Autore: Raoul Chiesa - *Gennaio 2000*

Il "criptocriminale" 60enne spaventa la N.S.A.

Risulterebbe colpevole di crimini federali punibili con svariati anni di prigione, il Sig. John Young, sessantatreenne fondatore del sito http://jya.com Vediamo di capirne i motivi.

John Young: who is who

John Young è un architetto della Big Apple, quella Grande Mela che molti vorrebbero mordere ed assaporare completamente e che corrisponde al nome di New York City.
Laureato alla Columbia University, Mr. Young è divenuto uno degli architetti più rispettati degli Stati Uniti, dopo aver "creato" negli anni per la sua città delle opere bellissime ed in molti casi uniche quali il Rockefeller Apartment, il Pierre Hotel e la Whittier Hall della Columbia University.

Negli ultimi 3 anni, però, il nostro amico John ha deciso di creare qualcos'altro: ha messo insieme la più grande collezione privata (ma resa pubblica attraverso la sezione ***Cryptome*** del suo Web Site) di documenti riguardanti privacy e tecnologia, spesso collegati alla crittografia, cifratura e libertà di parola.

Più di 4.000 documenti ? riservati o meno ? presenti sul suo sito, nell'apposita sezione: le altre sezioni riguardano esperimenti architettonici sul Web, oppure il mini sito della Natsios Young Architects, oppure ancora il DMZ Forum, per il quale (lo vedremo più avanti) l'Intelligence Koreana (i servizi segreti del governo koreano) visita regolarmente il sito di "zio John".

L'atto che dunque fa spuntare un sorriso da contrabbandiere anni '30 al Signor Young è il rintracciare, il raccogliere, il sottrarre documenti di tipo riservato e governativo pubblicarli on-line: un po' quello che fece il buon Creig con la documentazione 5-ESS dell'At&t, pubblicata su Phrack Magazine anni fa e che scatenò il finimondo oltre che una serie di arresti e perquisizioni degne del periodo della caccia alle streghe nella quale gli americani ? in questi ultimi anni ? si sono distinti, arrivando a superare la polizia italiana che sequestrava tappetini di mouse e monitor (!) .

The Sun Devil Operation: un triste predecessore

Credo sia importante spendere qualche parola e ricordare cosa successe a Craig, per arrivare a capire cos'è che spaventa il governo USA e spiegare quello che sta accadendo al buon John Young: nel 1990 avvenne il primo "raid" contro gli hackers e l'operazione fu chiamata Sun Devil (vedasi Hacker's Crackdown, Giro di vite contro gli hackers, di Bruce Sterling).all'operazione seguì il processo a Knight Lightning, ovverosia Creig Neidorf, accusato di aver sottratto (via rete, mediante hacking) il documento 5ESS, il quale spiegava il funzionamento delle nuove centrali telefoniche dell'At&t: in realtà questo file veniva inviato a casa dalla società stessa a chiunque lo avesse richiesto, alla modica cifra di 5 US $..! Arriviamo allora alla paura di chi si appropria direttamente di determinate e specifiche conoscenze?

Pare proprio che la risposta sia sì, vedendo cosa succede allo zio John da un po' di tempo: la sezione CRYPTOME del suo sito (http://jya.com/crypto.htm) contiene informazioni utilissime (al tecnico, all'hacker, all'agente governativo, al comune cittadino, al navigatore occasionale che vuole salvaguardare i suoi diritti o imparare meglio il funzionamento di alcuni strumenti di utilizzo comune, quale ad esempio i cellulari GSM) su argomentazioni quali Echelon, lo standard cellulare GSM e le insicurezze insite dello stesso, l'MI-6 (i servizi segreti inglesi), le regole di esportazione americana sui software di crittografia avanzata, il PGP in versione completa con la crittografia avanzata a 128 bit, e così via...un sito simpatico, insomma, diverso, radicale così come il suo fondatore.

The Cryptome Web Site

Ora, quello che è successo nasce proprio dalla possibilità di scaricare dal sito la copia della versione di PGP (Pretty Good Privacy, software per la criptazione dei dati) nella versione per la quale il Governo USA ha vietato l'esportazione nei paesi non americani: non sono state poche le preoccupazioni manifestate da zio John e da altre persone (spesso eminenti esponenti del mondo dell'I.T.) nei confronti del famigerato "clipper-chip", un processore voluto dai servizi segreti statunitensi il quale permetterebbe di decifrare molti degli algoritmi sui quali si basano i programmi di privacy e cifratura dei dati (non dimentichiamoci che il DES fu scelto ***e sviluppato*** insieme alla N.S.A.).
Il poter reperire la versione vietata del PGP ha fatto sì che jya.com divenisse un sito con moltissimi accessi e ? di conseguenza ? moltissimi downloaded ha fatto sì che la N.S.A. si interessasse al buon zio John.

Spiega Young: quando una Commissione Federale pubblicò nel 1996 una copia importante (ma solo in versione cartacea e non digitale) del "CRISIS Report" il quale raccomandava una certa attenzione nei confronti delle tecniche e dei prodotti di crittografia, decisi che la comunità Internet doveva venirne a conoscenza, era un diritto comune il poter apprendere queste decisioni, le quali riguardano direttamente la comunità. Quello che feci fu semplicemente il notare che qui in studio (di architettura, N.d.R.) avevamo un bell'equipaggiamento a livello di scanner, dato che li utilizzavamo per i nostri lavori grafici Presi il CRISIS Report, lo passai a scanner e lo misi in rete: quella fu la prima volta che lo facemmo ed ottenni ottime risposte da parte della comunità in Rete.

I visitatori "inusuali" del sito

Alcuni visitatori del sito di John si possono quantomeno definire "particolari, curiosi ed inusuali": la National Security Agency americana ? la quale è poi il soggetto principale di una sezione speciale all'interno del vasto archivio del web site di Young ? pare spedire un "robot" alle 7 di mattina, in ogni giorno della settimana, il quale scarica gli ultimi file. Lo zio John, con la sua innata simpatia ed ironia, commenta spiegando che "non ho ancora capito se e' un bot o una persona fisica, ma arriva ogni mattina, pieno di voglia di fare e speranza di trovare nuovi documenti, e prnede due copie di ogni file. Se non è un robotdi certo si comporta come tale !"

Che siano persone fisiche o programmi appositamente creati, i visitatori provenienti da agenzie di spionaggio sono una regolare fonte di divertimento per Young: i suoi log di sistema mostrano come questi "lettori della prima ora" visitino anche le altre sezioni di jya.com, come quelle di architettura: "alcuni dei tizi alla NSA visitano le sezioni 'normali' e capiscono che tipo di persona è John Young; in seguito non ritornano più in quell'area, ma vanno direttamente all'area crypto".

La settimana scorsa, però, John si è un po' preoccupato (e forse anche un minimo spaventato) quando ha notato un robot lanciato dall'agenzia informativa del governo koreano (Korean Information Security Agency, KISA): in un messaggio postato nel cypherpunks mailing list, Young ha detto che la KISA ha configurato un paio di robot per produrre un consistente flusso di richieste per gli stessi tre file, uno ogni secondo, arrivando quasi a bloccare i servizi del suo sito web.

Parrebbe dunque che un'Agency abbia fatto un DoS (Denial of Service) ad un hackerse fossi un giornalista di professione, questa notizia avrebbe lo stesso valore della classica "uomo morde cane in pieno centro" !

Un system administrator della KISA spiega in un'e-mail a John: "[]in questo caso, questo robot pare abbia un problema: è un processo che è entrato in modalità loop-back (ripete quindi senza fine, in loop appunto, le istruzioni, N.d.R.): mi lasci provare ad risolvere il problema, ma potrebbero volerci un po' di giorni, in quanto i manager del Twister Server sono assenti da oggi per i prossimi tre giorni, essendo appena iniziato il giorno del Ringraziamento koreano".

Conclusioni

Che la N.S.A. non abbia mai amato la diffusione di materiale tecnico, così come non ami la diffusione della cultura ***underground*** informatica e telematica, è cosa risaputa; che controlli sistematicamente ogni tipo di comunicazione terrestre ed aerea, telefonica od informatica, non è anch'essa una news: che arrivi a controllare la diffusione di ciò che lei stessa scrive, e che come la N.S.a. si comportino le maggiori Intelligence mondiali.credo debba far riflettere.

Si parla tanto di sicurezza su Internet e di hacking.ricordo ai lettori che se i cult of the Dead cow non avessero inventato il Back Orifice lo scorso anno, il mondo sarebbe ancora pieno di persone che ritengono i sistemi Microsoft Windows sicuri.che dire allora, se non "forza zio John ! " ?

Si ringrazia:
Wired News
Declan McCullagh
Manù