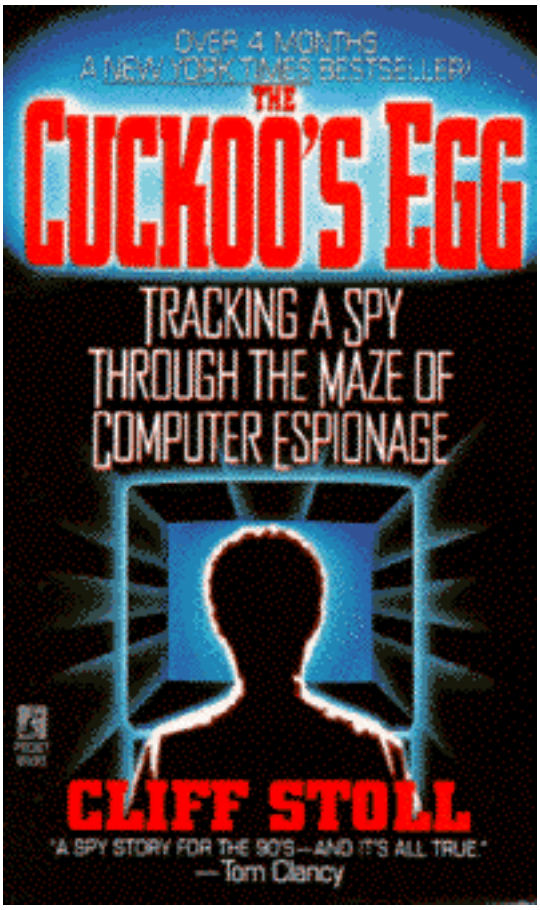
THE CUCKOO'S EGG:
Tracking A Spy Throught The Maze Of Computer Espionage



I libri sugli episodi di intrusione informatica si sono moltiplicati in questi ultimi anni, trattando argomenti diversissimi tra di loro: criminalità, spionaggio industriale e militare così come sociologia, evoluzione tecnologica ed hacking. The Cuckoo's Egg, però, è un caso abbastanza particolare…cerchiamo di scoprirne i motivi.

Torino, 21 Aprile 2001

Clifford Stoll, nome vero, è autore e protagonista del libro. Un "diario di bordo", fedele ritratto del vero diario dove Cliffy usava scrivere annotazioni, pensieri, i fatti del giorno. Non si tratta di un romanzo, ma di fatti veri. Episodi realmente accaduti che trasportano il lettore in un mondo sconosciuto e danno al ricercatore ed all'investigatore conferme inaspettate. Il primo punto il libro lo guadagna per un semplice fatto: è il primo nel suo genere. Anni dopo sono stati scritti libri e romanzi bellissimi, dove vengono narrate le gesta di hackers storici quali Kevin Mitnick, Roscoe, Kevin Poulsen, il gruppo dei LOD e dei MOD, mentre attorno a tutto ruotano i pilastri cult di Phrack e 2600 Magazine. Nessuno ha però saputo dare quell'insieme di veridicità, storia e pionerismo che fuoriesce da The Cuckoo's Egg.

Il titolo, tradotto, suonerebbe bene o male come "L'uovo del cuculo: inseguire una spia nel labirinto dello spionaggio informatico". Potrebbe essere un romanzo, sembrerebbe essere il nuovo titolo del nostro scrittore di successo..The Cuckoo's Egg è invece l'opera prima di Clifford "Cliffy" Stoll, americano, giovane ricercatore in astronomia. Penso che il "bello" del libro sia proprio il fatto che Stoll non aveva mai avuto nulla a che fare con il mondo dell'hacking, né tantomeno con quello dello spionaggio militare. Con "bello" intendo i pregi indiscussi del libro come il trattare argomenti tecnici abbastanza difficili da comprendere in maniera molto chiara, complice la capacità dell'autore di "spiegare ciò che stava imparando": non dimentichiamoci l'ambiente nel quale lui stesso ha vissuto per svariati anni, quel clima universitario che ben poco si sposa con un gruppo di hacker sbandati ed elementi vari appartenenti al CCC, il famosissimo Chaos Computer Club di Amburgo. Ma partiamo dall'inizio.

Cliffy lavora come ricercatore in astronomia ai Livermore Labs dell'Università di Berkeley, Stati Uniti d'America. E' uno dei ricercatori più giovani, siamo alla fine degli anni '80 e la tecnologia informatica sta invadendo le università. Un pò per colpa dell'età, un pò per le conoscenze informatiche di cui dispone - non eccessive ma comunque sopra la media presente in un laboratorio di astrofisica - Clifford viene incaricato della gestione informatica del suo dipartimento. In quel periodo le reti informatiche dei campus americani sono sempre più collegate tra loro e l'espansione completa avviene grazie alle reti a commutazione di pacchetto, prima tra tutte Tymnet USA.. Dati però i costi di acquisto e gestione degli impianti informatici, molte università avevano deciso di addebitare il tempo di utilizzo delle risorse: il compito di Cliffy era quello di supervisionare il corretto funzionamento ed utilizzo degli elaboratori nel dipartimento in cui lavorava.

Un giorno Stoll scopre una incongruenza nel tempo di utilizzo degli elaboratori di 75 centesimi di dollaro, una cifra molto bassa che normalmente non avrebbe dato adito a sospetti od indagini. Il nostro eroe è però cocciuto sin dalle prime pagine e, a forza di indagare, scopre che i sistemi informatici dei Livermore Labs sono stati violati da sconosciuti. Come se non bastasse, nel corso delle indagini – dove la collaborazione dell'Fbi prima e della Cia dopo è pressochè nulla – scopre come gli stessi sistemi server siano utilizzati come basi per attacchi verso computer militari e governativi degli Stati Uniti d'America.

A questo punto le Autorità americane si interessano al caso e si viene trascinati in una serie di mondi paralleli, tra agenti governativi e tecnici di compagnie telefoniche e dati che, attraverso il globo, inseguono dei segnali digitali per arrivare all'autore delle intrusioni informatiche. Il libro lancia, nonostante gli anni in cui è stato scritto, segnali su argomenti molto preoccupanti e tuttora da definire, quali la giurisdizione competente per reati eseguiti in forma telematica e gli standard di collaborazione tra le autorità di differenti paesi.

Se da un lato il grottesco comportamento americano, non ancora pronto per episodi di questo tipo, fa capire al lettore il clima e le reazioni di quel periodo, dall'altra parte scopriamo come l'Unione Sovietica, allora ancora URSS, riuscì a farsi prendere in giro da tre ragazzini accaniti fumatori di marjuana ed occasionali consumatori di cocaina, i quali approfittarono proprio dell'ignoranza in materia dei propri interlocutori. Uno di quei ragazzini era entrato, un anno prima, nel sistema centrale dei Livermore Labs.

Ci vuole quasi un altro anno di indagini per raggiungere l'obiettivo ed identificare i colpevoli. In mezzo a spie ed agenti governativi il nostro Cliffy capisce completamente le tecniche di attacco, le falle dei propri sistemi informatici e di quelli altrui, capisce cosa spinge un hacker ad attaccare e qual è il confine tra l'hacking "puro" e la criminalità. Questo libro ci fa scoprire il mondo hacking statunitense ma, soprattutto, ci fa capire gli inizi dell'underground europeo ed immaginare luoghi di ritrovo on-line come Altos, QSD o le BBS. Credo che solo avendo una piena conoscenza di quanto è accaduto alle origini sia possibile capire episodi quali l'Hacker's Crackdown americano del 1990 e

l'Italian Crackdown del 1994, per arrivare ai giorni nostri dove i cosiddetti "newbies" ricordano un pò quei tre ragazzi solitari tedeschi, tutto sommato ingenui ed innocui…

Raoul Chiesa aka Nobody
Network Security Manager @ Mediaservice.net – Divisione Sicurezza Dati – ITALY
(raoul@raoul.EU.org)
Founder Member of ClusIT, Italian Security Association (http://www.clusit.it)