IL CASO

TEEN AGER IMPIGLIATI NELLA RETE, ECCO LE NUOVE DIPENDENZE

EURO 1,90

ISSN 2037-2949

Settimanale di Informazione

il Punto ntc

ANNO II N. 26 **01 LUGLIO 2010**

www.ilpuntontc.it

LE FALLE DELLA RETE TELEFONICA

Le nuove rivelazioni dell'ex capo del Tiger Team di **Telecom Fabio Ghioni:** «In Europa un criminale non può acquistare la **bomba atomica,** ma può comprarsi l'azienda che la produce. Con **l'arbitrato** telefonico si possono esportare capitali senza lasciare traccia. Le **intercettazioni?** Stilai un report sul rischio di accessi non autorizzati»

NESSUNO E' AL SICURO

IL COLLOQUIO

Fabio Ghioni: «In Europa un criminale non può acquistare la bomba atomica, però può sempre comprarsi l'azienda che la produce, perché nel libero mercato nessuno glielo può impedire. Con la telefonia si possono esportare illecitamente, ovunque nel mondo, quantità enormi di danari»

Riciclaggio e tecnologi

Le ultime rivelazioni del capo del Tiger Team di Telecom. Che ha appena chiuso un accordo con il colosso informatico Dell

FABRIZIO COLARIETI

In Europa un criminale non può acquistare la bomba atomica, però può sempre comprarsi l'azienda che la produce, perché nel libero mercato nessuno glielo può impedire». A parlare è Fabio Ghioni, l'hacker più famoso d'Italia, reo di aver "bucato" decine di server, compresi quelli della statunitense Kroll e del *Corriere della Sera*, per nome e per conto di Marco Tronchetti Provera assicura lui, quando era a capo della sicurezza informatica del gruppo Telecom Italia. Lui, *Divine Shadow*, ombra divina, ormai fa informazione da sé - online, in decine di conferenze, con i suoi libri - e quando incontra un giornalista parla solo se le domande sono "sensate". Da dire ci sarebbe molto, ma ormai Ghioni campa d'altro e Telecom lo considera solo un inciampo: una macchia nera nel suo lunghissimo curriculum che da quell'incidente in poi non ha fatto altro che allungarsi. Vola da una parte all'altra del globo, scrive dalla sua *Hacker Republic* e basta digitare il suo nome su *Google* per entrare nel suo mondo "binario". Ora che è libero di parlare, che ha saldato il conto con la giustizia, patteggiando a 3 anni e 4 mesi la condanna per lo scandalo Telecom-Pirelli, ha cominciato a togliersi anche qualche sassolino dalle scarpe. Parla due ore con *Il Punto*, in un afoso pomeriggio romano, il giorno dopo la diffusione delle motivazioni della sentenza del gup milanese Mariolina Panasiti, che riguarda lui e altri 15 imputati, come il suo capo, Giuliano Tavaroli (4 anni e 2 mesi), ma anche Telecom e Pirelli (sanzionate per 7 milioni di euro). «Che Ghioni facesse tutto questo di sua iniziativa - lo si è detto - è palesemente inverosimile; che Tavaroli gestisse pratiche di questo genere nel

;ie, il grande buco nero

suo singolare interesse è, parimenti, altamente improbabile». C'è poco da aggiungere, la Panasiti sposa le conclusioni del gip che aveva spedito in carcere Ghioni e i suoi colleghi, affermando pure che le «richieste di acquisizione di informazioni e di intrusione informatica erano attività strettamente pertinenti a scelte aziendali». Gli spioni di Telecom, il *Tiger Team* di Ghioni e tutto l'apparato di sicurezza insomma era al servizio di Tronchetti Provera e «a soddisfare ed a corrispondere a specifici interessi delle due società e del gruppo dirigente». Del resto, a chi poteva interessare spiare la bella Afef o i concorrenti di Pirelli? L'ascesa di Ghioni, dopo la bufera Telecom e otto mesi di carcere, non si è mai arrestata. Appena fuori Jennifer Lopez lo ingaggia per proteggere le sue ville, rimette in piedi la sua attività, fino a incassare l'ultimo incarico, due settimane fa, quando il colosso dell'informatica *Dell Italia* lo sceglie come partner per garantire la sicurezza dei propri utenti, con un accordo che renderà la navigazione e l'utilizzo dei suoi prodotti più sicuri e immuni da rischi di incidenti informatici. Le soluzioni che *Dell* adotterà sono ideate dalla *Eusystemic Initiative*, la società di Fabio Ghioni, specializzata nell'homeland security and defense e nelle tecnologie non convenzionali. Nel passato di Ghioni di "soluzioni" avveniristiche ce ne sono molte, in particolare quelle sfornate da un'altra sua fortunata iniziativa, la *Ikon Srl* di Garbagnate Milanese, e quando afferma che in Europa un criminale non può acquistare la bomba atomica, «però può comprarsi l'azienda che la produce», è proprio agli strumenti da lui ideati che si riferisce. Vere e proprie "bombe atomiche".

«Quando uno Stato commissiona a un'azienda un'arma segreta - ribadisce Ghioni a *Il Punto* -, la questione è talmente segreta da eludere i normali controlli sull'azienda stessa. Sembrano barzellette, ma tutto ciò è già accaduto e probabilmente accade tuttora. È successo quando Gennaro Mokbel ha acquisito la *Digint* e i potentissimi virus spia prodotti dalla mia società, *Ikon*, che fondai anche per soddisfare le richieste della Procura della Repubblica di Milano di cui ero consulente. Quell'azienda - spiega a *Il Punto* l'esperto informatico - passò di proprietà, finché non finì nelle mani di un delinquente». Mokbel. «Io non lo conosco, Mokbel, ho letto di lui - prosegue l'hacker - sui giornali quando è scoppiato lo scandalo Fastweb-Telecom Italia Sparkle e, ripeto, apprendere che software segreti per lo spionaggio elettronico, tuttora in uso a procure e servizi segreti, impiegati anche nelle indagini sulle Br e

Le nuove rivelazioni dell'hacker italiano al centro di due interrogazioni all'Ue

per individuare pedofili in rete, sarebbero finiti nelle mani di un personaggio che è stato definito addirittura vicino alla Banda della Magliana mi lascia molto perplesso». Secondo gli inquirenti la *Ikon Srl*, dopo essere stata ceduta alla *Digint Srl*, è finita, insieme a tutti i suoi virus, sotto il controllo del Gruppo Mokbel. «Quelle applicazioni che ho progettato sette anni fa, che secondo *Finmeccanica* al momento sono ancora la migliore tecnologia in circolazione, - va avanti Ghioni - *Ikon* le ha date in uso a enti governativi, perché era dotata di un nulla osta emesso dall'Autorità nazionale per la sicurezza, perciò, sia chiaro, quegli applicativi potrebbero essere coperti da segreto». Di due software Ghioni fa anche il nome: *IK webmail* e *IK spy*. Virus informatici, molto noti negli ambienti della sicurezza, che in teoria potrebbe impiegare solo l'autorità giudiziaria e le agenzie di intelligence, versioni molto evolute di "Cavalli di Troia" utilizzabili per spiare caselle di posta elettronica e pedinare computer in rete. Software "segugio", altamente all'avanguardia con tutto che la loro progettazione risale a quasi dieci anni fa. Nelle mani di chiunque sono capaci di annidarsi nei sistemi operativi e "sniffare" dati e nessun antivirus in commercio è in grado di stanarli. Qualcuno nei mesi

IL CASO/ Distributore fonia dati

Dove c'è chi intercetta, c'è sempre un Dfd a fare il suo lavoro Ghioni: «Stilai un report sul rischio di accessi non autorizzati»

Dfd è un acronimo, che di per sé non dice nulla. Nell'ambiente giudiziario, invece, in particolare nelle security delle compagnie telefoniche, queste tre lettere sono assai note. È un apparecchio elettronico, che assomiglia a un server, acronimo di "Distributore fonia dati". Dove c'è qualcuno che intercetta c'è sempre un Dfd a fare il suo lavoro. È il sistema che permette - tuttora - di trasferire le telefonate "bersaglio" di intercettazione da parte dell'autorità giudiziaria dalle centrali telefoniche alle procure. Dopo il Dfd, a cascata, ci sono i registratori, cioè le apparecchiature installate nelle sale di ascolto dei tribunali. I Dfd sono prodotti dalla Urmet di Torino. La descrizione del loro funzionamento è in rete: «Costituisce la soluzione necessaria e sufficiente a trasferire al punto di ascolto di una intercettazione, oltre alla fonia, i dati di tracciamento che consistono essenzialmente nell'identificazione del numero telefonico chiamato, di quello chiamante oltre ad altri dati accessori». In sostanza quando la centrale rileva una chiamata, da e per il telefono "monitorato", il Dfd la spedisce alla procura interessata. Tra le carte dell'inchiesta Telecom-Pirelli si parla molto dei distributori Urmet.

A maggio 2007 è proprio Fabio Ghioni, infatti, a riferire ai pm milanesi che indagano sulla security Telecom alcune "debolezze" di quel sistema: «E' vero - afferma l'ex capo della sicurezza informatica di Telecom Italia - ho stilato un report relativo al funzionamento dei Dfd e al pericolo che qualcuno dall'esterno potesse accedervi e copiare la lista delle utenze intercettate. Infatti la Urmet aveva un contratto di teleassistenza e bastava digitare la username "urmet" e la password "urmet" e accedere a ogni singolo Dfd con l'espediente di fare manutenzione. La cosa dette molto fastidio a Bruno Pellero che lavorava per Urmet». I distributori fonia dati - secondo quanto è in grado di ricostruire

scorsi ha dato retta alle parole di Ghioni, come il parlamentare europeo del Ppe, vicepresidente della Commissione per il commercio internazionale, Cristiana Muscardini, che sulle sorti della *Ikon* e nel suo delicato know-how ha presentato un'interrogazione. «Negli Stati membri - scrive la parlamentare - esistono aziende che sono proprietarie di tecnologie critiche per la sicurezza dello Stato. Si presume che la proprietà pubblica di queste aziende sia una garanzia per l'utilizzo corretto, controllato e lecito di tali tecnologie, che in mani sbagliate potrebbero diventare pericolose. Per le ragioni più diverse può succedere che queste imprese vengano acquistate da soggetti giuridici che sono un paravento di organizzazioni criminali o addirittura terroristiche». La Muscardini chiede alla Commissione se esiste un controllo, e da parte di chi, sul passaggio di proprietà di queste imprese "sensibili". «In caso negativo, non ritiene opportuno - prosegue l'interrogazione - proporre una regolamentazione comune che vincoli il passaggio di proprietà a controlli appropriati sulla natura e qualità delle eventuali imprese acquirenti, e in particolare sulla "buona condotta" dei suoi azionisti? Possiede (la Commissione, *ndr*) un elenco delle imprese europee che detengono tecnologie sensibili di sicurezza?». La risposta è del 20 maggio scorso ed è firmata dal Commissario europeo agli Affari interni, Anna Cecilia Malmström: «Per quanto riguarda il commercio di prodotti o tecnologie sensibili con acquirenti di Paesi terzi, a livello sia nazionale che di Unione europea, esiste una legislazione piuttosto dettagliata sul controllo dell'esportazione di tali prodotti a doppio uso. Per quanto concerne i controlli sui trasferimenti di proprietà di imprese, non esiste attualmente un quadro legislativo o una prassi sistematica per tali misure in tutti gli Stati membri. Non si dispone - afferma ancora il Commissario - di un elenco sistematico delle imprese europee che detengono rilevanti tecnologie in materia di sicurezza».

«Quando Mokbel ha acquisito la Ikon ha acquisito anche i virus spia prodotti dalla mia società»

Sempre la vicenda Fastweb-Telecom Sparkle ispira un altro tema di discussione su cui Ghioni pare abbia molto da dire. «Lo sa - afferma ancora l'hacker a *Il Punto* - che volendo con la telefonia si possono esportare illecitamente, ovunque nel mondo, quantità enormi di da-

Il Punto - sarebbero ancora in uso presso tutti i gestori telefonici, sia mobili che fissi, e non è noto se quelle falle siano state o meno tappate. È certo che un consulente della procura, incaricato nel 2007 di verificare il grado di sicurezza dei Dfd, concluse che quei sistemi «necessitavano e necessitano tuttora di una idonea strategia di protezione degli accessi alle funzioni operative e di tutela dei dati sensibili che non può limitarsi alla mera osservazione del traffico ma deve primariamente porsi l'obiettivo di renderlo inaccessibile».

Da quella falla scoperta da Ghioni, va da sé, potrebbe essere uscito di tutto: informazioni su chi era sotto controllo, ma anche gli audio delle conversazioni telefoniche. Sarà un caso ma una società del gruppo Urmet, la Rcs Spa di Milano, è finita al centro di un'indagine che ha portato lo scorso 25 maggio all'arresto, per estorsione, di uno dei suoi soci, Fabrizio Favata. L'imprenditore ha raccontato di aver consegnato nel 2005 a Silvio Berlusconi il file contenente l'audio della celebre telefonata intercettata tra Piero Fassino e Giovanni Consorte sulla scalata Unipol, quella in cui fu pronunciata la frase, «Abbiamo una banca?». Quel file fu sottratto prima ancora che fosse ascoltato dal pm che aveva disposto l'ascolto. Favata, secondo l'accusa, avrebbe chiesto e ottenuto denaro dal numero uno di Rcs, Roberto Raffaelli, con la minaccia di raccontare che quella telefonata era uscita dalle apparecchiature Urmet-Rcs. In passato i Dfd sono finiti al centro anche di un'indagine della procura di Roma sui costi delle intercettazioni. Da quell'inchiesta, archiviata nel 2005, emergeva innanzitutto che il ministero della Giustizia aveva istituito un gruppo di lavoro, al quale collaborò anche l'ingegner Pellero di Urmet, che si occupò di stilare il "listino" che doveva servire a calmierare i prezzi "omnicomprensivi" delle operazioni di ascolto. Ma entrò in quell'indagine anche la scelta di Telecom, Tim e Omnitel di dotarsi, a partire dal 2001, del sistema Dfd. Un'operazione che diventò ben presto un business milionario e a guadagnarci, quasi in regime di monopolio, fu la sola Urmet. Incuriosì molto gli inquirenti, poi, il fatto che i suoi Dfd erano dotati di un software che criptava il segnale in uscita e che obbligava le procure a noleggiare, a 26 euro al giorno per ogni singola intercettazione, un altro apparecchio Urmet, il risponditore Srf, l'unico in grado di decodificare quei dati, compresi gli sms. Un'operazione che tra il 2001 e il 2003 costò al ministero della Giustizia, prima che la Urmet concedesse le "chiavi" di decodifica agli operatori di telefonia, oltre 200 milioni di euro in più.

F.Col.

Attraverso il sistema dell'arbitrato telefonico è possibile esportare soldi senza lasciare tracce

nari? Mi riferisco agli arbitrati telefonici». Non se ne comprendono i suoi interessi, ma quello di Ghioni è certamente il parere di un attento analista che in passato ha avuto modo, da una postazione privilegiata, quella che lo vedeva ai vertice della sicurezza informatica di *Telecom*, di osservare quanto avveniva e quanto la magistratura ha fatto emergere negli ultimi anni. In sintesi al mondo ci sono molti metodi per trasferire danaro, leciti e illeciti. Oltre i canali bancari esiste un altro modo, poco conosciuto, che viaggia dentro i cavi telefonici e nell'etere, rimbalzando da una parte all'altra del mondo grazie ai satelliti. Danari digitali, sequenze di 1 e 0 che alla velocità della luce, attraversano l'Atlantico. All'origine sono soldi veri, poi diventano minuti, scatti di conversazione telefonica, attraverso un complicato meccanismo. Poi, una volta venduti, tornano a essere danari. Secondo gli inquirenti che indagano sulla maxi operazione di riciclaggio messa in piedi da Fastweb e Telecom Italia Sparkle proprio l'uso illecito dell'arbitrato telefonico avrebbe permesso di distrarre milioni di euro. Ghioni ne parla da settimane ed è ancora l'europarlamentare Muscardini a prendere spunto dalle sue parole per una seconda interrogazione: «Le compagnie telefoniche - scrive l'europarlamentare del Ppe - usano il cosiddetto sistema d'arbitrato per gestire la compensazione economica nel passaggio di minuti telefonici da un operatore all'altro. In altri termini, il sistema controlla la compravendita di minuti telefonici quando la comunicazione viaggia tra operatori diversi. Questa operazione mercantile viene definita appunto "arbitrato telefonico" e corrisponde a tutti gli effetti al passaggio di denaro da un operatore all'altro, operatori che possono trovarsi in nazioni diverse». Un sistema che si presta a un «probabile e possibile utilizzo fraudolento e illecito e potrebbe succedere che la criminalità organizzata, se non addirittura il terrorismo internazionale, ne approfittino per trasferire, e quindi riciclare, denaro sporco». Per una compagnia prestanome sarebbe un gioco da ragazzi acquistare minuti da una compagnia di un altro paese e trasferirli altrove. «La Commissione è al corrente di queste operazioni? È a conoscenza di fatti criminali avvenuti con questo sistema?», chiede la Muscardini nella sua seconda interrogazione al parlamento europeo: «Non ritiene opportuno presentare una proposta per l'istituzione di un controllo efficace del traffico telefonico gestito con il sistema dell'arbitrato tra operatori, al fine di impedire l'utilizzo fraudolento e criminale del sistema stesso?». Risponde, il 6 maggio scorso, ancora il Commissario svedese Malmström: «La Commissione è membro del gruppo di azione finanziaria contro il riciclaggio di proventi illeciti e contro il finanziamento del terrorismo (Gafi) ma non è a conoscenza di un uso del meccanismo delle tariffe di terminazione delle chiamate a fini criminali o fraudolenti. Ove dovessero essere constatati modalità operative del genere, si provvederà a esaminare le soluzioni del caso». A parlare con il linguaggio di Ghioni, la "falla" esiste ed è ancora aperta.

IL GIALLO/ Le sonde

L'ombra della Cia sul "punto stella"

Secondo lei a un Paese alleato e potente come gli Stati uniti d'America è possibile negare qualcosa? Abbiamo perso la guerra, non se lo dimentichi». Quel qualcosa, che Fabio Ghioni dice e non dice rispondendo alle nostre domande, è il "rumors" - mai smentito né confermato - che l'intelligence americana abbia da tempo piazzato delle "sonde" sui cavi telefonici in transito in Italia. La posizione strategica dello stivale è definita dagli esperti "punto stella". Passano infatti per il Belpaese tutti i cavi che permettono - su scala globale - le comunicazioni telefoniche e lo scambio di dati. A gestire il "punto stella" è proprio *Telecom Italia Sparkle*. L'azienda, controllata da *Telecom Italia*, gestisce la sua rete attraverso Seabone, il backbone in fibra ottica di 375mila chilometri che in tutto il mondo provvede a fornire il "routing" per la maggior parte del traffico generato da *Telecom Italia*. In rete è possibile rintracciare molta documentazione sul sistema di intercettazione globale *Echelon*, nato dall'accordo *Ukasa* sottoscritto nel '46 da Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda, e gestito dalla statunitense *National Security Agency*. Le comunicazioni che avvengono tramite cavi sottomarini possono essere intercettate, tanto e quanto quelle che viaggiano nell'etere, e questo è noto fin dal '71 quando un sottomarino americano riuscì a registrare le telefonate passanti attraverso un cavo militare russo. Nel 2004 la marina Usa e la *Nsa* hanno messo in servizio il sottomarino "J. Carter" che, a detta di Duncan Campbell, uno dei massimi esperti di *Echelon*, sarebbe in grado di spiare i cavi sottomarini di mezzo mondo. L'interesse dell'intelligence americana al traffico telefonico italiano, in particolare verso il Medio Oriente, è ben noto già dalla fine degli anni Novanta, come ha confermato a *Report* un vecchio direttore della compagnia telefonica: «I servizi segreti - ha affermato l'alto dirigente di cui non si conosce l'identità - volevano avere accesso al nodo di Palermo. C'erano dei collegamenti con l'America tant'è che io andai dal Presidente del Consiglio (Romano Prodi, ndr)». La Cia, perciò, voleva accedere al "nodo" siciliano, uno dei più importanti dell'Europa centrale, e non è chiaro se alla fine il governo gli lo ha permesso e in che termini. Un centro di ascolto statunitense, ormai abbandonato ma rimasto in funzione fino al '97, sempre *Report*, lo ha filmato (puntata del 16 maggio scorso) a pochi chilometri da Aviano.

F.Col.