Raoul Chiesa

La storia di Otto Sync e White Knight

APOGEO

La storia di Otto Sync e White Knight

Autore:
Raoul Chiesa

Via Natale Battaglia 12 – 20127 Milano (Italy)
Telefono: 02-28970277 (5 linee r.a.)
Telefax: 02-26116334
Email apogeo@apogeonline.com
U.R.L. http://www.apogeonline.com

Responsabile editoria digitale: Alberto Mari
Copertina: Enrico Marcandalli

Indice

Il 2 dicembre del 1992 il venticinquenne Otto Sync, nome ovviamente fittizio, viene arrestato ed accusato di uso non autorizzato del network informatico Datapak. Le intrusioni avvengono nel novembre del 1992 a spese della Televerket, al tempo compagnia telefonica svedese di monopolio. La persona che ha tracciato l'hacker e ne ha ordinato l'arresto è Pege "White Knight" Gustafsson, allora zelante trentottenne, vecchio "security expert" il quale aspirava ad una brillante carriera.

Ho incontrato Otto per caso, in Rete, dopo molti anni: vediamo di capire come un francese che ora vive in un paese asiatico abbia finito per essere arrestato in Svezia. . .

1 Da Lione a Flen

Nazionalità francese, hacker, esperto in reti di trasmissioni dati, sistemi UNIX e VMS: dal dicembre del 1991 al febbraio del 1993 Otto serve il suo Paese, svolgendo servizi "non bellici" nell'esercito francese.

È arruolato nel "Volontaire Service National en Enterprises" come ingegnere PLC (computerized process controllers) in un'azienda francese di telecomunicazioni a Flen, Svezia. Dopo aver superato rigorosi test militari, con l'aiuto di un master in ingegneria e delle sue ampie conoscenze in matematica applicata e computer science, gli viene offerta l'opportuni-

tà di svolgere il servizio civile nella filiale svedese dell'azienda francese.

Essere un solitario francese nella cittadina di Flen non è il massimo. . . Otto narra di una città piena di rifugiati politici, con un'idea locale della fratellenza tra i popoli non eccessivamente aperta, dove i giovani di Flen tengono solo a se stessi e lo vedono come uno dei tanti immigrati, quando gli immigrati in questione non sono francesi bensì Iracheni, Curdi, Somali e così via. Come se non bastasse, Otto non è abituato alla vita delle piccole cittadine: "Partii direttamente da Lione, immagina la mia sorpresa quando mi ritrovai tutto solo, in quel buco di città, nel dicembre del 1991..ho sempre e solo vissuto in grandi città e mi ritrovo in un posto senza bar, pub o negozi di computer. . . "

Il risultato è semplice: Otto passa la maggior parte del suo tempo da solo, nel suo appartamento o nell'ufficio dell'azienda. Sorridendo, mi spiega che "Flen era così noiosa che, alla fine, vivevo praticamente nel mio ufficio attaccato al computer: cos'altro potevo fare in quel posto dimenticato da dio, se non hacking ??"

Per le ragioni sopra esposte, dunque, Otto utilizza la maggior parte del suo tempo per il suo hobby preferito: l'hacking J Quando arrivò in Svezia era già altamente skillato[1] e – man mano che il tempo passava – le sue capacità crebbero esponenzialmente.

[1]Esperto (Skilled)

Diviene un abituè della BBS[2] hacker più famosa del paese, Synchron City, esplora ogni sistema raggiungibile, dalla rete telefonica pubblica della Televerket all'AT&T, Internet, e così via..Nessuno di questi, però, era *veramente* eccitante per un giovane hacker con tanta voglia di correre per le Reti: la rete telefonica era semplice da "maneggiare" ed Internet era bene o male frequentata da persone "normali", quali ricercatori o studenti. I veri hacker, in quegli anni, giravano per BBS sulle reti X.25, ed Otto voleva mantenere i contatti con i propri amici, appartenenti a diversi paesi, con i quali aveva a che fare ogni notte prima di trasferirsi in Svezia.

La necessità era allora quella di avere accesso al più grande Conference System dell'epoca, la "mecca" degli hacker, QSD, e QSD era accessibile solo dalla rete internazionale X.25. Nel tentare di accedere a questa chatline, Otto commise il suo errore più fatale: esplorare il Televerket Datapak Network.

2 L'errore di Otto: X.25 & Datapak

Datapak è un network strutturalmente reminiscente ad Internet, una rete a tipologia packet-switching[3], dove gli utenti condividono poche linee dedicate e

[2]B.B.S., Bulletin Board System

[3]Commutazione di pacchetto

pagano in base alla quantità di dati trasmessi (a pacchetti, o *otteti*). Generalmente funziona in modo tale da permettere, mediante l'utilizzo di un modem, la chiamata ad un numero (POP[4]) di accesso Datapak attraverso un PAD[5] di accesso alla rete, connesso ad una numerazione di tipo 020 (come i numeri verdi in Italia, quindi a chiamata gratuita indipendentemente dalla durata della connessione): una volta connessi si chiama il numero identificativo (N.U.A.[6]) di un computer continuamente collegato alla rete Datapak. Tutti i computer connessi alla rete hanno dunque un proprio identificativo di utenza, esattamente come ogni abbonato alla rete telefonica pubblica.

Naturalmente ci si può collegare direttamente ad un computer connesso a Datapak nel caso in cui ci si possa permettere una costosa connessione dedicata al proprio computer, non avendo così la necessità di passare attraverso i punti di accesso alla rete. In questo modo due computer possono essere continuamente collegati, evitando gli alti costi telefonici di una connessione simile a mezzo modem e pagando solo le spese del traffico dati trasmesso.

Datapak è stata costruita – come ogni altra rete di dati dello stesso tipo – sullo standard X.25, il quale descrive come i computer in un network geografico

[4]P.O.P. – Point Of Presence, nodo di accesso alla rete

[5]P.A.D. - Packet Assembler Disassembler

[6]N.U.A. - Network User Address

possano "dialogare" l'un l'altro. Oltre ad X.25 viaggiano molti altri standard sul network, quali X.28, X.3 o X.75, ma X.25 è lo standard più comune e Datapak appartiene allo standard "X.25 network": la rete internazionale è utilizzata per interconnettere le reti informatiche di altri paesi, quali ad esempio TymNet (USA, la quale produce anche gli apparati utilizzati dal network svedese), SprintNet (USA), Telepac (Francia), Itapac (Italia), etc. . . ogni paese industrializzato ha dunque la propria rete dati su protocollo X.25.

Ogni paese ha anche un proprio identificativo di rete (prefisso, DNIC[7]), il quale va anteposto al NUA nel momento in cui si vuole inviare la chiamata in un paese differente da quello della nostra chiamata di origine. Ricordo che uno "sport" molto diffuso su QSD era proprio quello di collegarsi dai posti più strani del mondo (QSD identificava il paese e la rete chiamante a fianco del nickname[8]), ed apparvero allora simpatici e strani utenti del tipo "Nobody (Gabon)", "Bayernpower (Trinidad&Tobago)", "Sentinel" (Papouasia), Machine (Italy/Italcable), etc. . .

La rete internazionale di dati X.25 si è sviluppata in Europa dalla metà degli anni '80 in poi, ma in Svezia non è mai stata eccessivamente grande: il motivo è il target di utenza, il quale non è rivolto ad un

[7]D.N.I.C. - Data Network International Code

[8]Nickname, Alias: soprannome di rete, nomignolo utilizzato al posto del proprio vero nome

mercato consumer, bensì alle corporation. Il grande mercato consumer è stato poi conquistato da Internet, con l'iniziale diffusione in ambiti accademici e la nascita di svariati service provider, creando così una competizione nelle offerte di mercato: esattamente il contrario di X.25, dove i fornitori erano pochi e quasi in regime di monopolio. Questa tipologia di rete è sempre stata largamente utilizzata per gestire links logici tra reti private, ma è comunque usata anche per collegamenti alle dorsali Internet.

Quello che però Otto non sapeva o non credeva quando fece la richiesta di abbonamento a Datapak - al solo fine di ottenere i manuali e gli schemi tecnici dei PAD – fu che la rete Datapak era un piccolo sistema in un piccolo paese e che, quindi, la persona che avesse tentato "manipolazioni" strane sarebbe subito stata individuata dai sistemi di monitoring. La rete telefonica pubblica è estremamente sicura grazie a tutte le telefonate che la gente fa in posti strani in giro per il mondo e, di conseguenza, sporadici casi di manomissione o abuso si perdono nella vastità delle chiamate "legali".

3 NUI scanning e manuali ufficiali

Datapak è una rete di dati molto piccola e con pochi abbonati, i quali chiamano sempre gli stessi siste-

mi: ancor prima dello stupore dei tecnici nel vedere chiamate X.25 continue su QSD France, Otto catturò la loro attenzione iniziando a "scannare" i codici di accesso alla rete. Spiego anche il motivo - prima di raccontare il simpatico e curioso modo in cui il nostro eroe iniziò queste operazioni di "indagine" - del panico e della preoccupazione dei tecnici Datapak verso l'hacking: tra il 1990 ed 1992 il gruppo hacker inglese 8LGM (8-Little Green Men come li conobbi io, o 8-Legged Groovin' Machine, sull'onda di un gruppo pop degli anni '80, come dicono altri) effettuò una serie di scanning su 22.000 indirizzi X.25 Datapak, violando 380 sistemi informatici in tutto il paese. Una prima conseguenza di questo raid fu che da allora tutte le attività su Datapak sono registrate ed analizzate; violare un sistema era diventato un po' come il girare con luci di emergenza attaccate alla testa per il centro di Flen o a Passerano Marmorito: una presenza non troppo discreta. . . Quando Otto iniziò a scannare Datapak, la Televerket si accorse immediatamente di lui.

Il nostro amico non si abbonò a Datapak con il logico e banale scopo di utilizzarla, ma semplicemente per avere accesso alla documentazione tecnica data ad ogni abbonato e capire il funzionamento della rete.

In questo modo scoprì che ci si collegava a Datapak chiamando il numero 020-910037 e fornendo il proprio identificativo di rete (NUI): fatto ciò si po-

tevano effettuare tutte le chiamate X.25 che si voleva ed il traffico dati sarebbe stato addebitato alla NUI utilizzata, la quale identifica il cliente e funge da parametro per la contabilizzazione e l'invio della bolletta del traffico dati.

Il manuale Datapak della Teverket forniva anche una serie di informazioni estremamente utili, come l'esempio di seguito riportato, preso dalla pagina 4:

> "per collegarsi con un utente di rete, componete il numero 020-910037 utilizzando un modem. Quando il modem risponde, digitate tre volte "." seguito da un invio (CR, Carriage Return, il tasto invio).
>
> Poi scrivete:
>
> N123456XYZ123-024037131270 <CR>
>
> N indica al PAD con il quale siete connessi che quanto segue sono l'utente e la password (utente+password=NUI)
>
> 123456 è l'identificativo (utente) che vi assegnano nel momento della sottoscrizione all'abonamento Datapak
>
> XYZ123 è la vostra password segreta
>
> Il numero dopo il trattino "-" è l'identificativo di rete (NUA) che volete chiamare (il computer al quale volete collegarvi)."

Proseguendo nella lettura del manuale, viene spiegato dai gentilissimi e precisi signori della Televerket cosa l'utente 123456 debba fare per cambiare la propria password da BERTIL a CAESAR: la NUI 123456 è chiaramente utilizzata come esempio.

Ora, un lettore qualunque avrebbe sfogliato o letto il manuale, capito bene o male il funzionamento della rete e del PAD e si sarebbe fermato lì .

Otto legge, rilegge, e riflette. . .

Partendo dalla logica di 6 caratteri per l'utente e 6 per la password e prendendo come dato di fatto che l'utente è composto da una serie di numeri, Otto inizia una serie di pensieri i quali daranno come risultato finale il primo hacker tool svedese: un NUI scanner.

Lo scanning è una tecnica nata originariamente come strumento per le reti telefoniche pubbliche, la cui logica è quella di effettuare chiamate a dei numeri telefonici, in ordine sequenziale. Si inizia quindi ad esempio da 06-5555555, chiamando 06-5555556 (3 squilli e via), 06-5555557 e si prosegue, sino a quando non si trova un modem che genera un segnale di risposta. Quando si trova un computer si prende nota del numero telefonico e si passa al successivo. Alla fine si scelgono dall'elenco dei computer trovati i numeri e si prova a bucarli. Quest'esempio riguarda ovviamente lo scanning manuale e "casalingo", ma ritengo che illustri pienamente la logica dello scanning. Scannare a mano diventa, a

lungo andare, faticoso, e si arriva quindi a scrivere un software (o ad utilizzarne di già fatti) che, automaticamente, compone sequenzialmente numeri telefonici e registra su un file i modem trovati in risposta. E' importante puntualizzare come lo scanning, di sé, non sia illegale: si ha un abbonamento telefonico appositamente per effettuare telefonate, alle ore ed alle persone che si vuole.

Otto ebbe dunque l'idea di scrivere uno scanner che provasse diverse combinazioni di username e password per la rete Datapak.

Devo dire che, se si pensa come il tutto partì a causa della volontà di Otto di parlare con i suoi amici hacker di QSD, me incluso, questa storia ha dei risvolti veramente comici ed altamente ironoci: aggettivi che si addicono peraltro moltissimo al carattere di Otto.

Ad ogni modo lo scanner di Otto Sync era un po' differente dagli scanner scritti per le reti telefoniche. Non agiva infatti con la logica di trovare un numero attivo, ma delle NUI per avere l'accesso al Datapak network. In genere un PAD X.25 (il POP per gli accessi via modem alla rete) permette solo tre tentativi di identificazione prima che la chiamata venga fisicamente disconnessa. Provando tre identificativi ogni telefonata, lo scanner sarebbe divenuto molto lento, rallentato dalle fasi di chiamata/disconnessione-/ricomposizione del numero telefonico; inoltre Otto avrebbe speso parecchio e questo non rientrava ov-

viamente nella sua ottica di "economia casalinga". Si dice che la necessità aguzza l'ingegno ed il nostro amico scoprì che collegandosi con il sistema informativo della rete Datapak si potevano provare tre password alla volta, rifare la chiamata X.25 (senza dunque scollegarsi dal PAD) e provare altre tre combinazioni. In questo modo lo scanning era incredibilmente veloce e la rapidità di esecuzione combatteva contro il basso numero di probabilità nel trovare uno username attivo ed azzeccarne anche la relativa password.

A questo punto serviva una NUI di partenza per testare il programma, ed Otto inserì per puro caso una combinazione utent/password alquanto stupida, username 123456 (l'utente riportato nel manuale Datapak come esempio) e la password 654321: con un iniziale stupore seguito da una risata di puro divertimento, la combinazione funzionava ! L'identificativo 123456 apparteneva alla Televerket, una NUI di test che probabilmente era stata lasciata attiva per dimenticanza. Otto aveva finalmente la soluzione al suo problema, ed iniziò a chiamare regolarmente QSD ed incontrare i suoi amici: gente come SCSI, il quale è entrato in tutte le reti X.25 esistenti al mondo (nessuna esclusa, ci tengo a dirlo), Sentinel dalla ex Yugoslavia, Venix, giovane greca, Seven Up, sysop di SecTec, una BBS hacker X.25 tedesca.

I chat con gli amici proseguirono sino a quando, nella notte del 7 di novembre del 1992, Otto

viene contattato da un altro hacker dalla Svezia: il "Cavaliere Bianco".

La prima conversazione tra Otto Sync e White Knight viene di seguito riportata. È importante sottolineare come tutti i dialoghi intercorsi tra i due furono successivamente utilizzati come prove a carico dall'accusa.

> White Night : Hi! Hej! [Hej è "ciao" in svedese]
>
> Otto Sync : Hi! Hej! Sorry I'm not Swedish I'm French. Calling from Flen, a #$&% city 120 km from Stockholm.
>
> WN : I see. What are you doing there?
>
> OS : Working as an automation engineer at a French company. And you?
>
> WN : I'm working at Volvo.
>
> OS : Where? I worked at their factory in Olofström some months ago.
>
> WN : DA-verken in Göteborg. [Gothenburg]

Il dialogo prosegue con scambi di pareri su questioni tecniche, come tutti gli hacker fanno. Otto chiede a White Knight come riesca ad utilizzare il set di caratteri svedesi e poi i due discutono su diversi programmi di emulazione terminale. White Knight porta poi il dialogo sul come Otto faccia a collegarsi

a QSD e chiede se sa quanto gli costa (!). Otto gli parla di outdial[9] per chiamare BBS americane "H/P-/A", Hacking, Phreaking e Anarchy, file testuali perfettamente legali i quali descrivono tecniche e metodologie di hacking, e di Synchron City, BBS locale che lui chiama spesso.

White Knight non ha mai sentito parlare di Synchron City ed è subito curioso. Otto continua a chiamare QSD abbastanza regolamente nelle settimane successive e nella notte del 29 di novembre il Cavaliere Bianco riappare di nuovo. Non riconosce subito Otto - il quale usa un altro nickname - e Otto si è già dimenticato di lui. Otto ha detto della NUI solo ad un altro hacker, Phred, e si insospettisce vedendo che White Knight usa la NUI 123456: inizia così a parlare con lui.

WN : Hi.

OS : Phred?

WN : No, but I know him!

OS : I guess so... I know you?

WN : Fun, do I know U?

OS : Maybe, I'm usually Otto Sync here...

WN : Hi Otto, hm hm hm.

[9]NUA di computer connessi a reti di pubblico accesso come Internet, con modem collegati i quali permettono di effettuare chiamate in uscita accedendo ai modem stessi

OS : Hey, could you tell me who you are... cool!

WN : U speak Swedish?

OS : Very badly. But can’t you tell me who u are??? As for me, I’m the one who found the NUI you’re using.

WN : Why do U think I use the NUI "you"found?

OS : You can ask Phred if you don’t believe me.

WN : Why should I ask Phred?

OS : Because he was the first one to whom I gave the NUI. We talk voice sometimes.

WN : What NUI?

OS : The very obvious one with the very obvious password. And the second one that I see on QSD.

WN : Wow, I haven’t spoken to Phred 4 a long time!

Il “non capirsi” tra Otto Sync e White Knight è ovviamente dovuto al fatto che quest’ultimo non è un hacker. Infatti in realtà chiamava dall’interno della Televerket stessa, utilizzando la linea di test dell’azienda, NUI 123456. Quando Otto sottolinea di essere stato lui a trovarla, il cavaliere bianco capisce e si immedesima nella parte. Otto nelle settimane trascorse dal primo incontro ha realizzato il suo

NUI scanner ed utilizza le NUI trovate a rotazione, per non rischiare di "bruciarne" addebitando troppe chiamate su una singola utenza.

> OS : The previous [NUI I used] was 159800. Are you from Sweden by the way?
>
> WN : Sweden what.
>
> OS : Just wondering... If you don't want to chat, then why go on QSD?
>
> WN : Of course I want 2 chat. I'm Swede! R U?
>
> OS : Nope I'm French. But I like Televerket, except when they send me bills :)
>
> WN : Do they? Why?
>
> OS : I asked for a NUI some weeks ago to get the technical doc about the PAD... But I won't pay!

Al termine di queste parole White Knight si disconnette, va alla stampante e prende il print-out della conversazione. Questo tabulato è stato utilizzato come parte delle prove dall'accusa nel processo ad Otto Sync alla Katrineholm Court of Law, *Televerket Sweden contro* ********* ********, alias Otto Sync, per "violazione ed abuso di sistemi informatici statali di pubblica utilità".

4 Il Cavaliere attacca

Otto non sapeva che mentre la conversazione aveva luogo la Televerket lo stava tracciando per identificare la sua utenza telefonica: dal giorno precedente, 28 novembre, sino al 1° dicembre, giorno prima dell'arresto, la Televerket registra tutto il traffico telefonico in uscita dall'azienda francese verso l'esterno. Il riuscire in questo compito significò prendere misure quasi straordinarie per la tranquilla Svezia ed in particolar modo per la remota cittadella di Flen. La centrale del paese non era provvista dei commutatori elettronici di nuova generazione quali l'AXE, (Automatic Cross Connection Equipment) ma funzionava con vecchi sistemi di switch elettromeccanici. Se la centrale fosse stata fornita di una tecnologia di tipo AXE il monitoraggio sarebbe stata una questione tutto sommato semplice, in quanto il sistema avrebbe richiesto una serie di informazioni continue all'IS - l'Information System della Televerket - il quale può monitorizzare automaticamente un'utenza per un tempo illimitato ed effettuando incroci su una svariata mole di dati on-line ed off-line. L'attuale telecom svedese, Telia, risultato della privatizzazione della Televerket, è a tutt'oggi un carrier telefonico molto avanti sul fronte del controllo della risorsa e degli abusi di un sistema telefonico nazionale.

La Televerket sotto la direzione di Pege Gustafsson identificò e tracciò le chiamate abusive e fraudo-

lente al numero 020-910037 del PAD Datapak e ad un certo punto si trovò di fronte ad un group number, vale a dire un "fascio" di linee telefoniche collegate ad un centralino telefonico interno (PBX nella fattispecie) il quale smistava circa 500 telefoni interni. Arrivando al group number non avevano nessun tipo di prova in mano, dato che la chiamata poteva esser stata fatta da uno qualunque dei telefoni sparsi per l'azienda dove Otto presumibilmente lavorava. Nulla collegava le chiamate ad una persona fisica e questo è invece quanto richiesto in questa tipologia di reati.

Naturalmente l'intera fase di tracing fu supervisionata da Pege "White Knight" Gustafsson.

Il 2 di dicembre quando la polizia va ad arrestare Otto (con grande imbarazzo di quest'ultimo) al lavoro, Pege è lì , perquisisce il suo ufficio, sequestra blocchi di appunti e materiale per computer. Poi lo portano a casa, gli fanno aprire la porta dell'appartamento e proseguono la perquisizione.

La gita turistica termina alla stazione di polizia di Katrineholm, l'autorità di polizia più vicina a Flen, per l'interrogatorio. Durante il tragitto nella mente di Otto corrono tantissimi pensieri..Cosa dire ? Pensavo che fosse una BBS ? Credevo fosse un sistema libero ? Reverse charging ?

Arrivato sul posto ed iniziato l'interrogatorio, il nostro amico Otto prende tempo chiedendo la presenza di un interprete. All'arrivo di quest'ultimo chiede di un avvocato, ma accetta di proseguire l'in-

terrogatorio (in realtà non ancora iniziato !) senza la presenza dell'accusa (Televerket), i cui rappresentanti non erano ancora arrivati. L'azienda manda i dipendenti francesi alla scuola serale di svedese e così Otto riesce ad afferrare ogni tanto qualche parola di commento dei poliziotti, ma ritiene comunque "eccessivo" contattare l'ambasciata francese e declina così anche questa proposta. Spiega di essere sotto servizio civile in un'azienda di Flen e che pensava di continuare a lavorare lì anche alla fine del periodo di leva.

Alle 14.25 Otto vive quello che sicuramente è uno dei momenti più belli della sua vita: arriva l'avvocato a lui assegnato, il quale risulta essere una persona altamente professionale, con un proprio studio legale specializzato in dispute tra multinazionali dell'industria corporate. Il caso dell'hacker lo ha subito interessato e si è fatto avanti per prendere la difesa di Otto. Otto mi racconta di come abbia visto subito in quest'uomo "un capo, un vero professionista, e lo dico con tre processi alle spalle ;)". Un'ottima persona, molto ben educato ed amante dei vini francesi. . .

5 Interrogatorio e carceri svedesi

L'interrogatorio prosegue dunque con la presenza dell'avvocato difensore, l'interprete, la polizia e il giudice: i soli a parlare sono Pege ed Otto Sync, i quali narrano e disquisiscono su argomenti incomprensibili ai presenti. Otto insiste nel dire che era alla ricerca di un numero a reverse charge (l'equivalente del numero verde su X.25) e di come pensasse che la NUI 123456 trovata nel manuale Datapak (rete alla quale era regolarmente abbonato!) fosse una test line di qualche tipo.

Otto punta dunque la sua difesa verso l'innocenza più totale giocando sulla figura di un giovane francese volenteroso e ligio al dovere, estremamente appassionato di informatica e telecomunicazioni. Ammette la propria curiosità e sottolinea come sia proprio quest'ultima ad averlo spinto all'esplorazione dei sistemi informatici della Televerket.

Ovviamente Pege tira fuori gli stampati delle sessioni di chat dove si mascherava come White Knight e chiede un confronto rispetto a quanto scritto su QSD: Otto realizza per la prima volta di avere davanti a sé *quel* White Knight e capisce come lo vogliono intrappolare. Si adatta dunque ai fatti, evidenziando come chiunque avrebbe potuto utilizzare il suo alias su QSD. Pege chiede se ha mai "passato" la NUI 123456 ad altre persone ed Otto, ovviamente,

risponde di no.

Dopo tutti gli anni passati da allora, oggi Otto mi racconta di come "Pege tentò di farmi dire che sapevo benissimo quello che stavo facendo quando trovai la NUI, ma io continuai a negare e ripetei di come fossi convinto di utilizzare una linea pubblica in reverse-charge, continuando per quella linea. Naturalmente Pege pensava fossi un vero stronzo, lui sapeva perfettamente chi ero e cosa facevo: aveva ragione su tutti i fronti, ma non era proprio il caso di dargli ragione davanti a tutti !"

Quando l'interrogatorio terminò, verso le 6 di sera, lo portarono in cella, dato che si era fatto troppo tardi per andare in aula il giorno stesso. Otto rimase immediatamente impressionato dallo standard di custodia svedese: "In Francia c'è sporcizia, devi dormire con gli ubriachi ed i clochard, difficilmente ti danno da mangiare e subisci solo trattamenti duri. . . al Katrineholm era come essere in un hotel, avevo il mio piccolo letto in una stanza molto carina e pulita. La mattina mi hanno portato la colazione, buona come quella che ti danno in aereo, ed il tutto era semplicemente fantastico ! Certo, il mio spirito è sempre stato positivo e quindi prendo gli avvenimenti in tal senso, ma ho dormito veramente bene durante il mio soggiorno nelle patrie galere svedesi J"

Il giorno successivo portano il nostro amico alla corte di Katrineholm, la quale decide di non prose-

guire con lo stato di detenzione in carcere: Otto riceve un "travel ban", il che significa la requisizione del passaporto e l'obbligo di presentarsi ogni sera alla stazione di polizia di Flen (bisogna dire anche che i poliziotti locali non vedevano di buon occhio Otto già da molto tempo, essendo il solo giovane del paese a non uscire mai e stare sempre chiuso nel suo ufficio. . .) sino all'inizio del processo.

6 "Pericoloso Terrorista Internazionale"

Ciò che diede origine alla catena di eventi culminata con il tracciamento di Otto da parte della Televerket fu lo scanning del PAD Datapak. Quando Pege realizzò che qualcuno stava scannando il PAD per trovare NUI di accesso alla rete la sua prima reazione rasentò lo shock puro: il glaciale svedese tornò con la memoria a due anni prima, quando i fratelli Pad e Gandalf degli 8LGM – due hacker perfettamente normali ed estremamente curiosi – effettuarono il loro raid informatico. Nel 1990 quegli attacchi furono immediatamente scambiati per attacchi da parte di gruppi tettoristici stranieri e, probabilmente, nel 1992 il nostro Pege continuava a pensarla così , non avendo mai avuto l'occasione di conoscere di persona i due simpatici inglesi che tanti problemi hanno anche dato, nel corso della loro carriera, alle agen-

zie governative statunitensi ma che mai hanno avuto a che fare con organizzazioni terroristiche di alcun tipo.

Come tutti i "security official" in Svezia, Pege Gustafsson aveva letto il libro "The Cuckoo's Egg" di Clifford Stoll. Nel libro Stoll descrive come lui, utilizzando molta immaginazione e notti senza fine di lavoro non pagato, riesce a tracciare un hacker entrato nel suo sistema a Berkeley, il quale stava iniziando a cercare segreti militari attraverso la parte americana della rete Internet. L'hacker che svolgeva questa missione era del KGB e riceveva istruzioni da hacker come Pengo e Hagbard, fricchettoni cocainomani che operavano da Berlino Est.

Immedesimiamoci dunque nella mentalità di Pege, nella sua probabile volontà recondita di fare come Stoll ed avere a che fare con un'organizzazione internazionale di spie informatiche che congiurano contro la sicurezza della Svezia. . . il risultato è che, non appena Otto inizia a scannare la rete svedese, Pege accende le sirene di allarme. Gli eventi vengono probabilmente associati con altri avvenimenti simili precedentemente accaduti e l'idea che la Televerket se ne fa, grazie alla profonda conoscenza del mondo hacker di Gustafsson, non è quella di "una somma di piccole scorribande hacker con l'utilizzo di semplici scanner", bensì di "un sistematico piano di attacco e tentativi di intrusione generato da qualche potenza straniera". Pura e semplice paranoia, direi

io. E voi ?

Come se non bastasse (si sa, i casini si creano da soli ma hanno poi una capacità incredibile di espandersi e collegarsi esponenzialmente: Mr. Murphy e le sue leggi insegnano a tal proposito) dopo aver chiuso il cerchio attorno al "terrorista" Otto Sync in quel di Flen ci furono una serie di "conferme" ai forti sospetti di "congiura internazionale" avanzati da Pege: Otto fece diverse chiamate in Tailandia, le quali furono interpretate come comunicazioni con i fantomatici mandanti dell'operazione terroristica (nell'ottica di Gustafsson questi potevano essere chiunque, dal KGB all"IRA passando per il Mossad israeliano). In realtà le telefonate erano indirizzate ad un amico di vecchia data di Otto, al quale l'azienda aveva dato l'autorizzazione di effettuare chiamate in Tailandia in qualunque momento. Ogni hacker conosce giocoforza una serie di persone sparse per il pianeta, in quanto il "villaggio globale" è la loro casa naturale. Io stesso entrai in contatto con Otto Sync, Sentinel ed altri amici tra la fine degli anni '80 e l'inizio del '90 e, da allora, passo spesso ore al telefono – oltre che naturalmente on-line – con loro, anche se i miei interlocutori sono comunque disseminati tra Asia, Stati Uniti e Canada.

Così , quando la polizia e la Televerket fanno irruzione nell'ufficio di Otto Sync il 2 dicembre 1992 ciò che si aspettano di trovare è un pericoloso terrorista internazionale: quello che si trovano davan-

ti è invece un ingegnere venticinquenne socialmente disadattato, isolato dalla "vita sociale" di Flen ed alquanto annoiato, il quale si diverte esplorando la rete Datapak, non avendo nulla di meglio da fare.

Otto mantiene la sua innata e spiccata ilarità e senso dell'humour, descrivendo come "il mio amico Pege pensava di essere il buono che dava la caccia al cattivo. Mi disse di essere un fan di Clifford Stoll e che lo aveva addirittura incontrato in qualche security conference anni prima". Durante l'interrogatorio Pege disegnò delle mappe per illustrare i paesi ai quali l'hacker aveva accesso tramite connessioni X.25, mappe che sembravano, a detta di Otto, "schemi presi dal vostro manuale di terrorismo internazionale tascabile.

Sebbene questo comportamento da parte della polizia e delle squadre speciali informatiche possa sembrare strano, paranoico e circostanziato al caso specifico della Televerket, non dobbiamo dimenticarci del fatto che, negli arresti avvenuti in Europa tra il 1990 ed il 1995 per quello che viene definito hacking "elitario", tutte le persone arrestate, me incluso, furono inizialmente accusate di "terrorismo" dalle forze di polizia ed Interpol dei rispettivi paesi.

Per fare poi comprendere sino in fondo l'assurdità dei fatti è importante sottolineare come, proseguendo nelle indagini di polizia, l'accusa di terrorismo nei confronti di Otto andò sì a cadere ma, nonostante ciò, i sospetti su Otto rimasero a lungo anche dopo

la sua partenza dalla Svezia. Quando nell'autunno del 1993 furono rubati da un deposito militare i programmi informatici che controllavano e gestivano le liste di partenza, le misurazioni dei tempi ed i risultati finali per i Giochi Olimpici di Lillehammer del 1994, la polizia norvegese, per qualche motivo, credette in un'implicazione di Otto.

Il Quotidiano l'Expressen[10] lo definì "il leader hacker" e colse l'occasione per indirizzare i sospetti verso Otto e verso l'azienda per la quale aveva lavorato a Flen[11]. Tra le righe lasciarono inoltre trasparire come quella fosse la modalità utilizzata dai militari francesi per inviare spie in Svezia, usando quindi la filiale svedese come una copertura (!). "Personalmente", mi dice Otto, "in quel periodo ero in Tailandia e mi trovavo senza una lira e senza computer: la Tailandia è comunque molto distante da Lillehammer. . . ".

Grazie ad Otto si scomodò persino la SÄPO[12] la quale, attraverso il direttore generale Jörgen Almblad, rassicurò i cittadini e l'opinione pubblica svedese, sottolineando come i volontari del servizio civile operanti in Svezia – e Otto Sync in particolar modo – non rappresentavano un pericolo sul fronte della sicurezza dello Stato.

Persino il nostro amico Pege alla fine realizzò che

[10]Una delle più diffuse edizioni serali svedesi

[11]Expressen , venerdì 4 febbraio 1994, pagina 11

[12]Swedish counter-espionage

Otto non era quello che lui credeva. Privatamente Pege ammise ad Otto che se avesse saputo prima come stavano le cose molto probabilmente non avrebbe proseguito nelll'indagine o, almeno, non in quel modo e sino a quel punto e quei livelli di assurdità. "Disse persino che gli sarebbe piaciuto farsi una birra con me, quando il tutto fosse giunto alla fine". Oggi come oggi Otto nutre molti dubbi circa la competenza di Pege nella security: "Mi ricordo che mi raccontò del suo interesse nei 'security concerts', ed ancora oggi mi chiedo se fossero concerti rock. . . Nonostante lui fosse il responsabile security alla Televerket, non ne sapeva abbastanza di Unix Security e tecniche di hacking. In effetti risultava essere abbastanza ignorante persino su argomenti di base quali il reverse-charge su Datapak. Ed era il suo lavoro !"

7 "When the game gets tought, the toughts get playing". . . (l'Angelo e il Diavolo)

Alla fine il nostro Pege capisce e abbandona piano piano l'idea di difendere la Svezia dai terrorismi immaginari. Il 18 dicembre il Cavaliere Bianco della Televerket riesce nel suo intento di trasportare il Drago Francese in una corte svedese con l'aiuto del procuratore distrettuale Christer Pettersson.

Il processo è di per sé una farsa, la quale presto scopre le sue pecche: tra tutte le personi presenti, solo Pege e Otto hanno le conoscenze tecniche necessarie per comprendere le accuse della Televerket. Come diretta conseguenza a questa constatazione, la prima cosa che l'avvocato di Otto fa è sbattere fuori dall'aula Pege Gustafsson, dato che non vi è alcun motivo per giustificare la sua presenza. L'unica volta in cui Pege è ammesso all'aula è durante il controllo incrociato delle accuse richiesto dalla corte e dalla giuria.

Otto Sync rimane dunque il solo in grado di capire le accuse che gli sono mosse.

Otto a questo punto si illumina e mi spiega come "il processo fu veramente divertente, dato che nessuno dei presenti aveva la benchè minima idea dell'oggetto delle accuse. Alcuni dei documenti che produssi durante il processo era un pochino "a doppio senso", come un'e-mail di un tizio il quale mi spiegava come utilizzare il reverse-charge su Datapak. Portai anche una lista valida di tutte le BBS svedesi, spiegando al giudice che le stesse erano computer ad accesso libero. Naturalmente nessuno colse la profonda differenza esistente tra una BBS che gira su un 386SX nella stanza di un teeneger diassettenne e un data network X.25 mondiale. . . "

Otto Sync non si ritiene colpevole di nessun crimine ed è abbastanza sveglio da utilizzare semplici descrizioni affinchè la giuria possa comprendere i

fatti. Non nega assolutamente di avere utilizzato la rete Datapak esattamente come la Televerket accusa ed è pronto a pagare per quello che ha fatto. Ma crede anche di non essere responsabile dei costi che la Televerket ha dovuto supportare per identificarlo e non pensa che sia ragionevole una sua condanna al pagamento delle spese tecniche e di investigazione.

Pege viene chiamato solamente per descrivere come è avvenuto il tracing (il tracciamento e la localizzazione) di Otto: per tutto il resto dei dati il materiale di riferimento imposto alla giuria è rappresentato dal "preliminary investigation protocol", un'orribile pila di carta contenente per la maggior parte descrizioni tecniche e diversi log dei tracing portati avanti da Pege stesso. Tra le "prove" contro Otto troviamo invece i suoi stessi appunti, alcuni dei quali completamente incomprensibili ad Otto stesso: è bene spiegare che quando un hacker quando prende appunti lo fa in condizioni "off-limits", scrivendo in genere malissimo a mano già di suo e comunque dovendolo fare di fretta in quanto si deve proseguire nelle proprie opere di hacking e, in fondo in fondo, senza un enorme interesse verso il sistema appena violato ed i dati da trascrivere, in quanto si è già in procinto di sfondare il successivo. Ad ogni modo gli appunti sequestrati riportavano dettagliate informazioni tecniche su numeri telefonici e linee di accesso a differenti sistemi informatici sparsi per il mondo; per la giuria null'altro se non un lungo

elenco di numeri e parole incomprensibili.

Senza ulteriori informazioni sulla tipologia delle informazioni riportate, queste criptiche annotazioni vengono chiamate "hacker notes" dalla corte, unitamente ad un accrocchio di print-out di file trovati nell'hard disk di Otto.

Questo materiale viene inserito dall'accusa nella sezione prove con il chiaro intento di fare apparire Otto come una "parte oscura", una figura non ben definita e quindi altamente pericolosa, appartenente ad una certa subcultura "deviata".

8 And the Winner is. . .

L'effetto finale sulla corte è invece quello di dare una serie di impressioni:

- come primo punto, il risultato apparente è che la Televerket non è in grado di presentare e illustrare accuse attendibili e perseguibili ai fini del processo;
- in seconda istanza la giuria è tremendamente annoiata dalle spiegazioni di Pete Gustafsson, mentree viene trasportata dalle capacità illustrative di Otto (naturalmente utilizzate dallo stesso a proprio favore);
- come diretta conseguenza la sola certezza nella mente della giuria riguarda l'assoluta traspa-

renza ed innocenza di Otto (indipendentemente dal pensare o meno se Otto abbia effettivamente mentito sull'argomento), il quale espone chiaramente la sua posizione e insiste nello spiegare come reputasse quelle chiamate gratuite e completamente legali.

Data l'impossibilità del pubblico ministero a provare il contrario, la giuria esprime un giudizio di non colpevolezza. La Televerket, dal canto suo, tenta di richiedere i danni e richiede l'espulsione di Otto dalla Svezia: ambedue le richieste vengono respinte e la Televerket viene condannata ad assumersi i propri costi processuali e di indagine.

Telecom 0, Hacker 1.

Televerket perde, Otto Sync vince.

La sentenza fu emessa il 18 dicembre del 1992, ma non fu resa pubblica sino all'8 gennaio del 1993.

Ripensando a quanto accaduto Otto dice "sebbene fossi colpevole come un diavolo, ne uscii come un angelo e la Televerket perse il caso. Questo è quanto. Io proseguo per la mia strada".

La Televerket, oggi Telia, richiede un appello alla sentenza il 15 gennaio. Dato che Otto sarebbe stato fisicamente presente in Svezia solo sino al primo di aprile, viene richiesto alla corte di rivedere il caso prima di quella data (richiesta ovviamente priva di speranza).

Nel settembre del 1993 Otto è nuovamente in Francia e, altrettanto naturalmente, continua a fa-

re hacking. Una notte White Knight entra su QSD: "iniziai a chattare con Pege, il quale mi attendeva in aula ad ottobre. Non fu troppo felice di vedermi di nuovo su QSD, dato che quasi certamente stavo chiamando da un sistema bucato. Molto probabilmente non sarebbero stati in grado di richiedere l'estradizione in Svezia e, ad ogni modo, avevo già un biglietto aereo prenotato per Bangkok per il 4 ottobre". La Corte d'Appello riesamina il caso il 25 di ottobre. Siccome la Televerket non ha fornito nulla di nuovo all'evidenza delle prova e data la non reperibilità di Otto, la Corte d'Appello svedese decide di considerare il caso chiuso.

La Televerket e Pege perdono nuovamente.

Otto Sync ha lasciato nel 1994 il suo lavoro di ingegnere software presso una grande multinazionale operante nel mercato della telefonia cellulare, a Bangkok. Attualmente è amministratore delegato e fondatore della più importante azienda asiatica in campo I.T. Security; Pete Gustafsson continua ad occuparsi di sicurezza alla Telia, Sweden National Telecom Company. . .

Questa è la storia di Otto Sync e Pege Gustafsoon e di come un hacker solitario abbia vinto contro una serie di realtà molto più grandi di lui.

Credo che questi fatti possano essere una lezione di vita su più fronti: lascio ai lettori il giudizio finale. Da parte mia ho solo la felicità di avere ritrovato un vecchio amico, la gratitudine per aver ascoltato una

storia bellissima e l’autorizzazione a raccontarla al pubblico italiano. Grazie Otto, “c u l8r” ;) . . .