WWW.Criminologia.org
TELEMATIC JOURNAL OF CLINICAL CRIMINOLOGY

La psicologia degli hackers

di Marco Strano

ICT security 2003

Molto si è detto e si sta dicendo sul fenomeno hackers. Sono semplici trasgressivi, teppisti digitali o ladri di informazioni? In realtà le motivazioni che si celano dietro un tentativo di accesso clandestino ad un sistema sono molteplici e molteplici sono quindi gli "assetti psicologici" di chi li effettua. E' necessario quindi delineare una tipologia variegata del mondo dell'hacking contemporaneo. Troviamo una parte di loro in una classe di età dai 30 ai 45 anni che rappresentano ciò che è rimasto del periodo iniziale del fenomeno, (in Italia dall'inizio degli anni 80') molti dei quali inseriti nel mondo dell'informatica professionale. Sognano ancora degli ideali di "*etica dell'hacking*" ma hanno quasi completamente abbandonato le frequentazioni pericolose del mondo digitale underground. Ogni tanto gli viene volta di rimettersi all'opera, magari semplicemente di chiacchierare nelle chat tematiche. Ma un'occhiata alla moglie, ai figli e all'automobile nuova appena comprata gli fa cambiare idea. A loro si affianca poi un tipo di hacker "rampante", di età dai 25 ai 35 anni, che dopo un certo periodo di attività *underground* giovanile opera adesso nel mondo della sicurezza ed è deciso a mettere a frutto le esperienze maturate. Non ha ancora abbandonato i legami con le comunità digitali trasgressive da cui cerca di attingere le informazioni utili per le sue proposte di consulenza. E poi ci sono infine i "ragazzini". Orde di adolescenti (alcuni di loro immaturi mentalmente ma non anagraficamente) che utilizzano l'hacking per soddisfare la loro voglia di trasgressione e di distruzione. Cercano tools sulla rete e imparano a fare *port-scanning* selvaggio e qualcosina di più complesso come i defacement o i "disturbi" alle chat. Poi si vantano in rete o al pub sotto casa. Qualcuno li chiama *lamers*. Ti raccontano le loro gesta illegali sorridendo, ammiccando, autoincensandosi. Molti di loro hanno più paura della mamma che della Polizia Postale.

L'inganno degli ex hacker

Talvolta personaggi che si definiscono ex-hackers, allestiscono vere e proprie società di consulenza informatica grazie alle competenze acquisite durante il periodo "selvaggio". Ma le loro competenze divengono ogni giorno più obsolete: si sa, nel mondo del cyberspazio le abilità diventano rapidamente superate.

In alcuni casi questi personaggi hanno effettuato una serie di intrusioni nell'azienda a cui volevano offrire la loro consulenza per poi presentarsi con la "soluzione" dopo aver provocato il panico.

Allora inizia una sorta di sdoppiamento di personalità. Di giorno li incontri con il vestito buono, pettinati compiti ed ossequiosi, mentre tentano di vendere alle aziende importanti i loro prodotti di sicurezza, la notte invece si rimettono i jeans, la felpa larga e magari il berretto con la visiera all'indietro e frequentano i circoli telematici "trasgressivi" cercando di mischiarsi con i ragazzini impertinenti che defacciano i siti o lanciano i tools.

Frequentano gli *hack-meeting*, cercano di farsi fotografare dai giornalisti per mostrare in giro che appartengono ancora a quel mondo, che sono ancora al centro di un circuito di informazioni, che sono ancora in grado di fare hacking.

Note legali: il presente articolo o documento può essere riprodotto integralmente o in parte citando la fonte: *nome autore* - data - **Telematic Journal of Clinical Criminology** – www.criminologia.org

E ancora, a volte rilasciano interviste inneggianti alla "libertà sulla rete" e il giorno dopo partecipano ad un congresso sulla *security* promosso dal mondo aziendale e propongono un sistema di sicurezza adatto proprio alle famigerate compagnie telefoniche, le famose "telco", obbiettivi elettivi per Capitan Crunch e per i primi hackers storici degli anni 60'-70'.
E i "ragazzini" si ritrovano al centro di un processo di strumentalizzazione. Qualcuno gli continua a dire a mezza bocca che "*…..non siete delinquenti ma anzi contribuite alla sicurezza delle reti attaccandole, mostrando le falle del sistema, suggerendo indirettamente degli interventi di sicurezza…..*"
Del resto, "quando arriva uno sciame di cavallette i contadini bestemmiano ma i venditori di insetticida si fregano le mani…" Milioni di dollari guadagnati ogni anno dalle compagnie che si occupano di sicurezza o che producono antivirus sarebbero a rischio se improvvisamente gli attacchi dei ragazzini sulla rete dovessero diminuire. Molti esperti di sicurezza informatica dell'ultima ora tornerebbero a riparare i televisori.
Così i ragazzini si illudono, li ascoltano e quando si fanno beccare si prendono una denuncia penale. Assaporano una trasgressione apparentemente a basso rischio, una trasgressione intelligente, raffinata, unita all'illusione adolescenziale di possedere il mondo. Illusione che regolarmente fallisce per la maggior parte dei sognatori e che si concretizza solo in età adulta per quei pochissimi che riescono ad accedere a quelle definite dal Sociologo Vilfredo Pareto come *elìte di potere.*
L'illusione di poter governare subito un mondo parallelo, virtuale che gli adulti non sono ancora riusciti a controllare anche perché hanno sbagliato all'inizio a progettarlo con il protocollo a pacchetto di internet.
Ma il gioco è bello quando dura poco e questo gioco dura sempre meno. Si moltiplicano in tutto il mondo le denunce penali a carico di giovani hacker che prendono coscienza dell'inganno operato dai media nei loro confronti solo quando vedono arrivare nella loro casa, magari al mattino presto (come per i delinquenti…) la Polizia Postale del loro paese. Fare l'hacking è quindi attualmente, più che un'opportunità di lavoro, soprattutto un'opportunità per essere denunciato.
Sull'assunzione di ex-hacker da parte delle aziende sono infatti in corso parecchie dispute, in special modo sulla reale affidabilità a lungo termine di tali soggetti e sulla rapida obsolescenza delle loro conoscenze una volta abbandonato il mondo dell'hacking attivo. Secondo gli standard americani, ad esempio, un passato burrascoso nell'*underground digitale* mal si sposa con un'assunzione (anche come consulente) in una company seria.

Gli hackers contribuiscono a migliorare la sicurezza delle reti?
La giustificazione morale addotta da molti giovani pirati, rinforzata purtroppo anche da certa stampa, è che le intrusioni clandestine contribuiscono a testare la sicurezza della rete offrendo un servizio alla collettività. Questa giustificazione in realtà si rivela spesso un alibi psicologico perché è possibile provare e sperimentare la sicurezza dei sistemi tecnologici anche in "laboratorio", mentre i computer non stanno gestendo operazioni, magari iscrivendosi all'Università, senza provocare disagi e costi economici ai possessori dei siti web o delle banche dati violate. I produttori di serrature sperimentano l'efficienza dei loro prodotti senza andare a rubare di notte nelle case dei potenziali clienti.

Le vittime degli hackers sono solo grandi organizzazioni?
L'idea che gli hackers effettuino intrusioni solo a danno delle grandi organizzazioni è sbagliata. Le vittime dell'hacking, infatti, non sono solo grandi organizzazioni. Molte associazioni di pubblica utilità, Medici, Psicologi e ricercatori di altre discipline, piccole realtà che attraverso la rete riescono a diffondere informazioni utili, possiedono normalmente computer poco protetti (per scarsezza di risorse) e rappresentano una facile preda anche per gli hacker inesperti. Molti siti web violati appartengono statisticamente a piccoli imprenditori e commercianti che stanno tentando di realizzare del commercio elettronico con sacrifici enormi, impegnando i loro risparmi. I costi di realizzazione di un sito web professionale possono infatti essere anche elevati. Le intrusioni per tali imprenditori possono quindi costituire un danno enorme.

Note legali: il presente articolo o documento può essere riprodotto integralmente o in parte citando la fonte: *nome autore* - data - **Telematic Journal of Clinical Criminology** – www.criminologia.org

Gli hackers sono trasgressivi ma non criminali?
Le intrusioni telematiche sono punite da norme penali. Le sanzioni previste stanno rapidamente diventando elevate in tutto il mondo. Ogni violazione di una norma penale è di fatto un crimine e quindi di interesse della Criminologia. Nel cyberspazio si trovano ormai interessi da tutelare alla pari (se non di più) che nel mondo reale.

Dinamiche psicologiche dell'hacking giovanile
Gli hackers, specie se giovani, presentano una ridotta percezione del crimine e tendono a non autodefinirsi come dei criminali. La mediazione del computer tra loro e la vittima genera intorno all'azione illegale un'atmosfera tipica del videogame. La scarsa omertà che contraddistingue le comunità hacker (colui che riesce in qualche impresa telematica è solito infatti vantarsi facilitando, sovente, l'opera degli investigatori) offre ulteriori conferme sulla modesta percezione della gravità di tale comportamento. La presenza di tratti di personalità tipici (es. l'introversione) unita ad un sé ideale (immaginario) è spesso riscontrata in soggetti che praticano intrusioni clandestine. La motivazione che sovente emerge nelle loro azioni illegali è talvolta comparabile, con quella di certe forme di violenza contro le cose e contro le persone, apparentemente senza un vantaggio pragmatico per l'autore (es. danneggiamenti di pubbliche infrastrutture) ma spiegabili nella valenza comunicativa che tali azioni implicano, sia diretta verso l'ambiente esterno e sia diretta verso il sé dell'autore: *danneggio il sistema informatico per mostrare/mostrarmi che sono in grado di farlo e per aumentare il livello di autostima*. L'hacking rappresenta infine uno strumento per alcuni giovani per entrare in comunicazione con il mondo degli adulti "*a livello paritetico*" attraverso il canale criminale, costringendo la società a difendere i propri gangli vitali da coloro che, non essendo ancora direttamente implicati nei processi produttivi, vengono usualmente trattati con "sufficienza". L'essere considerati "importanti" (anche se in ambito illegale) può senz'altro costituire un elemento affascinante per alcuni soggetti che vivono particolari condizioni di disagio ed inseriti in una rete di interazioni subculturali con altri soggetti che, per così dire, condividono e rinforzano tale attività.

Hacking e disagio psicologico: quale confine?
Gli hacker snodano spesso il proprio cammino su un percorso comunicativo personale e per certi versi elitario, creandosi una rappresentazione esistenziale "mitica" che li conduce a lungo termine all'illegalità e alla solitudine. Le molte ore passate davanti al computer, i tentativi estenuanti di intrusione all'interno di un sistema, la soddisfazione ricercata nell'aggirare le difese di un sito web, al di la dei rischi di natura penale, si configurano sovente come una sorta di "*rifugio della mente*", all'interno di una realtà digitale offerta dalle nuove tecnologie di comunicazione. L'inadeguata capacità di definire un modello esistenziale confacente con le proprie potenzialità e corrispondente ai propri bisogni nell'ambito del sistema reale (fisico), sembra quindi spingere alcuni giovani al un modello esistenziale alternativo, che trova espressione all'interno di un sistema comunicazionale artificiale, fruito con modalità illegali. E tale modalità può però inserirli in un circuito di stigmatizzazione (a seguito di denuncia penale), analogo a quello che può produrre un comportamento antisociale tradizionale. Anche in tale contesto le dinamiche di illegalità possono essere quindi lo specchio di condizioni di disagio giovanile, esorcizzate attraverso azioni telematiche di disturbo e di danneggiamento, che presentano, attualmente, contorni meno definiti rispetto a quelli del sistema socio-culturale convenzionale.

Marco Strano è un Direttore Tecnico Psicologo della Polizia di Stato. Presta servizio presso la Polizia Postale e delle Comunicazioni come dirigente dell'U.A.C.I. (Unità di Analisi sul Crimine Informatico). Svolge inoltre attività di ricerca e di docenza in Cybercriminologia presso diverse Università italiane.

Note legali: il presente articolo o documento può essere riprodotto integralmente o in parte citando la fonte: *nome autore* - data - **Telematic Journal of Clinical Criminology** – www.criminologia.org