<internos>

Kevin Poulsen, Serial Hacker.

di *Raoul Chiesa*

dicembre 2000

Il Kevin più famoso al mondo è sicuramente Kevin David Mitnick aka "The Condor", arrestato nel febbraio del 1995 dopo anni di clamorose intrusioni in sistemi informatici. Ma un altro Kevin ha una storia molto interessante da raccontare...

Montreal, 27-10-2000

Sono partito da Parigi per Montreal e la distanza tra le due città significa, più o meno, otto ore di viaggio. La gente normale si prepara a viaggi di questo tipo comprando settimanali - spesso banali - da leggere durante il volo o, nei casi migliori, comprando l'ultimo libro di successo all'aeroporto, prima della partenza.

Il sottoscritto non si è mai definito una persona normale (la normalità è l'inizio della fine, diceva qualcuno) e si è collegato ad Amazon per vedere cosa offriva di bello il mercato dei libri: la ricerca si è direzionata, ovviamente, sull'hacking, ed ho scoperto come il mercato americano dei libri sia estremamente prolisso su questo genere di argomenti.

Inserisco la keyword "hacking" e scorro i titoli: **Masters of Deception, the Gang that ruled Cyberspace** racconta gli scontri tra il gruppo dei LOD (Lords of Doom) e quello dei MOD (Masters of Deception), **Where the Wizards stay up late, the Origins of the Internet** racconta la nascita di Internet, analizzando i fatti attraverso gli hacker storici del periodo 1980/2000 (dando però una visione prettamente americana al tutto) ed è scritto da Katie Hafner e suo marito, Matthew Lyon. Katie è la ex-moglie di John Markoff, il giornalista del New York Times che scrisse insieme a Shimomura il libro "Sulle tracce di Kevin", resoconto di parte sulla caccia e l'arresto di Kevin Mitnick: ho incontrato Katie l'estate di due anni fa in Italia e credo che il mio odio per il suo ex marito, primo responsabile del caos scoppiato attorno a Kevin, mi si leggesse negli occhi. Katie rifiutò l'intervista che le chiedevo non appena risposi, molto sinceramente, "sì", alla sua domanda *"Are you an hacker ?"*.

Continuo nella ricerca e un titolo mi colpisce più degli altri: è scritto da Jonathan Littman, autore del bellissimo **"The Fugitive Game: Online with Kevin Mitnick"**, il libro che racconta come andarono *realmente* le cose nel "caso Mitnick". Jonathan è riuscito ad entrare nella psicologia degli hackers (cosa che, a quanto ho appreso recentemente, non è riuscita a certi accademici molto rinomati ed, in genere, non è riuscita a nessuno), ha passato centinaia di ore al telefono con il Condor (nickname di Mitnick), ha conosciuto i suoi amici ed i suoi nemici, ha parlato con le autorità che hanno condotto l'indagine, FBI per prima. Nonostante sia riuscito a mantenere un'imparzialità completa nei suoi racconti le sue parole generano immagini, e le immagini richiamano un mondo completamente diverso, quel famoso cyberspazio di cui tutto parlano ma che ben pochi hanno ancora capito....il mio giudizio sul suo primo libro fu ottimo e quindi clicko sull'icona BUY IT di Amazon.

Littman iniziò a scrivere **"The Watchman: the twisted life and crimes of serial hacker Kevin Poulsen"** prima del libro su Kevin Mitnick, per sospenderlo ed iniziare il lavoro su quest'ultimo, mentre gli eventi correvano velocemente e Mitnick veniva accusato, dopo l'arresto, di danni per svariati milioni di dollari (vedasi i miei due articoli, **"Vola Condor Vola"** e **"Cosa Kevin David Mitnick non potrà fare nella sua vita: praticamente tutto"**, presenti su **www.apogeonline.com** e **www.internos.it**). Credo che questa pausa nella stesura di The Watchman sia stato un bene ed abbia permesso all'autore una visione completa dell'hacking statunitense di quel periodo, riuscendo a dare come risultato un "California noir thriller" in uno stile quasi Gibsoniano[1].

Jonathan riesce a conquistarmi sin dalla prima pagina, trasportandomi in un periodo storico per la tecnologia e l'Information Security, durante il quale furono commessi alcuni dei più audaci crimini informatici. The Watchman è il protagonista dei fumetti preferiti da Kevin (Poulsen), ragazzo americano nato alla fine del 1965, proprio nel periodo in cui il boom dell'alta tecnologia da dopoguerra inizia a diffondersi oltre l'industria della difesa, le università e le corporations. I '70 e gli '80 sono gli anni in cui gli hackers "get computers working better", li aumentano di potenza, li ottimizzano, scrivono le prime procedure ed i linguaggi standard che ci accompagnano ancora oggi: creano un mondo dell'informatica più potente, più facile da usare, disegnano un percorso che la prossima generazione potrà utilizzare per migliorare ancora più profondamente il mondo delle comunicazioni.

Voglio aprire una parentesi per quelle persone che, solitamente, mi rispondono dicendo che l'hacking è esclusivamente un reato e che gli hackers altro non sono che puri criminali: per queste persone dei personaggi altamente rispettabili (ma dipende dai punti di vista) e additate come veri e propri geni - dell'economia o della tecnologia, è poi da capire - come **Bill Gates** e **Paul Allen** (fondatori della Microsoft) o **Steve Jobs** e **Steve Wozniak** (fondatori della Apple Computer) sono dei luminari, delle realtà tutto d'un pezzo... Forse li sconvolgerà apprendere, leggendo il libro, come i due Steve sopra menzionati, ispiratori della prima brezza della rivoluzione nei microcomputer alla fine degli anni '70, furono anch'essi dei criminali e costruirono blue box[2] con il

[1] William Gibson, creatore del genere cyberpunk, autore di splendidi romanzi quali Neuromancer (Neuromante)

[2] Blue Box, Red Box, etc...: nell'America degli anni '70 ed '80 esplose un fenomeno tra i giovani studenti delle università statunitensi, il blue boxing. "Boxare" significava riuscire ad effettuare telefonate, di qualunque tipo, cioè nazionali ed internazionali, gratuitamente, sfruttando dei difetti propri del sistema telefonico di allora, inserendosi nelle linee operatore e gestendo le chiamate in uscita proprio come un operatore della compagnia telefonica. La Red Box era una variante la quale simulava il rumore del "coin" (moneta) inserito nei telefoni pubblici, permettendo così di effettuare telefonate senza spendere un cent, per tutto il tempo voluto.

solo intento di venderle ai compagni di college...

Poulsen, a differenza di Mitnick, nasce come phreaker[3] , dove *"Fare phreaking significava scoprire e comandare un invisibile mondo elettronico"*: sono molte, dunque, le sostanziali differenze tra i due Kevin. Arrestato all'età di 17 anni per intrusioni nel sistema informatico e telefonico della Pacific Bell, Kevin Lee Poulsen viene descritto nella sua psicologia più completa e Littman arriva ad identificare e narrare con una magia quasi unica il momento del "salto", il passaggio da ragazzino dotato di un'intelligenza fuori dal comune con una conoscenza "visiva" dei sistemi telefonici del proprio paese a criminale, personaggio capace di vincere concorsi radiofonici dirottando le chiamate in ingresso verso le radio ed ottenere premi quali Porsche coupè e decine di migliaia di dollari.

L'arresto di Kevin Poulsen è infatti una tappa temporanea nella carriera del phreaker, il quale esce immediatamente e senza problemi da ogni accusa, essendo ancora minorenne: sorte diversa tocca all'amico Ron Austin, allora maggiorenne, il quale viene incarcerato per un certo periodo. Diversissimi sotto ogni profilo - Austin alto, biondo e belloccio, rappresenta il classico californiano figlio della middle-class mentre Kevin, timido e silenzioso, a 7 anni gioca col suo primo "electronic test board" - i due rimarranno amici per tutta la vita, esattamente come accadde tra Kevin Mitnick e Lewis Depayne, amico del cuore ma, nel contempo, la persona che andò a vivere con la sua ex moglie.

Un Kevin quindi estremamente diverso dal ben più famoso omonimo.
Phreaker prima che hacker, Poulsen segue come molti altri giovani della sua generazione una tradizione, un mito, un codice. Un fattore comune ad ogni hacker, incluso il sottoscritto, è l'idea che la società, la tecnologia e persino le leggi potranno cambiare, ma per molti versi saremo noi, "creatori del domani" come qualcuno ci ha definiti in uno stupendo libro, a dare le direzioni. Il phreaking non consiste nell'effettuare telefonate gratuite, ma nel come riuscirci, nel *come* farle: è il processo di *accedere* a qualcosa, riuscire a comandare, avere il *potere*: Kevin usa questo potere nei modi più disparati, dalle vincite nei concorsi radiofonici sopra accennati all'ottenere i numeri riservati delle star di allora (stravedeva per Molly Ringwald, attrice in film come The Breakfast Club), per poi intercettare le loro chiamate e recarsi a cena negli stessi locali, con Madonna e Sean Penn dietro di lui.

Nel 1978, all'età di 13 anni, Kevin va ogni pomeriggio al Mall della sua zona, si dirige

[3] Dal termine To Phreak: utilizzare (ed abusare) le reti ed i sistemi telefonici, così come l'hacker utilizza i sistemi e le reti informatiche

verso i telefoni pubblici di Ma' Bell e sperimenta l'arte del phreaking: troppo povero per avere un proprio personal computer si allena segretamente e pratica "l'arte della telefonia", cercando di diventare un cyberpunk ancora prima che il termine stesso fosse coniato. Il microfono del telefono è la sua bocca, come il microfono per la rockstar..alza il ricevitore, compone una sequenza di numeri (routing codes) a sente il primo CLICK...poi il secondo, "CLICK", e poi la scarica elettromagnetica della centrale telefonica che ha raggiunto, "CLACK-SCLACK". Kevin ha appena "fischiato" a 2600 hertz, la tonalità che il sistema telefonico di Ma' Bell riconosce come il segnale dell'operatore per aprire una linea in uscita. Preso il segnale, compone il numero 121, il quale lo dirotta sull'operatore di Blythe, California. L'operatore vede una chiamata proveniente dalla rete "Long Distance Network" di AT&T.

- "Blythe", risponde l'operatore.
- "Sto chiamando da un testboard", dice Kevin, cercando di cammuffare la voce e sembrare almeno un tecnico diciannovenne appena assunto. "Mi serve che mi inoltri una chiamata". Gli dà il numero dell'operatore di Los Angeles e in pochi secondi la chiamata viene rimbalzata dove Kevin effettivamente si trova, nella sua città. Kevin ripete la sequenza per un'altra città, e poi ancora un'altra, e un'altra ancora... Alla fine l'ultimo operatore lo sente a malapena, tra gli echi ed i delays (avete presente quando fate una chiamata internazionale con un'oceano di mezzo, i ritardi sulla linea ?) ...
- "Operatore, mi può connettere al 213-..." e gli dà il numero della cabina telefonica a fianco del telefono dal quale sta chiamando, all'esterno del centro commerciale. Drinn..Kevin alza il telefono, e dice "Hello Kevin !!", tra gli echi infiniti di una telefonata che, per arrivare al telefono di fianco, ha girato e scorre tra differenti carrier telefonici nazionali trunk internazionali quali At&t, NTT, etc..New York, Santa Fe, Chicago, Portland, Washington D.C...le sue parole fanno riverbero attraverso il paese, interrotte dai continui rumori delle centrali di switching e dalla staticità delle linee telefoniche mentre il suo nome passa tra gli switch..Kevin è caduto nel buco del coniglio di Alice ed ha appena scoperto il suo Paese della Meraviglie, la propria voce che echeggia all'infinito..Hellooooooo Keeeeviiiin, hellooooooo...."

Potrei continuare raccontandovi episodi curiosi, intrusioni epiche, hacking che si intrecciano con i "preoccupanti casi" narrati da Clifford Stoll in The Cuckoo's Egg (dove, partendo da un ammanco di 75 cents ai Berkeley's Livermore Labs si arriva ad un caso di spionaggio militare tra gli Stati Uniti e l'allora Germania dell'Est), sino ad arrivare al colmo dove "the tapped guys has tapped the tapping guys", ovvero quando

una serie di hackers americani - tra i quali gli stessi Kevin Lee Poulsen, Kevin David Mitnick e il doppiogiochista Eric (Justin Tanner Pertersen, aka Agent Steal, l'"anti hacker") - "scroprirono" il S.A.S.[4] ed intercettarono tutte le chiamate dell'FBI, il quale era teoricamente incaricato di intercettare loro...

Anche in questo caso Poulsen si distingue, scoprendo una serie di intercettazioni non autorizzate ai danni dei consolati cinesi, israeliani (teoricamente "amici" del governo USA), russi e sud africani, smascherando la copertura dell'FBI quale "Studio Legale J.W. Collins & Associates" in un ufficio situato al piano superiore rispetto al consolato del Sud Africa, dove ben 13 linee telefoniche furono messe sotto controllo per anni. Potrei, ma preferisco avervi messo la classica pulce nell'orecchio, sapere di avervi fatto un pochino sognare con queste poche parole e farvi venire la voglia di leggere un libro veramente bello, curioso ed intrigante.

Tutto ciò, forse, anche perché *"hacking"* è oramai divenuto storia, cultura, voglia di capire cosa ha rappresentato e quanti accorgimenti e migliorie tecniche siano stati apportati ai sistemi informatici ed alle reti telefoniche di tutto il mondo, United States of America per primi. Anche se qualcuno dice il contrario...

Buona lettura.

Raoul Chiesa aka Nobody
Network Security Manager @ Mediaservice.net - Divisione Sicurezza

[4] Oggi l'evoluzione dell'S.A.S. è rappresentato dal DragonWare Suite (una serie di applicazioni sviluppate da una società in Arizona molto particolare, avendo di fatto un unico cliente, il Governo degli Stati Uniti d'America, ovverosia le principali Intelligence Agency statunitensi): i lettori probabilmente non avranno mai sentito parlare di tale suite software, utilizzata per monitorare ed intercettare ogni tipo di chiamata voce o dati, ma in questo ultimo periodo la stampa ed i mass-media hanno dato estremo risalto ad un componente software di questa suite, il Carnivore, un "grande fratello" in grado non solo di intercettare le comunicazioni e-mail di un soggetto ma anche di ricostruire la lista dei siti visitati da un indagato.