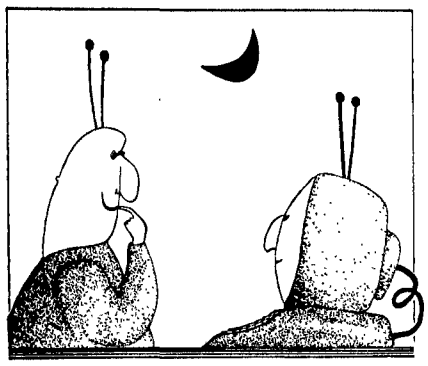


Il virus che ha bloccato la rete di elaboratori
Dietro la pirateria elettronica la saga di una famiglia
e una strana idea della creatività tutta «Made in Usa»

Pirati da computer orgoglio americano

Il virus che ha bloccato centinaia di computer negli Usa, mettendo fuori gioco la rete che li collegava, ha rivelato due storie così tipicamente americane da sembrare finte. Il «pirata» è un ragazzino che i genitori hanno allevato nell'adorazione maniacale per i computer e che a 14 anni «giocava» con i supercalcolatori dei laboratori Bell. La sua impresa ha suscitato più orgoglio che rabbia. La creatività delle nuove generazioni si misura in Usa anche su queste imprese. Il loro significato è indifferente. Conta la capacità di metterle in piedi e di portarle a termine con successo.

MARIA LAURA RODOTA'

WASHINGTON. Un raggio laser che, di notte, faceva splendere di luce innaturale un segnale di Stop, sconvolgendo gli automobilisti di Cambridge, Massachusetts. Un programma inserito nei computer usati dagli studenti della sua università, Harvard, che faceva apparire sugli schermi, improvvisamente, i ritratti dei compagni di corso. Un altro programma che provocava una tempesta elettronica sugli schermi ogni volta che uno studente sbagliava a scrivere certe parole sul computer. Poi, naturalmente, l'ultimo scherzo, il più celebre: un programma-virus introdotto di nascosto che ha bloccato 6.000 computer in tutti gli Stati Uniti e paralizzato la rete che li collega tra loro, tra università e università, tra laboratorio e laboratorio, nonché tra base militare e base militare.

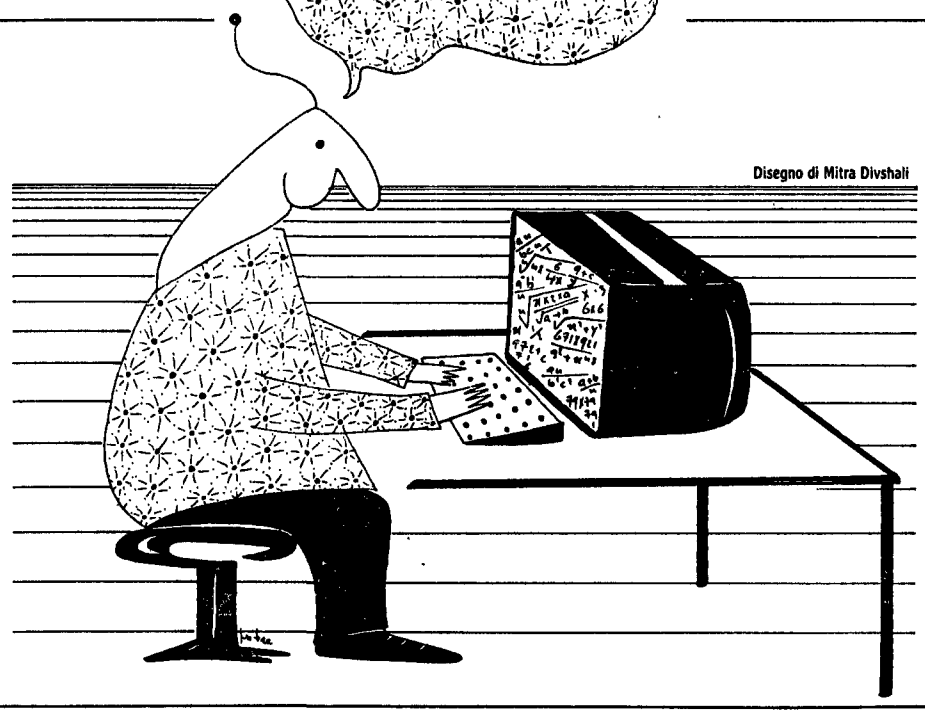
Questa volta, però, Robert Morris junior e davvero nei guai. I suoi dispetti goliardico-informatici degli anni di Harvard erano diventati punti a suo favore: i suoi professori alla Cornell University, dove Morris stava studiando per dottorato, hanno raccontato di averlo ammesso nel programma di «computer science» anche a causa della sua fama di «hacker», di mago dei terminali un po teppista. «Vogliamo gente creativa, qui», dice uno di loro Dexter Kozen. «E la creatività di Robert si manifestava attraverso i suoi scherzi da hacker. Il che ci andava benissimo». Ed è andata bene finché Robert non ha esagerato; e il Pentagono, che si è visto andare in panne il suo network di computer Arpanet, sembra meno intenzionato a incoraggiare il suo indubbio talento. Adesso, lo studente ventitreenne è stato messo sotto inchiesta dall'Fbi e dai dipartimenti della Giustizia di due Stati. Se si deciderà di mandarlo in tribunale, rischia una multa di alcune migliaia di dollari, e fino a un anno di carcere. Per il momento, ha ingaggiato un'avvocato, e aspetta notizie barricato in casa dei genitori, ad Arnold, Maryland, tra Baltimora e Washington. Bella casa, più di campagna che suburbana, vicina al luogo di lavoro di suo padre, Robert Morris senior. Che ha un ruolo in questa storia, e non solo in quanto parente stretto: Robert senior è scienziato capo al National Computer Security Center della segretissima National Security Agency, sede a Fort Meade; e uno dei massimi esperti americani di protezione dell'accesso ai computer; ed è il responsabile della sicurezza (e della difesa da intrusi elettronici) di varie reti di computer del governo americano; tra le quali, c'è quella messa in crisi da suo figlio, l'Arpanet.

La saga della famiglia Morris, finita sulle prime pagine dopo il grande disastro da virus di due mercoledì fa, ha scatenato curiosità e commenti. Per la continuità di interessi padre-figlio culminata nell'inserimento di un programma pirata nel computer del Masschusetts Institute of Technology, e in un piccolo errore di calcolo che ha fatto moltiplicare il programma a velocità centinaia di volte superiore al previsto, causando l'ingorgo nazionale. Per la vita di una famiglia innamorata dei computer come i Morris; che hanno insegnato a Robert, fin da piccolo, a fare di tutto con le tastiere, finché, a 14 anni, i dirigenti della Bell (dove lavorava il padre) gli hanno permesso di usare i loro terminali e di seguire i programmi sperimentali che venivano messi a punto. E per il neanche troppo nascosto orgoglio dei genitori, nonostante tutto, per le prodezze del loro figlio-hacker. Perché, per molti informatici americani, i giovani manipolatori non sono, come vuole l'opinione comune, «nerds», secchioni monomaniaci che, invece di giocare a basket e uscire con ragazze/ragazzi, passano le loro serate davanti al computer; sono, invece, la possibile carta vincente degli Stati Uniti nella competizione tecnologica. «Se ancora dominiamo il mondo del software, non è perché siamo più avanzati», suggerisce Paul Graham, compagno di corso di Robert Morris. «Noi produciamo il software migliore perché abbiamo la squadra vincente: composta da decine di migliaia di persone un po' matte che lavorano fino a tardi la sera». Chi è d'accordo con lui indica il caso della Silicon Valley, in California: dove tanti nuovi prodotti, e tante imprese ad alta tecnologia, sono nate nelle camere da letto e nei garage di hacker maniacali, come Steve Jobs e Stephen Wozniak, i fondatori della Apple Computer.

Qualcuno non è d'accordo. «Ho sentito dire: Morris ci ha fatto un favore. Ha fatto rendere tutti conto di quanto sia facile entrare in sistemi che dovrebbero essere protetti. C'è chi sostiene che è stata colpa nostra: non abbiamo risolto il problema in tempo. È un atteggiamento vergognoso», si arrabbia un nemico degli hackers, Eugene Spafford della Purdue University in Indiana. «È come quando, in un processo per stupro, si cerca di dare la colpa alla vittima. Che, magari, camminava da sola in una strada buia». Intanto, della prodezza di Morris continuano a occuparsi in molti. L'Fbi, che sembra stia cercando di calcolare a quanto ammontino i danni provocati dal blocco dei computer e dalla necessità di ripulirli dal virus; il National Computer Security Center, che la settimana scorsa ha riunito un gruppo di esperti per analizzare l'incidente.

Gli scienziati hanno rassicurato i preoccupati rappresentanti di dodici agenzie federali: quasi certamente, il virusa di Morris non produrra più danni. Qualcuno ha spiegato i piccoli errori che hanno trasformato lo scherzo in disastro; e qualcun altro ha sostenuto che programmi come quello creato da Morris potrebbero avere, in futuro, applicazioni legali e utilissime.

Il ragno telematico che cattura idee



Disegno di Mitra Divshali

Il computer sposato al telefono, cioè il calcolo automatico unito alle telecomunicazioni, stanno rendendo sempre più relativa e personalizzata la misura del tempo e dello spazio. Il *ragno telematico avvolge tutto il globo nella sua rete.* Anzi, l'idea stessa del risparmio sembra appaltata da un sistema integrato di tecnologie che fa viaggiare voci, messaggi scritti, calcoli, conoscenze di ogni genere in maniera ultrarapida.

È iniziata un'era nuova nella frequenza e qualità degli scambi d'informazione pubblici e privati prima di tutto per ragioni economico-scientifiche: trent'anni fa si concentravano in una sede unica grandi quantità di apparecchiature perché il costo per generare potenza di calcolo era molto alto. Adesso la microminiaturizzazione dei computer ha fatto passi da gigante. Ridotti i costi delle macchine, in proporzione sono care le linee telefoniche e la produzione si fa per dire della materia grigia da inserire in rete. Una sola linea serve più terminali piccoli, ma potenti come quelli grossi di un tempo.

Si può tracciare una mappa delle reti principali funzionanti:

1) Arpanet - Il settore più vecchio di Arpa-Internet. I due nomi vengono da Darpa (Defence Advanced Research Project Agency). Rete sponsorizzata dal ministero della Difesa Usa, collega parecchie migliaia di elaboratori eterogenei per dimensione e costruttore in gergo sistemi «ospiti». Funziona principalmente presso i più prestigiosi centri di ricerca, università e istituzioni militari statunitensi. Lo scopo è di facilitare la comunicazione fra ricercatori e di fornire un banco di prova per i nuovi sviluppi del sistema telematico. L'Italia vi è collegata tramite il Cnuce di Pisa. L'altro settore di Internet coordinato con Arpa si chiama Milnet, una rete interamente militare: 400 gli ospiti. Dopo il 1983, i nodi europei di Milnet sono stati separati in una rete chiamata Minet. Arpanet, Milnet e Minet sono le costituenti principali della rete dati della difesa americana.

2) Csnet - È la rete dei ricercatori in informatica. Concentrata negli Usa e in Canada, ha legami con affiliati in Australia, Francia, Germania, Israele, Giappone, Corea, Svezia e Inghilterra. In tutto 180 ospiti.

3) Ean - Rete sia americana che europea svolge servizio di posta elettronica, in modo conforme allo standard internazionale X.400. Numerosi gli ingressi (gateways) fra Ean e i servizi di posta elettronica delle altre reti internazionali. Gli investimenti per entrarvi sono l'acquisto del software (di basso costo) e l'accesso alla rete pubblica X.25 (Itapac per l'Italia). L'unico nodo Ean in Italia, per ora, è lo Iasi Cnr di Roma.

4) Bitnet - Rete cooperative che unisce 1500 ospiti situati in 21 paesi (Usa, Canada, Messico, Giappone, Austria, Belgio, Israele, Svizzera, Germania, Danimarca, Italia, Spagna, Francia, Olanda, Finlandia, Grecia, Irlanda, Norvegia, Portogallo, Svezia, Gb.). La prevalenza di ospiti è americana: 844 contro i 363 negli altri paesi; 130 in Germania, 38 in Israele che è alla pari con Francia e Olanda. In Italia 31. Collega università e centri di ricerca, ma non esclusivamente. Il settore europeo di Bitnet si chiama Earn; quello asiatico Asianet.

5) Earn - La rete delle accademie europee. Collega oltre 600 università e centri di ricerca. Insieme a Bitnet, Netnorth e Asianet costituisce un'unica rete internazionale per lo scambio di esperienze e idee nella comunità scientifica mondiale. Un sistema centrale, in ogni paese connesso, mantiene i collegamenti internazionali e offre servizi di interesse comune. Per l'Italia il Cnuce di Pisa, presso il quale è già in servizio l'ingresso che integra i servizi di posta elettronica di Arpa-Internet e Earn.

6) Hepnet - È la rete internazionale dei fisici delle altre energie. Responsabile per la parte italiana l'Infn.

7) Dfn - Rete nazionale della ricerca scientifica in Germania Ovest. Circa 30 ospiti e ingressi possibili in Earn, Csnet, Ean europea.

8) Uucp - Rete per gli utenti del sistema operativo Unix. Si estende sul Nord America e parti dell'Asia.

9) Osiride - Progetto affidato nel 1981 al Cnuce dalla Commissione generale per l'informatica del Cnr per costruire una interconnessione linguistica unificata fra computer di case diverse, tenendo conto della rete pubblica italiana Itapac.

Per l'Italia citiamo ancora la rete Organi - Cnr, che collega tutti gli Istituti e Centri Cnr. □ *R.A*

E se fosse la sua malattia infantile?

In realtà il virus del computer nasce più o meno con il computer stesso, assieme allo sviluppo dell'informatica. Negli anni Settanta si programmavano i calcolatori perché trovassero nella rete le macchine inattive e vi lavorassero dentro. Poi, qualche anno fa, Scientific American pubblicò un gioco nella sua rubrica dedicata alla «ricreazione al computer». Era la «guerra dei nuclei», programmi che si mangiavano a vicenda. Ebbe un successo tremendo. E dimostrò che il sistema informatico ha molti punti deboli che possono essere attaccati dalla sua malattia infantile.

ROSANNA ALBERTINI

«*Attenzione non è uno scherzo! Quello* che è successo all'università di Lehigh sta accadendo anche al Politecnico di Torino. Ma il nostro virus si comporta in maniera diversa: una pallina strana si aggira per lo schermo, rimbalzando sui bordi e sui caratteri delle parole. Quando la pallina si ferma, il computer è congelato. P. S. Se qualcuno viene contagiato noi abbiamo un programma di disinfezione». Il messaggio è del 7 dicembre 1987. Uno dei tanti scambiati fra università e centri di ricerca informatica e telematica, stando ai fatti di cronaca degli ultimi due anni. Le riviste specializzate moltiplicano articoli e suggerimenti per contrastare il fenomeno preoccupante dei programmi detti «virus» che immettono bachi in altri programmi e sistemi. Nessuna meraviglia fra gli esperti del settore, almeno fra i ricercatori del Cnuce di Pisa e i docenti dell'Isi (corso di laurea in informatica). Il principio che genera il virus, e il procedimento che lo diffonde, sono parte integrante del sistema di ricerca in ambito informatico, dall'inizio.

I computer sono oggetti fragilissimi, attaccabili, entrano in crisi in mille modi. «Al limite - dice Edoardo Bracci del Cnuce - sono meno difesi di un televisore o di una lavatrice, perché puoi entrare dentro di loro con una procedura logica inventata dalla mente umana che si incontra e interferisce con un'altra logica preesistente, un programma sempre fatto dall'uomo».

Partiamo, per spiegare, dal programmatore di laboratorio nella prima era del lavoro informatico. Al posto del personal c'era la stazione di lavoro personale collegata ad altre stazioni nello stesso edificio con una rete locale. Siamo alla fine degli anni 70. Viene scritto un programma per usare il tempo macchina inutilizzato. Eseguito su un elaboratore, questo programma era fatto in modo tale da sentirsi in dovere di cercare nella rete se altri elaboratori erano inattivi. In tal caso si autocopiava nella memoria, faceva i suoi calcoli e passava ad altre macchine. Fin qui niente di male, il fine era benefico, almeno quanto il produttivismo che lo aveva messo in campo. Ma nello stesso tempo era entrata pienamente in funzione una facoltà pericolosa, tipica dei virus che sarebbero venuti dopo, che è anche uno degli aspetti più importanti della programmazione: la facoltà del programma di *autocopiarsi*.

Un programma è una serie di istruzioni che operano su dati codificati in qualche forma, ma la funzione è ambivalente: si può considerarlo un insieme di istruzioni da eseguire, oppure un dato, per altri programmi che svolgono su di esso le loro operazioni. Il gioco diventa pericoloso quando è lo stesso programma che rivolge le sue operazioni a una copia di se stesso preso come dato. La copia deve poter essere eseguita e continuare all'infinito il lavoro di riconoscimento dell'altra copia che a sua volta diventa attiva e invasiva.

Gli effetti negativi della facoltà autoriproduttiva dei programmi diventarono di pubblico dominio per caso, in seguito a un miniconcorso proposto da A. K. Dewdney nella rubrica di computer Recreation della rivista Scientific American. Nel numero americano del maggio 1984 comparve uno schema di gioco chiamato Core War, nel quale due programmi cercano di distruggersi l'un l'altro. Lo schema della sua guerra di nuclei era lo stesso di un racconto di fantascienza in cui si ipotizzava un programma che, ogni volta che veniva azionato nel computer, faceva copie di se stesso su tutte le memorie di massa, infiltrandosi negli altri computer collegati, fino a distruggere tutti i dati e i programmi. Un altro programma faceva da contromisura, perché cancellava tutte le copie del primo, e alla fine distruggeva anche se stesso. Dewdney mise in vendita ai lettori su richiesta il codice di programmazione per due dollari. Arrivarono richieste a valanga, tanto che in pochi mesi furono pubblicati i programma virus e i «vermi» migliori proposti dai lettori.

La mente di un burlone, di un pirata ostile al mondo delle tecnologie, oppure di un criminale astuto può benissimo costruire un programma, o peggio inserire pezzi di programma nascosti che a un certo momento, non si sa quando, saranno attivati senza che l'utente sospetti la presenza dell'errore, né possa esercitare controllo preventivo. Il software ormai è un prodotto di mercato, dicono gli esperti che, se circolassero solo prodotti Doc, i virus non sarebbero comparsi. O sarebbero rimasti materia da esercitazione di laboratorio. Invece è dilagata la produzione pirata delle copie. Comunque nemmeno le ditte, attualmente, offrono vere e proprie garanzie sull'integrità della creatura. Leggiamo fra gli avvertimenti per l'uso: «In nessun caso siamo responsabili dei danni indiretti, dovuti a cause eccezionali. Le informazioni e le specifiche di questo documento sono soggette a cambiamenti senza avviso». Ancora: «Il programma non è garantito da questa ditta né dai suoi concessionari La ditta non garantisce che le funzioni contenute nel programma soddisfino le esigenze dell'utente o funzionino in tutte le combinazioni che possono essere scelte per l'uso da parte dell'utente. L'utente inoltre dovrà controllare il programma e ovviare a proprie spese a eventuali errori o malfunzionamenti». Si è autoriprodotto anche Ponzio Pilato. Ma dopotutto le regole del commercio mettono in guardia, si compra il rischio insieme all'oggetto. Il vero guaio per l'utente è di non sapere come è stato scritto il programma, e di non essere mai garantito che le indicazioni caricate nella macchina facciano solo quello che si aspetta. Perfino quando usa i giochini: all'improvviso, il giorno di Natale, un gioco di guerra ambientato nel deserto dell'Arizona con un fico d'India in mezzo al campo, ha qualcosa di strano; il cactus è diventato un abete di Natale. La cosa è divertente. Molto meno il caso di un software che copia cento volte un programma e ogni volta decrementa di uno un certo contatore, quando arriva a zero tutti gli archivi di disco sono cancellati. Per non dire del software avionico: si ha fiducia che tutto funzioni, altrimenti l'aereo sbaglia rotta.

Pare che la scadenza del '92 metterà ordine nell'anarchia di mercato imponendo un timbro Doc per tutta l'Europa, che uniformi le regole di validazione dei prodotti informatici. Per ora, ci assicurano, l'impatto dei portatori di virus non è catastrofico perché chi sa di essere esposto si protegge. Le forze armate non usano la Sip, come rete, e si servono di una rete privata. Le banche vanno via Sip, ma sono soggette a pirateria, e qui il problema non è il virus, bensì la manomissione. Si difendono crittografando i pacchetti che diventano mascherati come i messaggi segreti. E poi ditte di software serie e autorizzate ci sono. Ma c'è un problema nuovo: dai personal il virus sta passando alle grandi reti.

Tutti ne parlano, il caso Arpanet della settimana scorsa ha messo in allarme il mondo. «Non ti senti messo in crisi come uomo di scienza?» chiedo a Edoardo Bracci. E mi accordo che il mio interlocutore è terribilmente appassionato alla pericolosità del gioco. «La pirateria esiste da quando c'è l'informatica - risponde -, è in gamba, preme sui punti deboli di un sistema che ne ha tantissimi. Dieci anni fa uno studente pisano molto bravo aveva trovato il modo di fotografare la memoria del computer universitario, collegato al nostro, prelevando un'area dove c'erano tutte le parole chiave degli utenti, fisici, chimici, informatici. Un mare di tempo per scoprirlo. Una volta preso all'amo, gli è stata data una borsa di studio per laurearsi sulla ricerca dell'antidoto all'incidente che aveva creato».

Infine riconosce che è vero, importanti enti pubblici non si proteggono abbastanza; in fondo manca una cultura che abbia chiara la prospettiva della prevenzione.

Per ora abbiamo parlato solo della vulnerabilità della macchina computer tramite il software bacato o manomesso, ma c'è anche la fragilità della rete, della natura fisica del sistema di comunicazione fatto di fili, cavi, ecc. Chiediamo al prof. Renzo Orsini come vede il futuro della scienza informatica, in relazione alla gravità dei problemi che stanno emergendo. Ci risponde che il computer sarà più che mai uno strumento, come la penna o il pennello, dipendente dalla mano dell'artista. Però un mezzo assai potente alla portata di tutti. Di qui il pericolo: mentre l'elaboratore in sé è un oggetto neutro, l'informatica delle grandi banche dati, delle amministrazioni, per gestire soldi o attività militari, è pericolosa. Prevale la tendenza a delegare troppo alla macchina senza premunirsi. Non si è preparati a eventuali rischi. La ricerca scientifica sui modi di prevenirli non è in cima alla lista. L'establishment si sta svegliando adesso. In cima alla lista c'è un fare prorammi sempre più sofisticati, con comportamenti intelligenti, in grado di comunicare meglio con gli utenti, insieme alla tendenza ad automatizzare quante più informazioni è possibile. E si continua a sentire e a pensare la difesa e la prevenzione come un ramo secondario.