

Anche i veri non rapinano

Ma come, per mesi vi abbiamo stressato con l'etica dell'hacker, ripetendo che bisogna distinguere tra

1 giornalisti ancora oggi identificano l'hacker con il criminale informatico, ma quando non lo fanno distinguono tra hacker "buono", colui che non causa danni, e "cracker" dando per scontato che il termine voglia dire **hacker "cattivo"**. Descrivono il cracker come un "criminale" o un "pirata informatico", uno che ama bucare i sistemi, entrare e **violare la sicurezza solo per il gusto di esserci riuscito** e con l'obiettivo di sottrarre dati o danneggiarli. Per dimostrare quanto affermato, **ricorrono persino al Jargon File che in genere, per altre questioni, fingono di ignorare**. Ma ad una lettura più attenta del gergo hacker si scopre che il cracker non è mai definito, almeno apertamente, criminale e che eludere la sicurezza di un sistema non è un crimine nemmeno per un "hacker buono".

>> La prima abilità di un hacker

Se il significato 6 del Jargon File descrive l'hacker come **"un esperto o un entusiasta di qualsiasi tipo"**, il significato 5 limita la competenza dell'hacker a un unico campo. E', infatti, "un esperto di un particolare programma, o uno che ci lavora frequentemente", "un hacker di UNIX". Quando si

Jargon File

Nasce come dizionario per tradurre il gergo degli hacker in una lingua "comprensibile dagli umani". Vi si possono infatti trovare le definizioni di più di 2000 termini. A differenza di un normale dizionario, però, rivestono molta importanza anche le varie prefazioni e appendici, mirate a definire meglio la figura e l'etica dell'hacker. Qualcosa di simile al Jargon File esiste anche in italiano, anche se non si dilunga sulla filosofia hacker. E il Gergo Telematico curato da Maurizio Codogno (<http://xmau.com/gergo>).

tratta di veri esperti in un settore, però, i termini più appropriati sono **wizard** ("mago") o **guru** ("santone"). I significati 1 e 7 invece non solo danno una definizione più precisa di hacker, ma spiegano molto bene quale sia l'abilità di base di qualunque hacker. Ciò che l'hacker sa fare veramente è **"studiare un sistema (anche non informatico), scoprirne debolezze, peculiarità e caratteristiche nascoste, e utilizzarle per scavalcare o aggirare i limiti"**, persino quando è **"un ficcanaso maligno che tenta di scoprire informazioni delicate frugando qua e là"** (significato 8).

Quando si parla di hacker e in particolare di questa sua abilità, non si può non parlare di sicurezza. Un hacker, e quindi non solo un cracker, studia e conosce così bene i sistemi informatici che può scoprirne facilmente i buchi (bugs, bachi) attraverso i quali può aggirare tutti i sistemi di sicurezza ed entrare nel cuore della macchina fino a prenderne il controllo. Oppure sa entra-

re nel codice sorgente del software, individuare quelle porzioni di codice che fanno funzionare male o che limitano il programma, può modificarlo, migliorarlo ed anche in questo caso, se vuole, può aggirare le restrizioni. Un hacker sa fare la stessa cosa anche con i sistemi umani che pure non sono privi di bug, come dimostrato da alcune sue attività ben note, che si svolgono al di fuori della rete e del mondo dei computer. Il **Tech Model Railroad Club** del MIT promosse ad esempio il **Midnight Requisitioning Committee**, incursioni notturne nei magazzini e il **Lock Hacking**, l'hackeraggio di serrature delle porte per portar via i componenti necessari per costruire macchinari più efficienti o per usare gli strumenti contenuti nelle stanze chiuse. Ci sono poi il **social engi-**



CRACKER le banche!

ra hacker e cracker, e ora cambiamo idea? Non proprio, ma leggete cosa ha da dire a proposito DaMe' ...

neering, l'ingegneria sociale, una serie di metodi per spacciarsi per un altro ed ottenere così delle informazioni riservate; il **vadding**, l'esplorazione di posti dove le persone comuni normalmente non hanno accesso; il **trashing**, rovistare nei rifiuti, ad esempio di "Mamma Telecom", per saperne di più sul mondo delle comunicazioni in Italia (S. Chiarelli & A. Monti, Spaghetti Hacker).

>> Cracker: il Jargon File insegna

Sfruttando le debolezze di un sistema o di un programma si può ottenere ciò che non si è autorizzati ad avere. Alcuni dei metodi applicati dagli hacker sono **in contrasto con il diritto di proprietà**, e finalizzati quasi tutti all'accesso a informazioni a cui non si avrebbe diritto. Questo spiegherebbe in parte perché gli hacker siano temuti, considerati delle figure estremamente scomode, ma di certo non giustifica l'uso da parte dei giornalisti del termine "criminale" neanche quando è associato al cracker. Nel Jargon File si afferma che il cracker è **"uno che elude la sicurezza di un sistema"** (breaks security on a system), sa cioè violare le "serrature", i codici di accesso o i sistemi di protezione dei software e dei sistemi informatici. Non c'è scritto che

rompe o danneggia i sistemi! Il termine è stato coniato nel 1985 circa dagli hacker **"in difesa contro l'uso scorretto del termine "hacker" da parte dei giornalisti che lo intendevano nel significato 8 del Jargon File"** e cioè come "ficcanso maligno" (malicious meddler). "Un precedente tentativo di instaurare il termine "worm" in questo senso nel 1981-82 circa su USENET, fu un fallimento".

Il termine cracker viene quindi scelto per distinguere l'hacker da **uno che fruga e rovista** (by poking around) nei sistemi, non per distruggere ma per scoprire informazioni delicate (to discover sensitive information). Non viene però chiarito se siano queste informazioni ad essere distrutte o ad essere utilizzate in maniera illecita e cioè per altri scopi che vadano ben oltre il puro piacere di essere riusciti a "scoprirle". Il cracker entra in un sistema senza permesso e questo può anche essere considerato illegale, ma da qui a dire che ciò che è "illegale" sia anche "criminale" ce ne vuole! Certo è che il Jargon File descrive il cracker, non come un criminale, ma come un "maligno", **"una separata e più bassa forma di vita"** (a separate and lower form of life) e persino come un **"perdente"** (pretty losing), perché non riesce ad immaginare un modo più interessante di utilizzare il computer che quello di penetrare nei sistemi informatici altrui. Ciò che fa un cracker, sa farlo anche un

hacker, ma **"Mentre ci si aspetta che qualunque vero hacker abbia crackato per diletto e conosca molte delle tecniche di base, chiunque abbia passato lo "stato larvale" ci si aspetta che**

abbia superato il desiderio di farlo". L'atto di penetrare in un sistema informatico, infatti, "contrariamente al mito diffuso non richiede una qualche misteriosa brillantezza, ma piuttosto persistenza e la tenace ripetizione di utili e ben noti trucchetti e lo sfruttamento di debolezze comuni nella sicurezza dei sistemi che si intende attaccare. Di conseguenza **la maggior parte dei cracker sono solo hacker mediocri**" (mediocre hackers).

>> L'assalto degli script kiddies e dei lamer

Anche l'hacker, come si è visto, sa aggirare i limiti dei sistemi e dei software,



ma il suo interesse non è rivolto esclusivamente a questa attività. Un tempo praticare il cracking per un hacker significava soprattutto **sviluppare da soli i programmi per entrare nei sistemi informatici**, essere ottimi programmatori, conoscere il funzionamento dei software, il linguaggio macchina, i comandi diretti del processore. A partire dagli anni 80, con la diffusione della cultura informatica, la situazione cambia. Si avvera il sogno di Apple e Microsoft: "un computer in ogni scrivania e in ogni casa" e sono sempre più numerose le riviste informatiche che insegnano programmazione e persino tecniche particolarmente avanzate. Negli anni 90 il computer è già diventato un elettrodomestico e le riviste, ora un po' più scadenti, spiegano soprattutto come usare i programmi. Ed è proprio in questi anni che **si affermano gli hacker mediocri!** Chiunque abbia un minimo di conoscenze informatiche, e ormai sono pochi a non averne, e disponga di alcuni specifici software, sviluppati ovviamente da altri, ma disponibili in rete, **può facilmente lanciare degli attacchi di vario genere o nascondere la propria identità per penetrare in un sistema informatico.** Come nel caso dei metodi applicati ai sistemi umani, qualche volta basta semplicemente essere furbi e un po' psicologi. Tutti possono pratica-

re il cracking, e non solo gli hacker allo stato larvale, ma **anche i veri e propri criminali**, quelli che tanto per intenderci rubano i codici delle carte di credito per poi trarne profitto personale. E persino i ragazzini che i giornalisti definiscono hacker e che in realtà altro non sono che degli **script kiddies** o, quando danneggiano, dei **lamer** o **wannabe**, in pratica delle persone davvero poco esperte, che non dispongono neanche delle conoscenze di base necessarie.

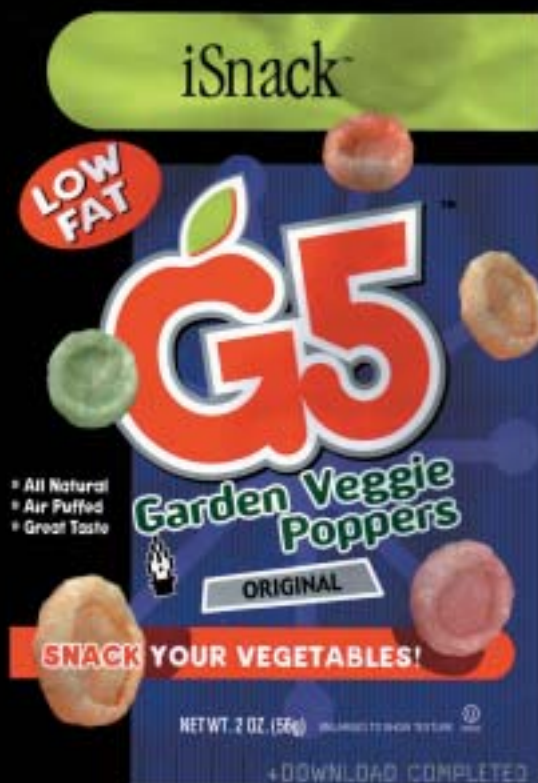
"Il passaggio di consegne del mondo dei computer dagli hacker alla gente comune, spiega Valerio Capello nel suo documento *Essere Hacker*, ha certamente avuto degli effetti generali positivi, ma si è rivelato un'arma a doppio taglio, soprattutto con l'avvento di Internet: chiunque oggi può avere degli strumenti potentissimi per danneggiare gli altri, delle vere e proprie *armi digitali*, senza avere alcuna idea di come questi funzionino e come debbano essere maneggiati. **Si può finire in galera con la convinzione di aver perpetrato soltanto un simpatico scherzo**, anche se un po' di cattivo gusto".

>> La mancanza di pudore dei giornalisti

I veri hacker, quelli che sviluppano la tecnica e realizzano dei programmi con cui poterla sfruttare ed hanno un senso etico molto forte, verso la metà degli anni 80 sentono l'esigenza di **prendere le distanze da coloro che agiscono senza alcuna motivazione valida** e senza neanche essere tecnicamente eccellenti. Non vogliono essere confusi con gli hacker mediocri di quegli anni identificati da forze di sicurezza e dai media coi criminali, "per permettersi di reprimere indiscriminatamente qualsiasi forma di dissenso sociale verso le politiche economiche dominanti di sviluppo delle nuove tecnologie della comunicazioni" (Di Corinto e Tozzi), forme di dissenso che gli hacker insieme ai programmatori, agli attivisti sociali e gli agitatori intellettuali hanno sempre praticato. I giornalisti, ancora oggi, **non distinguono mai, tra hacker-cracker, criminali e semplici lamer.** Preferiscono descrivere persino i lamer come degli hacker e chiamare cracker o criminale chiunque eluda la sicurezza di un sistema. "Nessuno, specialmente un giornalista, sostiene Capello, dovrebbe confondere un hacker con il povero sprovveduto finito in galera per aver utilizzato con troppa leggerezza qualche programma che gli è capitato tra le mani (anche se forse usare il termine hacker fa più notizia... **La differenza tra gli hacker**



+DOWNLOAD THIS!



e i giornalisti è che i primi hanno un'etica, i secondi neanche il senso del pudore)".

Se questi stessi giornalisti consultassero la voce "etica hacker" del Jargon File e non si limitassero solo a quella di "cracker", scoprirebbero che penetrare un sistema non è considerato neanche dai veri hacker un crimine. A proposito dell'etica hacker infatti si legge: "La convinzione che penetrare nei sistemi per divertimento ed esplorazione è eticamente a posto, finché il cracker non commette furto, vandalismo, o diffusione di informazioni confidenziali".

I veri criminali, per gli hacker, **sono quelli che non rispettano l'etica hacker ed entrano nei sistemi solo per danneggiare.** Nel Jargon File è considerato "criminal" solo il Dark-side hacker ("Hacker del Lato Oscuro"), colui che è "sedotto dal Lato Oscuro della Forza". Benchè sia altrettanto esperto di computer e assetato di conoscenza, abbia la stessa abilità e dignità di un hacker, è più proiettato verso il male anziché il bene. Il suo "orientamento" lo rende elemento "potenzialmente" (e quindi anche in questo caso "non necessariamente") pericoloso per la comunità.

HJ ALERT!

Nel nostro paese (e non solo) è illegale penetrare nei sistemi altrui anche senza commettere vandalismi, furti o altro. Quindi a prescindere da questioni morali, **NON FATE CA...ATE!**

>> Anche i cracker hanno un'etica

Bene e male per gli hacker non hanno lo stesso significato che per le persone comuni e le istituzioni. Penetrare un sistema, per un hacker, non è un atto criminale, ma **una sfida intellettuale.** Il fine non è danneggiare o provocare un danno a qualcuno, e neanche il guadagno personale, ma **trovare un mezzo di penetrare le sue difese.** Lo scopo primo per un hacker è sempre quello di acquisire

nuove conoscenze o migliorare quelle che già ha. Prova piacere nell'esplorazione e nella scoperta di nuovi modi per superare i propri limiti oltre che quelli dei sistemi con o attraverso i quali opera. Sfida innanzitutto se stesso e la propria abilità. Per un hacker è un dovere etico facilitare l'accesso all'informazione e per molti hacker non ci sono informazioni a cui non si ha diritto di accesso. "Il ragionamento è semplice, spiegano Di Corinto e Tozzi. Se l'informazione è potere e la tecnologia

il suo veicolo, per opporsi al monopolio dell'informazione "che serve a dominare le masse" ogni mezzo è legittimo per redistribuire informazione e conoscenza", persino penetrare un sistema. Anche un hacker quindi all'occorrenza può utilizzare il cracking e il cracker può sprotteggere un programma o irrompere in un sistema per motivi etici, perchè è convinto che si possa migliorare o perchè ritiene che certe informazioni e certi saperi debbano essere diffusi e condivisi da tutti. Insomma c'è una grande differenza, ad esempio, tra chi copia software per distribuirlo agli altri e chi copia il software per rivenderlo e trarne profitto. Penetrare illegalmente in un sistema protetto "per finalità etiche positive può rientrare nella definizione di cracker, **se invece avviene per scopi individuali e di profitto la definizione corretta è quella di criminale informatico**".

Il cracking, quindi, potrà anche essere considerato illegale dalle istituzioni, ma di certo va distinto dalla volgare pirateria e dai criminali, perché parafrasando un intervento di L. Felsenstein anche i **"Real Crackers Don't Rob Banks"**. ☞

DaMe`
www.dvara.net/HK

BIBLIOGRAFIA E SITOGRAFIA

<http://info.astrian.net/jargon/>
Jargon File (con possibilità di effettuare ricerche)

<http://www.s0ftpj.org/bfi/online/bfi7/bfi07-02.html>
Valerio Capello - Essere Hacker

Di Corinto e T.Tozzi - Hacktivism. La libertà nelle maglie della rete
In particolare i paragrafi:

1.1.2. Gli Hackers non sono tutti uguali:

http://www.hackerart.org/storia/hacktivism/1_1_2.htm

3.4.3. L'underground Telematico, Il Phreaking e i Crackers:

http://www.hackerart.org/storia/hacktivism/3_4_3.htm