

Storia e realtà dell'hacker italiano.

20 anni di storia

Flavio Bernardotti

flavio@bernardotti.al.it

Flavio Bernardotti
Via Trento, 10

L'inizio

Quanta passione dietro al senso del proibito e quante sfumature psicologiche a volte individualiste e a volte collettivistiche nascono da quello considerato come il superman virtuale della rete.

L'hacker viene considerato come un elemento di élite nell'ambito del villaggio globale grazie alla sua dimestichezza nei confronti delle nuove tecnologie, in grado a volte di mettere in crisi anche i tecnocrati che gestiscono i grandi sistemi sulla rete.

L'informatica amatoriale e parte di quella professionale si è evoluta ad una velocità mille volte maggiore di quella di qualsiasi altra scienza passando da pochi settori ben definiti ad un numero talmente elevato da poter essere quantificati con molta difficoltà.

Le stesse altre scienze in parte hanno creato e allo stesso tempo assorbito quello che era il metodo informatico legato all'analisi di tutte quelle particolarità che compongono il nostro mondo circostante.

D'altra parte è probabile che proprio le altre scienze siano state i motivi induttori legati alla creazione di questa disciplina in quanto l'informatica per se stessa è la scienza che permette di trattare le informazioni, ovvero detto in altre parole, è l'arte di osservare il mondo reale e di ricavare i modelli matematici che lo descrivono.

Alcune discipline sono cresciute insieme come appunto l'informatica e l'elettronica.

I grandi hackers che vivono all'interno del fantastico collettivo in genere sono superesperti di questi settori anche grazie al cinema che ha sempre descritto questi individui come geni in grado di progettare e realizzare gli strumenti stessi utilizzati per le loro scorribande telematiche.

La realtà è molto diversa da quella che viene descritta da quelli che non sono esperti del settore e ad ogni modo anche questi ultimi generalmente possiedono un'immagine distorta in merito.

La stessa distorsione è quella che esiste anche nell'ambito degli hackers veri in quanto molte tecniche che possono essere inserite tra quelle utilizzate a livello militare sono di fatto sconosciute anche ad hackers di alto livello.

Gli hackers convenzionali utilizzano tecnologie software finalizzate a permettere di acquisire risorse senza di fatto avere le autorizzazioni.

L'hacking professionale si supporta su determinati principi fisici legati alla natura dei sistemi di calcolo e di trasmissione come ad esempio i campi magnetici generati dai monitors dei computers oppure mediante altre tecniche che pretendono apparati particolari.

Ad ogni modo il concetto di hacker è comunque legato al furto di informazioni, quelle stesse informazioni che scorrono sotto forma di bits tra un computer e un altro mediante delle reti telematiche.

Sempre maggiormente le informazioni che descrivono il nostro mondo sono racchiusi dentro a sistemi informatici i quali sempre in modo maggiore sono interconnessi tra loro.

I computer trattati come scrigni dentro ai quali trovare i segreti del nostro mondo, scrigni dentro ai quali rovistare alla ricerca di chissà quali cose, informazioni che stuzzicano la nostra fantasia, quella stessa fantasia che è stata appunto per anni il terreno delle dicerie su quei fantomatici hackers i quali invece di vivere nella speranza di un 13 al totocalcio destinato a cambiare radicalmente l'andamento della loro vita, si arricchivano cambiando le cifre dei loro conti bancari tramite accessi non autorizzati ai sistemi bancari delle società che gestivano i loro conti oppure vendendo a ignote spie mediorientali i segreti industriali carpiri all'interno dei sistemi delle multinazionali.

In vita mia mi sono sentito dire centinaia di volte : 'ma te che conosci bene i computer perché non ti accrediti due o tre miliardi sul tuo conto ?'

L'informazione è considerata l'oro astratto del Villaggio Globale.

D'altra parte le potenzialità e le capacità di sviluppo di un paese sono sempre state espresse dalla disponibilità delle materie prime.

In un'epoca di concetti virtuali dove il mondo stesso deposita sempre più riproduzioni di se stesso

all'interno di questo enorme meccanismo di reti telematiche, il punto chiave dell'economia internazionalista ruota intorno alle conoscenze, ai saperi, ossia alle attività intellettuali di cui ciascuna società dispone.

La forte accelerazione nei processi di internazionalizzazione economica è dovuta anche alle rivoluzioni informatiche le quali hanno consentito a strati sempre più estesi di entrare nei circuiti del conoscere e del sapere, in condizioni sempre più favorevoli per accessibilità, costi, rendimenti e in modo sempre più affidabile.

Non che l'immagine dell'hacker di fatto ruoti soltanto intorno a questo mondo economico in cui il fatto di carpire informazioni viene paragonato ad una crescita monetaria dovuta all'uso commerciale delle informazioni stesse carpite, ma ad ogni modo anche il mondo economico ha dovuto ricreare negli ultimi anni la mappa dei rischi aziendali inserendoci dentro anche il rischio di invadenza nelle proprie reti da parte dei cybernauti.

I rischi in questo caso andavano oltre ai puri danni economici in quanto venivano inclusi anche quelli correlati alla perdita di credibilità e di immagine successivi alla pubblicizzazione di intrusioni dall'esterno dentro ai sistemi informatici di banche e aziende di credito.

Nell'immaginario collettivo l'immagine dell'hacker è, come abbiamo già detto, quella dell'individuo che accede tramite un modem ad un sistema bancario modificando le cifre del suo conto bancario.

Purtroppo il mondo hacker è vario e pericoloso in quanto di fatto spesso non possiede quella quantità di professionalità che si tende ad attribuirgli.

Personalmente non avrei timore di un hacker professionista in quanto questo possiede obiettivi ben definiti che non coincidono quasi mai con la finalità di arrecare soltanto dei danni dentro ai sistemi a cui questo accede.

I danni invece è facile che li possano fare i ragazzini i quali non avendo neppure ben presente i meccanismi su cui si basano alcuni software destinati a creare exploits, li usano in modo indiscriminato arrecando danni ai computers che vivono sulle strutture dei sistemi attaccati.

La nascita di queste derivazioni del mondo informatico legate alla trasmissione dati hanno portato ad estendere alcuni settori come ad esempio quelli legati alla psicologia criminale, introducendo quello definito con il termine di 'computer crime'.

Ma il mondo degli hacker è solo parzialmente coincidente con questa immagine quasi professionale del raziatore d'informazioni.

Secondo il mio modo di vedere le cose l'essere hacker significa essere alla ricerca della sommità delle conoscenze informatiche, in diversi settori.

Lo sviluppo dell'informatica ha portato a matematizzare e quindi a creare i vari modelli astratti di quella che è la realtà in cui viviamo creando in alcuni casi dei sistemi alternativi dove gli individui creano e modellano una loro identità.

Reti telematiche, come appunto internet, rappresentano un'alternativa nella quale gli individui possono crearsi una loro identità che in molti casi è più soddisfacente di quella che è la loro identità reale.

L'immagine ambita della persona forte quasi coincidente con quella del supereroe dei nostri fumetti può prendere forma all'interno di dove gli attributi possono essere scelti e trasmessi mediante informazioni.

In un mondo reale la forza del supereroe è fisica mentre in un mondo virtuale è pura informazione usata per creare e imporre la propria immagine.

In un mondo dove la fisicità conta solo come descrizione legata alla pura informazione anche il Superman non è una persona che infligge colpi terribili ma è l'hacker il quale ricava la sua Superforza da quella che è il suo pensiero o al limite lo Script Kiddie il quale sfruttando il sapere dell'hacker crea anche lui la sua scena da primo attore.

Ma questo non è sempre stato in questo modo in quanto in origine il tutto era completamente differente.

L'uomo ha sempre proclamato la sua intelligenza partendo dalla sua capacità di astrarre ed in particolar modo di quella di comunicare l'esperienza individuale.

L'informatica nata come scienza finalizzata all'analisi delle informazioni ha permesso di creare nuovi metodi che si sono aggiunti a quelli già esistenti relativi ai metodi di comunicazione interpersonali.

I vari filoni nati da questa scienza giovane hanno permesso la realizzazione di sistemi di comunicazione che hanno portato ad aggiungere forme a quella che sono i normali mezzi della comunicazione umana.

Negli ultimi anni lo sviluppo di internet ha portato anche alla nascita di quello che definiamo con il termine di Villaggio Globale, un mondo astratto parallelo al nostro reale in cui le varie realtà umane si muovono mediante sistemi matematici descrittivi e dinamici.

Come in tutti gli ambienti reali troviamo la creazione di nuovi gruppi in cui gli individui si identificano e che quindi utilizzano per creare il loro sistema di identificazione all'interno di questo mondo virtuale.

Purtroppo la crescita smisurata di queste forme tecnologiche ha agevolato una scissione tra gli individui del mondo reale, precisamente tra quelli che riescono in qualche modo ad osservare e quindi a vivere in questi ambienti e tra quelli che di fatto ne accettano l'esistenza pur non comprendendone i significati derivati da queste realtà astratte.

Ne è un esempio la realtà hacker che di fatto è spesso male interpretata anche dagli addetti ai lavori. La cattiva interpretazione del mondo hacker coinvolge sia il lato qualitativo che quello quantitativo e questo è derivato dal fatto che le valutazioni sono sempre state fatte su una classe sociale troppo trasformata rispetto quella che era la sua forma originaria in cui inizialmente la vera essenza di questo modo di essere era sufficientemente distante da quelle che erano delle caratteristiche puramente caratteriali degli individui.

Questa dichiarazione per ora deve essere presa così come è stata detta anche se nelle parti successive di questo scritto il concetto verrà chiarito.

Il significato relativo al concetto di hacker ha subito una radicale trasformazione nel giro di soli 20 anni tanto da diventare una cosa quasi completamente differente da quella che era all'inizio.

Per riuscire a comprendere questa evoluzione ed in particolar modo quella che è la vera realtà del mondo hacker al giorno d'oggi è necessario vedere l'evoluzione che i concetti collegati hanno subito.

Non è mia intenzione parlare di me all'interno di questo scritto in quanto pur essendo stato uno dei fondatori della realtà su cui si sono sviluppate determinate teorie, o che perlomeno hanno permesso di espandersi, sin dal 1984 non mi sono mai definito come tale in quanto la mia visione di questi concetti sono filosoficamente distanti da quelli che di fatto sono i presupposti reali su cui si fonda questo mondo.

Tutto quello che è descritto all'interno di questo testo nasce dall'analisi fatta personalmente su quella che è stata l'evoluzione della realtà hacker filtrata attraverso le informazioni passate attraverso le varie reti telematiche apparse in Italia dal 1984 in poi.

Per questo motivo, al fine di fare comprendere quelli che potrebbero essere i fattori qualitativi che hanno indotto il mio modo di vedere, mi sembra necessario dire due cose su quello che è sempre stato il mio modo d'essere.

Sin da giovanissima età ho sempre avuto una passione smisurata per quella che era l'elettronica facendola rasentare quella che avrebbe potuto essere al limite definita con il termine, in senso buono, di psicosi.

Questa passione era talmente forte da rendere qualsiasi altra attività secondaria.

Fortunatamente le mie qualità mentali mi spingevano anche verso una predilezione per quelli che erano i rapporti sociali, derivati da una visione quasi sessantottina, che mi spingeva a cercare in ogni modo le forme di dialogo inerenti a quelle che erano le mie passioni e alle caratteristiche umanitarie del dialogo stesso.

Il 1983 rappresento un pilastro fondamentale in quella che è stata la mia evoluzione psicologica e professionale.

La mia passione era legata alla forme di astrazione di tutte quelle che erano le realtà che ci circondavano.

La commercializzazione da parte di IBM del personal computer mi spinse verso quella che era l'informatica, cosa che possedeva una forma di astrazione molto superiore a quella che poteva avere l'elettronica.

In un certo senso la creazione dei modelli mentali legati all'elettronica poteva essere agevolata dall'utilizzo di sistemi visivi come ad esempio oscilloscopi, analizzatori e strumenti vari mentre l'informatica di quel tempo era puramente frutto di un astrazione totale.

Il 1984 fu l'anno in cui iniziai l'attività di consulente in informatica.

Mentre molti miei colleghi avevano optato per lo sviluppo di un singolo prodotto e quindi imbastendo tutta l'attività lavorativa verso l'assistenza di quello, io non avevo messo limiti ai settori in cui avrei voluto intervenire.

Consideravo qualsiasi commessa come un incentivo alla crescita e non solo a quella informatica. La mia idea era comunque quella che i problemi a cui mi dovevo dedicare professionalmente erano stati sicuramente affrontati e risolti da qualche altra persona e che quindi il problema fondamentale era quello di creare un meccanismo capace di permettere il dialogo tra persone geograficamente remote.

Verso la fine del 1984 fondai la prima rete telematica pubblica amatoriale, quella ancora oggi chiamata FIDONET italiana.

Inizialmente i sistemi erano tre e precisamente il mio, quello di Giorgio Rutigliano di Potenza e quello di Adolfo Melilli di Pordenone.

Nel giro di soli due anni il numero dei sistemi partecipanti alla rete erano più di 100 fornendo in questo modo un meccanismo di distribuzione delle informazioni molto efficienti, considerando le tipologie di instradamento e di collegamento che esistevano a quei tempi.

All'inizio la gestione venne eseguita con un software chiamato Opus scritto in USA ma questo durò poco in quanto dopo pochi mesi iniziai io stesso a progettare quello che dopo un anno di lavoro notturno fu chiamato ITALINK.

A quei tempi le documentazioni e i libri erano inesistenti per cui la possibilità offerta da reti come FidoNet erano essenziali per lo scambio di informazioni tra individui con interessi comuni.

L'esperienza di progettazione di ITALINK mi portò entro i primi due anni a scrivere i primi tre volumi che vennero distribuiti gratuitamente mediante la rete.

Chiaramente un fattore impossibile da ignorare era quello relativo alla diffusione che iniziava ad avere anche per uso amatoriale il personal computer.

L'uso di questo collegato alle metodologie di interconnessione dava vita a un nuovo metodo di comunicazione tra persone ubicate geograficamente in posti remoti.

In pratica il metodo epistolare acquistava la velocità di trasferimento implicito nel mezzo telematico stesso.

L'evento relativo alla nascita delle reti causò nella stampa una reazione che di fatto non mi aspettavo.

La tendenza a sottolineare sempre gli aspetti criminalizzanti delle cose aveva portato quotidiani come il Sole 24 Ore a fare articoli in cui si imputava all'uso della rete la nascita e la crescita del fenomeno hacker in Italia.

Chiaramente questo comportamento dei quotidiani ebbe un effetto bivalente in quanto il fatto di trattare questi "pericoli pubblici" portò in gran parte a creare dei veri e propri miti, colonne portanti di una cultura underground che possedeva in parte un carattere affascinante.

Questa caratteristica successivamente sarebbe diventata la chiave del successo dell'hacking.

Uno di questi miti fu sicuramente Raul Chiesa il cui "successo" fu conseguenza di alcuni arresti dovuti alle sue scorribande all'interno di sistemi aziendali.

L'importanza iniziale di reti come la FIDONET è descritta anche in alcuni scritti dello stesso di cui riporto un breve spezzone.

"Negli anni '80 vi erano alcuni appassionati i quali - a proprie spese - "tiravano" su e gestivano le

cosiddette BBS (Bulletin Board System): c'era la rete FIDO e non c'era Internet. Credo sia giusto ricordare questi avvenimenti e parlarne, per avere ben chiara la situazione attuale e, forse, evidenziare tutta una serie di problemi correlati.

Parlare oggi di FidoNet ai "navigatori" del Web e' arduo: mi metto infatti nei panni di un normale utente Internet al quale raccontare che si chiamava la BBS alle 4 di mattina per trovarla libera - al solo fine di scambiarsi messaggi con 30/40 persone o prelevare un file shareware - possa sembrare quanto meno "buffo". Eppure, tutta una generazione di telematici ed hacker e' nata in questo modo, chiamando la propria BBS di zona, ascoltando pareri e rimanendo chiusi nella propria citta'. Una mail via echomail-Fido poteva si' arrivare negli States, ma ci impiegava alcuni giorni ed implicava, comunque, delle spese aggiuntive per il gestore della BBS.

Il massimo era, quindi, poter parlare con qualcuno di un'altra citta' italiana, quando comunque ci si accontentava di "un qualcuno" della stessa citta'.

Parallelamente al circuito Fido nacquero poi altre reti, tutte pero' basate sullo stesso concetto di "circoscrizione" territoriale. Intanto l'Italia "casalinga" scopriva un nuovo fenomeno di comunicazione, il "Videotel", improntato per la maggior parte sulle famigerate Chat-lines. Su Videotel ho appreso molte cose, ho avuto i primi timidi contatti con hacker "storici" italiani, seguiti dalle prime connessioni su QSD (messenger francese, ritrovo di hacker americani ed europei). Ho incontrato le persone piu' diverse, piu' strane; persone che fa piacere e nostalgia ricordare, persone che mi hanno introdotto al "secondo livello", l'hacking vero. "

Questa realtà inizialmente nacque da due fattori ben distinti.

Il primo era sicuramente la grossissima curiosità e interesse che le nuove tecnologie incutevano su certe persone molte delle quali la possedevano già per quelle tecnologie legate al mondo elettronico. Personal computer, linguaggi di programmazione, sistemi telematici e mille altre meraviglie che giorno dopo giorno iniziavano a comparire orientate al grosso pubblico fecero passare infinità di notti insonni vicino ad un computer un numero sempre maggiore di persone.

Purtroppo le nuove tecnologie erano costose, anzi, molte volte insostenibili.

In quegli anni il costo delle linee telefoniche era notevole, tanto da costituire una spesa proibitiva per tutte quelle persone che erano interessate ad usare queste tecnologie.

Ci fu un fatto che entro nella leggenda in quegli anni relativo ad un ragazzo minorenni di Roma che si vide recapitare dalla SIP (ora Telecom) due bollette telefoniche da 20 milioni cadauna in soli quattro mesi.

Eppure la curiosità era infinita in quanto a quei tempi i sistemi sulle grosse reti erano mainframe con banche dati immense contenenti decine di milioni di voci su tutto quello che era la conoscenza dell'uomo.

Il sistema di rete da noi creato concepiva un certo numero di sistemi con software che gestissero determinate funzionalità, come ad esempio la lettura e la scrittura di messaggi, situati in diverse città in modo tale che i vari utenti si potessero collegare in tariffazione urbana.

I vari sistemi acquisivano localmente i messaggi scritti dagli utenti e solo ad una certa ora questi eseguivano i trasferimenti di questi su tutti gli altri sistemi della rete dando così l'impressione che messaggi scritti in tutt'altra città fossero stati di fatto scritti su quei sistemi su cui gli utenti si collegavano.

Questo favorì la creazione di aree di interesse comune su qualsiasi tipo di argomentazione comprese quelle legate al mondo degli hackers.

La filosofia hacker, a tratti individualista e altre volte collettivista, è permeata dalla coscienza di detenere un potere immenso, nato attraverso la domestichezza con le nuove tecnologie paragonabile a quella riscontrabile in un tecnocrate di alto livello che gestisce grandi sistemi aziendali.

Nel mondo aziendale generalmente l'hacking è oggetto di una notevole semplificazione in quanto questo è assimilato al crimine e ai rischi di perdite economiche.

Questo di fatto non è vero in quanto, come vedremo il mondo dell'hacker è di fatto molto più

sfaccettato e complesso essendo legato a questioni etiche e politiche talvolta altamente sofisticate. Questa bivalenza nell'ambito dell'individualismo e del collettivismo ha fatto sì che le reti telematiche che avevamo creato originariamente fossero usate spinti da impulsi differenti.

Il primo impulso era quello generato dalla voglia di condividere le scoperte fatte mentre l'altro impulso aveva origine in un senso egocentrico che permetteva di usare la rete quasi a modo di palcoscenico.

Le tecnologie emergenti erano a quei tempi molto rudimentali tanto che le trasmissioni dati di fatto erano limitate da una bassissima velocità di trasferimento, circa 300 bauds, indotte da una qualità delle linee telefoniche bassissima dovuta all'uso di centrali telefoniche meccaniche.

La velocità bassissima costringeva a tempi di collegamento enormi per cui questi, collegati ai costi esagerati delle telefonate, portò alla nascita di quella che da quel momento fu definita come realtà hacker.

Inizialmente le tecniche hacking erano quasi esclusivamente basate sul mero scambio di password che sistemi di rete come appunto FIDONET permettevano.

D'altra parte al giorno d'oggi l'infinità di tecniche hacker si basano sulla quantità enorme di protocolli, di software di gestione host e di tutto quanto permette la gestione dei servizi attuali.

18 anni fa il collegamento tra i sistemi era punto a punto per cui non esistevano molte tecnologie su cui cercare i punti deboli su cui agire.

Il 1987 costituì un altro punto chiave nell'evoluzione delle metodologie hacker in quanto venne creata la rete SUBLINK che a diversità di quella FIDONET utilizzava il sistema operativo UNIX per la creazione di servizi veri e propri di rete.

Tecnicamente iniziò ad ampliarsi la panoramica dei sistemi sui quali cercare i punti deboli.

Iniziarono a essere usati sistemi come UUCP i quali erano parti integranti del sistema operativo Unix.

Il movimento hacker ricevette anche un grosso impulso dalle università dentro alle quali era possibile individuare i codici di accesso mediante i quali i vari laboratori svolgevano le attività di connessione sulle varie reti mondiali.

Qualsiasi facoltà possedeva connessioni transoceaniche finalizzate a svolgere ricerche su grosse basi di dati come ad esempio molte di tipo bibliografico nei vari settori delle scienze come la medicina, la fisica ecc.

Gli abusi avvenivano già dall'interno delle Università ma le password comunque uscivano da queste e arrivavano ai computer casalinghi.

Le prime scorribande fatte dagli hackers italiani partirono dai vari sistemi VAX delle facoltà d'ingegneria e successivamente da quelle d'informatica.

Lo scambio di password era un'attività svolta in qualsiasi modo tanto che riviste specializzate riportavano tra gli annunci testi del tipo: 'Cerco password Cineca e do in cambio password Sperry 1000 del Ministero degli Interni'.

Il tipo di abusi di sistema che venivano fatti denotavano una cultura che solo all'interno delle università poteva essere presente.

I sistemi collegati alle reti come ITAPAC erano quasi tutti mainframe con sistemi operativi particolari come ad esempio il VMS sui sistemi Digital, il VM sui sistemi IBM 3090 e così via.

Come dicevamo prima il termine hacker ha subito negli anni un'evoluzione profonda tanto da essere quasi completamente differente dalla sua forma iniziale.

Nei primi anni in cui iniziò a verificarsi il fenomeno, l'individuo che costituiva il tipo standard dell'hacker si sarebbe potuto definire come una persona spinta da una fortissima sete di conoscenza in campo informatico, costretto a sfruttare abusivamente quelle che a quei tempi erano le grosse reti pubbliche mediante sistemi di accesso abusivi.

Spesso la ricerca fatta dall'hacker era indirizzata all'interconnessione delle varie reti.

Al giorno d'oggi Internet ci permette di ignorare quelli che sono gli instradamenti che i dati percorrono per passare dal sistema d'origine a quello di destinazione e il fatto che questi sistemi intermedi possano essere anche diverse decine a noi è trasparente in quanto ci sembra di passare direttamente dal nostro computer a quello legato al link scelto.

Una volta il lavoro era massacrante in quanto una volta entrati con codici d'accesso falsi all'interno di un PAD Itapac si doveva programmare questa in modo tale che si potesse creare una connessione con qualche altra rete come ad esempio TIMENET, che magari possedeva uno standard di trasferimento completamente differente dalla prima.

Molti sistemi erano scollegati dalle grossi reti e potevano essere raggiunti solo tramite connessioni modem.

Collegati alle reti esistevano dei sistemi definiti con il termine di outdial.

In pratica fornendo dei numeri di telefono a questi creavano una connessione tramite telefonia normale.

Questi sistemi outdial erano delle chicche per gli hackers in quanto gli permettevano di sganciarsi dalla rete normale.

La comparsa di Turbo Pascal nel 1985 rivoluzionò la filosofia hacker in quanto da mero programmatore di rete, con questo poteva iniziare a creare tutti quei softwares che con il normalissimo GwBasic presente sui vari sistemi Olivetti M24 o il PC IBM (un mostro di sistema senza disco fisso, con 512KB di RAM, con floppy da 360KB e con ben 4.77MHZ di clock) non era possibile scrivere.

Le notti passate tra i vari trilli dei modem e i duecento caffè bevuti tra una linea e l'altra di programma in Turbo Pascal diventavano sempre più lunghe.

Le attività da me svolte potrebbero essere un esempio per fare comprendere quanto di fatto la ricerca della conoscenza informatica e la voglia di trasmetterla fosse superiore a qualsiasi altra motivazione.

Queste attività portarono mia moglie a potersi definire una vedova bianca !

Il progetto ITALINK, quello che mi permise di gestire la rete FIDONET, mi aveva portato a studiare diverse metodologie di programmazione, molto avanzate per quegli anni.

Da questo studio nacquero 5 o 6 volumi i quali vennero distribuiti gratuitamente sfruttando il meccanismo stesso della rete.

L'idea che quel lunghissimo lavoro avrebbe potuto essere considerata anche come fonte per una resa economica era per me incomprensibile in quanto la voglia di comunicare i risultati di quella forte passione era di fatto talmente totalitaria da coprire completamente quella possibilità.

Il lavoro notturno mi aveva portato a scrivere circa 200.000 linee di codice e 2000 pagine di libri in meno di due anni.

La ricerca del materiale era assurda in quanto era solo disponibile qualche raro volume nelle librerie delle università come ad esempio la Clup di Milano.

A quei tempi la rete per eccellenza in Italia era ITAPAC mediante la quale era possibile richiedere la connessione con i maggiori sistemi informatici mondiali.

Spesso la SIP, ora Telecom, mobilitava il personale passandolo dalla gestione della telefonia a quella che era la gestione della rete per cui spesso i responsabili stessi erano un po' come pesci fuori dall'acqua.

Io stesso venni incaricato da SIP per tenere dei corsi di istruzione sulla rete ITAPAC ai responsabili della rete stessa.

Io che avevo appreso la programmazione di ITAPAC mediante il suo uso tramite accessi abusivi !

Il 1987 fu uno degli anni più prolifici dal punto di vista delle nuove tecnologie.

I vecchi 8088 e 286 venivano sostituiti dai primi processori a 32 bits come il 386 e i modem applicando meccanismi di compressione dei dati iniziavano a raggiungere velocità notevoli.

Chiaramente il numero dei sistemi nelle abitazioni non arrivava ancora ai livelli di oggi ma ad ogni modo l'informatica iniziava ad essere una cosa comune.

Il problema che inizio a modificare il concetto di hacker fu di fatto l'evoluzione troppo veloce delle tecnologie per cui il numero degli esclusi dalla comprensione di queste cose incominciava ad aumentare.

I sociologi stessi ipotizzando quale sarebbe stata l'evoluzione del modo di rapportarsi con le emergenti tecnologie da parte della società avevano parlato di un distacco sempre maggiore tra quelli che si sarebbero fusi con queste e quelli che invece le avrebbero subite più che vissute.

Nel 1968 quello che venne definito come 'Il santone dell'acido lisergico', Timothy Leary, fondatore delle filosofie psichedeliche di quel periodo aveva a quei tempi ipotizzato che l'uso di determinate droghe come appunto LSD25 avrebbe potuto facilitare il transfert nell'ambito delle sedute psichiatriche tra l'operatore e il paziente schizofrenico.

Dopo anni di silenzio, durante i quali T. Leary scomparì dalle scene, fece la sua comparsa con quella che sarebbe stata la filosofia di base delle frange estreme dell'hacking ovvero la teoria del CHAOS.

In altre parole Leary disse che l'evoluzione galoppante avrebbe creato nella società il CHAOS i quale avrebbe portato la maggior parte delle persone a viverlo con un certo senso di angoscia. La filosofia dei cyberpunk invece considerava questo come una eventuale possibilità dentro al quale cercare in caso di bisogno.

Il movimento hacker basato sulle teorie cyberpunk arrivavano a prevedere come forme estreme l'uso di Ecstasy al fine di fare cadere i tabù mentali bloccanti alla ricerca di un'evoluzione senza fine.

In questo caso il concetto hacker non è che una delle componenti di quello che è un movimento filosofico che ha moltissime attinenze con dottrine religiose.

I concetti propagandati da Leary consideravano appunto l'hacking come quella componente che portava l'individuo alla ricerca del programma senza errori frutto di una conoscenza assoluta che tendeva paragonare gli addetti ai computers ai custodi della luce eterna.

L'uso delle droghe in questo caso sono indirizzate a produrre flashes dentro ai quali il cybersoggetto può estrinsecare tutta la propria creatività interagendo con la macchina utilizzando anche tecniche di realtà virtuale.

Fortunatamente queste filosofie, almeno qui in Italia, non inquinarono più di tanto il pensiero del movimento hacker.

Personalmente, per qualche anno, mi addentrai in queste filosofie alla ricerca di quelle che erano le modificazioni nell'ambito dei meccanismi orientati alla creazione dei modelli mentali.

Non bisogna dimenticare che la ricerca spasmodica orientata ai sistemi informatici spesso include quella branca di questa scienza che è l'intelligenza artificiale al cui estremo si trovano le filosofie come quelle di Dennet orientate alla creazione degli stati di coscienza o alla matematizzazione degli stati emotivi.

IL CAMBIAMENTO

Il 1987, come abbiamo già detto prima, rappresentò l'anno in cui SUBLINK si consolidò come rete Unix.

Il grosso numero di adesioni, in questo caso ditte che professavano nel settore informatico, portò Olivetti a regalare alla rete un link su Cupertino il quale permise a SUBINK di entrare in connessione con al più grossa rete pubblica americana, USENET.

Questa portò la cultura americana in Italia anche se di fatto bisogna dire che anche la rete I2U, a cui erano collegate le maggiori università italiane, aveva gli stessi tipi di connessioni.

USENET possedeva qualche cosa come 16000 NEWSGROUP ovvero aree tematiche orientate allo scambio di messaggi.

Le sezioni HACKERS furono come la manna dal cielo per la comunità hacker italiana la quale fece oro delle informazioni da queste attinte compresi i numeri di nuovi sistemi e milioni di password di computer sparsi per il mondo.

Come per tutto quello che riguarda i fattori tecnologici anche le teorie hacker erano molto più avanzate in USA di quanto di fatto lo fossero in Italia.

Chiaramente questo filone trovò immediatamente migliaia di addetti in particolar modo all'interno delle università.

Anche in questo caso il fattore puramente economico era la base della deviazione filosofica che derivava comunque dalle basi dell'hacking.

L'università ad ogni modo è sempre stato considerato il centro focale di tutte le attività hackers non solo per il fatto che all'interno di queste esistono i sistemi connessi alle reti telematiche di tutto il mondo, ma per il fatto che la psicologia dello studente è quella che possiede tutte le caratteristiche ideali che sono la base di quella curiosità che l'hacker possedeva.

La storia degli hacker in USA ha circa 40 anni, ma senza andare cercare proprio negli albori di questa filosofia possiamo vedere alcune cose che hanno avuto origine dai movimenti all'interno delle università unite allo spirito hacker.

Dall'unione di questi fattori nasce ad esempio lo spirito che animava i ragazzi del MIT, ad opera di Linus Torvald da cui nacque il sistema operativo LINUX considerato il cuore operativo di quasi tutti gli hackers mondiali.

Moltissimi hacker americani erano nel frattempo diventati dei miti anche per altri tipi di attività a cui si erano dedicati.

Tra i più famosi di quel tempo c'era Stallman il quale era anche tra i fondatori del GNU Foundation. La filosofia che andavano a predicare era legata al fatto che per loro il software doveva essere libero e non vincolato a diritti commerciali.

Questa è ancora oggi la filosofia di base della GNU Foundation.

A seguito di questa il fattore criminalizzante implicito all'interno dell'hacking non poteva essere considerato in quanto se di fatto valeva questa mancanza assoluta di diritti di quanto poteva essere considerato software, come poteva esserci una violazione nel fatto di entrare all'interno di qualche cosa che era di dominio pubblico ?

Ad ogni modo, comunque la visione dell'hacker si fosse modificata in questi anni, questa doveva essere considerata da due punti di vista.

Il primo era l'immagine relativo a questa realtà che avevano le persone che vivevano il tutto dall'interno mentre il secondo tipo era quell'immagine che i mass-media avevano costruito mediante articoli opportunisti che erano comparsi sui giornali.

La scoperta dell'hacking da parte di questi diede alla luce l'immagine del "dark side hacker" legata in particolar modo ad un'immagine criminalizzante dell'hacker stesso, il quale veniva appunto descritto come un individuo dedicato all'assalto dei sistemi informatici con il solo scopo di arrecarsi un guadagno economico.

Gli anni dal 1989 fino al 1993 costituirono un periodo di ricerca da parte di quelli che sarebbero stati poi i fautori delle reti internet.

Purtroppo gli stessi anni iniziarono a rappresentare la mutazione completa della fisionomia hacker. Non per ripeterlo ma fino a questo punto l'hacker era una specie di ricercatore del binario che sfruttava certe tecniche per ricavare informazioni prese dalle banche dati in cui entrava abusivamente e anche per risparmiare soldi di connettività.

Chiaramente più il numero degli addetti all'uso di certe tecnologie aumenta più questa società virtuale assume l'immagine di quella reale.

Una nota che deve essere considerata è quella diversificazione che l'hacker italiano comunque possedeva rispetto all'immagine puramente americana.

Quell'immagine dell'italiano pizza e spaghetti gli viene attribuita anche in questo caso tanto che questa caratteristica è quella che ispira Monti e Chiccarelli all'interno del loro libro "Spaghetti Hacker" nel quale il termine viene trasformato in "smanettone italiano".

Nel 1994 inizio il boom di Internet.

Le connessioni iniziavano a diventare in tempo reale grazie a sistemi di instradamento offerti dalle compagnie telefoniche nazionali.

Migliaia di siti iniziarono ad offrire servizi sfruttando qualsiasi nuova tecnologia orientata alla gestione delle reti e degli host collegati a questa.

Le fasi di sperimentazione chiaramente furono coincidenti con un numero enorme di bugs identificati e sfruttati dagli hackers.

Questo era il prezzo che internet doveva pagare prima di riuscire a trovare una certa stabilità.

Fu inventata qualsiasi cosa.

Sistemi di analisi, worm, virus e chi più ne ha più ne metta.

Nasce il villaggio globale il quale grazie a modelli matematici atti a simulare i sistemi reali inizia a vivere diventando sempre più concreto nelle menti di chi ci vive sempre più tempo al suo interno.

Come dicevo prima l'aumento dell'utenza ha portato all'interno di questa società virtuale tutti gli schemi mentali degli individui reali.

In altre parole le personalità dei navigatori della rete venivano virtualizzate creando in questo modo la personalità virtuale la quale chiaramente possedeva gli stessi attributi di quella reale con l'unica differenza che questa poteva essere plasmata cercando di eliminare quelle caratteristiche che non erano apprezzate dallo stesso individuo che le possedeva.

Da qui la totale modifica del concetto di hacker.

Hacker nell'immaginazione delle persone equivale a potere.

Mentre prima l'hacker era appunto quello descritto precedentemente, a questo punto invece l'hacker iniziava ad essere l'adolescente che vedeva in quel potere che la conoscenza forniva, il mezzo perfetto per esprimere quel senso di ribellione nei confronti di una società sempre più soffocante nei confronti dei singoli individui.

Questa nuova filosofia permise la creazione di quello che personalmente definisco come 'fattore inquinante'.

Mentre prima l'hacker aveva la conoscenza ora questa è solo una forte ambizione, spesso difficilmente raggiungibile, e più frequentemente solo decantata, tanto che il concetto di hacker ha subito una suddivisione netta.

Nasce il termine di script kiddie.

L'hacker per se stesso possiede un'etica che lo porta a non fare assolutamente danni all'interno del sistema in cui entra, anzi spesso avvisa l'amministratore dei problemi riscontrati.

Lo script kiddie invece non possiede conoscenze ed usa tutti i programmi scaricati dalla rete spesso non conoscendone neppure lo scopo.

Questa persona, proprio per le motivazioni che o spingono a definirsi come hacker, identificano nel danno arrecato la prova per testimoniare agli altri membri della comunità la loro potenza.

Questo è testimoniato dalla nascita di un numero enorme di sistemi il cui unico scopo è quello di pubblicare il nome del sistema e quello dell'hacker che lo ha abbattuto.

Nell'ambito delle reti Internet si formano intorno a questi individui delle sette dove la gerarchia

viene mantenuta portando attacchi tra gli stessi membri seguita da successiva umiliazione pubblica. Alcuni ricercatori che si sono dedicati allo studio del fenomeno hacker hanno diversificato le classi a cui questi appartenevano creando ad esempio, come nel caso di Winkler, tre tipologie differenti. Queste classi erano precisamente :

i geni
gli sviluppatori
gli altri

I primi sono talmente all'interno delle filosofie e delle tecnologie informatiche tanto da esserne motivo di evoluzione.

Spesso l'attività lavorativa è legata alla ricerca nei vari settori dell'informatica e i loro livelli di conoscenza spesso non rientrano neppure nell'immaginario delle persone normali.

Un esempio è l'identificazione delle informazioni che vengono elaborate su dei sistemi informatici mediante la ricezione e l'elaborazione dei campi elettrici e magnetici rilasciati dai monitor dei computers tramite antenne direttive puntate sui centri di calcolo dall'esterno di questi.

Questo livello di hacking è generalmente legato a lavori fatti per scopi militari e comunque sotto il controllo dei servizi segreti.

L'utilizzo di sistemi hardware particolari fa sì che questi livelli non possano essere di fatto comuni. L'hacking ad ogni modo non viene quasi mai concepito socialmente a questo livello ed è forse meglio che non lo sia in quanto già normalmente certi tipi di attività creano leggende metropolitane legate alla debolezza dei sistemi che dovrebbero proteggere la privacy.

Molte attività commerciali sono svolte per evitare questo tipo di hackeraggio.

Il secondo tipo è invece costituito da persone che conoscono bene l'ambiente e grazie alle loro conoscenze creano strumenti software in grado di agevolare la vita a chi vive in questo ambiente.

Il terzo tipo è semplicemente quello che sfrutta quanto esiste.

In altre parole lo script kiddie di cui abbiamo già parlato il quale quantitativamente costituisce il numero maggiore.

Volendolo identificare come una figura CHING oserei usare il termine "L' AMBIZIONE".

Ad ogni modo quest'ultima classe è di fatto quella in cui sono presenti il maggior numero d'individui in quanto permette di contenere quegli individui che cercano nell'hacking un'affermazione del proprio io ma che allo stesso tempo vivono la necessità tecnologica quasi come un fatto frustrante, in un certo senso rimosso o perlomeno falsificato.

La falsificazione è rappresentata dal fatto che il sostenimento della loro immagine tecnologica viene di fatto ottenuta mediante una sopravvalutazione del loro livello cognitivo grazie all'attribuzione di notevoli capacità a quello che di fatto è il semplice uso di programmi reperiti sulla rete.

Questo processo psicologico è molto semplice che si verifica quando viene a mancare un metodo di confronto.

In questo caso è l'alterazione mentale dovuta alla carica aggressiva e a quella competitiva che la nasconde rendendo quindi vano qualsiasi confronto con quello che potrebbe rappresentare il punto da cui diventare consapevoli della loro bassissima cultura informatica.

Il mondo hacker è in ogni caso fonte di un complesso sistema di relazioni che nascono dai livelli cognitivi e caratteriali degli individui che lo compongono.

Chi ha occasione di assistere a mail list hacker od ad aree di chat come ad esempio in #Phreak.it si accorgerà immediatamente di questa situazione sociale.

In queste si denota un violenza di linguaggio che rasenta l'inimmaginabile, oltre che l'inutile, tanto che se non si comprende questa filosofia che ne è alla base non si potrebbe comprendere neppure la motivazione.

La bestemmia è la consuetudine e l'insulto è la norma.

D'altra parte lo scopo fondamentale di queste sezioni telematiche è quello di creare dei gruppi virtuali dove la gerarchia viene stabilita mediante forme violente di qualsiasi natura.

In questo sistema relazionale vivono esternamente altre figure che sono quelle trasparenti delle

forze dell'ordine che controllano le evoluzioni di questi ambienti.

Di fatto a questo livello l'hacking è controllato e sopportato in quanto le motivazioni che lo sostengono sono fermamente radicate nella psicologia adolescenziale.

Non che questo significhi che l'hacking non viene punito.

Diciamo che le forze dell'ordine non calcano in genere la mano in quanto di fatto spesso le stesse sfruttano alcune informazioni che derivano da questi ragazzi per arrivare a circuiti che vivono nell'ambito di internet come ad esempio la pedofilia.

Molte filosofie originarie legate all'hacking erano basate su forme umaniste molto profonde che derivavano da filosofie sociali post 68.

Da questi filoni sono nate la GNU foundation dove la libera circolazione del software e quindi la divulgazione globale dell'informazione era di fatto il pilone fondamentale da cui derivavano tutte le altre filosofie.

L'hacking, inteso originariamente come ricerca, possedeva come suo successivo passo quello legato alla divulgazione delle informazioni scaturite da queste attività.

La psicologia politica che era alla base di alcuni movimenti hacker vedevano i sistemi di protezione solo come ostacoli da rimuovere, inseriti da individui che vogliono controllare le informazioni al fine di dominare le masse.

Chiaramente il fatto di vivere all'interno di un ambiente illegale porta l'hacker a vedersi come un paladino dell'informazione libera con forti tendenze antiburocratiche piuttosto che come un delinquente senza nessuna motivazione filosofica.

La metamorfosi totale subita dall'hacking ha portato a rivoluzionare completamente anche questi concetti.

In questi gruppi l'ermetismo totale della conoscenza è di fatto il punto fondamentale intorno a cui ruota tutta la nuova filosofia.

D'altra parte quello che al giorno d'oggi è importante nell'ambito delle filosofie hacker non sono di fatto le conoscenze ai fini di se stesse ma queste usate come strumenti di potere nei confronti degli altri membri di questi gruppi.

La divulgazione del mio ultimo volume ha creato un sacco di polemiche in quanto gli individui che gestivano la loro superiorità in questi ambienti mediante il mantenimento di certe tecniche a livello di segreti non divulgabili hanno visto in queste 2.000 pagine di informazioni un vero e proprio attentato a tutto quello che fino ad ora gli aveva garantito una supremazia nelle varie crews hackers. Da parte degli osservatori del fenomeno esterni di fatto la complicazione è quella di comprendere se determinate figure possono essere considerate nell'ambito di una valutazione dell'entità del fenomeno.

La cosa sicura è che molti anni fa questo non esisteva per cui di fatto la realtà hacker era molto più delimitabile e quindi analizzabile in tutte le sue forme.

Sicuramente la filosofia di base è completamente cambiata ed ad ogni modo, indipendentemente dalle motivazioni psicologiche che spingono determinati individui a muoversi in un determinato modo, la realtà che permette di contemplare certi individui come entità di questo fenomeno è di fatto quella che è propria degli hackers.

Quantitativamente, anche se in generale si usa sempre il termine hacker anche per indicare quelle persone dotate di scarsissime conoscenze tecniche, una differenziazione dovrebbe essere fatta in quanto il termine stesso che viene utilizzato per suddividere la categoria è importante che venga mantenuto sia per quello che riguarda gli hacker veri e propri, sia per quelli che di fatto usano questo termine per identificare una voglia di violenza incomprensibile.

L'hacker tecnicamente dotato usa il termine Script Kiddie per differenziarsi da quelli che di conoscenze ne hanno pochissime.

I partecipanti a queste sette invece usano il termine per altre motivazioni.

In questi ambienti l'insulto è essere definito Script Kiddie.

Nel 1999 scrissi il mio ennesimo libro di circa 1.000 pagine intitolato 'Cracking & Hacking'.

Anche se a livello tecnico era sicuramente molto inferiore ad altri ottenne un successo incredibile da parte di migliaia di persone che ricercavano quella forza sociale che non possedevano nelle tecniche

descritte sul libro stesso.

Molti rimasero delusi in quanto di fatto il volume trattava più le tecniche legate al debug dei programmi e alle protezioni del software di quanto lo facesse con le metodologie hacker.

Da quel momento in poi ricevetti migliaia di richieste da parte di persone che mi dimostravano un'impazienza incredibile e che non vedevano l'ora che uscisse una pubblicazione che descrivesse delle metodologie di hacking.

Se una persona aveva una così grande fame di conoscenza e voglia di apprendere, per quale motivo non imparava un linguaggio di programmazione invece di perdere tempo a imparare tecniche che avevano il solo scopo di arrecare danni ?

Come ho detto precedentemente, nel 2002 uscì il mio ultimo volume di circa 2.000 pagine intitolato 'Hacker's Programming Book'.

Due mila pagine dedicate alle metodologie usate dagli hacker !

L'annuncio lo feci su internet circa 4 mesi prima della sua effettiva pubblicazione.

Sapevo perfettamente cosa avrei scatenato ma questo mi serviva per riuscire ad avere contatti con quello che era il mondo hacker italiano al fine di riuscire a confermare quelle che erano le mie ipotesi sia in campo quantitativo che qualitativo.

Moltissime persone con cui avevo dialogato per anni nelle varie mail list hacker avevano una cultura nel settore infinitamente inferiore a quella che era stata dichiarata e molti di fatto pur essendosi costruiti un'immagine di un certo tipo in pratica non avevano mai avuto nulla a che fare con certi tipi di attività.

Il libro venne atteso con una trepidazione mai vista come se di fatto questo avrebbe potuto fornire ai lettori il metodo per acquisire la forza virtuale per diventare quell'ambita persona che era l'hacker.

Persone che non avevano avuto la capacità di costruirsi quell'immagine forte che in genere la società attribuisce all'hacker sperava che il volume gli potesse trasferire, quasi come processo osmotico, quel numero di conoscenze necessarie ad acquisire finalmente quell'immagine sospirata ed ambita per anni.

Dopo tanti anni di metamorfosi il termine hacker aveva un significato molto più attinente a concetti sociali di quanto lo fosse a quelli di tipo informatico.

Il termine hacker veniva utilizzato semplicemente per crearsi un'immagine sociale destinata a rappresentare un individuo in questo mondo virtuale.

D'altra parte a chi nella realtà non piacerebbe dare un'immagine di se forte e decisa ?

Bene.

Nel mondo virtuale offerto da internet il concetto di forza è questo.

Tutto all'interno del villaggio globale è simulato per cui anche l'immagine che noi potremmo costruirci potrebbe di fatto essere falsata e poco coincidente con l'immagine reale.

L'osservazione di certe community hacker dà esattamente l'idea del tipo di socializzazione che esiste nel mondo animale.

I branchi di lupi ad esempio usano le lotte tra i maschi più forti per stabilire qual'è che deve assumere il ruolo di capobranco.

Capisco che sembra esagerato ma di fatto non lo è.

Spesso questa lotta non conosce limiti.

Per fare capire cosa intendo voglio riportare un fatto accaduto qualche mese fa nel canale IRC #Phreak.it, al quale ho dovuto fare da intermediario con la Polizia postale per mettere le cose a posto.

I membri tecnicamente più dotati attaccavano quelli tenuti a privilegi più bassi fino a quando uno di questi riuscì a portare un attacco ad uno dei reggenti della chat.

Questo per vendicarsi acquisì tutte le informazioni indirizzate a identificare l'altra persona.

Dopo essere entrato abusivamente in un sistema di un'università veneta cancellò un certo numero di files di sistema con il fine di arrecare un grave danno.

Dopo aver fatto questo modificò il file di log, quello che teneva traccia delle attività tenute sul sistema, inserendoci dentro i dati identificativi dell'altro ragazzo.

Dopo aver fatto questo avviso in modo anonimo l'amministratore di sistema invitandolo a fare

denuncia alle forze dell'ordine.

Per capire lo stato mentale che ha spinto ad un'azione del genere voglio solo dire che a seguito di leggi uscite nel 1977 legate al terrorismo gli attentati ai centri di calcolo eseguiti con tecniche virtuali vennero paragonati a livello penale a quelli condotti con esplosivi.

Per dire che con uno scherzo di questo tipo uno rischiava 4 anni di carcerazione.

Al giorno d'oggi l'essenza che descriveva il modo d'essere hacker è quindi radicalmente mutato.

La ricerca informatica che l'hacker faceva 10 anni fa è oggi diventata una ricerca spasmodica di tutte quelle utilities sulla rete orientate a creare danni sui sistemi remoti.

D'altra parte quel filtro sociale relativo alle sempre maggiori complicazioni concettuali e tecniche sta funzionando come dissipatore relativo al numero degli hackers vecchia maniera.

Ad ogni modo essere hacker, inteso dal punto di vista tecnico, è questione d'istanti.

Cosa significa questo ?

Una volta esistevano pochi insiemi tecnologici su cui si basavano le connessioni dei sistemi.

Al giorno d'oggi esistono hardware come ad esempio routers, firewalls, switch, hub.

I protocolli sono a numerosissimi strati ciascuno dei quali dispone delle proprie caratteristiche e dei propri modi di funzionamento.

I servers per gestire i servizi adottano sistemi operativi differenti ed in particolar modo complessi con migliaia di funzionalità e strati di controllo.

I vari sistemi operativi dispongono di un numero immenso di softwares che gestiscono le varie funzionalità da host dei sistemi stessi.

Insomma.

La realtà telematica è costituita da un numero enorme di realtà che collaborano insieme al fine di creare il nostro mondo di servizi virtuali.

In tutto questo enorme insieme di cose il malfunzionamento è sempre in agguato.

Il tempo che l'hacker può utilizzare è quello che intercorre tra la sua scoperta e l'emissione da parte della casa produttrice del software della patch atta a tappare il buco.

In altre parole l'hacker interroga i sistemi che segnalano questi problemi, reperiscono il software sulla rete adatto a sfruttarlo ed infine iniziano un rastrellamento dei sistemi alla ricerca di quello che non ha ancora corretto il tutto.

La vita tecnica dell'hacker ad ogni modo ha sempre meno possibilità in quanto i sistemi di sicurezza stanno diventando sempre più sofisticati e i softwares di correzione dei sistemi praticamente immediati.

LE CONOSCENZE ATTUALI

Le attività svolte dagli hackers possono essere suddivise in tre tipologie differenti.

Analisi e ricerca dei sistemi vittima sulla rete
Individuazione delle caratteristiche software e hardware e quindi attacco.
Cancellazione delle tracce.

Se il lavoro di attacco viene tenuto partendo da sistemi in cui non è possibile identificare l'utente chiaramente la terza parte dei lavori svolti dall'hacker viene annullato e quindi di conseguenza i rischi vengono ridotti notevolmente.

Questo significa annullare completamente il significato che in genere le persone possiedono relativamente agli hackers.

Se fino a questo punto abbiamo detto che essere hacker vuol dire possedere un certo numero di conoscenze, al fine di testare nel mio piccolo qual'era il campionamento di individui che potevano avere i requisiti per essere considerati come tali, avevo creato un questionario sul mio sito www.crackinguniversity2000.it.

I risultati erano stati questi (su 200 persone) :

Conosce dei linguaggi di programmazione :

Linguaggio C	23
Assembler	8
Non conosce un linguaggio	120

Conosce a basso livello i sistemi operativi

Windows	43
Unix	31
Non conosce a basso livello	132

Conosce l'uso di sistemi operativi

Windows	188
Unix	89
Altro	23

Conosce la teoria delle reti

Protocolli e strati	41
Sicurezza in generale	78
Metodi di programmazione	25

Conosce metodi vari da hacker

Unicode bugs e altri simili	59
Buffer overflow	24
Spoofing	52

Password cracking 121

Conosce programmi generali analisi

Sniffers 143

Fingerprinting 105

Altri programmi 171

Da quanti anni usa internet

Da 1 a 2 anni 68

Da 2 a 3 anni 42

Da di più 76

Chiaramente la comunicazione tra individui che non vivono intensamente all'interno di questa community potrebbe sfalsare le informazioni che descrivono realmente il fenomeno.

Il problema di fatto è quello di fraintendere i significati sia in termini qualitativi che quantitativi. Detto in altre parole l'hacking vive nell'immaginario collettivo in un modo completamente differente da quello che è in realtà.

Come abbiamo detto determinati gruppi definendosi con il termine di hacker testimoniano un fenomeno quantitativamente rilevante.

Le informazioni legate a determinati miti nel campo dell'hacking descrivono socialmente quelle caratteristiche che dovrebbero essere particolari di questi elementi.

A riguardo di fatti capitati realmente bisogna anche individuare quanto la casualità abbia di fatto portato a sopravvalutare certi casi.

Come ho detto prima l'hacking è spesso un fatto di istanti.

E si arriva a individuare la tecnica giusta nel momento giusto si ottiene il risultato voluto.

La stessa tecnica utilizzata anche solo qualche giorno dopo su un determinato sistema potrebbe non portare più a ottenere gli stessi risultati.

D'altra parte si deve pensare alla rete internet e a tutti i sistemi informatici come ad entità dinamiche che mutano in continuazione sia come contenuti che come realtà.

La divulgazione da parte della stampa di determinate informazioni, percepite da persone che per mancanza di cultura specifica del settore hanno dovuto immagazzinarle come tali, senza poterle analizzare e considerare personalmente, hanno portato a sfalsare ulteriormente il fenomeno.

La somma di tutte e due le informazioni fanno sì che socialmente si pensi che le persone tecnicamente evolute, come di fatto lo dovrebbero essere gli hackers, in grado di manomettere i sistemi sulla rete siano di fatto in numero ben maggiore di quanto lo siano in realtà.

La filosofia hacker intesa come di fatto è in realtà al giorno d'oggi potrebbe trovare più punti comuni in quella che è la filosofia sociale dei gruppi più di quanto lo potrebbe fare relativamente al concetto di hacker di dieci anni fa.

D'altra parte questo poteva essere immaginato.

Quando quantitativamente internet non poteva essere considerata come alternativa alla realtà, in quanto le virtualizzazioni di queste erano poche e qualitativamente scarse, la proiezione di entità sociali non poteva essere presa in considerazione.

L'aumento incredibile avuto da questa realtà ha portato a ricreare virtualmente delle situazioni sociali.

D'altra parte sembra quasi assurdo paragonare le lotte tribali che esistevano all'inizio della creazione delle varie civiltà con le lotte che si stanno verificando virtualmente in questa realtà astratta.

Ma come ho detto prima quello che nella realtà può essere concepito con il termine di forza o violenza usata per ottenere certi privilegi sociali, nel mondo virtuale di internet è l'hacking.

L'hacking è la virtualizzazione della violenza e delle forze fisiche orientata a ottenere la supremazia nell'ambito del villaggio globale.

Il filoni con forti sfaccettature legate all'umanesimo negano con determinazione queste definizioni anche se di fatto alla fine non sanno rispondere a certe domande.

La nostra realtà è una continua dimostrazione di quanto la forza bruta usata per l'ottenimento di fini sociali venga moralmente condannata, ma in mezzo alla quale l'uomo continui a viverci.

Se di fatto la crescita delle reti ha come fine quello di portare l'uomo in un ambiente virtuale, e quindi l'uomo con tutte le sue qualità e i suoi difetti, questa violenza implicita nella sua natura come si trasforma e diventa ?

Nel 2000 l'hacker non è più un tecnico con conoscenze avanzate ma è l'uomo virtuale l' hacker !

La valutazione del fenomeno, a parte quella legata al tentativo di identificare le capacità tecniche eseguita con il fine di valutare se in effetti quanto si vede sulla rete corrisponde con la realtà, viene eseguita mediante una quantificazione degli incidenti informatici avvenuti in un determinato lasso di tempo.

Il fenomeno dell'hacking ha portato alla nascita di moltissime organizzazioni che possiedono come fine quello di incentivare la cultura delle protezioni e quello di individuare i punti deboli ovvero quelli a cui gli hackers si legano per l'esecuzione delle tecniche illegali.

Una di queste è il CERT-IT .

Dal 1994 al 1997, il numero di incidenti registrati al CERT-IT è andato progressivamente aumentando, passando dai 30 del 1994 ai 103 del 1997, per un totale di 492 macchine coinvolte.

Delle 103 segnalazioni ricevute, il 34% circa è di provenienza non accertata poiché spesso le segnalazioni degli incidenti sono incomplete, o per mancanza di dati o per incompletezza delle informazioni fornite nella segnalazione.

Del rimanente 66%, circa il 65% è costituito da segnalazioni di origine straniera (per metà europea e per metà statunitense) e il restante 35% di origine italiana.

Di queste, circa metà proviene da università e istituti di ricerca (macchine in aule attrezzate liberamente poste a disposizione degli studenti ma prive di qualunque protezione), e metà da Internet Service Provider.

La dinamicità degli indirizzi assegnati a chi si connette al provider viene spesso percepita come una sufficiente protezione in caso di azioni illecite.

Chiaramente questo è dovuto al fatto che moltissime attività svolte dagli hackers sono di fatto dei lunghissimi lavori di analisi svolti sui sistemi remoti.

L'identificazione dei sistemi avviene tramite il numero di identificazione in rete ovvero quello chiamato IP.

Se questo IP associato ad una macchina è fisso, l'hacker disporrebbe anche di molti giorni per svolgere le sue attività di indagine, cosa che non potrebbe avere se questo identificativo variasse di seduta in seduta.

Poiché i dati relativi alla provenienza degli attacchi si basano sulle informazioni raccolte e memorizzate dai vari strumenti di auditing disponibili sulle macchine attaccate, le quali sono facilmente modificabili da un hacker con un minimo d'esperienza, la loro attendibilità è limitata e non si devono trarre conclusioni assolute.

Analizzando gli obiettivi degli attacchi per capire se esiste una preferenza o una logica nella scelta da parte degli hacker dei siti da attaccare, si nota che spesso non esiste un disegno preciso, ma semplicemente si sfrutta l'individuazione casuale di una macchina poco protetta.

La scelta è indipendente dalla natura dei dati presenti sulla macchina, quindi il solo fatto di non

avere dati appetibili o di qualche valore (progetti aziendali, dati amministrativi ecc.) non rende una macchina connessa in Rete meno interessante a un hacker.

Le vittime sono divise tra macchine «aperte» (57%), quelle delle istituzioni accademiche e di ricerca, e quelle in teoria più protette delle aziende (43%). In questo caso, si tratta solitamente di server Web aziendali esposti alla curiosità degli hacker o di macchine firewall.

Le tecniche utilizzate per effettuare gli attacchi costituiscono un indicatore delle capacità tecniche dell'hacker, da una parte, e della robustezza dei sistemi, dall'altra.

La stragrande maggioranza delle macchine coinvolte in incidenti è stata compromessa utilizzando tecniche che non richiedono particolari competenze informatiche e possono essere impiegate anche da principianti.

Infatti, come abbiamo già detto precedentemente, le attività degli Script Kiddie sono di gran lunga le più diffuse e pericolose.

Nella psicologia di questi individui l'attività è composta da due componenti.

La prima è quella legata alla creazione del danno mentre la seconda è quella in cui avviene la diffusione della notizia.

Questo metodo possiede il significato di comunicare agli altri elementi del gruppo la propria forza e quindi la pericolosità contro la quale una persona dovrebbe pensarci su due volte prima di andarci contro.

Io definisco questa attività con il termine di "morso del lupo".

La diffusione sulla Rete di informazioni relative a nuovi attacchi basati per lo più su errori scoperti nei programmi e agli exploit per sfruttarli per accedere a un sistema senza esserne autorizzati, si riflette negli incidenti registrati.

La valutazione di questi errori è comunque complicata a fini della valutazione dell'entità dell'hacking in Italia in quanto di fatto è complicato identificare la provenienza dell'attacco.

L'identificazione dell'origine delle attività degli hackers potrebbe essere agevolata dallo studio delle tipologie di attacco portate ai sistemi.

Molte di queste metodologie denunciano determinate "scuole di pensiero" mediante la quali potrebbe essere, chiaramente senza una sicurezza assoluta, identificato il gruppo attaccante.

Questo tipo di valutazione porta ad ogni modo a giungere a conclusioni che solo parzialmente condivido.

Quello che segue è una breve conclusione del CERT-IT derivante appunto dall'analisi della tipologia dei tipi di attacchi portati dagli hackers.

"La tipologia degli incidenti e le tecniche di attacco impiegate permettono di trarre le seguenti conclusioni sullo stato dell'hacking in Italia.

Quasi certamente esiste in Italia una «scuola» di hacking di buon livello: abbiamo infatti rilevato alcune intrusioni, quasi sicuramente provenienti dall'Italia, effettuate con tecniche molto avanzate che presuppongono solide basi di conoscenza e padronanza della materia. Fortunatamente però il fenomeno non ha ancora assunto le connotazioni tipiche della criminalità informatica in altri Paesi.

Infatti, sono molto rare le intrusioni informatiche operate con finalità strettamente commerciali, cioè finalizzate al furto o alla deliberata alterazione di dati e flussi aziendali.

Ciò è in parte dovuto alla tipologia dell'impiego di Internet a livello aziendale italiano (siti Web aziendali a scopo promozionale, posta elettronica, navigazione sul Web).

Le aziende italiane che impiegano Internet per scambiarsi dati critici o per offrire servizi di tipo dispositivo e transazionale (quali per esempio trasferimento di fondi, l'acquisizione di ordini di acquisto, la vendita di beni) sono ancora molto poche, e rari sono quindi i presupposti economici che motiverebbero e anzi favorirebbero azioni di hacking criminali. Per contro, quando tali presupposti si verificheranno, l'Italia potrebbe diventare uno dei Paesi maggiormente esposti a tale minaccia.

Sebbene in Italia l'hacking non sia ancora un problema grave, tuttavia si osserva un fenomeno preoccupante: la scarsa attenzione alle problematiche di sicurezza degli addetti ai lavori. Circa nell'80% degli incidenti gestiti dal CERT-IT sono state utilizzate tecniche di intrusione per cui erano già state definite le necessarie contromisure da almeno 6 mesi.

Tutto ciò equivale a dire che, se quelle organizzazioni avessero affrontato il problema della sicurezza informatica per tempo predisponendo personale ben addestrato, l'80% delle intrusioni verificatesi quest'anno nel nostro Paese si sarebbero potute evitare.

Purtroppo in Italia prevale un atteggiamento di attesa rispetto alla sicurezza informatica per cui si tende a posticipare il momento in cui affrontare il problema fino a quando non sia necessario. Un simile atteggiamento non è stato sinora penalizzante, soprattutto in virtù delle condizioni sopra descritte.

Con la diffusione in Internet di applicazioni di commercio elettronico i presupposti sopra menzionati verranno meno e il perdurare di una simile mentalità nei confronti della sicurezza informatica potrebbe far diventare il nostro Paese uno dei bersagli preferiti dagli hacker di tutto il mondo.

È nostra ferma convinzione che il problema della sicurezza informatica debba essere assolutamente considerato da un qualunque individuo o ente che voglia connettere il proprio calcolatore alla rete Internet.

È altresì nostra convinzione che il problema della sicurezza informatica possa essere significativamente contenuto, purché affrontato con la giusta dose di consapevolezza e di preparazione.

Ricordiamoci a ogni modo che la sicurezza informatica deve in gran parte essere affrontata alla radice dai creatori dei sistemi operativi in quanto i metodi di accesso ai sistemi tramite reti è in gran parte dovuta a problemi di base di questi.

Chiaramente un fattore legislativo deve essere anche affrontato politicamente mediante un seria valutazione del problema dal punto di vista reale, analisi che di fatto solo un supporto tecnico può sostenere.

La cultura legislativa deve anche pubblicizzare i vari difetti che la legge potrebbe avere in funzione dell'impossibilità di valutare un casistica personale.

Questo per dire che l'azione informativa dovrebbe portare anche il ragazzino a comprendere che il reato informatico non può possedere come giustificativo il fatto del "commesso per gioco" e che quindi il procedimento penale avrebbe come risultato lo stesso di quello condotto nei confronti di hackeraggio "professionale".

Spesso la gravità non viene considerata fino a quando le cose non capitano e a volte a fatti compiuti si viene a creare un atteggiamento di vittimismo quasi orientato a creare un martire legato alla libertà dell'informazione.

Le varie statistiche fatte da organismi come il CERT sono relative ad anni passati e alcune volte potrebbero essere troppo differenti dalla realtà attuale.

IL PERICOLO PER IL FUTURO

Le problematiche legate alla criminalità informatica rischia di interessare svariate categorie legate a numerose aree sociali.

Come abbiamo visto sino ad adesso l'evoluzione del concetto di hacking ha toccato fondamentalmente aspetti caratteriali degli individui legati alla curiosità e al modo di rapportarsi all'interno di un gruppo.

Il continuo crescere di attività economiche sulla rete porterà sicuramente a indirizzare il futuro andamento dell'hacking verso una criminalità legata a truffe e raggiri.

Le attività svolte dagli hackers non coinvolgono soltanto quelle tecniche orientate agli accessi abusivi a sistemi messi in rete, ma anche ad altri tipi di tecniche come ad esempio quelle legate allo sniffing di dati legati a transazioni economiche, ad esempio su siti di ecommerce, finalizzati a carpire numeri di carte di credito da utilizzare successivamente in acquisti di merce sempre mediante la rete.

Queste attività svolte dagli hackers con il fine di arricchimenti personali sono già di fatto il punto forte dell'immaginario collettivo, ovvero l'hacker viene visto come un individuo che svolge le sue attività illegali sulla rete con il fine di trarne profitto.

Infatti, come abbiamo appena detto, lo sviluppo delle reti telematiche sta modificando radicalmente le dinamiche commerciali creando un "mercato globale diffuso".

Chiunque può offrire merci e servizi sulla rete con una drastica riduzione dei costi di gestione.

IL RISENTIMENTO

Il settore degli hackers teatrali diventa sempre più numericamente grosso per cui spesso gli individui non percepiscono più i proiettori su di loro per cui molti rinnegano pubblicamente quell'ambiente che precedentemente avevano utilizzato come palcoscenico.

Se la mia teoria legata alla nuova essenza degli hacker è di fatto esatta, la crescita come numero dei partecipanti a questi gruppi porterebbe ad un aumento dell'anonimità degli individui stessi e quindi ad una crescita del senso di rivalsa rispetto agli altri partecipanti.

Essendoci allo stesso tempo l'impossibilità di cambiare questo andamento molti individui potrebbero arrivare a ripudiare questo mondo.

Di fatto questo è stato il motivo per cui molti dei ragazzi che si definivano come hackers hanno fatto marcia indietro scrivendo cose del tipo (nota: riporto senza commento) :

"...sinceramente ne ho piene le scatole di essere e di stare tra gente che crede di valere solo perché sa usare bene un computer.

internet e' strapiena di gruppi hacker, cracker e via dicendo, ma fatti dire una cosa: la stragrande maggioranza di loro sono solo degli esaltati che sanno a stento usare le backdoor per dar fastidio alla gente, una parte conosce abbastanza di hacking e vuole imparare ancora per fare chissà che cosa, e i pochi che restano conoscono tanto bene l'argomento che possono impiegarlo soltanto in due modi: per fini criminali, oppure per passare dall'altra parte e guadagnare qualcosa.

...ho fatto un esperimento: ho creato un finto gruppo hacker straniero, con tanto di sito web, indirizzi email e tutto il resto; ho contattato hacker di un certo livello, ho infarcito le comunicazioni e le pagine con stupidità presentate in modo professionale, ragionamenti sull'etica...

ci sono cascati tutti... i complimenti dei membri di webfringe, di phrack, di gente vicina ai lopht... basta insomma apparire, non essere.

l'hacker e' come una rock star, in tutti i sensi, non e' niente altro, non e' nessuno ...pensa che c'e' gente che va in giro vantandosi (ma di che poi?) di essere lord shinva. c'e' anche un forum che sfrutta il mio nick per fare soldi con i banner (salvo poi che la gente che visita il forum dice: sì, ma lord dove cavolo sta?)

...hai fatto caso che l'hacking e la libertà di espressione su internet sono quasi sempre collegati? (blue ribbon, manifesto di mentor, i commenti tristi sulla cattiveria delle forze dell'ordine quando chiudono quel povero sito che distribuiva i codici delle carte di credito a fin di bene e via dicendo)... non solo perché l'hacking sia illegale in quasi tutti i suoi aspetti, ma anche perché e' un modo per attirare la gente, tipo "legalizzala".

...ci ho creduto anche io alla falsissima etica hacker, alle vuotissime parole di mentor, alla pratica dell'hacking in maniera contrapposta alle dilaganti manie di protagonismo

...sfrutta l'ignoranza e incita la gente con slogan tipo "la conoscenza e' potere", "l'informazione vuole essere libera"... il phreaking (rubare, a tutti gli effetti), i testi anarchici (costruire bombe, avvelenare, preparare attentati... sempre associati all'hacking in virtù della libertà di espressione e della necessità di fare controtendenza, o soltanto di essere "contro").

...sono un mucchio di spazzatura e propaganda, e di tempo ne perso pure troppo. mi restano quelle conoscenze informatiche "avanzate" talvolta utili nel mondo del lavoro.

ma a parte questo, e a parte la sensazione di sfida che da' fare qualcosa che, in fin dei conti, e' ai limiti della legalità (bella emozione, rischiare sulla fedina penale e stravolgere la propria vita passando da esperto informatico a esperto di giustizia penale)..."