Thunderbyte Anti Virus Utilities

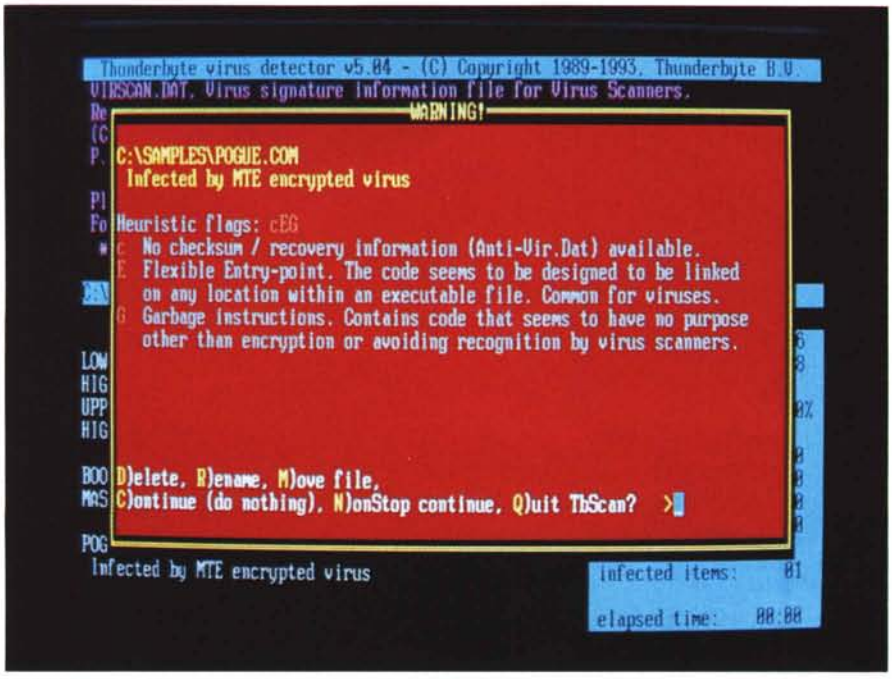
Diamo un'occhiata questo mese a un programma antivirus poco noto al grande pubblico, ma di alta qualità e molto noto tra gli esperti. Il produttore è conosciuto per aver sviluppato un altro prodotto antivirus, una scheda da inserire in uno slot del PC per il monitoraggio delle attività sospette. Le Thunderbyte Anti Virus Utilities sono un piccolo insieme di programmi che mancano quasi completamente dei fronzoli che abbelliscono prodotti dai nomi più altisonanti, ma che funzionano assai meglio e in modo ben più affidabile di molti concorrenti più celebri.
Virus uguale Ms-Dos? No, certamente. Anche se quasi tutti i nostri articoli hanno fatto riferimento in un modo o nell'altro al più diffuso sistema operativo del mondo, questo non vuol dire che noi ignoriamo che esistono altri ambienti, altre piattaforme. Ospitiamo in questo numero un contributo sul problema dei virus nei sistemi Archimedes. Queste interessanti, seppure poco diffuse, macchine RISC offrono alcuni spunti per la difesa dai virus che ci piacerebbe fossero ripresi anche da sistemi che hanno incontrato maggior favore di pubblico.
Riprendiamo infine il tema più generale della sicurezza per accennare a un problema tipico dei sistemi di controllo degli accessi: la scelta delle password

di Stefano Toria

Avevo progettato di terminare la recensione dei programmi antivirus. Ritengo di aver presentato ai lettori di MCmicrocomputer una selezione dei migliori prodotti disponibili sul mercato, e non vorrei dare fondamento all'idea che i virus siano un fatto di cui si deve parlare il più possibile per incrementare le vendite di programmi antivirus.

Recentemente ho avuto occasione di esaminare un prodotto shareware, meno noto di F-PROT o VIRUSCAN, ma di altissimo livello qualitativo. Il programma si chiama ThunderByte Anti Virus Utilities (TBAV), e incorpora delle funzioni del tutto particolari, che possono risultare essenziali in alcuni casi specifici; al di là di queste particolarità si tratta comunque di un ottimo programma antivirus, che merita di affiancare i suoi colleghi di maggiore «lignaggio» nella dotazione dell'utente previdente (regola numero uno: non affidarsi mai a un solo programma antivirus).

TBAV si compone di un insieme di piccoli programmi compatti, ciascuno dei quali svolge una funzione ben precisa e circoscritta. La prima, indispensabile, è l'installazione: TbSetup predispone il sistema al funzionamento e crea un file (ANTI-VIR.DAT) con il codice di controllo dei programmi presenti sul sistema, per poterlo successivamente verificare ad ogni scansione.



TBAV

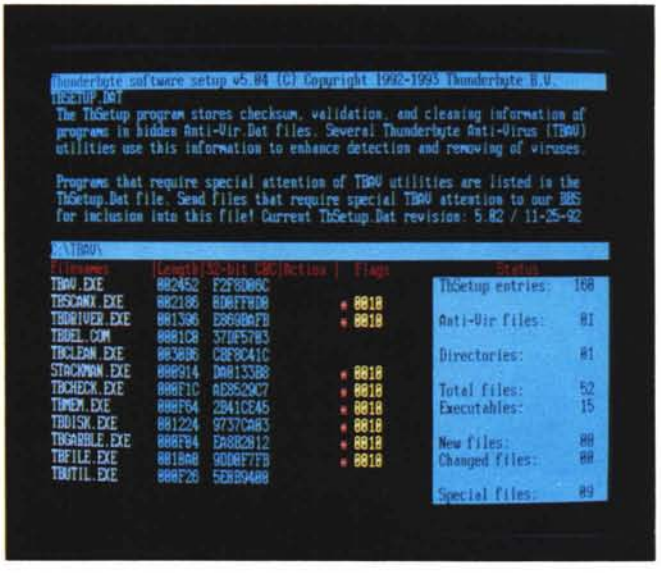
Produttore:
Frans Veldman, ESaSS B.V., P.O. Box 1380, 6501 BJ Nijmegen, Paesi Bassi. Tel. +31 (80) 787881 — fax +31 (80) 789 186 — BBS +31 (85) 212 395 (FidoNet 2:280/200) — Internet: veldman@esass.iaf.nl
Prodotto reperibile tramite i normali canali dello shareware (su sistemi telematici nazionali ed esteri)
Prezzi di vendita:
TBAV è offerto in quattro pacchetti differenziati, contenenti ciascuno un sottoinsieme di funzioni. Ciascuno ha un costo di registrazione di $24; l'insieme dei quattro pacchetti costa $62. Le licenze collettive vanno da un minimo di $124 a pacchetto ($312 per l'insieme) per un gruppo di almeno 6 licenze, fino a un massimo di $6.249 a pacchetto ($14.624 per l'insieme) per oltre 3.000 licenze.

Uno scanner a firme esterne

La più ovvia funzione antivirus è la scansione: la ricerca della presenza delle impronte dei virus conosciuti. TbScan, lo scanner di TBAV, è molto efficiente, e ha identificato senza problemi tutti i virus del nostro insieme di prova, in un tempo molto breve.

La particolarità di TbScan sta nel fatto che il file delle firme è esterno. Ne viene rilasciata una nuova versione ogni mese, e pertanto gli aggiornamenti al programma vero e proprio sono assai meno frequenti. Inoltre, poiché il file delle firme è un semplice testo ASCII, è possibile aggiungere in qualsiasi momento la firma di un nuovo virus, magari dopo averla fatta identificare dallo stesso TBAV (ne parleremo più avanti).

TbSetup è la funzione di installazione del pacchetto. In apertura la rilevazione di un virus.



Ricerca combinata: scansione/euristica/controllo di integrità

Abbiamo già avuto occasione di parlare di ricerca euristica qualche mese fa, a proposito di F-PROT.

Rammentiamo di cosa si tratta: la ricerca euristica è un metodo per identificare un virus non già grazie alla presenza di una sua «impronta digitale» ma analizzando il codice che compone il programma sospetto, per determinare se il tipo di funzioni svolte può essere caratteristico di un virus.

È un lavoro molto vicino all'intelligenza artificiale, poiché si basa sullo stesso tipo di procedimenti messi in atto dai ricercatori. In realtà nessuno degli antivirus che attualmente si servono di questo metodo di ricerca può essere ritenuto un vero e proprio sistema esperto, poiché manca la funzione di apprendimento.

Se attivato con le opzioni di default TbScan esegue un triplo controllo sui file eseguibili: la scansione delle firme, l'analisi euristica e il controllo di integrità. Se tutti e tre danno esito negativo, se cioè non risultano presenti firme di virus, né sequenze di istruzioni sospette, né variazioni nel codice di controllo, allora il programma viene passato; in caso contrario TbScan attira l'attenzione dell'utente sul programma, chiedendo istruzioni su come comportarsi.

L'utente potrà decidere di distruggere il programma sospetto, ovvero di cambiargli nome o spostarlo in una diversa directory, ovvero di proseguire indisturbato.

L'utente può scegliere di disattivare le funzioni di cui non intende servirsi.

Riconoscimento algoritmico

In aggiunta alla funzione di scansione delle firme, TbScan è in grado di andare alla ricerca dei virus più difficili — tipicamente quelli polimorfi — servendosi di un approccio algoritmico. Alcuni virus, come ad esempio quelli codificati con l'MtE, non sono identificabili con una stringa; è necessario analizzare il codice, con un procedimento simile a quello della ricerca euristica, sebbene non esattamente identico. È noto infatti il tipo di algoritmo utilizzato dall'MtE, che rimane invariato sebbene la sequenza di istruzioni corrispondenti al decodificatore si modifichi di volta in volta.

TbScan si avvale di specifici moduli di ricerca algoritmica, facili da aggiornare anche da parte dello stesso utente.

Disinfezione a prova di bomba

Sebbene ci siamo pronunciati più volte a favore della reinstallazione dei programmi infettati e contro la disinfezione, dobbiamo riconoscere che TbClean, il programma di disinfezione di TBAV, è a suo modo geniale. Non soltanto offre la possibilità di una ricostruzione ad altissima affidabilità, grazie anche alle informazioni accantonate da TbSetup all'atto della installazione, ma contiene anche una funzione di disinfezione euristica, che si avvale di un disassemblatore e di un emulatore per tentare di ricostituire l'originaria funzionalità del programma infetto anche nella totale assenza di informazioni sul tipo di virus che lo ha infettato.

Si tratta di una funzione estremamente avanzata, certamente al di là della portata dell'utente comune, ma è significativo vedere che una simile funzione è stata implementata, e può dare l'idea della direzione in cui si svilupperanno i prodotti antivirus destinati a rimanere sul mercato.

Peraltro la tecnologia della disinfezione euristica non è ancora a livello di maturità, e questo lo ammette lo stesso autore del programma nella documentazione, quando afferma che è in grado di funzionare in circa l'80% dei casi di virus sconosciuti. Tuttavia abbiamo effettuato una prova con un vi-

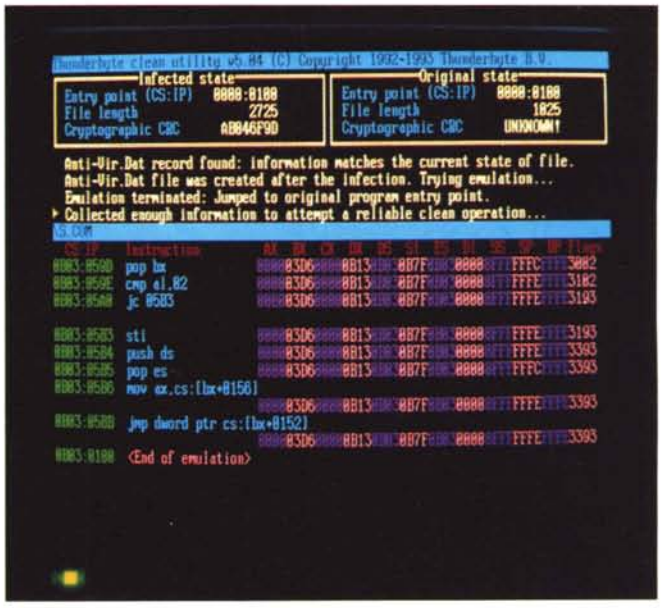
Le prove dei prodotti antivirus vengono effettuate in redazione su un PC Unibit 286 a 12 MHz con 640Kb di RAM, scheda Hercules e video monocromatico, disk controller ST-506, disco fisso Seagate da 60Mb e drive per floppy da 3,5« 1.44Mb.

Sul disco fisso sono installati i seguenti virus (il numero tra parentesi indica il numero di campioni differenti per i virus di cui sono presenti più copie e/o varianti):

512, 855, 1244, 1381, 1554, 4096, AIDS, AIDS-II, Alabama, Ambulance, Amoeba (2), Anarkia, Anthrax, Anti-Pascal (2), Anti-Pascal II (3), Attention, Bebe, Burger (3), Cascade, Crash, Dark Avenger (2), Darth Vader (3), Datacrime (2), Datacrime-2, Destructor, Devil's Dance, Fish 6, Flip, Fu Manchu, Icelandic (2), Invader, Jerusalem, JoJo, JoJo-2, June 16th, JW2, Kennedy, Leprosy, Liberty, Lisbon (2), Lozinsky, Murphy, Nomenklatura, Ontario, Oropax, Plague, Pogue, Polish 529, Saturday 14th, September 18th, Smack, Stupid, Suomi, Suriv-A, Sverdlov, Taiwan (3), Taiwan-3, Traceback, Typo-712, USSR-600, V801 (2), Victor, Violator, Old Yankee Doodle.

La collezione sperimentale di MCmicrocomputer, utilizzata per questa prova, contiene inoltre tre virus da boot sector: Stoned, Ping-Pong e Michelangelo.

rus recentemente scoperto in Italia (l'«Aragorn») e non ancora contenuto nell'archivio delle impronte dei più diffusi antivirus shareware. TbScan lo riconosce senza problemi, anche se ovviamente non sa dargli un nome; se l'installazione è stata effettuata in modo corretto ed è presente il file ANTI-VIR.DAT, TbClean riesce anche a rimuovere totalmente il virus, riportando il file infetto allo stato precedente l'infezione.



TbClean in opera per la disinfezione di un programma.

TBAV e Windows

Ci ha fatto molto piacere leggere ciò che è riportato nella documentazione a proposito della scansione sotto Windows, perché è perfettamente in linea con quello che scrivevamo nello scorso nu-

Controllo degli accessi? Grazie, sì (ma con serietà)

Sta lentamente prendendo piede una misura di sicurezza consistente nel controllo degli accessi.

Non stiamo parlando, ovviamente, del controllo posto all'accesso ai sistemi multiutente; in quel contesto il controllo è sempre esistito, e sebbene venga gestito con maggiore o minore affidabilità a seconda dei sistemi operativi su cui è implementato, costituisce di fatto la prima barriera di qualsiasi sistema di medie o grandi dimensioni.

Stiamo parlando di controllo dell'accesso alle risorse di personal computer. Sono molti gli ambienti che potrebbero trarre beneficio da una ben progettata struttura di controllo dell'accesso ai PC; il primo esempio che ci viene in mente è nell'ambiente bancario, dove si stima che il 45% dei posti di lavoro informatizzati si serva di personal computer, ma un sistema di controllo dell'accesso può essere utile anche a chi si serve di computer portatili: un notebook dimenticato su un tavolo può attrarre l'attenzione non necessariamente di un ipotetico ladro ma più semplicemente di un onestissimo collega di lavoro che vuole provare l'ultimo giochetto che gli ha riportato a casa il figlio.

I requisiti di un buon controllo degli accessi sono quelli di qualsiasi sistema di sicurezza: deve garantire la riservatezza, l'integrità e la disponibilità dei servizi. La porta deve restare chiusa per chiunque non sia autorizzato a entrare, e deve aprirsi immediatamente e con semplicità davanti a chi possiede la chiave. Ritorneremo in seguito e diffusamente sui dispositivi di controllo dell'accesso; per ora vogliamo guardare in dettaglio a una caratteristica, spesso trascurata assai più di quanto non meriterebbe: la chiave.

I sistemi attualmente conosciuti di chiavi informatiche sono di due tipi: a possesso di oggetto e a conoscenza di informazione. Spesso i due sistemi vengono combinati, ad esempio nel Bancomat. Il possesso di oggetto consiste nella definizione del requisito che distingue la persona autorizzata, in quanto possiede un determinato oggetto riconoscibile dall'elaboratore (tessera magnetica o a microprocessore o altro dispositivo), dalla persona non autorizzata che non possiede l'oggetto. La conoscenza di informazione definisce la persona autorizzata in quanto è a conoscenza di un dato noto (teoricamente) soltanto a lui e all'elaboratore.

In alcuni grandi sistemi ha preso piede da tempo il possesso di oggetto, più costoso in termini di investimenti. Ma la chiave dei più diffusi sistemi di sicurezza consiste nella conoscenza di una informazione, una «parola-chiave» o «password». Ed è questo schermo sottilissimo che divide il mondo in due, da un lato quelli che sono autorizzati a entrare e a servirsi delle risorse di un determinato sistema, dall'altro tutti gli altri.

E lo schermo è tanto più sottile quanto meno il sistema di password tiene conto di alcune basilari esigenze di sicurezza. Esaminiamone alcune in dettaglio.

— *Banalità:* un buon sistema di password dovrebbe impedire all'utente di fare uso di password banali. Purtroppo questo è un problema di difficile soluzione; le password banali sono facili da ricordare (es. codice «Toria», password «Stefano»), ma sono anche le prime che vengono in mente a chi vuole tentare di penetrare illegalmente un sistema. Tutti rammenteranno il film «War Games» e il famoso «Joshua»; questo è il più vecchio trucco da hacker, ma purtroppo funziona sempre perché spesso gli utenti dei sistemi di controllo di accesso non prendono la elementare precauzione di utilizzare una password non banale.

Alcuni sistemi, particolarmente ben progettati, arrivano al punto di imporre l'uso di una password non banale. È il caso del nostro MC-link, la cui password, composta da sei caratteri, deve obbligatoriamente comprendere almeno un carattere alfabetico maiuscolo o minuscolo (A-Z; a-z), almeno una cifra numerica (0-9) e almeno un segno di punteggiatura (.,—&^%, etc.). In altri casi viene lasciata la libertà all'utente di scegliere la password, ma suggerendo l'uso di una password complessa, eventualmente composta da più parole collegate da segni di punteggiatura. E non è necessario che la password sia incomprensibile, anzi è opportuno che sia facile da memorizzare. Un esempio: SMTF-550402, composta con le iniziali di una coppia di persone di mia conoscenza e la loro data di matrimonio.

— *Riservatezza:* è inutile scegliere una buona password se poi la si scrive su un Post-it e lo si appiccica sul frontalino del computer. Per questa ragione è opportuno scegliere password che abbiano un senso ben chiaro per l'utente, perché una password come quella dell'esempio precedente è più facile da ricordare (per il diretto interessato, ovviamente) che non una sequenza di simboli extraterrestri.

Ma un buon sistema di prevenzione va anche oltre: chiunque abbia un minimo di dimestichezza con la telematica sa che i più diffusi programmi di comunicazione consentono di automatizzare il processo di collegamento, compreso eventualmente l'invio della password. Il sistema è indubbiamente

mero. L'autore di TBAV ha previsto la possibilità di far eseguire alcune funzioni delle Utilities sotto Windows, ma non intende fornire una piena interfaccia Windows per il suo prodotto. Citiamo dal manuale: «Uno scanner sotto Windows non offre mai funzioni addizionali. Per contro (...) richiede maggiori risorse, diviene più grande e più lento, ed è meno affidabile. L'unico vantaggio sono schermate più attraenti. (...) [Inoltre] per affrontare i virus nascosti (stealth) è indispensabile avviare il Dos da dischetto prima di lanciare lo scanner. Ma avete mai provato a far partire Windows da un dischetto?».

Non crediamo di dover aggiungere commenti.

Protezione permanente

TBAV offre alcune funzioni residenti di protezione del sistema dalle infezioni da virus, e alcune altre non residenti. In particolare, sono disponibili uno scanner e un sistema di verifica dell'integrità, entrambi residenti; e dei programmi per il salvataggio e il ripristino di Master Boot Record/tavola delle partizioni e del contenuto della CMOS.

Anche il Boot Sector del DOS può essere protetto, sostituendolo con delle funzioni particolari di immunizzazione dalle infezioni.

Sono previsti inoltre dei programmi di monitoraggio delle funzioni critiche verso la memoria, verso particolari categorie di file su disco (tipicamente programmi eseguibili) o verso l'intero disco.

Funzioni per gli utenti registrati

TBAV è un prodotto shareware. In quanto tale può essere utilizzato prelevandolo da un qualsiasi sistema telematico, oppure acquistandolo da un rivenditore di shareware. Tuttavia per avere il diritto (morale, più che giuridico, almeno nel nostro Paese) di continuare a utilizzare il programma è necessario pagare il costo di registrazione; il produttore offre una varietà di «pacchetti», che comprendono diverse combinazioni delle funzioni sopra descritte; ciascun pacchetto costa all'utente singolo $24, il pacchetto globale $62. Sono previste inoltre delle offerte di site licensing a scaglioni crescenti, fino a un massimo di quasi $15.000 per oltre 3.000 licenze.

Gli utenti registrati hanno diritto all'assistenza gratuita in caso di incidente da virus; inoltre hanno accesso ad alcune funzioni supplementari, tra cui l'estra-

comodo, perché tutto quanto l'utente deve fare è scegliere da un menu il sistema a cui vuole collegarsi e a tutto il resto pensa il programma; ma se un estraneo mette le mani sul computer, ad esempio in occasione della riparazione di un guasto, la riservatezza delle password va a farsi benedire.

Sarebbe opportuno quindi non scrivere le proprie password su nessun supporto, cartaceo, magnetico o altro.

— *Variabilità:* le password «invecchiano». Per utilizzare una password la si deve digitare su una tastiera, e più la si utilizza più cresce la probabilità che qualcuno stia osservando mentre si digita e memorizzi la password. Ben lo sanno gli hacker, che proprio in questo modo si procurano «materiale» per il proprio «lavoro». Basta una fiera, una mostra di informatica, basta una standista un po' distratta (o, peggio, disinformata) e un hacker che tiene d'occhio la tastiera, e il gioco è fatto. Per questa ragione bisognerebbe cambiare spesso la password; anzi l'ideale sarebbe che lo stesso sistema tenesse il conto di quanto tempo è passato dalla data dell'attivazione della password, o dall'ultima volta che è stata cambiata, e imponesse all'utente di sostituire la password dopo un periodo di tempo ragionevole, diciamo venti giorni-un mese. Volendo migliorare le cose si potrebbe mantenere la traccia delle ultime password utilizzate dall'utente e impedire di riutilizzare le più recenti.

In ogni caso un sistema che non consenta all'utente di sostituire la propria password è estremamente insicuro e se ne sconsiglia l'utilizzo.

— *Solidità:* stavolta non spetta all'utente soddisfare questo requisito, ma all'amministratore o al progettista del sistema. Un meccanismo di controllo dell'accesso che preveda password non banali, che ne imponga la sostituzione ogni quindici giorni, che impedisca il riciclaggio delle ultime dieci password utilizzate, e che poi mantenga le password lì in vista, in chiaro, a portata di mano di chiunque, non è sufficientemente sicuro. Perché sarà difficilissimo entrare illegalmente, ma una volta entrati si avrà libero gioco, un eventuale hacker potrà farsi passare per chiunque.

Il sistema deve sapere quale password è associata a ciascun nominativo, e questo è ovvio, altrimenti non si vede come sarebbe possibile accedere al sistema. Ma al tempo stesso il sistema non deve consentire un facile accesso alla tabella di associazione tra nomi degli utenti e password. Il metodo più semplice consiste nella codifica della password, prima di inserirla nella tabella. Successivamente, all'atto della richiesta di accesso, l'utente digiterà la propria password che dovrà essere codificata e confrontata con il valore memorizzato nella tabella. Se i due dati corrispondono la password è esatta.

Il punto debole di questo schema sta nella solidità del metodo di codifica. Lasciare le password in chiaro, come abbiamo visto, è sciocco; ma anche una codifica debole può essere una cattiva misura di prevenzione. Prendiamo ad esempio un sistema di codifica che preveda lo scambio posizionale tra lettere adiacenti dell'alfabeto: a<=>b, c<=>d, etc.: codificando la parola «albero» viene fuori «bkafqp». Chiunque abbia un minimo di dimestichezza con la crittografia è in grado di decodificare questo codice in pochi secondi: la sicurezza non è sufficiente.

Uno dei sistemi operativi più diffusi, lo Unix, prevede un meccanismo di codifica delle password a senso unico; il suo inventore, Bob Morris, era talmente certo della sua impenetrabilità da ritenere superfluo che il file delle password codificate venisse nascosto, e infatti quasi sempre lo si trova lì bene in vista: /etc/passwd. Il ragionamento era semplice: se prendiamo la parola «albero» e la facciamo passare per il procedimento di codifica ne viene fuori una serie di caratteri apparentemente casuali, ad esempio «qwF55;Aa=09?7@1&».

Il procedimento non è reversibile, non esiste cioè alcun modo per risalire da «qwF55;Aa=09?7@1&» ad «albero», ma è ripetibile, cioè ogni volta che si sottopone la parola «albero» al procedimento viene sempre fuori «qwF55;Aa=09?7@1&».

Però se al posto di «albero» si codifica la parola «alberi» viene fuori qualcosa di completamente differente, ad esempio «6##?wN=^JI/pio2+». Anche stavolta, ogni volta che si codifica «alberi» vien fuori «6##?wN=^JI/pio2+» ma non c'è modo di risalire da «6##?wN=^JI/pio2+» ad «alberi».

Il file delle password, codificato secondo lo schema di Morris, sta seduto nella directory /etc e contiene la versione codificata della password di ciascun utente autorizzato. Nel momento in cui un utente chiede di accedere gli viene richiesto di digitare la password; ciò che egli scrive viene codificato e il risultato viene confrontato con quanto è contenuto in /etc/passwd. Se corrisponde, bene; altrimenti l'accesso viene negato. E quand'anche un utente si impossessasse del file /etc/passwd potrebbe farci ben poco: abbiamo visto che è sempre possibile passare dalla versione in chiaro a quella codificata ma che il passaggio contrario è impossibile.

Alcuni hacker particolarmente ingegnosi hanno divisato un sistema per ottenere il passaggio inverso, dalla versione codificata a quella in chiaro. Il procedimento, che non staremo a descrivere, si chiama «dictionary cracking», e presuppone due cose: che la password da decodificare sia banale, e che lo schema di codifica sia standard. È facile decodificare «qwF55;Aa=09?7@1&» e tirare fuori «albero», quando si sa come è stata fatta la codifica; ma non è possibile risalire a una password complessa, come ad esempio SMTF-550402, né si può decodificare alcunché se si cambia, anche di un minimo dettaglio, il procedimento di codifica.

Da ciò deriva la necessità dell'adozione simultanea delle misure di non banalità della password e di solidità del procedimento di codifica.

Stefano Toria

zione automatica di una impronta di riconoscimento da qualsiasi virus, da utilizzarsi in situazioni di emergenza, e la disponibilità di versioni differenti dello scanner residente, ottimizzate per i diversi microprocessori presenti su sistemi Ms-Dos (8086/8088, 80186/V20/V30, 80286, 80386/80486).

Un giudizio globale

L'impressione che abbiamo ricavato dall'analisi di TBAV è di un sistema scritto da qualcuno che sa il fatto suo, e che ha le idee ben chiare su come ci si difende dai virus.

Probabilmente l'utente sarebbe più contento se i vari programmetti che compongono il sistema fossero raccordati tra di loro da uno shell interattivo, che renda il tutto più user friendly, ma tutto sommato non se ne sente una forte mancanza: forse TBAV non sarà al primo posto nella classifica della identificazione corretta e precisa al 100% di ceppo e variante dei virus, ma fra tutti i sistemi che abbiamo provato è uno di quelli che ci sono piaciuti di più. MC

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170 tramite Internet all'indirizzo MC0170@mclink.it.

I virus dell'Archimedes

Come ogni computer anche l'Acorn Archimedes ha i suoi virus. Ma l'Acorn Archimedes non è come tutti i computer, c'è una differenza sostanziale oltre all'adozione di un processore RISC: il sistema operativo è su ROM. E i virus, allora, come funzionano?

di Andrea Gallo

Il sistema operativo è su ROM, ma ciò non significa — come si dice in giro — che i virus non possono diffondersi. È vero, invece, che all'accensione la macchina sarà sempre pulita, perché non si deve caricare in memoria nessun IBMBIO o IBMDOS o file come il COMMAND.COM. È già tutto pronto. Pertanto è vero che la situazione è molto meno grave rispetto a tutti gli altri computer. Eppure ci sono diversi modi di infettare un Archimedes, alcuni banali, altri più smaliziati. E ci sono anche i corrispondenti anti-virus o «scanner».

Potrebbe sembrare scontato, ma è bene precisare che, nonostante l'Archimedes possa utilizzare applicativi DOS tramite il suo PCEmulator, i virus PC non potranno mai diffondersi in un Archimedes, perché scritti per un microprocessore e per un sistema operativo completamente diversi. Casomai, potranno infettare la memoria riservata al PCEmulator o sporcare la partizione DOS dell'hard disk, ma non passeranno mai da un sistema all'altro, non infetteranno mai i file e i programmi RISC. L'unica interazione possibile per un virus tra questi due mondi altrimenti separati è cambiare la velocità del floppy e danneggiare i dischi dell'uno o dell'altro sistema.

Se i virus non possono infettare la macchina all'accensione e non possono risiedere nella memoria CMOS, perché lì per definizione non può esserci un programma, ma solo dati di configurazione, l'unico modo consiste nel porre una routine virus su disco, sia rigido che floppy, all'interno degli applicativi che vogliamo lanciare.

Nel RISC OS, il sistema operativo dell'Archimedes, ogni application che ha una sua icona nel desktop è in realtà costituita da una directory contenente almeno i seguenti file:

a) !Boot, il file eseguito automaticamente dal sistema operativo la prima volta che quest'ultimo «vede» l'applicativo (il RISC OS ha infatti una tabella contenente il nome, l'icona e il path completo di ogni application incontrata a partire dall'accensione della macchina). Serve per inizializzare alcuni parametri.

b) !Run, il file da eseguire ad ogni lancio dell'applicativo;

c) !Sprites, il file contenente l'icona in bitmap;

d) !RunImage o altro, il programma vero e proprio.

Il metodo più semplice per infettare un Archimedes consiste proprio nell'aggiungere al file di boot di un'application un'istruzione che attivi il virus. In questo modo il virus ha la possibilità di essere caricato in memoria solo una volta per ogni application dall'accensione della macchina.

L'altra via spesso usata consiste nel cambiare l'indirizzo di lancio di un file Assembler, facendolo puntare a quello di attivazione della routine di virus. Quest'ultima di solito viene aggiunta in coda al file, determinandone così un aumento nelle dimensioni. In questo modo il virus può essere attivato ad ogni lancio del programma assembler in questione.

Una volta attivato, il virus si comporta in diversi modi. Nel caso sia in Basic difficilmente può diffondersi molto e in ogni caso solo copiandosi in altre directory già «viste» dal sistema operativo e modificandone il relativo file di boot.

Qualora sia in Assembler, può modificare i vettori di sistema che gestiscono i load e save dei file su e da disco o RAMdisk. In questo modo può intercettarne le chiamate e riprodursi, modificando tutti i file in linguaggio macchina che incontra.

Per gli effetti di un virus, si lascia alla fantasia dell'autore. Nel caso dell'Archimedes, data la sua distribuzione ristretta soprattutto alla Gran Bretagna, i virus finora trovati sono quasi tutti di origine inglese, a parte uno o due di dubbia provenienza tedesca e fortunatamente sono quasi tutti innocui. Infatti, a parte il fastidio della loro propagazione e relativa occupazione dell'hard disk, solo un paio sono pericolosi.

La maggioranza di essi si limita a scrivere sul video messaggi spiritosi o anche offensivi in particolari occasioni, come tutti i venerdì 13 del mese (come il BBCEconet o il Link virus) o a Natale (come il MyMod o BigFoot). Alcuni si «divertono» a cambiare la configurazione della macchina, il numero di floppy disk disponibili, il tipo di monitor, la velocità del mouse e altro.

L'Extend e l'IrqFix decrementano lo spazio libero nella RMA (area riservata ai moduli di sistema) di 1Kb ad ogni attivazione.

Il più temibile è T2: in determinate date (1 gennaio, 14 febbraio, 25 dicembre e tutti i venerdì 13) cancella la mappa dei file e il settore di boot di tutti i floppy che incontra, rendendoli inutilizzabili, oltre a eliminare il settore di boot dell'hard disk. Poi visualizza a seconda del giorno un particolare messaggio seguito da una serie di insulti, oltre a cambiare la forma del puntatore del mouse in sconcezze varie.

Gli anti-virus

Ci sono vari programmi di pubblico dominio di rivelazione ed eliminazione di virus, come Guardian, Hunter, Interferon e Scanner. C'è poi il !Killer della Pineapple Software che, previa sottoscrizione, viene inviato aggiornato ogni tre mesi circa.

Analogo al VShield sotto DOS, VProtect è un modulo, fornito insieme a !Killer, che si installa residente in memoria e interviene a ogni chiamata di load o save e controlla le finalità della chiamata stessa, studiandone la provenienza.

In conclusione, seppure ancora pochi (circa 50), i virus per l'Archimedes si stanno diffondendo e occorre prendere opportune precauzioni. Per gli utenti nostrani ci sono due vie: mettersi in contatto con banche dati di pubblico dominio, quale l'ottima Res Publica di Cristian Ghezzi e Sergio Monesi (Res Publica, c/o Cristian Ghezzi, Via B. da Urbino 2, 20035 Lissone (MI)), oppure sottoscrivere l'abbonamento (25 sterline l'anno) con la Pineapple Software, 39 Brownlea Gardens, Ilford Essex, IG3 9NL England.

Fonte: AVRD — The Archimedes Virus Reference Document, 3 gennaio 1993.

TTI Artiscan
300, 600, 800, 1200 punti di riferimento.

I nuovi scanner a colori TTI costituiscono il nuovo punto di riferimento per velocità, definizione, fedeltà, numero di colori, flessibilità, prezzo.

• 24 BIT, ovvero oltre 16 milioni di colori • 4 modelli con rispettivamente 300, 600, 800 e 1200 DPI di risoluzione • Alta velocità grazie all'interfaccia SCSI meno di 10 secondi per una pagina con 256 toni di grigio e meno di 60 per una a colori • Collegabile a sistemi Macintosh e IBM compatibili

• Zoom: da 12,5% fino a 800% • Hardware Gamma Correction per immagini perfette • Luminosità e contrasto variabili da +100 a -100, con passo 1 • Software in dotazione: Colorshop 24 per Windows 3 o Macintosh, Aldus Photostyler per Windows, Adobe Photoshop 2 versione completa per Macintosh • Compatibile con i principali programmi di riconoscimento caratteri (OCR) • Slide scan kit opzionale per acquisire immagini direttamente da lucidi, diapositive, lastre radiografiche di qualsiasi formato fino all'A4.

ARTISCAN 300 DPI	**L. 1.500.000**
ARTISCAN 600 DPI	**L. 1.900.000**
ARTISCAN 800 DPI	**L. 2.500.000**
ARTISCAN 1200 DPI	**L. 3.900.000**
SLIDE SCAN KIT	**L. 900.000**

ATTENZIONE: Verificare al momento dell'acquisto che il vostro Artiscan sia corredato della garanzia Megabyte, unico importatore ufficiale. Megabyte non effettuerà alcun servizio di assistenza hardware e aggiornamento software sugli scanner sprovvisti di tale garanzia.

Gli scanner TTI sono distribuiti da:

MEGABYTE

DESENZANO (BS) - Via Castello, 1 - Tel. 030/9911767

E SONO IN DIMOSTRAZIONE PRESSO I PUNTI VENDITA DI:
DESENZANO (BS) - Piazza Malvezzi, 14 - Tel. 030/9911767
BRESCIA - Corso Magenta, 32/B - Tel. 030/3770200
BERGAMO - Via Scuri, 4 - Tel. 035/402402
GRUMELLO (BG) - Via Roma, 61 - Tel. 035/833097
VERONA - Piazza S. Tomaso, 10/11 - Tel. 045/8010782
MANTOVA - Via Calvi, 95 - Tel. 0376/220729

RIVENDITORI ED ACQUIRENTI PER CORRISPONDENZA
TELEFONARE ALLO 030/9911767 R.A.