

APOGEOnline

<http://www.apogeonline.com>

15 Luglio 1999

Vola Condor, vola

di Raoul Chiesa [raoul@raoul.EU.org]

La storia infinita di Kevin David Mitnick, l'hacker più famoso del mondo, sotto processo negli Stati Uniti. È in carcere da quattro anni e gli è stata respinta ogni richiesta di libertà su cauzione.

Vola, Condor, vola

Autore:

Raoul Chiesa

Text copyright © 1999 Raoul Chiesa

Copyright © 1999 – APOGEO srl

Viale Papiniano 38 – 20123 Milano (Italy)

Telefono: 02-461920 (5 linee r.a.) – Telefax: 02-4815382

Email apogeo@apogeoonline.com

U.R.L. <http://www.apogeoonline.com>

Tutti i diritti sono riservati a norma di legge e a norma delle convenzioni internazionali. Nessuna parte di questo libro può essere riprodotta con sistemi elettronici, meccanici o altri, senza l'autorizzazione scritta dell'Editore.

Nomi e marchi citati nel testo sono generalmente depositati o registrati dalle rispettive case produttrici.

This is the End. My only friend, the End...

E' il 14 febbraio del 1995, giorno di San Valentino. In una cittadina americana sta accadendo qualcosa che scatenerà ribellioni, dimostrazioni, appelli via rete, la nascita di siti spontanei di contro-informazione, la creazione di una colletta per realizzare un fondo spese legali...

Arriva un camioncino blu, un Van, con la scritta Sprint Telecommunications. Dal Van esce un giapponese, due tecnici della Sprint, le forze speciali dell'FBI con giubbotti antiproiettile ed armi alla mano. Sembra di vedere un film di azione. Ma non è così.



A Raleigh, piccolo centro nello Stato del North Carolina, stanno per arrestare Kevin Mitnick. Le conseguenze di questo arresto saranno molteplici e non solo per le comunità underground ed hacker.

Iniziata nel 1981 con l'attacco da parte di Kevin, allora diciassettenne, ai sistemi Cosmos della Pacific Bell (compagnia telefonica americana), la "caccia all'uomo" dell'FBI si conclude nel 1995, dopo 14 anni. Centosessantotto mesi di appostamenti, intercettazioni, false piste, arresti mancati. Il 14 febbraio si arriva alla conclusione di una lunga corsa, un inseguimento interminabile attraverso le reti di mezzo mondo. Quel giorno nasce il mito di Kevin Mitnick, l'hacker più famoso al mondo.

Gli inizi

Kevin nasce in California. I suoi genitori divorziano quando lui ha appena 3 anni. Nella sua adolescenza rispecchia lo stereo-

tipo classico dell'hacker: a 13 anni è un ragazzino solitario, grassotello. Inizia con i "CB", a 8 anni è già radioamatore. Da ex-hacker, interpreto questa sua passione come una ricerca comunicativa: là fuori c'è qualcuno e lui ci vuole parlare, la distanza fisica non è più importante, a otto anni può dialogare con degli adulti che si trovano in altre città. Credo che in quel periodo sia nata in lui, forse inconsciamente, la passione per l'hacking, le reti, la comunicazione.

Nella più classica immagine americana della prima metà degli anni '70, il ragazzino brufoloso, occhialuto e ciccione ha 9 anni e vagabonda per i negozi di elettronica della sua città, prende pezzi usati, li ricicla, costruisce, assembla tecnologia trasmissiva tutto solo nella sua stanzetta, mentre i coetanei giocano a basket o "simply, they are hangin' on around the school" (cazzeggiano davanti alla scuola): diventa cliente assiduo di alcuni negozi, fa amicizia con i proprietari, forse inizia a fare qualche lavoretto da bravo teen-ager americano, ricevendo come paga dell'hardware usato.

Il ragazzino cresce, scopre i PC. Va oltre, fin da subito, scoprendo i modem: a 13 anni viene cacciato da scuola dal preside, perché entrava negli archivi degli altri istituti. Trasferisce la bolletta telefonica di un ospedale (30.000 US\$) sul conto di uno che detestava. Si battezza Condor, dal film "I tre giorni del Condor", con Robert Redford. Credo che un alias, un nickname, non sia mai stato più azzeccato: il Condor è solitario, lavora da solo, non si fida di nessuno, vive con la solitudine. E probabilmente Kevin/Condor trova nella Rete e nell'hacking una compagna ideale, un qualcosa che lo rende meno solo.



Verso la fine degli anni '70, a 16 anni, come ogni bravo ragazzo americano, prende la patente: la targa della sua auto è X-HACKER. A 17 anni viene arrestato per la prima volta: furto di manuali informatici. Immagino Kevin, andatura insicura, occhiali da vista spessi, andare a cercare manuali per *imparare*, per capire dei sistemi informatici ai quali non poteva

accedere, a cercare l'*informazione*. Io facevo trashing (letteralmente, rovistare nella spazzatura; farlo davanti alle sedi di aziende di informatica, università e compagnie di telecomunicazione produce spesso informazioni molto riservate), per trovare i manuali della Digital e imparare a programmare su VAX/VMS.

Seguono altri arresti, nell'83, nell'87 e nell'88, sempre per reati informatici. Un giudice di Los Angeles, la signora Mariana Pfaelzer, lo mette in carcere emettendo una condanna superiore a quella richiesta dal D.A (District Attorney, il Pubblico Ministero). Prima di farlo uscire dall'aula, gli dice: "Questa è l'ultima volta che fa una cosa simile, signor Mitnick". Indubbiamente una frase profetica. Viene successivamente rilasciato, ma gli viene imposto il divieto di svolgere lavori che richiedano l'uso di un personal computer.

Oggi, nel 1999, ad alcuni anni di distanza, quello stesso giudice dovrà decidere se le richieste di risarcimento - presentate da multinazionali informatiche e pari ad un totale di ben ottanta milioni di dollari (sì, avete letto bene: hanno chiesto 80.000.000 US\$ di danni al Signor Kevin David Mitnick) - dovranno essere soddisfatte o meno. Buona fortuna, giudice Mariana.

Le aziende che hanno richiesto il risarcimento sono la Motorola, la Fujitsu, la Nokia, La Sun Microsystems, la Novell, la Nec. Il solo **utile netto** della Motorola nel 1995 è stato di 22.247.000.000 di dollari. Con che coraggio queste aziende chiedono ottanta milioni di dollari ad un carcerato sotto processo, il quale non ha fatto altro che copiare delle informazioni per propria cultura personale, senza rivenderle, modificarle o distruggerle?

Il "Condor" vola troppo in alto

Anni '90. Kevin è cresciuto. E' sempre più Condor. È un fantasma, come scrissero in seguito. Non esiste. Vive dirottando i propri conti su altre utenze. Gira gli States, notebook e cellulare modificato. Pone molta attenzione durante le connes-

sioni, cambia spesso numeri telefonici, appartamento. Si sposta di continuo. Esplode, probabilmente, il suo odio verso le "Big Companies": IBM, Digital, Sun Microsystems, Fujitsu. Tutte hanno dei segreti da custodire. Il Condor cerca la libertà d'informazione. Vuole la verità, vuole i bug, i famosi difetti, errori di programmazione compiuti dalle software house, per poter accedere ai sistemi informatici protetti.

Dalla prima metà degli anni '90, sino al suo arresto, Kevin cresce ancora. E' molto attratto dai sistemi VAX della Digital: sono i soli a non avere praticamente bug, a non essere "sfondabili". Allora il Condor agisce, silenzioso. Utilizza Social Engineering, una tecnica hacking per carpire telefonicamente informazioni spacciandosi per un'altra persona, un collega di una filiale. Ottiene tutto quello che vuole. Viola il sistema di un Internet Provider inglese. A quel sistema è abbonato, come utente regolare, un consulente della Digital.

E' stato tra i creatori del VMS, il sistema operativo proprietario dei VAX Digital, ed ora effettua consulenze alla Digital sulla sicurezza. I bug ci sono. Vengono scoperti da quest'uomo. E Kevin gli spia le e-mail. Apprende i segreti più segreti della Digital, il suo intento era quello: se non posso ottenere le informazioni in un modo, le ottengo in un altro.

L'FBI è sui suoi passi. Lui lo sa. Spia le comunicazioni tra la sede centrale dell'FBI e gli agenti dislocati, i quali lo stanno cercando per mezza America. Non appena l'FBI dà l'ordine "*ok, andate a prenderlo*", lui sparisce. Li prende in giro. Falsifica le comunicazioni. E' un'ombra sulla Rete, nessuno sa dove sia fisicamente.

Kevin nel frattempo è entrato ovunque: multinazionali, società d'informatica, agenzie governative. Entra e copia: progetti, piani, budget, business plan, contatti, consulenze esterne. Non vende nulla, non baratta, non cancella: apprende, impara, conosce. Per lui la conoscenza è importante. Sa come funzionano le cose. Capisce che il nuovo business sta partendo: telecomunicazioni, telefonia cellulare, satellitare, pay-Tv. I bit avanzano, l'analogico scompare. Kevin lo sa. Forse inizia a capire il potere che ha in mano.

Lo capiscono anche altre persone. Kevin ha accesso ad informazioni riservatissime, e questo dà molto fastidio alle multinazionali. Le lobby USA si muovono, l'FBI lo inserisce ufficialmente tra i "Top Wanted", come per i peggiori criminali.

L'Fbi ha capito, le multinazionali anche, le lobby hanno provveduto: mancano i mass-media. Come per magia, appare un articolo sulla prima pagina del New York Times, il 4 luglio 1994: racconta dell'esistenza del Condor. Kevin diventa un personaggio. Ma è sempre più braccato. John Markoff, l'autore dell'articolo, fa di tutto per incontrarlo. Corrompe alcuni suoi "amici", collabora con l'FBI per incastrarlo.

Inizia la guerra: Davide e Golia

Nel dicembre del 1994, appare un messaggio sul computer di Tsutomu Shimomura, nippo-americano, super esperto di sicurezza, consulente del Governo USA. Non c'è scritto molto, solo un "Found me: I am on the Net". Trovami, sono sulla Rete, gli dice Kevin.

La sfida ha inizio. Per la prima volta, le armi sono diverse: è una caccia all'uomo on-line. Le maggiori compagnie di telecomunicazione americane collaborano con l'FBI. La Sprint Corporation fornisce manuali, schede, tecnici specializzati. Il Condor è braccato. Kevin ha utilizzato, tra i primi al mondo, la tecnica dell'IP-spoofing, nel dicembre del 1994, per attaccare i server di Shimomura con sede a San Diego. Shimomura commenta questa tecnica ad una conferenza americana (CMAD), nel gennaio del 1995. Pare dunque che inizi, sin da subito, lo sfruttamento del Condor, delle sue tecniche, della sua abilità, del suo stile stile e delle sue competenze.



Markoff scrive altri articoli, accusa Kevin, lo dipinge come il "criminale". Kevin ama, come molti hacker, la stampa. Vuole dire la sua. Non accetta giudizi senza poter ribattere. Contat-

ta Jonathan Littman. Arriva a chiamarlo tre volte al giorno. Forse, da questo momento in poi, il Condor perde la sua freddezza, la sua lucidità, i suoi attenti calcoli. Compie degli errori. Deve cambiare città sempre più spesso. Non capisce le motivazioni di tanto clamore attorno al suo caso. Discute con il giornalista "buono" di hacking, di politica, di tecnologia, di donne, di costume. Littman lo definirà "una mente esplosiva, incontrollabile, incredibilmente potente". Littman sbaglia: come in ogni "grande rovina", all'origine c'è un errore. Parla con Markoff, si confida. Gli rivela dove si trova Kevin. Lo rivela al collega giornalista, all'amico John. Markoff, il quale informa immediatamente Shimomura. Il cerchio si stringe. Kevin crede di essere tranquillo. Ha fiducia nel suo confidente. Una volta un hacker mi disse: "Trust no 1: non fidarti mai di nessuno". Kevin avrebbe dovuto incontrare quell'hacker, forse sarebbe andata diversamente. John Markoff o Shimomura - ma è indifferente - informano l'FBI. Il Condor sta per cadere.



Torniamo al 14 febbraio del 1995. Kevin viene arrestato. Non uscirà mai più dal carcere. Amici, conoscenti, hacker, amanti della libertà d'espressione, dell'open source, della libera comunicazione, anarchici, hanno fondato un sito web, <http://www.kevinmitnick.com> ^[1]. Sull'home page c'è un contatore. Non è il classico counter per gli accessi. Scorre veloce, di continuo. Purtroppo non testimonia una cosa allegra, come l'alto numero di visitatori. Le cifre scorrono, a rotazione, e contano:

4 ANNI, 4 MESI, 22 GIORNI, 13 ORE, 8 MINUTI, 33 SECONDI...

4 ANNI, 4 MESI, 22 GIORNI, 13 ORE, 8 MINUTI, 34 SECONDI

4 ANNI, 4 MESI, 22 GIORNI, 13 ORE, 8 MINUTI, 35 SECONDI

La frase sopra recita: " Kevin Mitnick è stato imprigionato dal Governo Americano, **prima della sentenza**, da:..."

Vola mio Condor, vola sempre più in alto.

Kevin Mitnick è la punta di un iceberg, a mio parere. E' diventato il capro espiatorio. Gli Usa, le multinazionali, le aziende d'informatiche, vogliono una vittima. Un caso esemplare. Una condanna altrettanto esemplare. Vogliono un esempio, un precedente.

Negli Stati Uniti la *detenzione media* per **omicidio colposo** è di 3 anni: Kevin è dentro da 4; non ha ancora avuto un processo; il numero dei capi d'imputazione assegnatigli farebbe impallidire Al Capone; è stato messo in isolamento per otto mesi; ci sono migliaia di persone al mondo che lottano per i suoi ideali, ma lui non lo sa; gli è stata rifiutata **ogni richiesta** di libertà su cauzione; gli furono sequestrati computer, modem, persino la radio: avrebbe potuto modificarla per comunicare con l'esterno, dissero.

L'amato Mr. Shimomura, insieme al degno compare Markoff (sembrano il gatto e la volpe), nel frattempo, hanno incassato un anticipo di 750.000 US\$ per il libro che hanno scritto, "Sulle tracce di Kevin" (edizione Sperling & Kupfler). Recentemente hanno venduto i diritti per il film, e Kevin marcirà in una prigione americana, e continua a non sapere cosa gli succede intorno, cos'è diventato il Web - quelle "3 W" che tanto ci stanno cambiando la vita - che lui ha contribuito a rendere più sicuro.

Il ragazzo che voleva il "cyber-world" libero, gratuito ed accessibile a tutti, l'uomo che voleva dei sistemi sicuri, l'uomo che ha ispirato due generazioni di hackers, guarda dalle sbarre i fili telefonici, immagina i segnali satellitari, le reti GSM a 1800 MHz che spingono i segnali. Io telefono, e la "centrale" sa dove sono fisicamente, voi vi collegate al Web, e pagate la connessione, l'abbonamento, gli scatti, i megabytes scaricati. L'hacker che voleva l'informazione come un diritto innegabile dell'uomo, l'informazione gratuita, vera e totale, il *condor* che voleva volare in alto, è stato rinchiuso, è stato ridotto al silenzio.

Non posso dire altro, a voi che leggete, se non farvi riflettere su una cosa: se i diritti costituzionali possono essere messi da parte nella *Grande America* per Kevin Mitnick, cosa vi fa pensare che non sarebbe lo stesso con voi al suo posto?

E non posso augurare altro, al buon Kevin Mitnick, se non di volare. Vola mio Condor, vola sempre più in alto.

www.apogeonline.com

APOGEO per i professionisti della sicurezza

Hacker 2.0
Nuove tecniche di protezione dei sistemi
di McClure
Scambray
Kurtz
pagine 672,
Lire 78.000



"L'informazione contenuta in questo libro vale oro"
Bruce Schneier, il maggiore esperto mondiale di sicurezza

Hacker Linux
Tecniche e segreti per la sicurezza in ambiente Linux
di Hatch
Lee
Kurtz
pagine 552,
Lire 69.000



Pensare come un hacker,
per poterne prevedere le mosse!