PIRATI

A LAS VEGAS A FORZARE SISTEMI INFORMATICI. SUCCEDE AL DEFCON, IL PIÙ GRANDE RADUNO MONDIALE DI HACKER. NOI C'ERAVAMO

testo e foto di **EMANUELE BOMPAN**

«Solo chi è in grado di mettere in crisi i sistemi di sicurezza informatici può rendere più sicuro questo mondo». EvOl, cappello nero, tatuaggi ovunque, stappa una cerveza *Dos Equis*, la tredicesima. Siamo sul bordo della piscina del Caesar's Palace, Las Vegas. «Attaccare database di organizzazioni come Onu e Fondo Monetario o compagnie come Sony sta diventando sempre più facile». In meno di 30 minuti penetra nella pagina di un quotidiano italiano, senza toccare nulla. «Le persone, le corporation, i governi non hanno percezione della vulnerabilità. Siamo interconnessi e siamo più a rischio. E non c'è nulla di più utile per un cracker, un hacker malintenzionato, che la stupidità umana».

Benvenuti a DefCon, il più grande meeting di hacker Usa, che si tiene ogni anno a Las Vegas. Pirati anarchici, hacktivisti (*attivisti informatici*, ndr), esperti di sicurezza, goth girl esperte in penetrazioni di reti protette, criptografi, reverse engineer, federali dell'unità cyber-terrorismo, phreaker (*in-*

APPUNTAMENTO AL CASINÒ

Sopra, hostess tra gli stand del DefCon. L'edizione di quest'anno (la 19ª) si è svolta a Las Vegas dal 4 al 7 agosto.






UMANITÀ VARIA Cavalieri cyberpunk, nerd sovrappeso, federali "mocassino e calzino bianco": si trova un po' di tutto.

tercettatori telefonici, ndr), bambini esperti di social network e accademici esperti di social engineering. Se pensate che hacker significhi criminale vi sbagliate, qui si definiscono hacker tutti gli smanettoni di computer e sistemi informatici. Alcuni sono buoni e hanno il cappello bianco, altri si definiscono black hat (cappello nero), o cracker, e spesso hanno intenzioni ostili (anche se non necessariamente criminose). Qualcuno è anarchico o lo fa per motivi politici, qualcuno per divertimento. Tanti per lavoro e per dimostrare la vulnerabilità dei sistemi. Una piccola nicchia è mossa da sano spirito autodistruttivo. A ognuno dobbiamo essere grati, perché se i sistemi informatici sono così sviluppati e così sicuri è solo per le falle scovate dagli hacker nei programmi e nelle fortezze digitali. «Crediamo nella libertà di espressione e nel codice libero», spiega ancora EvOl. E il tappo della 14esima birra rimbalza nella piscina.

Quarantotto ore prima. Ricevo una mail dal mio direttore. "Ok, DefCon, Vegas. Porta foto". Mi imbarco a San Francisco, triplo espresso in mano e lattina di bibita ipercaffeinica. «Dove si reca?». Un meeting di hacker, rispondo distrattamente. In un attimo la sicurezza aeroportuale mi è addosso. «Lei è un hacker?», mi urla uno sbirro dell'Homeland Security, che penso mi abbia scambiato per un terrorista informatico. «No, giornalista», spiego, «la differenza è poca: cerchiamo in fondo di aprire le porte del potere e del mondo economico». Due ore più tardi sono al Rio Hotel&Casinò, sede di DefCon. Il mio badge rilasciato dal dipartimento di Stato Usa, insospettisce l'addetto, ma la bottiglietta di Southern Comfort che sorseggio lo convince che sono innocuo. Ottimo, sono dentro, penso, riprendendo una celebre linea di *Matrix*.

Alle due di sabato incontro il mio collega Steven Levy che mangia *tacos* e *burrito* con foga. Steven, abbigliamento da sfigato, iPad e grande sorriso, oltre a essere una delle firme di punta di *Wired Usa*, è uno dei più grandi conoscitori del mondo hacker. Nel 1984, in tempi in cui era appena uscito il Commodore 64, Steve pubblicava il primo studio sulla genealogia del fenomeno hacker, nato al Mit di Boston. «Oggi la comunità è molto più solida. Negli anni Ottanta quando gli hacker erano Bill Gates, Richard Stallmann, Steve Wozniac e Steve Jobs, erano molto più dispersi. L'etica di base non è però cambiata». Accesso alle macchine informatiche. Condivisione delle informazioni. Non fidarsi dell'autorità e promuovere la decentralizzazione dei poteri. Il ruolo dei computer per cambiare il mondo. «I veri hacker sono rimasti tali. Quello che fanno gruppi come Anonymous o Lulzsec rientra in parte in questo pensiero, solo in maniera più esplicita e dirompente. Lo fanno per una ragione politica, come tradizione del mondo hacker. Ci mostrano le falle di un sistema. Informatico e non solo».

Si incontra un po' di tutto qua a DefCon, tra nerd sovrappeso, cavalieri cyberpunk, e federali *mocassino-e-calzino-bianco*. In tanti cercano lavoro presso agenzie nazionali di cybersicurezza, che fanno di tutto per smettere i panni dei cattivi con gli stivali. Ahmed Saleh, un esperto di analisi informatica Nasa, descrive un'occupazione che può fare gola a molti dei presenti. «Se sei uno smanettone e

PIÙ SIAMO INTERCONNESSI PIÙ SIAMO A RISCHIO. LE FALLE DEI SISTEMI CRESCONO

SBLOCCATO!
Sicurezza informatica e sicurezza "fisica": al DefCon gli hacker si occupano anche di scardinare lucchetti e serrature.

ti piace impegolarti ovunque e dare la caccia ai cattivi noi possiamo offrirti un lavoro. Meglio con noi che contro di noi». Il governo federale è scatenato: la Nsa, l'Agenzia per la sicurezza Nazionale, vuole assumere 1.500 hacker il prossimo anno. «La priorità della sicurezza è soprattutto informatica. È possibile fare più danni con un computer che con una rivoluzione armata», spiega Kenneth Geers del Cooperative Cyber Defence Centre of Excellence.

Mi risveglio che il sole di mezza mattina già brucia sulle pareti del Hotel Riviera.

Meno di un'ora dopo, caffè e uno shot di Mescal, rimango sbalordito dalla dimostrazione di Silverhack nel craccare documenti superprotetti excel. «Potrebbero essere codici di sicurezza o sistemi di difesa. Basta poco per scatenare la terza guerra mondiale», ridacchia l'hacker. Bruce Sutherland, esperto di sicurezza, spiega come preservare la comunicazione in caso un governo ostile (pensate all'Iran...) spenga la Rete. Reti wireless locali, hub satellitari, ponti radio, ogni possibile soluzione quando il flusso di informazioni non può fermarsi.

A un certo punto vedo un modellino di aereo a motore volare sulle teste dei partecipanti. Una piattaforma volante di hackeraggio, mi spiega MikeT, uno degli inventori, capace di avvicinarsi di nascosto a reti governative e infiltrarle. Numerose conferenze parlano di sicurezza della rete elettrica nazionale, attacchi cibernetici di grande scala, DoS, denial of services ovvero interruzione di un servizio, può essere *Twitter* come un database di trading online. «Per questo che i federali sono qua a fare shopping di teste pensanti. Mai come ora hanno bisogno di noi contro cinesi o terroristi», mi spiega EvOl, mentre facciamo scivolare bigliettoni da 20 $ sul tavolo del BlackJack.

Metà convegno, metà party, a DefCon orde di hacker si sfidano per gioco, rompendo muri informatici, infiltrandosi nei network, cercando bug nei programmi, ma anche bevendo strani cocktail e cercando di manipolare una macchina elettorale Diebol (e-voting? Meglio la carta). Domenica mi infilo dentro il contest "Schmooze Strikes Back". Lo scopo di questa gara è testare l'abilità di social engineering degli hacker su compagnie come Apple, Oracle, Symantec e Walmart.

Per social engineering, ingegneria sociale, s'intende l'analisi del comportamento di una persona al fine di carpire informazioni. Finzione, inganno, travestimento, role-playing, qualsiasi strategia legata al raggiro è utile (per fini nobili, intendiamoci, come mostrare la vulnerabilità del personale).

Inizia la telefonata. Risponde un impiegato di una compagnia dotcom Usa. «Sono un addetto del dipartimento XY», spiega il social engineer, «avrei bisogno di questi codici». In men che non si dica ottiene informazioni sensibili di grande importanza, mettendo a nudo la vulnerabilità dell'impresa. Per eroi del mondo hacker come Kevin Mitnik (tra i primi a essersi intrufolato nei computer del Governo Usa) a volte «è più facile chiedere una password che craccarla.

Mentre vago per il Rio Hotel finisco nel villaggio dei LockPicker. Si occupano di sicurezza fisica. Serrature. Dopo 25 minuti sono seduto con un fantastico set di utensili da picklocker, proibiti per legge, a scardinare lucchetti e serrature. «Un gioco da ragazzi!», commenta Lysa che ha appena aperto un enorme lucchetto da moto. Avrà 12 anni. Qui è pieno di mocciosi hacker. Come Anna, seconda media, che è riuscita a fregare il social game *Farmville*, con un trucchetto sull'orologio interno. «Spostando il tempo sul computer la mia fattoria si espande più velocemente», ha spiegato. C'è una sezione DefCon kids, dove occhialuti sbarbati battono sulle tastiere, craccano reti wireless e saldano mini processori. Piccoli anonymous crescono.

Per curiosità finisco alla conferenza di due italiani sulla sicurezza delle carte di credito. Andrea B. e Daniele B. di InversePath sono due reverse engineer ma, precisano, «ci definiamo esperti di sicurezza». Sono qui per presentare un'analisi sui metodi di intercettazione del PIN degli utenti di carte di credito. La semplicità con cui si può effettuare un pagamento è disarmante. Mi stupiscono ulteriormente con un altro progetto, presentato lo scorso anno a DefCon, di un sistema per leggere i testi digitati dalla tastiera del computer attraverso l'analisi della corrente elettrica nella centralina di un edificio. "Très chic", senza dubbio.

Cammino nella notte iperilluminata di Las Vegas fantasticando su interruzioni del servizio elettrico, annullamento di conti bancari in un clic, iPad bianchi senza contenuto, social network bloccati da regimi spietati. Spie, falsi informatici, ladri, scassinatori per sport. Il rumore della città si perde nel deserto, in questo mondo costantemente a un click dalla fine. Che in fondo, grazie anche agli hacker, si salva sempre, nonostante tutto.