Virus a Edimburgo: 2° convegno internazionale del «Virus Bulletin»

di Stefano Toria

Si è tenuto il 2 e 3 settembre a Edimburgo il secondo convegno internazionale organizzato dal «Virus Bulletin», una delle più autorevoli pubblicazioni che trattano i nostri temi. L'articolo di questo mese si sofferma sui vari aspetti trattati nel convegno, con particolare rilievo per gli sviluppi previsti

Due giornate intense

Edimburgo è una bellissima città che ho sempre molto amato. Mare, montagna e città si armonizzano perfettamente, e due o tre fabbriche di birra condiscono il panorama con il profumo dolce e corposo dei cereali cotti.

Se non fosse stato per il tempo, freddo e piovoso, sarebbe stata un'ottima scelta quella del Virus Bulletin, che qui a Edimburgo ha organizzato il proprio secondo convegno internazionale.

Nato nel luglio del 1989, il Virus Bulletin si è rapidamente conquistato una reputazione di autorevolezza e ha costituito il catalizzatore che ha portato tanti ricercatori di primissima qualità a lavorare insieme, dimenticando spesso le divergenze di vedute e in alcuni casi le aperte rivalità.

Rivalità che non hanno mancato di farsi sentire comunque nel corso delle due intense giornate dedicate all'analisi approfondita degli ultimi risultati della ricerca sui virus.

Insicuri e preoccupati

L'apertura dei lavori, con britannica puntualità, è alle 9:15 nel salone dello Sheraton Hotel di Edimburgo. La relazione introduttiva, tenuta dal direttore del Virus Bulletin Edward Wilding, traccia un quadro d'insieme di come viene affrontato attualmente il problema dei virus (cioè male) e insieme fornisce alcune indicazioni di massima sulle pratiche di «igiene informatica» che dovrebbero essere adottate da chiunque si serva di un computer.

La prima giornata avrebbe dovuto aprirsi con un intervento autorevole, quantomeno per la fama dell'oratore invitato a tenere la relazione d'apertura. Ma pochi giorni prima del convegno John McAfee ha dovuto annullare la propria presenza per via di un impegno intervenuto; gli organizzatori tuttavia sono riusciti a sostituirlo con un personaggio ancora più autorevole e carismatico.

Per gli esperti di virus e i semplici curiosi un po' informati Fred Cohen non ha bisogno di presentazione. Per gli altri basti dire che è l'autore di una pubblicazione che nel 1984 portò per la prima volta all'attenzione del pubblico scientifico la possibilità della costruzione di un virus informatico. Il curriculum di Fred Cohen è enorme; ha conseguito titoli accademici in tre università e si occupa di integrità avanzata delle informazioni, tutela dei dati, vita artificiale e informatica distribuita.

Nella sua relazione Cohen ha dimostrato come le barriere poste in atto contro i virus dai due più diffusi server di rete locale, Novell Netware e i server Unix, offrano in realtà ben poca sicurezza. Per fare ciò si è soffermato a lungo sui concetti di «attributi», «trustee rights» e «inherited rights» in ambiente Netware, dimostrando come il diritto di un utente a scrivere in un file dipenda talvolta dallo stato di centinaia di bit, e come tale situazione sia potenzialmente insicura.

Parlando di pratiche di sicurezza in rete Cohen ha commentato ironicamente l'indicazione, contenuta negli stessi manuali del Novell Netware, di attribuire ai file eseguibili i soli attributi di «read only» e «file scan» al fine di ottenere la massima sicurezza: in pratica l'unico server realmente sicuro sarebbe uno dal quale si può soltanto leggere, ma è ben difficile che un utente installi un server per poi limitarsi a leggerne il contenuto!

Non dissimile la situazione in ambiente Unix, dove gli attributi sono controllati dalle maschere di accesso, ben note a chi abbia familiarità con quel sistema operativo, e dove i problemi si riproducono in modo analogo.

Il lavoro di Cohen, svolto in collaborazione con la Queensland University australiana presso la quale egli è visiting professor, non si è ancora espanso al di là di questi due sistemi, ma da un'analisi sommaria e preliminare che è stata fatta sulla più recente versione di LAN Manager in OS/2 sembra che le cose lì non stiano molto meglio.

Struttura dei virus, oggi e domani

All'intervento di Fred Cohen ha fatto seguito quello di Jan Hruska. Abbiamo già avuto modo di presentare il dr. Hruska in occasione del convegno del Club sul Computer Crime che si è tenuto lo scorso maggio a Roma, al quale egli è stato invitato a tenere una relazione.

Hruska ha fornito al pubblico una impeccabile presentazione delle diverse tipologie virali, suddivise per modalità di attacco e per la scelta del bersaglio. Nel corso della relazione ha fornito anche alcune indicazioni sulle linee di azione che gli autori di virus potrebbero intraprendere in futuro, in particolare nella direzione di virus impossibili da rilevare con l'ausilio di uno scanner.

I «buoni» e i «cattivi» delle statistiche

La mattinata si è conclusa con la relazione di Jeffrey Kephart del centro di ricerche «T.J.Watson» della IBM.

Fred Cohen.

Molti hanno tentato di fare statistiche sulla diffusione dei virus, con risultati per lo più scadenti; alcune statistiche sono irrimediabilmente distorte per via del fatto che nascono più come argomenti di marketing che come effettivi lavori scientifici, mentre in altri casi sembra che le distorsioni abbiano avuto origine dal modo in cui erano poste le domande nel questionario. In ogni caso a tutt'oggi le statistiche veramente affidabili sono poche e hanno avuto scarsa risonanza, mentre ovviamente i media si sono buttati addosso ai sedicenti «esperti di virus» che vantavano improbabili statistiche con fattori di errore a livelli astronomici. Secondo alcuni, ad esempio, la diffusione del virus «Michelangelo» poteva collocarsi «tra lo 0,05% e il 10% dell'installato Ms-Dos»; traducendo queste percentuali in numeri viene fuori che il numero di macchine infette sarebbe stato compreso tra 25.000 e 5.000.000: un dato che lascia il pubblico privo di informazioni sul fenomeno.

Ma anche senza queste grossolane esagerazioni, che sono al limite tra la ricerca del sensazionale e la manovra di marketing, c'è la possibilità di ottenere risultati falsati anche in una ricerca peraltro condotta in modo accettabile, come è accaduto all'indagine svolta lo scorso anno da Dataquest, i cui risultati sono stati pubblicati nel novembre 1991.

Ma allora esiste un modo per fare correttamente queste estrapolazioni? Secondo Kephart la risposta è affermativa; egli si è soffermato lungamente sulle analisi a medio e a breve periodo e anche sulla stessa terminologia da adottare. Particolarmente rilevante ad esempio è la distinzione tra «numero di incidenti» e «numero di computer infetti», ed è essenziale che i due concetti non vengano confusi tra di loro.

Altrettanto importante è risultata, a un'analisi approfondita, anche la periodicità con cui vengono effettuate le analisi. Nelle statistiche trimestrali della IBM appariva una inspiegabile riduzione del numero di incidenti riportati nel secondo trimestre del 1992 rispetto a quelli riportati nel primo. Tabulando i dati rispetto a intervalli di tempo più ridotti, di due settimane anziché di tre mesi, si è visto che il crollo si verificava poco dopo il 6 marzo: è così risultato chiaro che la furibonda attività di caccia al virus nei giorni precedenti l'innesco del «Michelangelo» ha portato alla scoperta e alla eliminazione di una quantità di altri virus ben più diffusi, tra cui lo «Stoned», il «Form» e il «Cascade».

Due distinte sessioni

Nel pomeriggio le attività del convegno si sono divise in due diverse sessioni. Mentre da un lato si affrontavano argomenti come la cultura della sicurezza informatica in azienda, la implementazione di una strategia aziendale antivirus e la risposta delle banche ai problemi causati dai virus, dall'altro tecnici come Fridrik Skulason, Roger Riordan e Jim Bates discutevano sulle recenti tendenze riscontrate nella struttura dei virus, e su sistemi di classificazione e identificazione degli aggressori.

Fridrik Skulason.

Che cosa fare e come farlo

È questo il tema della relazione presentata da Gary Leader di KPMG Management Consulting, uno dei più grandi gruppi internazionali di consulenza presente in numerosi Paesi tra cui anche l'Italia.

Secondo Leader il problema va affrontato non soltanto a livello tecnico, ma anche e soprattutto dalla direzione dell'azienda; perché se è vero che i tecnici sono presumibilmente già sensibilizzati al problema, non sempre si può affermare lo stesso del management.

L'azienda si dovrà quindi dotare di strumenti adeguati, e di procedure opportunamente disegnate in funzione della struttura aziendale che debbono costituire la principale linea di difesa. Tutto il personale esposto al rischio deve seguire una formazione ad hoc. Le procedure debbono essere chiare, concise e debbono esistere in forma scritta. Ciascuno deve sapere cosa deve fare e a chi deve rivolgersi in caso si verifichi un evento sospetto. Non è sufficiente acquistare un pacchetto antivirus per tutelare il patrimonio informativo dell'azienda.

Il caso delle banche e delle grandi aziende

Nelle aziende di maggiori dimensioni il problema si moltiplica, e gli scambi crescono in modo esponenziale. Le due relazioni successive nella sessione aziendale, tenute rispettivamente da Mick Wigfield della Centre-File Ltd e da Paul J. Faulkner della Barclays Bank, hanno illustrato i rispettivi punti di vista delle due aziende, una grande società di servizi informatici e una tipica azienda del settore finanziario.

Gli aspetti tecnici, immancabili quando si tratta di virus, si sposano nel caso delle grandi aziende a considerazioni di carattere gestionale e organizzativo, che vanno tenute in identica considerazione nella creazione del sistema immunitario aziendale.

Dove stiamo andando

La sessione tecnica si è aperta con una relazione di Fridrik Skulason. L'autore di F-PROT, il prodotto antivirus che abbiamo recensito nello scorso numero (che in questa occasione mi ha consegnato personalmente la nuova versione, subito messa a disposizione degli abbonati di MC-link), ha esaminato i virus che si sono succeduti negli scorsi anni alla ricerca di possibili linee di tendenza.

I fatti più rilevanti sembrano essere soprattutto la tendenza a sviluppare sempre più virus con uno sforzo sempre minore, la maggiore disponibilità di virus, anche per via dell'esistenza di BBS clandestine dedicate allo scambio di virus, e l'aumento nel numero degli autori di virus; di positivo c'è da segnalare una maggiore cooperazione tra i ricercatori e una minore attenzione dei media al fenomeno dei virus.

Quest'ultima in particolare è una circostanza assai favorevole: si ritiene infatti che una delle motivazioni che spingono gli autori dei virus consista nella speranza che il proprio «prodotto» raggiunga la massima diffusione e la massima notorietà possibile; con il ridursi dell'attenzione dei media è possibile che si riduca anche questo tipo di motivazione.

Alcuni tentativi di analisi semiautomatica

Nella sua relazione Skulason ha accennato alla recente realizzazione di due kit per la costruzione di virus. Già da tempo si era ipotizzata la possibilità di realizzare questo genere di kit, e i ricercatori antivirus erano convinti che fosse semplicemente questione di tempo prima che se ne cominciassero a vedere in giro. Realizzare un virus diventa un'operazione semplicissima quando tutto ciò che si deve fare è scegliere poche opzioni dai relativi menu, e uno degli incubi che tormentano «Frisk» è che due-tre ragazzi in un paio di giorni siano in grado di mettere insieme un migliaio di virus diversi, metterli su un dischetto e mandare il dischetto a lui, con tanti auguri di buon lavoro.

Analizzare un nuovo virus è un lavoro difficile e lungo, e all'attuale tasso di crescita pari a circa due nuovi virus al giorno sta diventando quasi impossibile tenere il passo. È comprensibile quindi che si cerchi di automatizzare in parte il lavoro di analisi, come fa VI-RELATE, il sistema presentato da Roger Riordan.

È difficile che i nuovi virus siano interamente «nuovi». Gli autori di virus sono noiosi, i loro prodotti sono gene-

Vesselin Bontchev: da Oriente a Occidente, una carriera dedicata alla ricerca

Il nome assolutamente indimenticabile di Vesselin Bontchev è ben noto a chiunque abbia affrontato anche solo marginalmente il problema dei virus.

Laureato in informatica all'Università Tecnica di Sofia, già ricercatore e direttore del Laboratorio di Virologia Informatica presso l'Accademia Bulgara delle Scienze, è stato il primo a portare all'attenzione del mondo la «fabbrica bulgara» di virus, come egli stesso l'ha definita.

Questa sua posizione ha fatto ritenere ad alcuni, erroneamente, che egli fosse connesso con l'attività illegale in corso nel suo paese di origine, e c'è stato addirittura chi ha avanzato la fantasiosa ipotesi che l'or-

Vesselin Bontchev.

ralmente scritti male e senza il minimo guizzo di fantasia. Con la sola eccezione di Dark Avenger e forse di uno o due altri autori, non c'è nessuno nell'attuale squallido panorama che sia in grado di fare qualcosa di originale. Nell'analizzare un virus quindi è molto probabile che un ricercatore esperto si dica «questo l'ho già visto, ma dove l'avrò visto?». Con circa milleseicento virus in circolazione è verosimile che un semplice essere umano abbia qualche problema a rispondere a questa domanda.

VI-RELATE è ancora in fase sperimentale ma si propone come un sistema particolarmente efficiente nel soddisfare questa necessità, e lascia intravedere la possibilità di intense applicazioni nel settore della ricerca antivirus.

In una direzione simile si è mosso il Micro-BIT Virus Center della Università di Karlsruhe, realizzando un pre-processore di virus che fornisce una serie di supporti tecnici a coloro che hanno la responsabilità di capire cos'è che un virus effettivamente fa o tenta di fare. Christoph Fischer ha illustrato le possibilità di un simile strumento, attualmente in corso di sviluppo.

La giornata si è conclusa con la relazione di un altro personaggio fortemente carismatico. Jim Bates, ricercatore antivirus della prim'ora, ha illustrato con chiarezza e dovizia di particolari alcuni aspetti dell'attività di ricerca, in particolare quelli che portano alla minimizzazione dei falsi positivi e dei falsi negativi nel corso della scansione.

La «Gala Dinner»

Annunciata con discreto rilievo, la serata di gala che ha concluso la prima giornata di lavori è risultata una piacevole occasione per socializzare, formare nuove alleanze e consolidare le vecchie. In un'ambientazione spettacolare, forse con qualche concessione di troppo a un gusto un po' pacchiano all'americana, gli organizzatori hanno saputo offrire un'ottima cena scozzese completa di «haggis» (un piatto tradizionale delle Highlands) con annesso show di diversi interessanti personaggi, tra cui Jim Bates al sassofono.

Il resto del mondo

Quando si parla di virus nel 99% dei casi si finisce per parlare di tecnica o statistica dei virus in ambiente MsDos. A rammentarci che gli aspetti del problema sono anche altri hanno provveduto gli oratori della mattinata del secondo giorno, che nella sessione comune hanno trattato argomenti legali e giudiziari, oltre a fornire una visione dell'estensione del problema negli ambienti Unix e Macintosh.

La giornata si è aperta con l'intervento di Barbara Cookson, un avvocato di uno studio associato che ha acquisito una notevole esperienza nella problematica al confine tra tecnologia e legge.

mai mitico «Dark Avenger» non fosse altri che lui, o quantomeno che egli agisse attivamente per schermarlo.

Bontchev in realtà non ha niente a che vedere con l'attività di sviluppo dei virus in Bulgaria; conosce personalmente alcuni dei più prolifici sviluppatori di virus, ma ammette di non essere mai riuscito a incontrare Dark Avenger.

Quanto all'ipotesi che egli sia una sorta di «pentito» dei virus, in realtà L'unico peccato che gli si può attribuire è di avere incautamente distribuito, diversi anni fa, una copia di un dischetto contenente una versione attiva del virus «Vienna», come egli stesso mi ha raccontato in un recente scambio di messaggi in posta elettronica.

Vesselin Bontchev collabora attualmente con il Virus Test Centre dell'Università di Amburgo.

Credo che lei sia stufo di sentirsi fare domande sulla Bulgaria; ma c'è qualcosa di nuovo da dire sul suo Paese?

Sì, ci sono buone notizie. L'attività di sviluppo di virus in Bulgaria è diminuita in modo significativo; la ragione di ciò sta nel fatto che molte delle condizioni preliminari, che ho illustrato nella mia comunicazione dello scorso anno, non esistono più. Il sistema economico si sta modificando; si è riscontrato un rilevante sviluppo delle piccole aziende private e il tenore globale di vita sta cambiando.

Non c'è ancora nulla di definitivo in questo, tuttavia sta cambiando.

Inoltre la gente ha molto più bisogno di denaro rispetto a prima, perché l'inflazione ha portato i prezzi a livelli quasi equivalenti a quelli occidentali mentre i salari sono rimasti ai vecchi livelli. La gente deve darsi molto da fare, spesso con due o tre attività contemporanee, per guadagnare abbastanza da vivere. Perciò i programmatori esperti hanno ben poco tempo rimasto per creare nuovi virus.

Compreso Dark Avenger?

No, lui è un caso particolare e ne riparlerò tra poco. C'è da dire anche che molti degli autori di virus da me personalmente conosciuti non vivono più in Bulgaria: uno si trova in Olanda, un altro negli Stati Uniti, altri due in Francia e ce n'è uno che è all'estero, ma non saprei dire dove si trovi. Le difficili condizioni di vita in Bulgaria hanno determinato una notevole emigrazione di cervelli, in cerca di occupazione in altri Paesi. E anche nei Paesi in cui vengono ospitati debbono lavorare sodo, il che lascia loro poco tempo per scrivere virus.

Chi invece continua attivamente lo sviluppo di virus è Dark Avenger. Durante quest'ultimo anno in cui sono stato lontano dalla Bulgaria ha prodotto due oggetti molto significativi: il Mutation Engine e un nuovo virus, che non è apparso recentissimamente (è in mio possesso da tre mesi, forse anche di più), noto con il nome di «Commander Bomber».

Questo virus è stato inviato a un BBS di scambio di virus in Inghilterra, ed è stato inviato direttamente dalla Bulgaria. Ciò significa che questa persona si trova ancora lì e ancora scrive virus. Credo che stia cercando di dimostrare a noi ricercatori antivirus di essere in grado di scrivere un virus non identificabile dagli scanner. Infatti il Mutation Engine è un passo, la tecnica di infezione del Commander Bomber è un altro passo e il passo successivo è ovviamente la combinazione delle due tecniche. Sarà maledettamente difficile identificare un simile virus servendosi di uno scanner, soprattutto se si vogliono ottenere al tempo stesso una buona velocità di scansione e un ridotto livello di falsi positivi, o meglio ancora nessun falso positivo. Temo che sarà impossibile.

Passando a un altro argomento, può descrivere l'origine, la natura e l'attività del Virus Test Centre?

Non sono io la persona più adatta per parlarne perché mi trovo lì soltanto da un anno. Comunque si tratta del primo centro di questo genere in Europa, e di uno dei primi nel mondo insieme al CERT negli Stati Uniti.

L'attività del VTC consiste nello studio di virus per diverse piattaforme: al momento ci occupiamo di MsDos, Atari ST, Amiga, Macintosh e Unix. Non siamo ancora in grado di dare supporto agli Acorn Archimedes, ma ci stiamo attrezzando.

Abbiamo in progetto anche la conduzione di test di qualità sui prodotti antivirus, che è un'attività estremamente difficile da condurre in modo accurato perché abitualmente l'utente finale non ha l'esperienza per sottoporre a prova un prodotto antivirus e manca anche di una vasta biblioteca di virus da sottoporre ad analisi. Inoltre non basta essere in possesso dei virus: è necessario anche essere a conoscenza di diverse altre cose, ad esempio di come si scrive un buon programma antivirus, e verificare se ciascun programma rispetta le specifiche. È un lavoro difficilissimo, e al momento non abbiamo sufficiente personale per svolgerlo.

La nostra attività comprende inoltre una serie di scambi con altri ricercatori antivirus nel mondo; nei prossimi mesi saremo visitati da ricercatori provenienti dalla Cina e dal Giappone che verranno a lavorare da noi per qualche tempo.

Naturalmente teniamo anche corsi ai nostri studenti; non abbiamo un programma specifico sui virus, ma il prof. Brunnstein tiene corsi sulla sicurezza informatica in genere; inoltre insegniamo agli studenti a fare «reverse engineering» e a indagare sugli incidenti da virus.

La sua relazione ha proposto alcuni punti interessanti, sebbene l'ottica fosse prevalentemente quella della normativa in vigore nel Regno Unito. Tuttavia la raccomandazione alle aziende di stabilire con chiarezza i limiti imposti al comportamento dei propri dipendenti rispetto al sistema informativo, in modo da rendere ben chiari in anticipo quali siano i comportamenti passibili di sanzioni aziendali, va al di là della situazione locale e dovrebbe essere presa in seria considerazione da qualsiasi azienda.

Noel Bonczoszek, nonostante il nome di chiara origine slava, è un simpatico signore inglese sulla cinquantina, dall'aspetto placido dietro al quale si nasconde il poliziotto inflessibile. Membro di Scotland Yard dal 1970, fa parte della task force con la quale la polizia inglese ha ingaggiato la lotta alla criminalità informatica. L'attività della Computer Crimes Unit segue una linea attualmente ben definita dal Computer Misuse Act del 1990, una normativa avanzata in materia di illeciti informatici, che prevede esplicitamente virus, accessi illegittimi a sistemi informativi altrui e altri atti di pirateria e sabotaggio.

La normativa del 1990 impone alle vittime di incidenti virali di informare la polizia del fatto, fornendo informazioni circostanziate che possano servire da supporto alle investigazioni ed eventualmente al procedimento penale, nel caso che l'autore del virus venga identificato. E Bonczoszek è risoluto in proposito: anche se l'autore di un virus viene identificato in un Paese che non ha attualmente una normativa sui crimini informatici dovrà prima o poi accadere che gli venga in mente di venire a farsi una vacanza in Inghilterra, magari per perfezionarsi nella lingua: la polizia di frontiera sarà ben pronta e disposta ad accogliere un simile personaggio. D'altra parte non potrà durare a lungo il vuoto legislativo che esiste tuttora in alcuni Paesi, o almeno questa è l'opinione di Bonczoszek.

Due interventi tecnici hanno concluso la mattinata. David Ferbrache si è intrattenuto sulle possibilità di sviluppare virus in ambiente Unix, in una presentazione fortunatamente quasi del tutto teorica. «Fortunatamente» soprattutto dal punto di vista degli amministratori di sistema e dei proprietari di sistemi Unix, che possono per il momento dormire sonni relativamente tranquilli perché l'esistenza di virus in quell'ambiente, ancorché non sia di per sé impossibile (e i primi lavori di Cohen si svolgevano proprio in ambiente Unix), è resa molto difficile da una serie di circostanze; non si sono ancora visti in circolazione virus per Unix, né si prevede che se ne debbano vedere a breve scadenza. Ferbrache si è intrattenuto su diversi aspetti della sicurezza in ambiente Unix, soprattutto sulle tecniche di cui potrebbe servirsi un virus per diffondersi e sui modi di impedirlo.

Chris Johnson è analista di sistema alla University of Texas, ed è anche l'autore di uno dei più diffusi antivirus per Macintosh, il «Gatekeeper». La situazione per gli utenti Mac è notevolmente più rosea rispetto a quella in ambiente MsDos; c'è stato addirittura un periodo aureo, tra il giugno 1991 e i primi di quest'anno, in cui non è apparso nessun nuovo virus. Purtroppo la situazione è cambiata rapidamente, e un «diluvio» di nuovi virus si è presentato all'orizzonte nei primi mesi dell'anno in corso. Almeno, il viziato ambiente Macintosh ha ritenuto tale l'apparenza di quattro nuovi virus nel corso di pochi mesi.

Johnson ha presentato un quadro idilliaco, che ha fatto sospirare d'invidia alcuni dei ricercatori MsDos presenti nel pubblico: in ambiente Mac i virus sono pochi, facili da controllare e da intercettare e soprattutto è estremamente più pericoloso trafficare con il sistema di quanto non lo sia su un PC basato su CPU Intel; inoltre i ricercatori antivirus sono una confraternita affiatata che sin dall'inizio ha preso a collaborare, e le eventuali divergenze di opinioni non interferiscono minimamente con la piena circolazione di informazioni tra i ricercatori. Ogni volta che esce un nuovo virus colui che lo scopre lo mette immediatamente a disposizione di tutti gli altri ricercatori; ciascuno scambia liberamente con gli altri le informazioni di cui è in possesso, e si arriva in breve tempo a sviluppare le nuove versioni di tutti i prodotti antivirus esistenti.

In occasione dell'arrivo del virus MBDF lo scorso febbraio (i cui autori, due ragazzi di 19 e 20 anni, sono stati identificati e arrestati nel giro di una settimana) la macchina della ricerca antivirus si è mossa con la massima efficienza; appositi strumenti messi a punto in precedenza hanno permesso di analizzare in brevissimo tempo i 1.200-1.300 archivi di software di pubblico dominio sulla rete Internet, identificare le copie dei programmi infetti e toglierle dalla circolazione oppure disinfettarle.

Fino a qualche tempo fa gli utenti Macintosh hanno avuto la fortuna di non essere soggetti a virus intenzionalmente dannosi. La festa è finita, e il virus «Init 1984» scoperto lo scorso marzo è il primo virus per Macintosh con effetti intenzionalmente distruttivi. Si attiva in qualsiasi venerdì 13 in un anno successivo al 1990 (ma quanto sono originali questi autori di virus), e corrompe alcune informazioni identificative nel file system. Fortunatamente si tratta di un virus a infezione lenta, perché si trasmette esclusivamente tramite i documenti di sistema, che generalmente non vengono scambiati tra utenti.

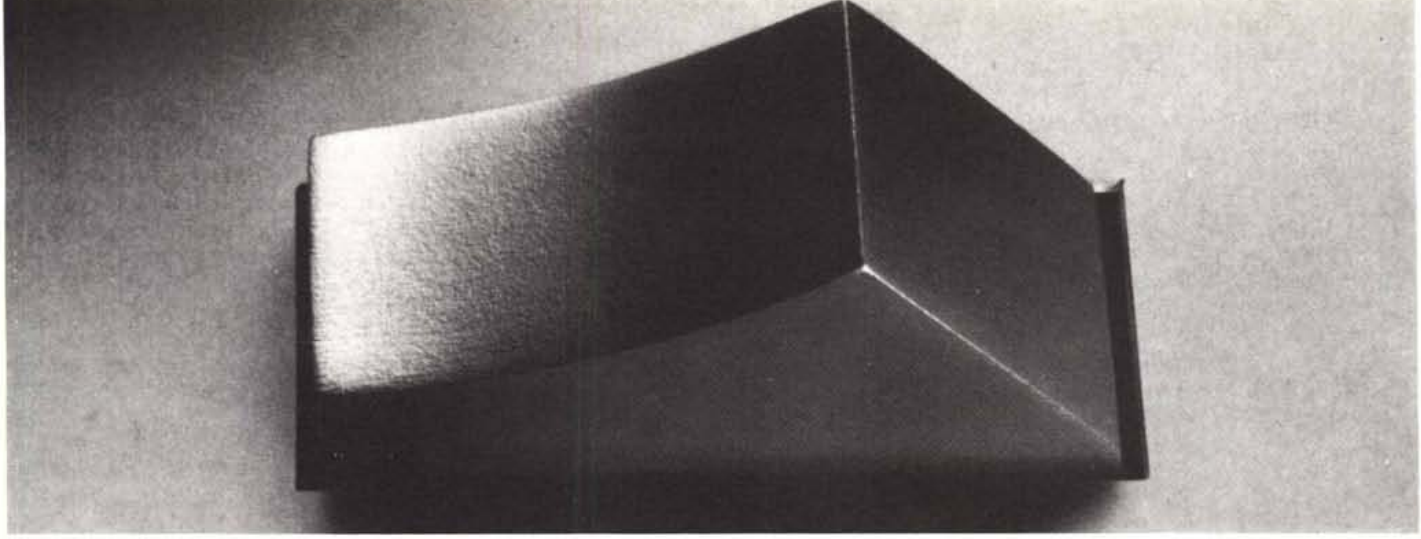
Tra gli interventi del pomeriggio sono risultati particolarmente interessanti quello di Vesselin Bontchev sui programmi di controllo dell'integrità, e quello di Jonathan Lettvin della Lotus Corporation.

Bontchev si è intrattenuto per qualche tempo sulle possibilità di condurre un attacco mirato ai programmi di controllo dell'integrità. Abbiamo già accennato in passato a questo tipo di programmi, e contiamo di soffermarci molto a lungo su di essi nei prossimi numeri. Si tratta in breve di programmi che anziché identificare i virus in base alla loro apparenza li identificano dopo che hanno effettuato anche una minima modifica in un sistema; hanno pregi e difetti, ma nel complesso sembrano promettere un notevole contributo nella lotta ai virus. Tuttavia è indispensabile che gli autori di programmi di controllo di integrità siano bene a conoscenza delle possibilità di attacco a questi sistemi, perché tutti gli attacchi possono essere facilmente evitati se gli autori mettono in atto alcune semplici misure preventive che Bontchev ha illustrato con dettaglio.

Jonathan Lettvin è un personaggio accattivante, capace di «magnetizzare» il pubblico (e l'uso di questo termine è intenzionale, vedremo perché). Nella sua relazione ha illustrato la strategia che la Lotus ha messo in atto per ridurre praticamente a zero il rischio di far circolare copie infette dei propri prodotti. E infatti i risultati sono ottimi: non si è mai verificato che un prodotto Lotus sia uscito infetto dai circuiti di produzione. Può accadere per contro che un prodotto venduto venga ritornato al negozio, dove viene nuovamente incellofanato e posto in vendita; è accaduto più volte che in questi prodotti sia stata riscontrata la presenza di virus, ma un'accurata analisi dei segnali magnetici sulla superficie dei dischi rispediti ai laboratori della Lotus ha consentito di determinare con certezza che i dischi infetti erano stati modificati dopo l'uscita dai centri di duplicazione, e che pertanto i virus erano stati introdotti successivamente.

I lavori si sono conclusi con una sessione comune con tutti gli oratori a disposizione del pubblico per un dibattito finale. L'appuntamento è per settembre 1993. MC

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



Accendilo e dimenticalo.

I modem ad Alta Velocità COURIER sono così affidabili che una volta accesi puoi dimenticarti di loro

Se anche tu pensi che un modem in grado di raggiungere velocità fino a 38400 bps non debba avere un temperamento tranquillo, ricordati che:

Solo i modem Courier hanno l' ASL™ , un sistema in grado di mantenere sempre la massima velocità consentita dalla qualità della linea telefonica.

Ti accorgerai della differenza già alla prima connessione.
I Modem Courier con l' ASL™ sono fino a 3 volte più veloci di altri modem V.32 bis.

Tutti i Modem ad alta velocità in caso di disturbi di linea abbassano la loro velocità di connessione, ma **due modem Courier connessi insieme sono in grado di risalire alla massima velocità non appena le condizioni della linea migliorano.**

I Modem Courier sono compatibili con una moltitudine di altri modem, poiché supportano tutti gli standard Europei ed Americani da 300 a 14.400 Bauds, inoltre funzionano sia in modo sincrono che asincrono.

U.S.Robotics
The Intelligent Choice in Data Communications

BLAST
Communications Research Group
A U.S. Robotics Company

Per sfruttare al massimo le capacità dei modem Courier, **U.S.Robotics Software vi propone BLAST**, un software nato per lavorare al meglio anche su linee disturbate, disponibile per una moltitudine di sistemi operativi e computers, MS-DOS, Mac, Unix, Xenix, Vax/VMS, Vax/Ultrix, ogni modello di Data General e Risc/6000 IBM.

BLAST con il suo potentissimo protocollo di trasferimento dati é in grado di effettuare **trasferimenti in full-duplex.**

BLAST, in caso di interruzione involontaria della trasmissione, é in grado di riprenderla partendo dallo stesso punto in cui é avvenuta l'interruzione.

NESSUN MODEM E' IN GRADO DI LAVORARE MEGLIO DEI
MODEMS U.S.ROBOTICS
NESSUN SOFTWARE E' IN GRADO DI LAVORARE MEGLIO DI
BLAST

COURIER + BLAST: LA SOLUZIONE VINCENTE !

Distributore per l'Italia:

SPIDER electronics

Via Boucheron 18
10122 - Torino
Tel. 011-530921/545712
Fax 011-531206