

Dall'editore

La letteratura scientifica ci ha abituati a un criterio espositivo che fa prevalere il risultato sul processo della scoperta, ridotto al più all'insieme delle "prove" o delle "evidenze" che sostengono il risultato; la manualistica tecnica, nel campo delle scienze dell'informazione in particolare, è improntata di norma all'esposizione degli strumenti del mestiere ben più che ai processi creativi di ricerca delle soluzioni. Sì, è vero, abbiamo tutti poco tempo, e prima "si va al sodo", meglio è; altrettanto vero è che così si perde gran parte del fascino di queste attività e si finisce per coglierne solo parzialmente il senso. Perché alla fine l'esito sembra spesso ridursi a ben poco (tanto rumore per nulla?) e quasi non giustificare lo sforzo fatto per raggiungerlo.

A chi partecipa all'impresa e a chi può seguire dall'interno, invece, si aprono ben altri orizzonti: perché il risultato, per quanto piccolo, certo conta, ma conta assai di più il processo e c'è molto più da imparare dalla genesi delle idee, dai vicoli ciechi imboccati, dai tentativi falliti, dalla strada – anche tortuosa e sofferta – che si è percorsa. A raccontare quella storia si cimentano qualche volta i libri di "divulgazione", ma raramente non fanno rimpiangere la parola diretta dei protagonisti.

Così, quando qualcuno impegnato nel mondo della ricerca, a qualunque livello, è disposto a raccontare la gestazione di un progetto e a far partecipi tutti dei processi costruttivi che lo fondano e contribuiscono alla sua realizzazione, fascino e senso dell'impresa ci vengono restituiti in tutta la loro pienezza. Per questo, la proposta di Raoul Chiesa e dei suoi coautori non è rimasta a giacere e a prender polvere su qualche scrivania in redazione: poter documentare i "lavori in corso" di un progetto di ricerca che ha concluso solo alcune delle sue fasi previste e gettare ben più di uno sguardo sul

modo di lavorare di una eccellente squadra di ricercatori ci è sembrato quasi ancora più attraente dello stesso tema del progetto.

Il tema peraltro si inserisce benissimo nel catalogo dell'editore, che ricorda con particolare soddisfazione libri come *Spaghetti hacker* di Stefano Chiccarelli e Andrea Monti, pubblicati ormai una decina d'anni orsono; e sorride un po', all'idea di mettere, a fianco della gran mole di letteratura di fantasia e di prodotti d'ogni medium su indagini criminali, *crime scene investigations*, analisi forensi e scienze criminologiche, un libro di autori italiani, su un progetto di ricerca unico nel suo genere e nato in Italia con un respiro internazionale sull'*hacker's profiling*. A dimostrazione che la realtà supera ancora la fantasia, e che leggere il racconto di un'intrapresa scientifica può essere coinvolgente e appassionante quanto leggere (o vedere) *fiction*.

Che, nel loro percorso, progetto e testo tocchino da vicino argomenti che ci sono molto a cuore, dall'esplorazione degli spazi virtuali, ai concetti di libertà e controllo nella Rete, dall'etica di tutti gli attori internettiani fino a sfiorare questioni di proprietà intellettuale e diritto d'autore – beh, tutto questo non ha fatto che semplificare la decisione di pubblicare il libro, all'inizio, e aumenta oggi il piacere di vederlo andare alle stampe. Nella convinzione che i lettori a cui lo proponiamo possano trovarci molto; e con un augurio al gruppo di ricerca, per il completamento delle ulteriori fasi del loro lavoro.

Virginio Sala
Direttore editoriale

Premessa

Io sono un hacker, entrate nel mio mondo...

Questo libro vuole testimoniare i primi due anni di vita del progetto ISECOM denominato HPP, Hacker's Profiling Project. Quello che vi accingete a leggere, i risultati fin qui ottenuti, non ha pretesa di validità assoluta, bensì vuole essere solo il primo passo di un percorso non semplice, che ci auguriamo porterà alla formulazione di una metodologia di profiling applicabile al mondo dell'hacking.

Ciononostante riteniamo che, in conclusione del primo periodo di indagine, coincidente alle prime due fasi delle otto costituenti l'intero progetto, fosse utile e interessante cominciare a fissare lo "stato dell'arte", i tentativi fatti in passato per studiare il "fenomeno hacker", confrontandolo con quanto fin qui emerso dai nostri studi: dati che riteniamo estremamente importanti per comprendere, senza esprimere giudizi, questo affascinante mondo.

*Il Core Research Team di HPP – Hacker's Profiling Project -
ISECOM*

*Raoul "Nobody" Chiesa
Dott.ssa Stefania Ducci
Alessio "mayhem" Pennasilico
Dott.ssa Elisa Bortolani*

Novembre 2006

Introduzione

Ne è stato arrestato un altro oggi, è su tutti i giornali: “Ragazzo arrestato per crimine informatico”, “Hacker arrestato dopo essersi infiltrato in una banca”... Dannati ragazzini. Sono tutti uguali.

Nonostante l'argomento che ci accingiamo a trattare possa essere etichettato come “Hacker's Profiling”, è opportuno premettere che ogni hacker è diverso dagli altri: si tratta di persone che hanno una propria storia, un proprio background culturale e familiare, un proprio vissuto. Tutti questi elementi li hanno forgiati rendendoli unici e irripetibili, come del resto succede per ogni essere umano. Tuttavia, si possono individuare delle costanti, dei caratteri comuni che accomunano tutti questi soggetti. Nel fare questo bisogna però stare attenti a non generalizzare, poiché questo sarebbe l'errore più grosso.

Sarebbe infatti scientificamente scorretto attribuire alla generalità degli hacker caratteristiche che sono proprie solo di alcuni individui, così come non è ammissibile estendere le peculiarità che sono comuni alla maggioranza degli hacker, a tutti gli esponenti del mondo underground, poiché ci potrebbe sempre essere un individuo che rappresenta la cosiddetta *eccezione alla regola*. Se quindi non si possono fare generalizzazioni in senso orizzontale, come ora esemplificato, è anche vero che ciò vale, a maggiore ragione, ad un livello verticale-cronologico.

Per spiegarci meglio, se alcune caratteristiche sono tipiche degli hacker degli anni Ottanta e Novanta, non è detto che queste siano ancora valide per gli hacker del 2000. Infatti, come vedremo nei prossimi capitoli, esistono diverse generazioni di hacker, ognuna delle quali presenta caratteristiche, motivazioni e finalità diverse dalle altre. Nel cercare di delineare un profilo criminale degli hacker, occorre quindi stare attenti a non cadere in facili luoghi comuni, spesso privi di base scientifica ma costruiti *ad hoc* dai mass media e, al tempo stesso, cercare di identificare i diversi profili esistenti.

Per fare ciò è necessario individuare i punti di contatto che hacker di una stessa tipologia condividono, senza però tralasciare le peculiarità proprie di ciascun individuo.

In sintesi, si può affermare che la stragrande maggioranza degli hacker presenta i seguenti caratteri fondamentali:

- hanno generalmente un quoziente intellettivo al di sopra della media e grandi abilità tecniche e di problem solving;
- si tratta di adolescenti brillanti ma soffocati da un sistema educativo non adeguato e da insegnanti non preparati o scarsamente equipaggiati;
- provengono in prevalenza da famiglie problematiche;
- presentano una ribellione verso tutti i simboli e le espressioni dell'autorità.

Occorre fra l'altro notare che esistono hacker di tutte le età, ceti sociali, professioni, provenienze geografiche ed etnie.

Con riguardo alle costanti che abbiamo analizzato nel corso dei primi due anni del progetto Hacker's Profiling, occorre tenere presente che esse sono qui formulate positivamente, ma possono anche essere viste in negativo, come per esempio l'evoluzione verso conoscenze tecniche più approfondite o la stabilizzazione, così come la presenza o l'assenza di qualità e caratteristiche specifiche e puntuali.

Prima di analizzare i dati raccolti, ci sembra però necessaria un'altra premessa, ovverossia l'evidenziare come sia doveroso evitare l'uso di terminologie come “mondo reale” e “mondo virtuale”, le quali sono state e sono tuttora abusate, oltre che palesemente sbagliate. Infatti, non solo per chi commette attacchi informatici, non esiste alcuna differenza tra i due, ma soprattutto, la seconda categoria è inesistente, dato che ciò che avviene in un network, rete, o “dietro le quinte” delle linee e delle centrali telefoniche, non è affatto virtuale ma, anzi, accade realmente.

Riteniamo quindi piuttosto più corretto e meno fuorviante parlare di *mondo elettronico* e *mondo fisico*. Vi sono peraltro hacker che riescono perfettamente a stare a cavallo tra questi due mondi, attraverso l'hacking da un lato e il *social engineering*¹ dall'altro.

1. Social Engineering. Letteralmente, “Ingegneria Sociale”. Si tratta di una tecnica hacker per carpire informazioni – utili all'esecuzione di successivi attacchi o semplicemente fini a se stesse – e che utilizza azioni di persuasione della persona, al fine di convincere e influenzare l'interlocutore.

Nel corso della loro carriera hacker – dove con “carriera” ci riferiamo sia all’evoluzione delle capacità tecniche, sia a quella personale – essi si pongono delle domande a cui cercano di dare risposta.

- Perché sono interessato all’hacking?
- Quali sono i miei fini?
- Cosa voglio ottenere attraverso l’hacking?
- Cosa voglio diventare?
- Cosa voglio che la gente pensi di me?
- Come voglio essere ricordato, e per cosa?

Si tratta di quelle stesse domande a cui cercheremo di dare risposta nei prossimi capitoli, ma riteniamo che questa premessa fosse quantomeno obbligatoria.