

La cronaca della rete

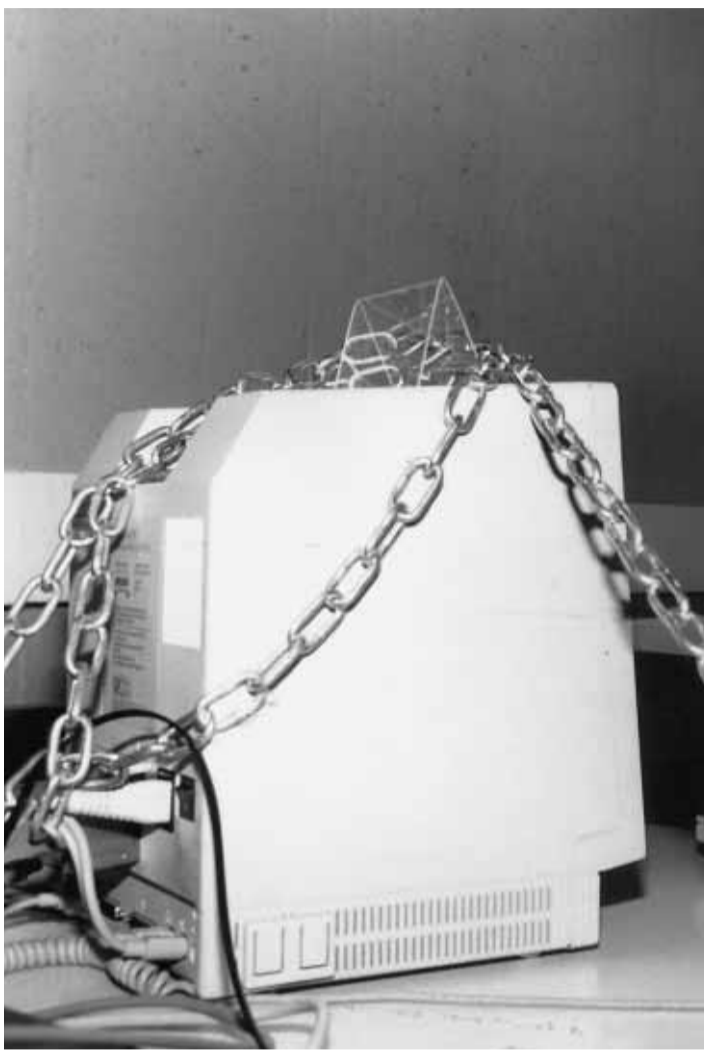
Cavalli di Troia e tunnel di servizio, le tecniche dei criminali informatici

Cos'è il computer crime? È una domanda che ci viene posta spesso e pertanto abbiamo deciso di illustrare - in maniera semplice - qualche caso di crimine informatico e alcuni dei termini usati quando si affronta l'argomento per spiegare che cosa può avvenire alle persone, alle aziende o agli enti colpiti. Un argomento che cominciamo ad affrontare in questo numero del Cibervillaggio tentando di chiarire cosa si intende con il termine di "computer crime" che tutti usano, ma cui spesso vengono dati significati non perfettamente in sintonia col suo senso storico. Una premessa che porterà a definire come crimine informatico qualsiasi atto improprio commesso attraverso i sistemi informatici (primo fra i quali, ben inteso, il computer) o concernente l'uso di tecnologie legate all'informatica.

Non è che sia così importante dare una definizione scientifica al crimine informatico, ma è bene avere le idee chiare. Secondo molti studiosi, il computer crime è quell'evento criminoso che si compie ai danni di un terzo, attraverso l'uso illegale di mezzi informatici e su questa enunciazione tecnici e giuristi hanno sfornato un'infinità di teoremi. Per altri, e noi condividiamo questa idea, bisogna invece attribuire al concetto di computer crime un significato più ampio che abbraccia qualsiasi uso improprio - sia esso criminoso o meno - di apparecchiature informatiche.

Ovviamente siccome in tutti i Paesi l'evoluzione della tecnica e quella della legislazione non seguono i medesimi ritmi (e quindi generalmente le leggi vengono aggiornate sulla base di casi già avvenuti), vi è molta confusione sulle definizioni e sulla classificazione del computer crime.

Alcuni esempi concreti? Generalmente anche la falsificazione di una carta bancomat viene fatta rientrare in questa fattispecie. Molti però sostengono che non si tratti di un vero e proprio computer crime, ma che questo tipo di reato debba essere considerato alla stregua della semplice contraffazione di un "documento" o alla falsificazione di denaro, anche se per manipolare la



L'avvento dell'editoria elettronica e quindi dei sistemi automatizzati da un lato ha semplificato i compiti degli addetti ai lavori, ma dall'altro ha creato non pochi problemi nella sicurezza.

Mentre una volta era ben difficile riuscire a penetrare in un giornale alterandone i dati che venivano digitati con del piombo in enormi linotype (materiale di per sé falsificabile solo intervenendo fisicamente) con i moderni sistemi, dove tutto è in rete ed in formato elettronico, questo mondo sta diventando il paradiso degli hackers che, con obiettivi specifici o meno o soltanto per gioco, riescono con estrema facilità a penetrare nei sistemi e a fare "scherzetti" come, per

esempio, quello riuscito a Louis Richardson che ha giocato un brutto scherzo all'Herold Tribune approfittando del fatto che la trasmissione dei dati del giornale tra le varie nazioni sono online ormai da svariati anni.

Da molto tempo Louis Richardson riusciva a penetrare nel sistema e leggere comodamente il giornale e a furia di "smanettare" con il computer un giorno riuscì a penetrare nella rete dedicata da e per la redazione principale e nel sistema automatico di impaginazione e stampa.

Una domenica il quotidiano doveva uscire con un gran numero di pagine, ma era a corto di personale. I controlli furono quindi

banda magnetica di una carta bancomat occorrono dei mezzi informatici. E con lo stesso ragionamento se un criminale riesce ad avere da un dirigente la password per entrare nel sistema informatico di una banca e quindi potrà eseguire un trasferimento elettronico di fondi, questo tipo di crimine viene considerato, da alcuni, come un'infedeltà del dipendente.

Disquisizioni giuridiche da lasciare agli esperti di diritto, mentre in un'ottica maggiormente tecnica ci sembra preferibile adottare una visione allargata e far rientrare sotto l'etichetta di "computer crime" tutti i crimini commessi con l'ausilio di sistemi informatici o telematici (qualsiasi essi siano e con qualsiasi mezzo vengano eseguiti) anche se per provocarli ci si è avvalsi anche di altri mezzi, come ad esempio l'infedeltà di un dipendente, la minaccia di un attentato o al limite, anche se non vi è alcuna intenzione criminosa, il penetrare o interrompere un

sistema dipendente da un apparato informatico. Chiarito il concetto nel quale ci muoveremo ecco alcuni dei più comuni sistemi di attacco usati dai criminali informatici per entrare nei computer e nei sistemi. **I Cavalli di Troia:** il nome non lascia dubbi e normalmente si tratta di un programma che è mostrato all'utente indicandolo come una soluzione o un'implementazione del proprio computer utile per incrementare l'efficienza del sistema. Dietro l'apparenza invece si trovano nascosti altri programmi invisibili all'utente che una volta all'interno del sistema possono causarne la distruzione completa. Nei casi più intelligenti i Cavalli di Troia scatenano la propria opera distruttiva grazie ad un meccanismo legato ai tentativi o al tempo. Al secondo o al terzo uso del programma "pulito", oppure a una determinata ora o in un certo giorno, si attiva il programma nascosto.

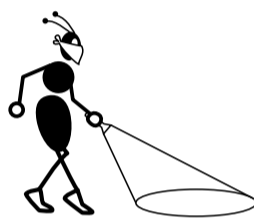
Il Tunnelling: è una delle

tecniche più sofisticate che si può tramutare facilmente in un attacco. Normalmente, il metodo del Tunnelling è usato per trasferire i dati tra due sistemi di computer in rete, incompatibili fra loro. I dati sono preparati a pacchetti e trasferiti tra una rete e l'altra. Chi usa in maniera illegittima questo sistema, non fa altro che preparare il pacchetto dei dati e invece di trasferirli nella rete legittimata a riceverli, li trasferisce ad altra rete o altro sistema.

Le entrate di servizio: uno dei più classici attacchi al software sfrutta le Trap Doors (specie di entrate di servizio) usate dai programmatori per entrare rapidamente in un programma "by-passando" i sistemi di sicurezza che sono stati predisposti nel software. Se un programmatore prevede di modificare in futuro un programma, usa normalmente il sistema della "Trap Door" ed invece di adottare il normale sistema che userebbe l'utente per entrare nel programma vi accede da una scorciatoia che normalmente viene eliminata nella versione finale del programma, quando tutti i test dello stesso sono completi. A volte però, intenzionalmente o non, queste rimangono nel programma; alcune altre possono essere immesse per errore nel software, e magari scoperte casualmente.

Una tipica Trap Door usa dei sistemi e dei Tools che permettono di convertire automaticamente alcune aree del programma, da riservate e nascoste, in accessibili. Fortunatamente, per usare questi sistemi occorrono dei criminali informatici esperti. Le Trap Doors rappresentano però un modo facile per entrare in un sistema, per avere accesso a informazioni riservate o per immettere virus o altri programmi nel sistema stesso, avendo così a disposizione una specie di entrata riservata e sconosciuta ai più (a volte Trap Doors si chiamano anche Back Doors).

Riuscire a determinare l'esistenza delle Trap Doors è un'operazione abbastanza complessa che richiede personale altamente specializzato e possibilmente la presenza degli autori del programma.



Computer crime

Attacco alla notizia

ridotti al minimo indispensabile e fu lì che il "buontemponone", nella notte del sabato, ebbe l'idea di aumentare la dimensione verticale di alcune immagini, provocando il taglio di alcune righe degli articoli. Pertanto il giorno dopo il giornale uscì senza buona parte degli articoli.

L'hacker fu preso perché il giorno successivo acquistò un numero consistente di copie e prese a vantarsi del colpo che gli era riuscito con degli amici. Qualcuno lo riferì alla polizia che nel computer di Richardson reperì tracce dell'azione commessa perché, si giustificò Louis Richardson, da tempo inviava le lettere al giornale, ma nessuno gli aveva prestato attenzione.

Novità nel cybershop

Dalla Quark programmi per creare qualsiasi prodotto editoriale



Dire Quark vuol dire una delle software house più importanti nel mondo dell'editoria in genere e particolarmente dei giornali.

In pochissimo tempo questa giovane azienda produttrice di programmi che ha sede a Denver in Colorado è riuscita a diventare un punto di riferimento nel mondo della carta stampata (ed oggi anche delle realizzazioni multimediali) grazie alla pietra miliare posta da Tim Gill e Fred Ebrahimi (i due fondatori della società) undici anni fa. Nel 1987, infatti, dopo 6 anni di ricerca iniziata con la fondazione della Quark nel 1981, i due sfornarono QuarkXPress, il software per Macintosh che ha rivoluzionato il sistema di composizione grafica e di edizione di giornali, riviste, libri e prospetti.

Il successo nel settore tanto del prodotto quanto delle idee della geniale coppia fu tale da portare la società ad acquisire una posizione leader in tut-

to il mondo. Non vi è, infatti, Paese o giornale, modernamente attrezzato che non usi questo software. QuarkXPress è sempre presente indipendentemente dalla lingua e dai caratteri usati nella pubblicazione siano essi cirillici, cinesi, giapponesi, arabi o quant'altro. Tanto più che QuarkXPress ha dato vita a una serie di tools, come QuarkXPress Passport, che permettono di impaginare una pubblicazione in qualsiasi lingua, tradurla e stamparla.

I vantaggi per le società editrici, ma anche per le grandi e piccole aziende che hanno rapporti con tutto il mondo, per la preparazione di prospetti o altri stampati in differenti lingue sono evidenti.

Nel 1992 la Quark, intuendo il futuro di quanto sarebbe accaduto con Internet, ha creato una serie di prodotti integrati tra loro, che hanno dato vita ad un sistema completo di desktop publishing e un sistema digitale di

presentazione di aziende e prodotti denominato Quark Digital Media System.

Nel 1996, pronta all'entrata nel terzo millennio, la Quark ha iniziato la presentazione di un prodotto estremamente innovativo fondando una divisione denominata QuarkImmedia, con un prodotto omonimo che rappresenta e rappresenterà la rivoluzione totale dei sistemi di comunicazione di massa sia cartacea, che su Internet. Il prodotto può realizzare davvero tutto quello che riguarda la comunicazione.

In sostanza si tratta di un'implementazione e non solo di QuarkXPress che si trasforma così in un sistema aperto in cui gli sviluppatori possono integrare autonomamente le proprie personalizzazioni. Il prodotto però può anche creare progetti e comprimere font di carattere. Ma soprattutto sarà esteso a piattaforme non Macintosh ma anche Window. Le pre-



Con XPress l'azienda ha rivoluzionato la carta stampata, con Immedia si lancia nel multimediale

sentazioni ottenute con QuarkImmedia saranno completamente interattive e allo stesso modo si potrà importare o esportare file di qualsiasi genere.

I supporti potranno anche avere la forma di Cd-Rom e quindi il prodotto è adatto per produzioni digitali su qualsiasi supporto opto magnetico. Con esso potranno essere creati suoni, immagini, effetti speciali, che vengono oggi comunemente usati nell'industria del cinema e nella televisione.

Si è badato particolarmente a Internet e alla necessità che hanno oggi le aziende di far vedere in tempo reale un prodotto funzionante nelle sue particolarità ad un cliente che è, magari, in Nuova Zelanda.

Tutto questo sarà possibile con la rivoluzione rappresentata da QuarkImmedia. L'ultima trovata della Quark il cui sito è visibile su Internet all'indirizzo www.quark.com dal quale si possono scaricare bellissimi e interessanti demo.

@ E-mail @

In Ticino si sta creando una radio on line

«Egregio signor Penco, seguo con interesse la pagina Cibervillaggio in quanto sto sviluppando una radio in Internet. Dopo esperienze negative con QuickTime3 per quanto riguarda la parte audio e video, vorremmo avventurarci con Real Player che, a quanto sembra, dovrebbe risolvere i nostri problemi di ascolto immediato senza che l'utente debba scaricarsi pesanti file audio-video prima di ascoltarli e di vederli. Infatti Real Player permette all'utente, dicono, di ascoltare e vedere mentre si scaricano i file.

Cosa conosce di questo programma? Conviene comperarlo direttamente dall'America (o

dalla filiale a Londra) o ci possono essere problemi? RealPlayer comperato come spiegato sopra è uguale a quanto venduto da EUNET?

Per il momento mi fermo con la bordata di domande, sperando di ricevere da lei preziosi consigli. Cordiali saluti»

EGON MAESTRI

Caro signor Maestri, innanzitutto complimenti per l'iniziativa di cui, spero, in futuro ci farà conoscere i progressi. Debbo dire che in molti si stanno buttando in questa attività e fare i pionieri è senz'altro difficile anche se è ormai sicuro che la direzione non è sbagliata

tanto che anche le case costruttrici di software e hardware si stanno concentrando in questa area.

Per quello che riguarda i programmi debbo dire che la nuova versione di Real Audio è un buon prodotto e lo stesso vale anche per RealPlayer che viene sviluppato da una équipe di israeliani che conosco e a proposito del quale potrò darvi più ampie informazioni su aspetti specifici.

Dove comperarli? Anche online direttamente negli Usa oppure dove lo si paga di meno e dove è reperibile la versione più aggiornata. Da quanto so EUNET usa una versione specia-

le definita Oem che non ritengo abbia limitazioni. Il consiglio per il vostro progetto è quello di acquistarne una copia originale professionale ed integra.

Vorrei comunque ricordare che il problema della buona e rispettivamente della cattiva qualità dell'ascolto non dipendono solo dal software ma anche da un'altra serie di fattori fra cui i più importanti sono: la velocità di accesso ad Internet e conseguentemente il tipo di linea (normale o Isdn) e di modem (il migliore è l'analogico 56 kb o Isdn 64 o 128 Kb) di cui dispone l'ascoltatore ed infine (ma non certo da ultimo) il computer ricevente che, per

avere una buona qualità, deve essere fornito degli ultimi processori Pentium minimo 233 Mb o Motorola per Mac ultima generazione.

Avete domande, critiche, suggerimenti, spunti e proposte su argomenti legati alle nuove tecnologie della comunicazione? È possibile recapitarci i vostri testi scrivendo a laRegione Ticino, "Cibervillaggio", Via Ghiringhelli 9, 6500 Bellinzona; oppure inviando un fax allo 091/825 23 74; o ancora via e-mail a: ciberegione@laregione.ch oppure a mpenco@unipius.ch.