Protezione antivirus: la certezza assoluta

di Stefano Toria (MC0170 su MC-link)

Nell'articolo pubblicato sul numero di luglio abbiamo espresso delle riserve sulle attuali misure di protezione contro i virus, arrivando apparentemente alla conclusione che non esiste una prevenzione ma soltanto una serie di cure, le quali peraltro debbono essere opportunamente predisposte (vedi il caso dei backup) perché possano garantire una minima efficacia.
L'articolo di questo mese modifica questa visione apparentemente pessimistica: è possibile una protezione efficace, anche se non particolarmente efficiente. Un'accurata opera di installazione di un sistema di controllo crittografico consente una rilevazione immediata dell'azione di un virus

Determinazione di un criterio generale nell'azione dei virus

I lettori che hanno seguito questa serie di articoli possono aver tratto l'impressione che non sia possibile determinare alcun criterio uniforme di azione nel comportamento dei diversi virus, e oltretutto che questi stessi, crescendo continuamente di numero, stanno diventando un fenomeno impossibile da controllare. Per inciso, questa mentalità può portare delle conseguenze pericolose, determinando un abbassamento della guardia e una possibile recrudescenza di attacchi da parte di nuovi virus.

Tuttavia questa convinzione è errata. Nel comportamento di tutti i virus conosciuti, e di tutti quelli che verranno realizzati in futuro per quanto è possibile prevedere attualmente, si riscontra un'azione uniforme che è uguale in tutti, e che consiste nell'uso di un unico veicolo per la diffusione e l'esecuzione delle azioni dannose: il programma eseguibile che li ospita. Può trattarsi di un .COM o di un .EXE, di un record di boot di partizione o del master boot record; su un Apple Macintosh può trattarsi di una delle risorse contenute in un'applicazione, mentre nell'ambiente Microsoft Windows un virus può attaccarsi a una «Dynamic Link Library» (.DLL); ma in ogni caso un virus determina necessariamente una modifica in un programma, modifica senz'altro illecita per definizione in quanto non specificamente richiesta, avviata e desiderata dall'utente.

Il fatto di aver isolato un simile criterio è molto importante, in quanto ne deriva direttamente una conseguenza altrettanto importante: realizzando un sistema che consenta di tenere traccia di ogni minima variazione a un programma eseguibile, nelle diverse forme che esso può assumere, e che ne renda consapevole l'utente, si è realizzato il perfetto sistema di protezione antivirus. Non esiste né può esistere un virus che agisca senza modificare nessun programma; quindi un controllo sulle modifiche di un programma rileva rapidamente la presenza di un virus.

Si può obiettare che un simile programma risolve soltanto in parte il problema della tutela di un sistema dagli aggressori, in quanto esistono anche i cavalli di Troia; ma l'azione di un cavallo di Troia è necessariamente immediata, per definizione, e non c'è alcun modo di proteggersi da una simile azione se non l'aver preventivamente effettuato una copia di backup che consenta di neutralizzare o almeno minimizzare il danno causato da un cavallo di Troia maligno; mentre nel caso di un virus il rischio può rimanere annidato per giorni o per mesi, senza che l'utente si avveda di ciò che sta accadendo nel proprio personal computer, ed è quindi importante che egli abbia modo di essere avvertito per poter prendere le opportune misure di disinfezione senza dover aspettare che il virus abbia distrutto dei dati per poterli ricostruire.

Un aiuto dalla matematica: la crittografia

La crittografia è una tecnica antica quasi quanto la scrittura. Nella sua accezione più semplice, un sistema crittografico consiste nella sostituzione di segni convenzionali ai normali segni alfabetici, come avviene ad esempio nei giochi enigmistici che vanno appunto sotto il nome di «crittografie». Anzi, per maggiore precisione si dovrebbe parlare di «sostituzione di un alfabeto a un altro», in quanto per definizione ciascun alfabeto è una convenzione. Ad esempio, adottando una cifratura banale,

quella che sostituisce a ciascuna lettera dell'alfabeto italiano il proprio numero di posizione, la parola «libro» diventa «10 9 2 16 13».

La crittografia è stata molto sviluppata soprattutto in ambienti militari in cui viene utilizzata da molto tempo per assicurare un livello accettabile di segretezza nelle comunicazioni. Anche in ambito civile la crittografia trova alcune applicazioni, tra cui le principali nell'ambito dell'informatica.

Si è detto che la cifratura consistente nella sostituzione di un numero posizionale a ciascuna lettera dell'alfabeto è un'operazione banale perché la chiave di cifratura è facile da identificare; il risultato quindi non è particolarmente protetto. Sistemi più sofisticati rendono più difficile la decifrazione da parte di chi non possegga la chiave, assegnando al codice cifrato un diverso numero di simboli rispetto al messaggio non cifrato. In alcuni casi il risultato della cifratura può consistere in un solo numero, che rappresenta in sintesi tutto il messaggio.

Sistemi di questo genere trovano applicazione ad esempio nel controllo di identità, quando sia necessario verificare che la persona che utilizza un determinato programma sia effettivamente colui o colei che afferma di essere. In questi casi si utilizza una parola chiave o password, che può essere conservata cifrata all'interno del sistema per far sì che un eventuale intruso non venga a conoscenza della parola, ma soltanto del risultato della cifratura. In questi casi addirittura si possono utilizzare sistemi di cifratura a senso unico, costruiti in modo tale per cui dal messaggio originale si determina con certezza il messaggio cifrato, ma dal messaggio cifrato non è possibile risalire al messaggio originale. Nel caso del controllo di identità questo non costituisce affatto un problema: dovendo verificare se una data persona conosce la parola chiave, è sufficiente che tale parola gli venga chiesta e quindi immediatamente cifrata: il confronto del risultato della cifratura con il codice cifrato all'origine e memorizzato consente di stabilire se la persona ha scritto la parola chiave esattamente.

La crittografia per il controllo delle infezioni: la «firma crittografica»

Così come è possibile codificare un messaggio consistente in una parola di pochi caratteri, è altrettanto possibile codificarne uno più lungo costituito da decine o centinaia di migliaia di caratteri, come ad esempio un programma eseguibile: un intero file contenente un programma può dar luogo a un codice univoco consistente in un numero di alcune cifre, definito «firma» o «firma crittografica» del programma. L'utilità di una simile procedura nella prevenzione dai virus sta nel fatto che una variazione nel programma, per quanto minima, dà luogo alla generazione di un codice completamente diverso; pertanto è sufficiente generare il codice di controllo partendo da una copia del programma certamente non infetta per avere un elemento di riferimento che consente di verificare rapidamente l'integrità del programma. La verifica consisterà nel codificare nuovamente il programma e confrontare il nuovo risultato della codifica con il risultato di riferimento: se coincidono il programma non ha subito modifiche, altrimenti si può sospettare che il programma sia stato attaccato da un virus.

Non è opportuno affrontare in questa sede la trattazione dei procedimenti crittografici; a tal fine si rimanda alla numerosa bibliografia sull'argomento, che è stato approfondito nella letteratura sulla sicurezza dei sistemi informativi.

L'organizzazione di un controllo crittografico

Si è detto in apertura di questo articolo che la protezione antivirus costituita dal controllo crittografico è efficace, ma non particolarmente efficiente. L'efficacia è facile da dimostrare: l'identificazione di una chiave corretta, fatta in modo tale per cui due programmi identici forniscano l'identico risultato, ma due programmi diversi anche in un solo byte non possano mai dare lo stesso risultato, fa sì che il confronto dei codici risultanti equivalga al confronto tra il programma sospetto e il programma originale certamente non infetto. Quest'ultima operazione, che garantirebbe in assoluto la massima certezza, non è possibile per diverse ragioni; il raffronto tra i codici ne è un sostituto accettabile.

Peraltro un'operazione di questo genere non è particolarmente efficiente, in quanto aggiunge un tempo morto nel ciclo di utilizzo di un personal computer: se il confronto venisse effettuato ogni volta che ciascun programma viene eseguito, il tempo di caricamento si allungherebbe in maniera percettibile, che crescerebbe in proporzione esponenziale al crescere della dimensione del programma. Per contro, effettuare saltuariamente i controlli non garantisce una copertura totale perché nel periodo di tempo intercorrente tra un controllo e l'altro il sistema potrebbe infettarsi, l'infezione diffondersi e raggiungere molti altri sistemi prima di essere individuata.

Il sistema delle firme crittografiche trova quindi applicazione in quei contesti in cui la protezione delle informazioni è di vitale importanza. In questi casi essa dovrà essere eseguita di routine ad ogni esecuzione di un programma.

In altre situazioni il controllo crittografico potrà essere apprestato per essere eseguito soltanto dopo aver eseguito una nuova applicazione. Questo caso merita un approfondimento.

Si è visto più volte che il momento critico per la diffusione di un virus consiste nell'esecuzione di un nuovo programma, che porta con sé l'infezione. Ora, fintanto che un utente di un personal computer non esegue nuovi programmi, ma si limita all'esecuzione di programmi già installati, non corre alcun rischio di infezione. Nel momento in cui inserisce nel drive del proprio computer un dischetto proveniente dall'esterno, e ne preleva un programma per avviarne l'esecuzione, allora si sottomette al rischio che il programma sia infetto e che trasmetta l'infezione agli altri programmi installati sul disco fisso.

È questo il momento in cui va fatto il controllo crittografico. L'utente dovrà predisporsi per il controllo preparando un dischetto di sistema, sicuramente pulito e incontaminato, da cui avviare il sistema operativo per effettuare i controlli. Infatti è inutile e controproducente effettuare i controlli senza avere la certezza di trovarsi in un ambiente non infetto. Dopo aver avviato il Dos da dischetto, si eseguirà il controllo delle firme crittografiche. Se il controllo passa senza segnalazioni di errore, il programma può essere utilizzato con tranquillità, anche se è opportuno tenerlo in «quarantena», effettuando ripetuti controlli crittografici nei giorni successivi. Diver-

Nel prossimo numero

Abbiamo annunciato che non intendiamo recensire, per il momento, programmi antivirus. Siamo invece in grado di recensire programmi di controllo crittografico, facili da testare in quanto basta modificare manualmente un byte di un programma eseguibile, a mezzo di una utility di edit esadecimale su un file, per verificare se il controllo crittografico rileva la differenza.

Stiamo completando il reperimento di alcuni di questi programmi. Nel prossimo numero ne presenteremo una gamma, elencando pregi e difetti e criteri di funzionamento.

samente, se il controllo segnala qualche discrepanza, il nuovo programma dovrà essere immediatamente isolato, ne dovrà essere impedito in ogni modo l'utilizzo finché non siano stati effettuati gli opportuni accertamenti, e se possibile il dischetto dovrà essere inviato presso la nostra redazione.

L'uso simultaneo e regolare di un sistema di backup correttamente organizzato, e di un sistema di controllo crittografico dei programmi eseguibili, garantisce un livello di protezione che ai fini pratici è equivalente al 100%.

I costi

Un simile sistema di protezione costa, quantomeno in termini del tempo che l'utente gli deve dedicare. Per questa ragione è sempre opportuno tenere a mente il fatto che tutta la materia della protezione dai virus va trattata con i metodi della statistica: il danno da virus è sempre un danno potenziale (finché il virus non si «scatena»), che ha un costo potenziale dato dal costo del massimo danno possibile moltiplicato per la probabilità che tale danno si verifichi. Pertanto il costo statistico del danno da virus deve essere raffrontato con il costo del tempo dedicato alla protezione dai virus, ottenuto moltiplicando il costo orario che l'utente assegna a se stesso per il tempo richiesto dalle misure di protezione. Quando i due costi si equivalgono, la protezione è ottimale.

Tutta questa è teoria. In pratica il «massimo danno possibile» è difficile da valutare, perché difficile da valutare è in sé l'informazione. Ancor più difficile da valutare è la probabilità del massimo danno, che è necessariamente soggettiva (cioè determinata «a occhio» dall'interessato) poiché mancano dati statistici sulle infezioni da virus tali da poter stimare quantitativamente il valore oggettivo della probabilità. Essendo soggettiva, tale probabilità è destinata a oscillare in funzione di diversi fattori, ad esempio a seconda della maggiore o minore fortuna giornalistica dell'argomento virus, dei toni più o meno apocalittici con cui il problema viene affrontato dai mezzi d'informazione di massa e così via.

Quindi si deve concludere che la convenienza di una protezione antivirus non è determinabile? Certamente no; ma non è possibile determinarla in modo così rigorosamente quantitativo. Ciascun utente ha la sensazione del valore dei propri dati. Uno studente che prepara la tesi, un commercialista con le contabilità (magari ...«non ufficiali») dei propri clienti, un'azienda leader di mercato i cui dati strategici si trovano nel PC del direttore marketing, un ragazzo della scuola media con i primi programmi scritti in Basic, sono utenti che debbono necessariamente avere approcci diversi al problema del rischio da virus. La sensibilità individuale suggerirà le misure più opportune da adottare, caso per caso; si deve comunque tenere sempre a mente che qualche misura è sempre meglio che nessuna misura, e che in mancanza della Protezione Perfetta e Infallibile è sempre meglio accontentarsi di una protezione perfetta e fallibile, ma adottata con razocinio, piuttosto che non fare niente e affidarsi irrazionalmente al caso.

MC

La posta

Sono arrivate in redazione numerose segnalazioni di lettori, tutte corredate di dischetti con programmi più o meno infetti. Nel ringraziare quanti hanno inviato i propri contributi (che sono in corso di esame, i cui risultati verranno pubblicati quanto prima) invitiamo chiunque capiti in possesso di un programma infetto, o sospetto di infezione, ad inviare il programma in redazione.

Un messaggio, tra quelli pervenuti, merita particolare attenzione per due ragioni. La prima è che dà occasione di approfondire un argomento trattato nello scorso numero, e cioè l'organizzazione dei backup di protezione contro l'attacco di un virus. La seconda è che mi è giunto a mezzo di MC-link, ed è tuttora una delle pochissime segnalazioni che mi sono arrivate tramite questo sistema. Ho chiesto all'autore il permesso di riportare il testo del messaggio:

MAILBOX
Msg# 90057, 14/07/91 00:42 [1526]
Da: MC6681 Francesco Andreani
A : MC0170 Stefano Toria

Oggetto: Privato Ma Non Troppo

Caro Stefano,
sono un tuo affezionato ed attento lettore ma in informatica sono piuttosto ingenuo, cosa che capirai subito dalla mia domanda.

Ho scelto di scriverti privatamente perché non ho saputo trovare una area adatta, se credi di renderla pubblica fammelo sapere: mi affido a te.

Nel numero di giugno di MC parlando di tecniche per salvare i propri dati da una eventuale aggressione da virus, giustamente affermi che nelle copie di backup non devono essere inclusi i file .COM e .EXE perché sono quelli ai quali il virus si attacca...

Questa sera mi è venuto in mente di riconfigurare il mio programma di backup (PC-Tools Backup v 6.0 su PC IBM-comp 286) ed ho eliminato tutti i file .COM e .EXE, ma poi mi è venuto in mente che non saprei come fare il restore. Mi spiego. In caso di formattazione di disco rigido io farei:
1) — installazione del DOS;
2) — installazione del PC-Tools;
3) — -+ restore oppure
— installazione del TC++ ecc.; ossia mi chiedo se nella copia restore non ci sono gli eseguibili ma le directory nelle quali questi eseguibili devono andare, riusciranno i programmi di installazione a riconoscere le directory già create dal restore? Ed in caso si decida di fare prima l'installazione di tutti i programmi riuscirà il restore a inserire il resto dei file (esclusi gli eseguibili) riconoscendo le directory create dai programmi di installazione? Spero di non aver fatto troppa confusione ed attendo salutandoti con simpatia.

Franz

Rispondo all'amico Andreani in pubblico, come gli ho annunciato con un messaggio nella sua mailbox su MC-link, perché il suo quesito mi permette di approfondire e precisare quanto scritto nello scorso numero.

Si è detto che non è consigliabile effettuare il backup delle applicazioni in quanto è possibile che si siano corrotte a causa dell'infezione. Tuttavia molte applicazioni generano, nelle directory in cui risiedono, dei file contenenti la configurazione personalizzata secondo le specifiche dell'utente. Questa configurazione è spesso il frutto di approssimazioni successive, che possono essere costate ore o giorni di impegno dell'utente. È quindi opportuno salvaguardarsi dal rischio di perdere questi file, facendoli oggetto di un backup separato. Meglio ancora sarebbe effettuare un unico backup dell'applicazione subito dopo aver terminato l'installazione, prima quindi che un

qualsiasi virus abbia la possibilità di contaminare i programmi eseguibili. Il tutto dovrà far parte di una accurata pianificazione dell'installazione: si dovranno prima definire le directory in cui il programma verrà inserito; quindi si procederà alla installazione e alla personalizzazione, e infine — quando si è soddisfatti della funzionalità dell'applicazione — si farà un backup che va riposto per essere utilizzato in caso sia necessario reinstallare il programma. In quest'ultimo caso quindi, anziché rifare l'installazione, si potrà effettuare il restore del backup originario.

Si badi bene tuttavia che questa procedura non garantisce il ripristino di una copia dell'applicazione perfettamente immune da virus: se durante il procedimento dell'installazione l'utente... «si è distratto» giocando ad esempio con un videogioco che è poi risultato infetto, può essersi infettata anche l'applicazione in corso di installazione. Non si raccomanderà mai abbastanza di usare prudenza in questi casi, e di cercare di comprendere a fondo le implicazioni di ciò che si fa sul proprio computer. Un discorso a parte meritano i programmi coperti da schemi di protezione che prevedono una installazione limitata, registrando sul disco fisso un indicatore di avvenuta installazione, determinante per l'avvio del programma, e impedendo al tempo stesso una successiva installazione del prodotto a meno che non sia stata effettuata nel frattempo una disinstallazione che disabilita il programma sul disco fisso.

Personalmente riteniamo che questi schemi di protezione siano anacronistici e che andrebbero aboliti perché si sono dimostrati più un intralcio per gli utenti onesti che un vero ostacolo per i pirati determinati a copiare illecitamente e magari a rivendere i programmi copiati. Tuttavia si deve considerare che tali protezioni esistono, e c'è la possibilità che un programma acquistato sia protetto da un simile schema.

Un programma del genere crea non pochi problemi all'utente che sia stato vittima dell'attacco di un virus, e il cui disco fisso sia stato formattato senza possibilità di recuperarne il contenuto. Infatti una copia del programma recuperata da un backup non funziona, né sarebbe possibile la reinstallazione a partire dai dischetti originali, che consentono una sola installazione.

Il nostro consiglio a chi abbia acquistato regolarmente un programma protetto è di avvalersi del diritto morale a tutelare il proprio investimento, cercando in tutti i modi possibili di copiare il dischetto-chiave dell'installazione e utilizzando questo dischetto per l'installazione stessa. Siamo consapevoli di aver affrontato un argomento delicatissimo, in cui interessi economici rilevanti sono tutelati quasi esclusivamente (nel nostro paese) da considerazioni di ordine morale; ma chi legge da tempo questa rivista ben conosce le posizioni della redazione in merito alla pirateria del software, ed è facile comprendere che questo invito a copiare un disco con del software di proprietà è ben lungi dall'essere un invito alla pirateria.

MC

COPROCESSORI

ULTIMO ROUND !!

IIT 80c287 - 08	99.000
IIT 80c287 - 10	129.000
IIT 80c287 - 12	139.000
IIT 80c287 - 20	199.000
IIT 80c387 - 16	279.000
IIT 80c387 - 20	299.000
IIT 80c387 - 25	329.000
IIT 80c387 - 33	349.000
IIT 80c387 - 40	599.000
IIT 80c387 - 16sx	189.000
IIT 80c387 - 20sx	209.000

Finalmente anche la INTEL ha riconosciuta la forte presenza sul mercato dei coprocessori IIT riducendo drasticamente i prezzi ..... ma noi abbiamo ridotto i nostri all'osso. Inoltre abbiamo introdotto, per coloro che rimangono ancorati al Blasone, la linea INTEL **a prezzi incredibili**. Quindi ora, presso la DIGITRON, potrete scegliere il coprocessore che più Vi aggrada senza dover perdere altro tempo basta una telefonata ed inoltre **NON SIAMO LEGATI AL DOLLARO** che può riservarvi amare sorprese dall'ordine alla consegna. Per ogni problema riguardante i coprocessori matematici non esitate a chiamarci saremo a Vs disposizione per consigliarVi quale installare o per inviarVi una documentazione più completa. Sono a disposizione gratuitamente le librerie sia in Assembler che per i compilatori Microsoft C, Microsoft Quick Pascal, Turbo Pascal, Turbo C, Aztech C, Prospero PC Pascal, Zortech C++, per sfruttare la rotazione di matrici 4x4 possibile solo sui coprocessori IIT.

INTEL 80287 XL	149.000
INTEL 80387 - 16	369.000
INTEL 80387 - 20	369.000
INTEL 80387 - 25	369.000
INTEL 80387 - 33	369.000
INTEL 80387 - 16sx	219.000
INTEL 80387 - 20sx	239.000

I coprocessori INTEL e IIT sono garantiti 5 anni.
Tutti prezzi indicati sono in Lire + IVA 19% senza alcun legame valutario.

DISTRIBUTORI UFFICIALI E CENTRO ASSISTENZA AUTORIZZATO

VEGAS COMPUTER COMMUNICATIONS

star SEIKOSHA

Concessionario PASSEPARTOUT

MODELLO	COLORS	AGHI	COL.	SPEED	FNT	BUFF.	DPI	OFFERTA
STARLC20	1	9	80	180	4	4Kb	240	249.000
STARLC200	7	9	80	225	4	16Kb	240	419.000
STARLC24-200	1	24	80	222	5LQ	7Kb	360	509.000
STARLC24-200	7	24	80	222	5LQ	30Kb	360	609.000

Gestione Aziendale Integrata da 1 a 8 terminali in Dos od OS/2. Fino a 128 posti in UNIX.

DIGITRON

Tel. (06) 74.59.25
74.31.39 - 76.05.69
(FAx su tutte le linee)

Computer Shop - Via Lucio Elio Seiano, 13/15 - 00174 ROMA
Centro Ass. Tecnica - Via Dei Quinzi, 7 - 00175 ROMA

Il Grillo Parlante

VIA S. CANZIO, 13 - 15 - 17 r. - Tel. 010 / 415592
GENOVA SAMPIERDARENA
VIDEOGIOCHI PER:

PUNTO COMPUTER ITALIA

COMMODORE-ATARI-AMSTRAD-MSX-SPECTRUM-NINTENDO-SEGA-ATARI 2600

Interfaccia Midi Amiga	L.	45.000
Digitalizzatore VID Amiga	L.	80.000
Syntetic Sound Amiga	L.	120.000
Espansione 512Kb. Amiga Int.	L.	90.000
Espansione 1.5Mb. Amiga Int.	L.	245.000
Espansione 2Mb. Amiga Est.	L.	350.000
Genlock Esterno Amiga	L.	349.000
Genlock Professionale Amiga	L.	1.799.000
Data Switch 2 Posizioni	L.	40.000
Data Switch 4 Posizioni	L.	50.000
Drive Esterno 3"1/2 Amiga	L.	165.000
Scheda Televideo	L.	180.000
Selettore Mouse/Joystick Amiga	L.	32.000
Mouse ottico Amiga-PC-Atari	L.	110.000
Dischetti 3"1/2 (minimo 100 pz.)cad.	L.	750
Joystick a distanza ad infrarossi	L.	60.000

NOVITA':

MODEM 1200 Baud
MODEM 2400 Baud

MINI- PORTATILE
MISURE
11 Cm x 6 Cm x 2.2 Cm

1200 B **L. 195.000**
2400 B **L. 340.000**

Si Prenota **Vision Colorbust,** scheda grafica con 16.000.000 di colori + software MEGAPAINT. Lavora su tutte le risoluzioni grafiche AMIGA. Collegabile al VIDEON e compatibile con tutti i Genlock. Funziona su tutta la serie AMIGA.

L. 950.000