PLAYBOY

IL PIACERE DI VIVERE DA UOMO

numero 8 · € 3,00

MOANA
L'IMMORTALE
DA REGINA DELL'HARD A *MITO*. E LA TV LE DEDICA UNA SERIE

20 DOMANDE A
JORGE LORENZO
IL **RIVALE NUMERO UNO** DEL DOTTOR ROSSI VOLA VELOCE... E NON SOLAMENTE IN PISTA

PLAYBOY INTERVISTA...
BOB SINCLAR
IL **DJ FRANCESE** PARLA DELLA SUA PASSIONE PER L'ITALIA E RENDE OMAGGIO AL CONIGLIO PIÙ FAMOSO DEL MONDO!

PER UN'ORA D'AMORE...
IL DDL CARFAGNA RISCHIA DI MANDARE DEFINITIVAMENTE IN PENSIONE LA LEGGE MERLIN!
INCHIESTA SUL FENOMENO DELLA PROSTITUZIONE IN ITALIA

Valeria Marini

Regale, seducente e assolutamente unica
PERCHÉ DIVE SI NASCE E NON SI DIVENTA!

Poste Italiane S.p.A. - Spedizione in A.P. - D.L. 353/2003 (conv. in L.27/02/2004 n°46) art. 1, comma 1, DCB Milano

www.playboy.it

90008>
9 771125 667003

Non chiamateci SMANETTONI!

DICI HACKER E PENSI SUBITO A RAGAZZINI CHE SI DIVERTONO A "BUCARE" I SISTEMI INFORMATICI ALTRUI. COLPA DI HOLLYWOOD. E DI UN'IMPRECISA TRADUZIONE ITALIANA CHE PORTA PIUTTOSTO FUORI STRADA... *{di Alessandro Calderoni}*

Chi diavolo sono oggi gli hackers? Chi sono questi cosiddetti "pirati informatici", pessima traduzione italiana del termine anglofono che ai suoi albori accademici, mezzo secolo fa, non aveva alcuna connotazione negativa ma indicava esclusivamente l'attitudine alla ricerca e alla comprensione? E chi sono in Italia, soprattutto? Gente che smanetta sul pc per far evolvere la tecnologia, maniaci della sfida, persone che si divertono a bucare sistemi altrui, pericolosi criminali informatici? O ancora: cervelli prestati alle industrie e ai governi, attivisti che teorizzano la libera circolazione delle informazioni, violatori perpetui del diritto d'autore? O tutto questo insieme?

Di sicuro appaiono remoti quegli anni Ottanta in cui Loyd The Mentor Blankenship, hacker statunitense classe 1963, scrive dal carcere il suo manifesto: «[...] Noi esploriamo... e ci chiamate criminali. Noi cerchiamo conoscenza... e ci chiamate criminali. [...] Sì, io sono un criminale. Il mio crimine è la mia curiosità». Al cinema è appena uscito Wargames e Matrix è un'apoteosi ancora lontana. I nerd dell'epoca scoprono che i computer possono connettersi tra loro via telefono e cominciano a scambiarsi conoscenza e a formare una comunità. Poi, verso la metà dei Novanta, internet esce dalle università e anche in Italia diventa una possibilità per tutti. Il mondo si apre al mondo. E gli hackers proliferano.

«Nel 1986 non facevi hacking per denaro ma per curiosità e pionierismo». Chi parla è Raoul Chiesa, 36 anni, all'epoca noto

Getty Images

New
Open...
Save

Quattro diversi scenari per capire il mondo on line

1 Da anni, in diverse parti del mondo, si combattono battaglie e guerre elettroniche contro le istituzioni di vari paesi, basate su attacchi via internet orditi da altri paesi o da aggregazioni spontanee di liberi cittadini in rete. Nel 2007 l'episodio più noto: l'Estonian cyberwar, una serie di attacchi coordinati di origine russa, a tutte le principali organizzazioni civili e militari estoni.

2 Nasce il Cyber Command, l'organismo statunitense costituito per difendere da attacchi online i 7 milioni di computer della Difesa americana. L'esecutivo di Obama ha chiesto la consulenza di Dark Tangent, pseudonimo del fondatore di due convegni di hackers, Black Hat e DefCon. In Italia nasce, il Centro Nazionale Anticrimini Informatici (Cnaipic).

3 Il processo a The Pirate Bay, celebre sito web svedese per il libero scambio di file tra internauti, si chiude in primo grado nell'aprile 2009 con la condanna a un anno di reclusione per violazione del diritto d'autore comminata ai quattro titolari del sito, che dovranno anche risarcire tre milioni di euro alle industrie discografica, cinematografica e dei videogiochi.

4 Alle europee 2009 il Piratpartiet svedese, nato nel 2006, ottiene il 7,1% dei voti, riuscendo a conquistare un seggio in Europarlamento. Altri partiti pirata esistono ufficialmente in Spagna, Austria e Germania, movimenti attivi si trovano anche in USA, UK, Australia e Polonia, mentre in Italia, con sede a Trento, esiste un'associazione di promozione sociale senza scopo di lucro.

come Nobody. Fu arrestato dopo anni di incursioni nei sistemi di aziende pubbliche e private. Dal 1995 ha cambiato vita, dandosi al cosiddetto hacking "etico", e gestendo un'azienda di sicurezza a Torino. Da qualche tempo, inoltre, si occupa di HPP, Hackers Profiling Project, un sistema integrato di studio criminologico, nell'ottica della prevenzione degli attacchi informatici. «Abbiamo somministrato questionari a 1200 hackers e ne abbiamo intervistati decine, girando il mondo attraverso le conferenze di settore. Prossimamente riempiremo le reti di honeypot, specchietti per le allodole, server vuoti e sprotetti ma resi interessanti, in modo da capire chi attacca e perché, ottenendone un profilo». Insomma il ladro che diventa guardia e tenta di diffondere la cultura dell'hacking inoffensivo, anche attraverso manifestazioni ludiche, come quella organizzata la scorsa estate a Orvieto, con sessanta partecipanti, tra cui due intere famiglie.

«Underground is dead, il movimento è finito», sentenzia Vecna, "ex" hacker lombardo 29enne, profondo conoscitore del funzionamento e della sociologia delle reti. «Già quindici anni fa ero attratto dalla scrittura di software che sfruttassero anomalie della rete. La mia specialità era la comunicazione invisibile. Tra quella prima fase, in cui l'aspetto romantico era predominante, e la seconda, in cui la new economy ha insegnato il valore della sicurezza e il pericolo di chi la viola, molti hackers si sono ritrovati ad avere competenze utili al mercato, e quindi si sono trasformati da ragazzini smanettoni in professionisti iperqualificati».

Un esempio di declinazione sociale della cultura hacker è l'Hackmeeting, un incontro annuale tra i protagonisti italiani del settore, in cui la rete è intesa come mezzo di equità e di apertura dell'informazione. L'ultimo si è tenuto alla Fornace di Rho nel mese di giugno. TiBi, hacker donna, uno dei promotori dell'iniziativa, spiega che «hackmeeting potrebbe essere vissuto come un luogo deputato alla sperimentazione tecnica ma la differenza rispetto ad altri spazi è che in questo ambito si agisce per esprimere una critica ai sistemi che portano controllo».

Ha scelto una strada formalmente diversa Stefano Zanero, ingegnere milanese alla soglia dei 30, ex hacker con il nick Raistlin, docente di Sicurezza informatica al Politecnico e conferenziere internazionale. «Ciò che mi ha sempre appassionato è la vulnerabilità di sistema, cioè la possibilità di individuare punti deboli macroscopici nel funzionamento di una cosa, mentre tutti si dannano a cercare qualcosa di sbagliato in ambito microscopico. L'hacking resta in me sotto forma di modello di pensiero interiorizzato. Prima si partiva dall'etica per arrivare alla tecnica, oggi è il contrario. Difficile trovare un vero esperto di information security che sia favorevole al blocco e al filtraggio dei contenuti. Ci fanno percepire la necessità di rinunciare alla privacy per garantire la sicurezza, basti pensare ai semplici aeroporti. Non è così. Non ha senso sapere tutto di tutti, sempre e comunque. Il volume di informazioni ricavate non è

proporzionale al volume dei dati posseduti, senza un metodo efficace per interpretare i dati medesimi». Gli studenti di Zanero sono una piccola popolazione di potenziali hackers. «Li vedo, sono disincantati, nessuno pensa più di poter cambiare il mondo. Fanno il buco e scovano la vulnerabilità per mettere tutto in curriculum e trovare subito lavoro».

Un altro quasi trentenne geniaccio del pc, emerso dall'ambiente hacker, è Fabio Pietrosanti, originario di Latina, noto come Naif, una delle menti della mailing list sikurezza.org, già consulente per la corporate security di Telecom Italia, attualmente responsabile tecnico di Khamsa, un'azienda svizzera che si occupa di sistemi anti-intercettazione telefonica. Fabio è un furbo, principalmente. Ama cercare soluzioni. Per esempio usa Facebook in modo atipico. «Ho aggiunto come amici soltanto persone che hanno il mio stesso cognome, soprattutto all'estero. In questo modo, con pochi messaggi, riesco a combinare viaggi e farmi ospitare in luoghi remoti, perché l'ipotetica parentela alla lontana è un vincolo più forte della semplice amicizia su FB». A 15 anni il primo successo per lui fu trovare un modo per non pagare la connessione a internet. «Si faceva un processo di war dialing, cioè si scansionavano tutti i numeri telefonici verdi, quelli gratuiti, finchè non se ne trovava uno attaccato a un modem e non a un telefono: riuscendo a entrare nelle reti aziendali agganciate, si poteva sperare che esistesse anche una porta d'uscita verso internet e navigare così a zero lire». Ancora ragazzino Naif diventa famoso in rete, quando trova tre vulnerabilità nel blasonato sistema di sicurezza Cisco Pix Firewall. «Oggi l'associazione "hacker uguale violare sistema" non è più corretta perchè chiunque può andare in edicola o su internet e trovare software, uno su tutti Metasploit, che da soli individuano vulnerabilità altrui e le sfruttano come suite di attacco». Esemplare la storia di Albert Gonzalez, un tizio statunitense attualmente condannato a trent'anni, che aveva ideato una geniale economia di scala basata sulle truffe ai grandi magazzini: ti attacchi al sistema informatico di una catena di maxistore, sniffi tutte le transazioni con bancomat, quando hai un database di alcune migliaia di carte e codici pin imprimi i dati su schede magnetiche vergini e in un weekend fai prelevare quattrini dalle carte clonate in diversi punti del mondo grazie al supporto locale della criminalità organizzata. Un altro versante è quello delle invenzioni hardware quasi fantascientifiche. «In Germania ho visto presentare un attacco Tempest per intercettare le parole scritte da un normale utente di computer sulla tastiera, sparando un laser sul retro di un monitor, nel caso di un portatile, o su una presa elettrica, nel caso di normali tastiere da pc desktop». Certo, una volta il mercato della security non era molto sviluppato, mentre oggi le competenze sono ricercatissime, anche tra i governi. «Gli americani prendono esperti per formare i loro militari, mentre gli inglesi vanno a pescare anche civili che hanno le mani nel torbido. L'attitudine è utilizzare le competenze d'attacco a fine di difesa. In Italia, fino a questo momento, il governo si è ridotto semplicemente a pagare consulenze da società private che vendono virus e li inoculano su commissione, per rendere sistemi di terzi accessibili e controllabili. Mentre il presente degli attacchi d'intelligence consiste nell'acquisizione silente di informazioni, il futuro prossimo sta sicuramente nell'azione reale su enti fisici connessi in rete. Spegnere centrali, acquedotti e radar da un pc remoto sarà una forma di guerra preventiva e mirata».

Più giovane, ma già ottimo aggregatore nella comunità hacker italiana, Francesco Ascii Ongaro, 24 anni, di origini venete, più di dieci anni fa ha fondato un team di ricerca indipendente, USH.it, per la condivisione online di tecniche di settore. «Il fascino dell'hacking, non è tanto nel risultato che ottieni, ma nello sforzo costruttivo che ci metti e nell'eredità di conoscenza che lasci». A 16 anni Ascii comincia a fare lo sviluppatore web per un'azienda. Oggi è consulente senior in abito Security. «Si è passati da un mondo di applicazioni separate a un mondo di applicazioni integrate e online. Dalla chiusura dei dati all'apertura dei dati. L'enorme disponibilità di informazioni rende la vita facile all'esercito di kiddies che si autodefiniscono hackers. Ma l'unico modo per tornare ad avere giovani hackers con le palle è che il lavoro torni a essere difficile. L'insicurezza diffusa è il declino della cultura hacker perché se violare qualunque cosa è facile nessuno si applica davvero e la tecnica scema». Come dire: se non c'è il danno, non c'è evoluzione. «Oggi la gente ha paura di essere frodata on line dagli hackers. Ma non sono loro il pericolo, bensì la criminalità organizzata che ha messo le mani su una tecnologia ormai facile e disponibile. Gli hackers si occupano di tematiche più complesse. Non perdono tempo a fregare la signora che fa la spesa sul web. Magari hanno inventato la tecnica usata dai ladri per farlo. D'altronde non applicarvisi sarebbe stato come evitare di studiare il nucleare per paura che qualcuno inventasse la bomba atomica». ■

La nuova criminalità organizzata passa dal web

Intere organizzazioni criminali si avvalgono di sistemi intrusivi occulti per tele controllare i pc di milioni di ignari internauti. Basta un messaggio di posta elettronica con un link o un sito web in cui sono inserite alcune righe di codice in grado di sfruttare le specifiche vulnerabilità del browser di chi naviga. Queste istruzioni anomale possono fare compiere azioni imprevedibili al software, senza che l'utente se ne avveda. Il primo esempio di questo tipo di crimine è emerso negli ultimi tre anni con la cosiddetta RBN, Russian Business Network: un'organizzazione malavitosa con base a San Pietroburgo e specializzata in botnet, ma anche in hosting di siti pedopornografici e produzione di software per il telecontrollo dei pc. Perché dall'Est? «L'humus scientifico era ottimo - risponde Stefano Zanero, docente di Sicurezza Informatica al Politecnico di Milano - Le forme di telelavoro possono essere molto utili nei paesi in cui dal lavoro fisico si guadagna molto poco. Terzo, l'informatica consente di ottenere grandi risultati. Quarto, esiste un pregiudizio per cui colleghiamo spesso il malfattore alla persona dell'est, e questo contribuisce a non farci vedere crimini analoghi in altre zone del mondo».