetti più moderni, viene effettuata automaticamente. Inoltre bisogna controllare tramite antivirus non solo tutto quello che entra nella nostra macchina, ma anche tutto quello che esce (ad esempio, la posta). ■

GLOSSARIO

AD-WARE
Termine usato per descrivere software gratuito che spesso (ma non sempre) contiene cookie e chiavi di registro che vengono inserite nel computer dell'utente al momento dell'installazione. Questi ospiti permettono di "tracciare" i movimenti sul Web dell'utente, in modo da seguirne le abitudini a scopi pubblicitari. Talvolta i programmi ad-ware mascherano all'interno del codice spyware (vedi sotto).

BIOS
(Basic Input/Output System) Particolare software di sistema, contenente routine che controllano la macchina durante il processo di startup, assieme ad altre funzioni di base, come verifica e abilitazione della tastiera, del display, dei dischi rigidi. Sulle macchine più vecchie il BIOS era inserito in una memoria di sola lettura, mentre sui computer più recenti esso risiede su una flash ROM, che può essere cancellata e riscritta se l'utente ha necessità di eseguire, appunto, l'upgrade del BIOS.

BLENDED THREAT
Si tratta di un fenomeno recentissimo, nella storia dei virus, che fa convivere insieme caratteristiche di tutti gli esemplari del mondo virale (virus, worm, cavalli di Troia). Grazie alla loro natura tanto subdola quanto inafferrabile, i blended threat (letteralmente minaccia mista) riescono a propagarsi in maniera più veloce di qualunque altro tipo di virus, e sono più difficili da rintracciare e bloccare rispetto alle forme tradizionali.

CERT
(Community Emergency Response Team), www.cert.org organizzazione fondata per raccogliere e fornire informazioni sulla comunità Internet, in particolare per quanto riguarda la sicurezza della navigazione. Scopo dell'organizzazione è studiare le vulnerabilità presenti sulla rete, fornire report degli incidenti e delle possibili aree compromesse, e pubblicare un bollettino di informazioni relative alla sicurezza. Voluto dal governo federale americano, e insediato presso la Carnegie Mellon University, pubblica un bollettino e una serie di newsletter di notevole interesse.

BOOT
Al momento dell'accensione, il computer esegue una serie di operazioni di base, generalmente custodite nel BIOS. I
I boot è il primo passo nell'utilizzo di un PC, e precede, immediatamente, il caricamento del sistema operativo. La parola, abbreviazione della più lunga "bootstrap", si riferisce all'azione di calzare da sè gli stivali (boot) tirando una striscia o asola alla loro sommità (strap).

BOOT SECTOR
Un boot sector è una sezione di un disco, generalmente un disco rigido, riservata a funzioni del sistema operativo, che devono essere caricate per prime durante lo startup. Generalmente sono localizzate nel primo settore della prima partizione di un drive.

EURISTICO
Nella forma più generale, un metodo euristico rappresenta la soluzione di un problema che si basa sulla tecnica della prova e dell'errore; per fare un esempio l'uso di un mazzo sconosciuto di chiavi per aprire una porta adotta una tecnica euristica.
Il contrario è rappresentato dalla tecnica algoritmica, che si basa su formule e procedure collaudate.
Il vantaggio della prima tecnica sta nel fatto che i programmi euristici sono capaci di sviluppare regole di buon senso per risolvere problemi analoghi a quelli già affrontati, acquisendo, per così dire, una esperienza nella gestione dei problemi futuri.
La maggior parte dei programmi antivirus si basa su tecniche algoritmiche, che confrontano una stringa caratteristica (una sequenza di caratteri ASCII rinvenuta nel codice) con una libreria incorporata nel programma.
Questa procedura è efficace, ovviamente, solo in caso di virus già noti; nel caso invece di un'infezione ancora ignota, i pacchetti antivirus che adottano questa tecnica aggiuntiva monitorano continuamente l'attività del PC e, in caso di procedure sospette, intervengono avvisando l'utente e chiedendo il suo intervento. Sebbene capaci di offrire maggior livello di protezione, le tecniche euristiche possono rappresentare, spesso, un fastidioso rallentamento all'uso della macchina.

MACRO
Una macro è una serie di azioni e procedure, registrate in un file e assegnate a una combinazione di tastiera, un simbolo, a un nome. Le macro sono sovente utilizzata quando occorre eseguire con rapidità e precisione procedure ripetitive. Un macro virus è una macro, dotata di codice maligno, che viene portata a termine all'insaputa dell'utente, per generare un effetto distruttivo sul documento corrente o sull'intero sistema.

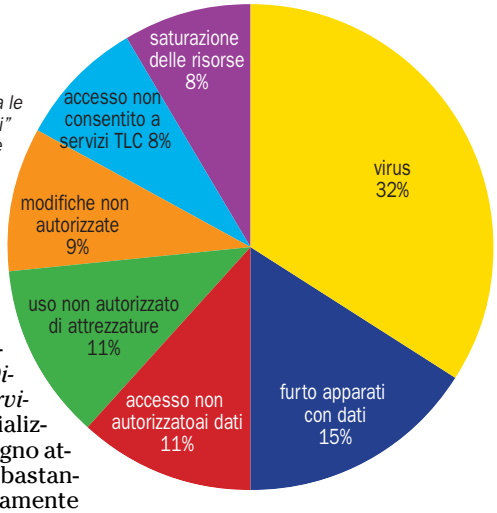
MALWARE
Detto anche pestware, vandalware, punkware , è un software intenzionalmente disegnato per scopi non leciti, come cancellare file o contenuti di memoria, o guadagnare accesso non autorizzato a un sistema. Sotto questo termine generico viene non solo raccolto tutto quel che interessa i virus, ma, più genericamente, ogni codice che, in qualche maniera, coinvolge tematiche legate alla sicurezza.

CAVALLO DI TROIA
Viene così indicato un programma che, mascherato sotto funzioni utili (nella maggior parte dei casi utility o giochi), nasconde invece un'applicazione non lecita del gruppo del malware

SPYWARE
Si tratta di una categoria di software che "traccia" le abitudini dell'utente senza che questo ne sia conoscenza. Lo spyware si affida oggi a nuove tecniche più sofisticate, tra cui quella di farsi trasportare da programmi ad-ware. Talvolta la rimozione del programma originario non elimina dall'interno del PC la routine di spyware, tanto che occorre adottare, per lo scopo specifico, un programma ad hoc.

WORM
Programma con funzioni, nella maggior parte dei casi, distruttive, contenente codice che replica se stesso fino a riempire o bloccare un drive o un network, provocandone il malfunzionamento.
Molto spesso i worm contengono routine capaci di propagarsi autonomamente ad altre macchine, utilizzando, pressoché universalmente, il canale della distribuzione di e-mail con i client di posta Outlook e Outlook Express.

Quando dire I Love You costa 17 miliardi di dollari



I virus la fanno da padrone *tra le cause di "danni informatici" derivati da azioni fraudolente*

Se, una volta, la sicurezza informatica poteva essere considerata un aspetto marginale dell'uso del PC, alcuni dati (fonte Symantec), relativi agli ultimi quattro anni, ci permettono di comprendere, effettivamente, quanto questo aspetto dell'utilizzo della macchina informatica abbia assunto, via via, importanza fondamentale.

Nel 1999 solo un messaggio di posta elettronica su 1400 era infetto, ma il rapporto aumenta vertiginosamente l'anno successivo e, almeno nelle previsioni e considerando il trend attuale, nel 2002 raggiungerà almeno 1/100.

In particolare, l'impatto economico derivante dagli attacchi di virus e worm sui sistemi informatici sta assumendo valori difficilmente prevedibili, se non fossero ampiamente documentati; nel 2000, l'anno del micidiale ILoveYou, il danno prodotto superò i 17 miliardi di dollari, valore che, a ben pensarci, rappresenta un costo superiore a quello necessario per ripristinare le infrastrutture ICT distrutte dall'attentato dell'11 settembre 2001 (studi effettuati da Computer Economics/ICSA)

"Cyberterrorismo pericoloso come le bombe?", si chiede uno studio messo a punto dalla Symantec.

Al di là delle iperboli, i dati esposti fanno capire perché la sicurezza sia diventata una delle principali fonti l'investimento in informatica, tanto per gli utenti individuali quanto, a maggior ragione, per le istituzioni civili e militari e per le imprese che, secondo lo stesso studio, investono almeno l'8% del proprio budget per proteggere i propri dati e le proprie strutture.

Ma qual'è la tipologia degli attacchi, in particolare in Italia? Il "danno informatico" verificato è rappresentato, per oltre il 32%, da virus, seguito da furto materiale di apparati con dati (15%), accesso non autorizzato ai dati (11%), uso non autorizzato di attrezzature (11%), modifiche non autorizzate (circa il 9%), accesso non consentito a servizi TLC (oltre all'8%) e, infine, saturazione delle risorse (8%) (Fonte "Information Security - Implementazione" di Dario Forte, Mondadori Informatica).

Un esempio di attacco

Nel febbraio del 2000 alcuni colossi americani del Web (Yahoo, eBay, Amazon, Cnn) subirono un violento attacco da parte di hacker, la cui conseguenza fu "l'oscuramento" del loro siti, bloccati per diverse ore. Si trattò di un attacco del tipo DDoS (*Distributed Denial of Service*, una forma più specializzata di DoS), messo a segno attraverso una tecnica abbastanza semplice ma estremamente distruttiva

L'attacco fu eseguito inviando a questi siti, già di per sé molto trafficati, un numero enorme di messaggi di posta elettronica, determinando così il blocco dei server e impedendo agli utenti "regolari" di accedere al sito. Operazioni di questo genere, certo dannose per i siti appena nominati, diventano davvero disastrose quando lanciati verso locazioni finanziarie, in cui il tempo di fermo macchina è direttamente proporzionale alla perdita di danaro. Gli attacchi, in questo caso, possono avvenire attraverso vari modi; il più semplice è quello di mettere in circolazione un hoax che, a fronte di una improbabile donazione di danaro a una bambina malata o un'associazione benefica, richiede di spedire per conoscenza a una grossa organizzazione una copia conforme, assicurando che l'organizzazione provvederà a versare un tanto per ogni messaggio di posta ricevuto. Una tecnica ancora più raffinata, ormai di uso comune, è quella di portare alle infrastrutture IT attacchi combinati, attraverso una minaccia tecnicamente definita "blended", come quella sostenuta dal worm *Code Red*. Altra tecnica molto diffusa è quella del *defacement*, che consiste nel modificare, sostituire, far sparire addirittura una o più pagine di quelle che costituiscono il sito Web. Sebbene questo sistema non sia distruttivo come il primo, è mirato soprattutto a creare una perdita d'immagine e, curiosamente, rientra nella categoria di eventi e più alta frequenza. ■

Chi fabbrica i virus?

Liquidare rapidamente il fenomeno virus writer come legato a delinquenti di mezza tacca è pericoloso e lascia abbassare imprudentemente il livello di guardia.
Pacifici e Girardi, nel "2° Osservatorio sulla Criminalità ICT del FTI" (Forum Permanente per la Tecnologie dell'informazione), edito da Franco Angeli, individuano le motivazioni che animano questa forma di criminalità in tre categorie principali, e cioè:

- volontà di sottrarre dati per utilizzarli o rivenderli a imprese o istituzioni concorrenti
- desiderio di distruggere, non per interesse personale, ma per semplice volontà e piacere di procurare danno o per semplice gusto del vandalismo
- volontà di autoaffermazione, dimostrando un'intelligenza e una capacità "superiore" alle difese e alle leggi.

Nello stesso studio gli autori riferiscono: "... il virus writer è definito mentalità scientifica, con volontà distruttiva e motivazioni aggressive". E ancora: "... si tratta di persone generalmente giovani o molto giovani, con una mentalità fortemente ludica, talvolta con disturbi, più o meno seri, della personalità".
Sarah Gordon, ricercatrice di Symantec Corporation, afferma in un'intervista che i virus writer "...più sono giovani, meno sono consapevoli delle responsabilità giuridica del loro atti; mentre, più si sale con l'età, più si acquisisce consapevolezza delle conseguenze di determinate azioni".
Lo studio della Gordon, basato su osservazioni molto lunghe nel tempo, riferisce che, dieci anni fa, l'età media degli scrittori di virus oscillava tra i 14 e i 17 anni, mentre oggi si aggira tra i 25 e i 28.
David L. Smith, riconosciuto per aver scritto e distribuito il virus Melissa, aveva trent'anni al momento del suo arresto nel 1999.
Nella maggior parte dei casi, gli scrittori di virus, superata questa età, continuano a lavorare come ingegneri o amministratori di sistemi nell'industria informatica.
È impressionante, comunque, venire a sapere che esiste un vero universo parallelo, alimentato da *fanzine on line*, newsletter, liste di distribuzione, forum, tutorial, il cui scopo è a far crescere la cultura della scrittura e della creazione e modifica dei virus. Nonostante queste generalizzazioni, è ben difficile individuare gli scrittori di virus in un gruppo ben omogeneo.
Le caratteristiche dello scrittore medio possono cambiare in maniera anche molto vistosa; essi variano in età, disponibilità economica, dislocazione geografica, posizione sociale, livello educativo e culturale, preferenze, struttura familiare.
L'aspetto della "sfida" è sempre presente, anche se, con l'andar del tempo, l'obiettivo si sta spostando dagli obiettivi militari e governativi alle organizzazioni commerciali.
Gli studi riferiti evidenziano come la maggior parte dei produttori ignori le implicazioni penali dei loro gesti, tanto che la paura di una possibile punizione rappresenta solo l'8% del motivo per cui poi, lo scrittore, rinuncia.