

## **Intruders informatici**

E' stato detto molto sui virus del computer. Ogni addetto all'informatica ed ogni responsabile di azienda che usa il computer per il trattamento delle informazioni e dei dati sa a grandi linee di che cosa si tratta. Ha certo sentito dire che esiste una varietà di fenomeni che vengono indicati con lo stesso termine. Sa, in ogni caso, che i cosiddetti virus altro non sono che programmi che in vari modi agiscono nel computer e provocano spavento o anche danni, più o meno gravi, a dati ed applicazioni (software). Questi programmi si propagano per tutte le vie per cui vengono comunicati dati e programmi (reti, dati, dischetti, supporti magnetici ...). Nel caso dei personal computer la via preferenziale sono i dischetti.

I virus vengono accuratamente nascosti nei dati o nelle applicazioni. Una volta arrivati nel computer, i virus rimangono inerti finché si verificano certi eventi. Questi ultimi li rendono attivi. La loro attività si manifesta in varie forme: si replicano utilizzando a loro beneficio memorie e tempo di elaborazione; danneggiano dati, applicazioni o entrambi; e si manifestano anche con messaggi più o meno scherzosi sul video dell'utente. In alcuni casi simulano complesse situazioni del tutto innaturali, quali la caduta verticale, quasi gravitazionale, delle lettere sul video, oppure danno all'utente la sensazione che la macchina si stia riempiendo d'acqua. In altri casi si limitano a far comparire una pallina o qualche messaggio. Non sono mancati virus che, sfruttando difetti di progettazione dei computer, riuscivano a danneggiare fisicamente parti del computer. Ciò è possibile facendo sì che ordini contraddittori e scorretti vengano dati a componenti che risultano sottoposti, di conseguenza, ad azioni fisiche capaci di danneggiarli, come ad esempio il corto circuito di una linea di alimentazione.

E' noto anche che non esistono sistemi assolutamente sicuri di protezione da questi intrusi. E' una difficile battaglia difendersi da agenti nemici che non si sa come attaccheranno. Una prima strategia sarà quella di impedire che entrino programmi non autorizzati. Sistemi di difesa di ingresso esistono e sono anche alquanto efficaci, soprattutto nei computer di medie e grandi dimensioni. Tali difese si basano sull'impiego delle parole d'ordine che l'utilizzatore delle risorse di elaborazione dovrà dare. Con più parole d'ordine entrare diventa difficile. Ma non impossibile. E laddove chi progetta di entrare clandestinamente è al corrente di difetti del sistema di difesa, il superamento delle barriere diventa relativamente facile. Naturalmente, non è un'attività che qualsiasi informatico sappia fare: occorrono persone molto, molto preparate per penetrare in un sistema di elaborazione ben protetto.

Una volta penetrati, occorre nascondersi, impedire che l'operatore che siede alla consolle si accorga di ciò che avviene all'interno. Esattamente come si sfugge ad una sentinella. Occorre eventualmente sfruttare ogni possibile disattenzione degli operatori al fine di impedire che la presenza dell'intruso sia scoperta. Quindi con molta calma si prepara il piano di intervento.

Naturalmente, ed anche questo è ben noto, esistono varie strategie di difesa dai virus conosciuti. Ciò è possibile poiché esiste ormai di fatto un complesso sistema di allerta per cui, appena un nuovo virus si manifesta, una serie di preparatissimi tecnici cerca di isolarlo e lo analizza; viene poi preparato un programma capace di sostituire i tecnici stessi nell'operazione di identificazione ed estirpazione del virus. Gli stessi programmi permetteranno anche di prevenire danni e la stessa propagazione del virus nell'interno del computer.

Tutto ciò ha fatto nascere un cospicuo numero di mercati di difesa ed ha sollecitato le società costruttrici di elaboratori e le aziende produttrici di software a cercare di prevenire danni, predisporre difese, e, soprattutto, ad iniziare una campagna tendente a capire come risolvere il problema.

Ne è nata una vera e propria economia (di guerra) che ha fatto perdere ore di lavoro a molti. In un primo tempo, la minaccia sembrava limitata ai personal. Lentamente, si è compreso che il fenomeno riguarda tutti i sistemi di elaborazione, sebbene con modalità differenti.

Ma chi fabbrica i virus? Le ipotesi si sprecano. Certamente, una certa frazione di virus è stata predisposta da chi intende scoraggiare la diffusione clandestina del software nei personal computer. E' molto improbabile che solo gli hacker e alcuni sviluppatori di software che non riescono a vendere correttamente i loro prodotti siano i soli sviluppatori di virus o cavalli di Troia. Il fenomeno è diventato alquanto ampio ed è certamente importante conoscerlo e dominarlo. Non poco si può ricavare dalla diffusione clandestina di virus o altro: ritardi nelle consegne, immagini negative sul fornitore, danni economici di varia natura, .... Non è quindi impossibile che alcuni moventi di quel genere possano essere intervenuti in taluni casi nella decisione di diffondere un virus. Si tratta, comunque, di un fenomeno underground e, come tale, di difficilissima decifrazione.

Naturalmente, anche con i virus del computer ogni medaglia ha il suo rovescio. E, per identificare il rovescio, non occorre far ricorso a dietrologie di varia natura. Infatti, il fenomeno degli attacchi ai sistemi di elaborazione, mettendo in evidenza una certa fragilità di tali sistemi, ha contribuito a promuovere un notevole impegno verso la realizzazione di sistemi più sicuri. Ciò non sarebbe certamente accaduto senza gli hacker, come si evince da un'analisi a posteriori (i sistemi non sono risultati sicuri all'attacco degli hacker).

Dunque la lotta intrapresa dagli hacker ha avuto lo scopo di indicare alla società rischi che gli addetti ai lavori hanno tranquillamente trascurato. Tali rischi sono seri e, senza gli hacker, avrebbero potuto dar luogo ad autentici disastri in casi di conflitti militari, politici o solamente economici. Dunque, la battaglia di quegli hacker che cercano di evidenziare la debolezza dei sistemi informativi denunciando le frequenti inconcludenze di esperti della sicurezza hanno un ruolo vitale nella costruzione della società informatica di domani. Ovviamente, è giusto che, laddove la legge prevede pene, gli hacker regolino i conti con la società secondo le modalità della legge. Ma è anche giusto che la società riconosca, non di rado, il valore costruttivo di quei gesti, quando non sono accompagnati da finalità distruttive.

Difficile dire quali siano state le conseguenze dei virus fino ad ora. Una complessa guerra psicologica è stata, in un primo tempo, giocata da alcuni che giustamente, segnalando la debolezza dei personal computer, indicavano nell'elaboratore centrale

la difesa da intrusi informatici di tutti i generi. Questa linea di azione psicologica non poteva lentamente non favorire la comparsa di fenomeni virali atti a smentire anche quelle tesi, come era facile prevedere. Puntualmente è stato così. Il fenomeno oggi è diventato alquanto uniforme e le difese vengono predisposte da tutti. Naturalmente la circolazione del software clandestino si è ridotta e, comunque, è diventata alquanto più guardinga. Molte organizzazioni hanno preso consapevolezza dei problemi della sicurezza ed hanno iniziato a studiare in modo sistematico i loro problemi. La consulenza sulla sicurezza ha tratto un po' di forza dalla diffusione dei virus e spesso ha organizzato corsi che trascurano un po' di analizzare la complessa traiettoria degli intruders informatici: chi progetta questi conosce bene le qualità del software esattamente come le conoscono gli esperti di sicurezza, ma assai spesso conoscono anche i difetti del software ed è questi che sfruttano per rendere difficile la difesa.

Quest'ultimo aspetto non è secondario al futuro dello sviluppo dell'informatica che non può considerare il fenomeno intruders come se non esistesse. Il problema è purtroppo autocontraddittorio: se si studia con cura il fenomeno degli intruders informatici si preparano persone che possono anche produrli. Se non si studia il fenomeno non si è capaci di costruire difese opportune.

La speranza che qualche genio possa da solo costruire una difesa assoluta da queste entità è stata matematicamente esclusa. Anzi c'è chi ha dimostrato che in teoria si possono costruire intruders immortali (nel senso che se il computers in cui sono immessi continua a funzionare, loro potranno continuare ad agire). La teoria però per ora può dare ben poco al fenomeno che si configura soprattutto nel classico rapporto guardia/ladro, rapporto che è stato da sempre alla base dello sviluppo degli armamenti.

Certamente, un grande genio della programmazione può fare molto per costruire sistemi di elaborazione robusti rispetto agli assalti di intruders. Ma, ahimè, nessuno può escludere che un tale genio sia disponibile anche a costruire intruders. E, nel caso i virus vengano usati per conflitti fra nazioni, si può giurare che la cosa si verificherà. Dunque che fare ora? Che sarà domani? Per rispondere a queste semplici e giuste domande occorreranno più anni.

Tuttavia, qualche cosa si può dire, se si inizia a guardare il fenomeno con gli occhi di domani, non più con gli occhi di ieri. E l'informatica di domani sarà proprio ispirata dalle conseguenze dell'esistenza degli intruders informatici.

Vediamo come. A questo scopo partiamo dall'osservazione del famoso intruder che fa giocare una pallina sul video. Questo intruders può essere considerato un agente che, entrando nello spazio di lavoro, si manifesta giocando (la pallina è solo una manifestazione). Per giocare, il nostro intruder deve disporre di una infrastruttura funzionante, la stessa infrastruttura che viene impiegata dalle applicazioni. Si può quindi immaginare un qualsiasi computer come una sorta di edificio in cui ci sono agenti che agiscono su certe entità (dati, segnali, immagini ...) ed infrastrutture. Gli agenti avranno a disposizione attrezzi da impiegare laddove tali attrezzi sono utili. Fra gli agenti riusciranno ad infiltrarsi anche gli intruders. Questi si nasconderanno quasi nel senso ordinario della parola: eviteranno che tentativi di scovarli possano avere successo o eviteranno di farsi notare pubblicamente. Così gli agenti che non intendono farsi scoprire non lanceranno palline visibili sul video, né parteciperanno ad azioni che

permettano di scovarli.

Gli agenti intruders saranno specializzati nel cercare di alterare gli ordini di servizio di altri agenti o di modificare le entità su cui gli altri agenti dovranno agire, alterando cioè dati, segnali, immagini, ... . Cercheranno di fare come certi roditori: tenteranno di indebolire le infrastrutture, in modo che l'edificio (l'architettura ) del sistema si danneggi ed inevitabilmente nascano difficoltà.

Questo sarà un caso estremo e sempre meno probabile poiché nel frattempo saranno comparse nella società usi non distruttivi degli intruders, mentre le infrastrutture diventeranno più robuste. Gli intruders copieranno certi dati, ne altereranno altri, introdurranno un po' di confusione, e comunque cercheranno di sopravvivere a tentativi di scovarli: faranno, non di rado, finta di essere stati scoperti e cesseranno le loro ostilità. Ma continueranno a vivere in attesa di nuove munizioni, di ordini o di altre parti. Lentamente, si annideranno nei sistemi di difesa, i quali sono molto complessi, così che i tecnici anche molto preparati avranno difficoltà a scovarli. E, se non saranno parte dei sistemi di difesa, li attaccheranno poco alla volta o con decisione, secondo tattiche che in taluni casi si sono già viste, dove certi virus, come prima parte della loro attività, hanno cercato di rendere innocui i cosiddetti vaccini.

Tutto ciò tuttavia non sarà la sola direzione del futuro. L'importanza della sicurezza e l'importanza che l'uomo sia ben presente responsabilmente avrà intanto sviluppato nell'informatica un atteggiamento antropocentrico. Tale atteggiamento, che è già ben osservabile oggi grazie al miglioramento del dialogo uomo-macchina conseguente all'impiego di interfacce grafiche d'utente (GUI), farà sì che il video diventi un posto di lavoro in un'organizzazione virtuale: sul video ci saranno gli elementi dell'organizzazione come in un'antica organizzazione senza computer. Si potrà parlare con il direttore, con i funzionari, con gli addetti come se fossero presenti. I dati si vedranno nascere, e se ne comprenderà l'essenza ed il significato. I modelli matematici, anche i più astrusi, potranno essere impiegati: in ogni caso questi modelli parleranno sul video lo stesso linguaggio dell'utente. E quest'ultimo girerà nell'organizzazione laddove gli sarà concesso (un utente normale non sa superare le difese previste). Spesso l'utente entrerà nell'organizzazione in forma di agente con delega limitata. Questa delega permetterà all'agente delegato dall'utente di andare nell'organizzazione per effettuare le operazioni delegategli. Naturalmente ogni utente potrà avere molti delegati. Allorché tali agenti entreranno, autorizzati, in parti dell'organizzazione di responsabilità di altri utenti, costoro potranno interrogarli per conoscere gli atti delegati. Gli agenti non di rado avranno la sembianza dei loro utenti. Anche le segretarie avranno segretarie: saranno i loro agenti che rovistano nei documenti per estrarne dati significativi da tenere ordinati: date, indirizzi, impegni, eventi...

Insomma, il video diventerà una sorta di vista su un mondo perfettamente comprensibile al suo utente. Gli spazi (virtuali) dell'utente come quelli dell'agente saranno resi visibili ed osservabili nella loro esternalità. E sempre più la tecnologia farà vedere qualche cosa in corrispondenza ad operazioni interne.

Ciò avrà molte conseguenze: sarà sempre più difficile che a invasioni di intruders non corrisponda qualche azione visibile (e le azioni informatiche

avranno spesso un ritmo umano come conseguenza dell'antropocentrismo emergente). Naturalmente, i dati trattati in gesti umani potrebbero essere non pochi: dovranno quindi essere accompagnati da tecniche di verifica che ne impediscano la contraffazione. Le infrastrutture saranno visibili costantemente sul video di qualche utente: non tutti vedranno la stessa infrastruttura. Ma qualche utente osserverà certamente, in periodi attivi, la sua infrastruttura. Inoltre, opportuni agenti osserveranno chi è in azione e faranno molti controlli, non solo sugli accessi quindi, ma anche sui gesti. Attacchi all'infrastruttura diventeranno così assai difficili e comunque spesso immediatamente osservabili. Ancora, poiché l'infrastruttura è sostanzialmente determinata da dati costanti, potrà essere facilmente ricostruita con rilevazioni da appositi supporti di sola lettura.

Per aumentare l'affidabilità, l'infrastruttura del sistema informativo sarà descritta completamente in ogni sua cellula: queste saranno costituite da elaboratori che, nella più probabile versione, corrispondono alle attuali work stations: cioè potenti elaboratori monoutenti, connessi in rete. Sia che cada la rete sia che altre celle vengano distrutte la (cellula) stazione lavoro che sopravvive potrà funzionare: basterà che legga nel suo indistruttibile archivio (ad esempio un CD ROM) la sua infrastruttura ed i compiti degli agenti meno recenti. Infrastruttura ed agenti non recenti saranno stati accuratamente registrati in un opportuno supporto indistruttibile (una sorta di DNA dell'organizzazione). Gli agenti più recenti non potranno essere stati registrati ancora, ma saranno pochi e comunque saranno ottenuti dalla combinazione di agenti già registrati. Poiché inoltre ogni stazione lavoro sarà dotata del "DNA" di tutta l'azienda, sarà sempre possibile usare una cella per sostituirla un'altra fuori uso per qualsiasi ragione. molta attenzione dovrà essere posta ai dati: tutti i dati dovranno fluire in modo ridondante su appositi archivi puramente passivi al fine che nessun intruders possa effettuare gesti dall'interno di quegli archivi (al più si potrà distruggere fisicamente l'archivio). Se la scelta della ridondanza (carta, supporti magnetici, supporti ottici, ...) sarà oculata, si potrà risalire con cura a tutti i dati prima dell'azione di qualsiasi intruders. Insomma, i rischi saranno praticamente quasi annullati.

E' interessante analizzare alcune possibili interpretazioni dell'immagine che abbiamo fornito dei sistemi informativi, che, fra l'altro, preferiamo chiamare sistemi informativi cognitivi. Secondo l'immagine che ne abbiamo dato, i sistemi informativi altro non sono che spazi strutturati nei quali utenti e loro agenti delegati effettuano delle attività con l'aiuto di strumenti. Le attività si esplicano su dati che gradualmente finiranno con il diventare un'orma o, se si preferisce, un'astrazione del reale.

Ma tali dati non rappresenteranno finzioni, ma autentici aspetti del reale ed una loro modifica ha un peso determinante sulla vita del reale esterno al computer (se si modifica uno stipendio in un programma, il danaro che viene assegnato all'interessato viene alterato di conseguenza). Dunque, gli intruders operano su una virtualizzazione del reale, oltre che sulle infrastrutture che rendono possibili tali virtualizzazioni. Ciò potrebbe consentire una notevole semplificazione dei problemi giuridici e potrebbe suggerire che, ad esempio, un'azione degli intruders su agenti delegati corrisponda ad un atto contro la

persona utente che ha delegato gli agenti. Un'azione contro le infrastrutture e gli strumenti corrisponderà ad atti contro il patrimonio (dell'utente? del proprietario del sistema?). Un atto contro dati, orme del reale, andrà considerato un atto sulla corrispondente realtà. Guastare uno strumento ed alterare un agente delegato (un programma) può avere conseguenze civili: queste andrebbero considerate nella valutazione delle conseguenze. Naturalmente, la diffusione su larga scala dovrà essere tenuta in conto nella valutazione di colpe e danni.

Infine, che dire di uno scherzoso intruder che non produce danni o ne produce di molto limitati? Potrà essere certo una forma di violazione di domicilio. Ma la valutazione della pena dovrà forse tener conto del vantaggio che deriva a chi riceve il virus dall'aver scoperto anzi tempo i rischi che stava correndo.

Giusto quindi punire, ma occorrerà riconoscere a chi ha prodotto quell'intruder meriti per la segnalazione. Ma se ciò non potrà essere fatto individualmente, la società nel suo complesso dovrà farlo. Nessun isterismo quindi contro gli intruders, ma solo attenzione e responsabilità, su tutti i fronti.

Tutto ciò sembra indicare che la lotta virus/sistema informativo (organizzazione) oggi iniziata, anche se continuerà, non vedrà perdente l'organizzazione. Una frazione dei gesti umani sarà certamente orientata alla trasgressione. Se il clima culturale sarà favorevole, la trasgressione avrà un solo significato: quello di irrobustire la società e le organizzazioni che ne fanno parte. Se il clima culturale non sarà favorevole, la trasgressione avrà ben altri significati. In tal caso le organizzazioni avranno imparato a difendersi grazie all'attuale campagna di esercitazioni messa in atto dagli hacker.

Ovviamente occorre vigilanza: infatti, intruders umani non hacker ma autentici sabotatori potrebbero avere imparato che la pace da virus indebolisce le difese. Quando saranno abbastanza basse, allora questi riattaccheranno. Ciò va evitato e, anche se tutto ciò ha un costo, un certo livello di presenza di intruders va accettato ed impiegato con cura per capire come organizzare difese, quarantene, valutazione di vaccini, preparazione di tecnici, scelta di consulenti...