Panorama
15 MARZO 2007 N.11

Basta una confezione di patatine e... SIAMO TUTTI

PIRATERIA INFORMATICA **Antenne ricavate da scatole di snack, valigette in grado di ascoltare le chiamate e leggere gli sms, software di facile reperibilità: sono gli strumenti dei nuovi intercettatori che possono rubarci, senza troppi sforzi, soldi, informazioni e perfino la nostra identità.**

di Pino Buongiorno

Se vedete qualcuno sotto casa vostra o davanti alla vostra azienda con una scatola di Pringles in mano, non pensate che sia solo un divoratore di patatine. Quel tubo in alluminio può essere modificato (costa 10 dollari e si compra su internet) e diventare una potente antenna direzionale in grado di captare i segnali delle vostre reti wi-fi aperte o solo parzialmente protette. Una volta che so-

perché

Non molti anni fa gli strumenti per intercettare telefonate ed email erano a disposizione dei soli servizi segreti. Oggi invece quasi tutti possono procurarseli. Detective, giovani hacker e semplici curiosi possono, con poca spesa, ascoltare i cellulari, penetrare nelle reti senza fili, rubare l'identità personale e i conti in banca. Da queste considerazioni è nata l'inchiesta di *Panorama* che svela per la prima volta tecniche, metodi e anche protagonisti del cybercrimine che rischia di mettere a repentaglio privacy e segreti industriali.

Panorama
15 MARZO 2007 N.11

INTERCETTATI

PETER BOWATER

Uffici di un'azienda. Se la rete informatica non è adeguatamente protetta, rischia di diventare un facile obiettivo per gli hacker.

no riusciti a entrare, questi hacker svuotano l'hard-disk, leggono la posta elettronica e i file più delicati, si impossessano delle credenziali per accedere ai conti bancari online. In pratica si trasformano in scippatori del bene più prezioso: l'identità personale. Con la quale possono commettere qualunque reato. Anche di pedofilia. Anche consegnare ad altri i segreti industriali dell'azienda in cui si lavora.

È l'ultima frontiera degli intercettatori illegali, quella che nel gergo telematico è nota come «wardriving», l'arte di penetrare nelle reti senza fili altrui con la certezza di non essere né visti né rintracciabili. Basta un computer portatile o un palmare, un software libero per catturare il traffico in internet, come il NetStumbler per Windows o il KisMac per Macintosh, e il magico barattolo di Pringles. Tutto qui. La rapina elettronica può cominciare.

E chi non volesse solo rubare soldi, ma anche informazioni riservate in tempo reale, segreti industriali o gossip di corna? Anche qui >

Un'antenna ricavata da un tubo di Pringles. Sotto, il colonnello Umberto Rapetto, che guida il Gat della Guardia di finanza. In basso, uno scorcio di Roma con le reti protette e quelle violabili più o meno facilmente.

> gli intercettatori dell'ultima generazione hanno trovato la lampada di Aladino: il Gsm interceptor, un'attrezzatura sofisticata composta da una stazione mobile basata su un computer, da un software di buon livello e da una o due antenne assai potenti e più professionali del tubo Pringles. Le dimensioni sono quelle di una valigetta ventiquattrore, da piazzare in un raggio di 500 metri dall'obiettivo. Ogni chiamata effettuata o ricevuta dal cellulare sotto osservazione, ogni sms, tutto viene captato e registrato dallo spione di turno.

È un mondo orwelliano che prevede il controllo assoluto della vita privata, di ciò che fai e pensi o solo sogni. Ma non è il futuro prossimo venturo. È la realtà di oggi. «L'infrazione della privacy non è più privilegio dello spionaggio professionale, ma intrattenimento reso disponibile a chiunque abbia tempo e qualche soldo da spendere» ammonisce il colonnello Umberto Rapetto, comandante del Gat, il nucleo speciale antifrodi telematiche della Guardia di finanza (30 agenti specializzati, che lavorano in un bunker alla periferia di Roma). La ragione è semplice. Se un tempo queste macchine per intercettare le conversazioni telefoniche, di produzione americana, australiana o israeliana, costavano anche 400 mila euro, oggi il prezzo è calato grazie alle clonazioni in Cina e in India: bastano 50 mila euro o anche meno.

Per una anomalia della legislazione italiana, che fatica a stare al passo con i tempi, importare i Gsm interceptor non è vietato. Quello che è proibito dalla legge è l'utilizzo. Ma chi acchiapperà mai questi 007 dell'etere, che possono nascondere l'attrezzatura in un'auto appostata fuori da un ristorante o dalla sede dell'azienda dove mangia o lavora la vittima prescelta?

«Non è così semplice intercettare i telefonini, ma sappiamo che oggi gli interceptor sono molto diffusi» afferma Pierpaolo Poli, il titolare della Speeka, società con sede a Milano nata nel 1991 per vendere apparati satellitari e successivamente specializzatasi nella commercializzazione di telefoni criptati e software antiintercettazione. «A noi si rivolgono banchieri, assicuratori, imprenditori, liberi professionisti e commercianti che vogliono proteggersi nel miglior modo possibile».

GRUPPO MOLTO SPECIALE

Il Nucleo speciale frodi telematiche della Guardia di finanza ha sede a Roma. Nato nel 2001 come Gruppo anticrimine tecnologico (Gat), ha assunto dal 2004 l'attuale denominazione. È composto da 31 uomini ed è guidato dal colonnello Umberto Rapetto.

Un tempo il Grande fratello era Echelon, la rete di spionaggio globale gestita dalla National security agency americana con la collaborazione di altri quattro servizi segreti di lingua inglese dell'Australia, della Nuova Zelanda, del Canada e della Gran Bretagna. Le cinque immense stazioni a terra e i 120 satelliti geostazionari del patto Uk-Usa hanno consentito e ancora in parte consentono alla Nsa e ai suoi alleati di catturare qualsiasi conversazione telefonica, qualsiasi email, qualsiasi telex o fax: si calcola il 95 per cento delle comunicazioni mondiali. Il limite unico è l'oceano di informazioni raccolte, difficilmente catalogabili nel tempo necessario per poterle utilizzare. Di qui l'uso di un dizionario chiamato Memex con le parole chiave dapprima di tipo economico-finanziario per lo spionaggio industriale e poi sempre più di carattere politico e terroristico: Bin Laden, Bush, kamikaze e via dicendo. Ma anche così, tanti i problemi di traduzione dalle varie lingue e dialetti, come ha rivelato tragicamente l'11 settembre. Solo sei mesi dopo è stata trascritta una telefonata fra due membri di Al Qaeda che, parlando in arabo, accennavano all'attacco alle Due torri di New York e al Pentagono.

Echelon è stata messa in pensione forzata mentre al suo posto, con la scusa della guerra al terrorismo globale, è nato il Super fratello, il Tia, Total information awareness, un progetto del Pentagono così segreto che nemmeno il Congresso americano riesce ad avere tutte le notizie che pure richiede in continuazione. Il Tia funziona con Babylon, un traduttore elettronico simultaneo, che migliora la qualità dei database della Nsa.

Bastano software facilmente reperibili in rete per bucare le reti di imprese o abitazioni, stando sulla strada di fronte.

Ma qui siamo nel campo dell'intelligence più elaborata, che l'Unione Europea ha cercato di imitare con l'Enfopol e la Russia con il Sorm2. Scendendo a terra dalle orbite siderali dei satelliti-spia, troviamo i piccoli fratelli, tutti quei sistemi per intercettare illegalmente le conversazioni. Sono più semplici, ma non meno penetranti. Il meno costoso si basa sulla corruzione di chi ha accesso ai tabulati conservati dalle quattro aziende telefoniche italiane (Telecom, Vodafone, Wind e Tre).

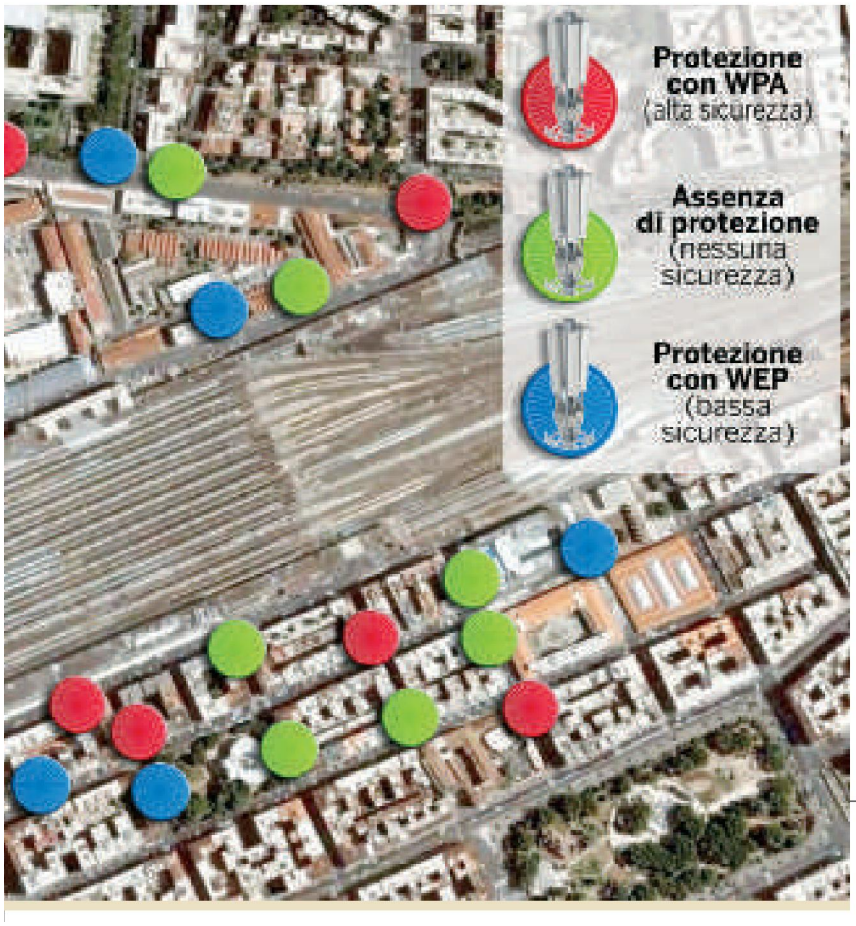
«Alcuni casi giudiziari recenti, sia nel Lazio sia in Toscana e in Lombardia« racconta Umberto Vulpiani, direttore del servizio di Polizia postale e delle comunicazioni, oltre 2 mila funzionari e agenti sparsi in tutta Italia, «ci hanno rivelato che con 100 dollari è possibile ottenere i tabulati da un impiegato che ha accesso al traffico dei cellulari». Lo scandalo Telecom con le attività di spionaggio e dossieraggio ordinate dall'ex capo della security Giuliano Tavaroli e il Laziogate, per il quale è stato rinviato a giudizio l'ex governatore Francesco Storace, sono due fra gli esempi più recenti che dimostrano quanto siano a rischio la privacy, la sicurezza aziendale e la legalità politica.

Un altro sistema, anche più banale, è quello dei cosiddetti cellulari spia. Sono telefonini comuni nei quali è introdotto un software in grado di trasmettere a distanza tutto ciò che si fa e si dice. Un cellulare di questo tipo, che costa poco meno di 1.000 euro, era stato regalato dall'immobiliarista Danilo Coppola a una sua «fidanzata», scrivono i magistrati romani nell'ordine di cattura, per spiarla 24 ore al giorno, soprattutto nel periodo delle feste di Natale e Capodanno.

Il salto di qualità avviene quando invece di andare a caccia dei tradimenti si mettono sotto controllo i capi di governo, gli imprenditori più noti, le stesse forze di polizia, la magistratura e perfino i giornalisti. Un recente caso venuto alla luce in Grecia la dice lunga su quello che potrebbe accadere anche in Italia (se non è già accaduto, senza essere scoperto). Nei primi mesi del 2005 alcuni utenti della Vodafone Grecia protestarono perché avevano notato una serie di disservizi sulla rete. Dalla casamadre in Gran Bretagna sbarcò ad Atene una squadra di esperti informatici che rintracciarono quasi subito un software maligno nel sistema centrale della Vodafone.

Questo software deviava le telefonate di 100 importanti personaggi greci verso 14 telefonini cellulari abilmente intercettati. In questo modo sono stati spiati abusivamente per un anno, a partire dal giugno 2004, immediatamente prima delle Olimpiadi di Atene, il primo ministro Costas Caramanlis, mezzo governo e diverse personalità. Nessun colpevole è stato individuato, anche se i quotidiani locali hanno messo sotto accusa non meglio identificati «agenti della Cia». La Vodafone Grecia è stata pesantemente multata.

Senza arrivare alle mirabilia greche ci sono apparecchi infernali in grado di carpire i colloqui di qualsiasi cellulare Gsm. Li gestiscono i cosiddetti «men in the middle», coloro che in pratica si interpongono abusivamente fra la stazione trasmittente dell'operatore telefonico e il cellulare che chiama o riceve. Si potrà obiettare: i telefoni mobili sono criptati. «Sì, ma diversi studi internazionali hanno dimostrato tutte le vulnerabilità degli algoritmi del Gsm» spiega l'ingegnere Pavel Ivanov, uno dei >



PAROLE PER CAPIRE

Man in the middle (Mitm). Chi spia i cellulari

Wi-fi. Reti locali senza fili

Wardriving. L'attività di chi va a caccia di

reti wi-fi non protette

Phishing. Pesca di dati finanziari

Pharming. Furto di carte di credito e conti bancari

Wpa. Crittazione sicura dei dati

> manager della Caspertech di Torino, che ha inventato e commercializza il primo criptofonino interamente made in Italy con una protezione di tipo militare.

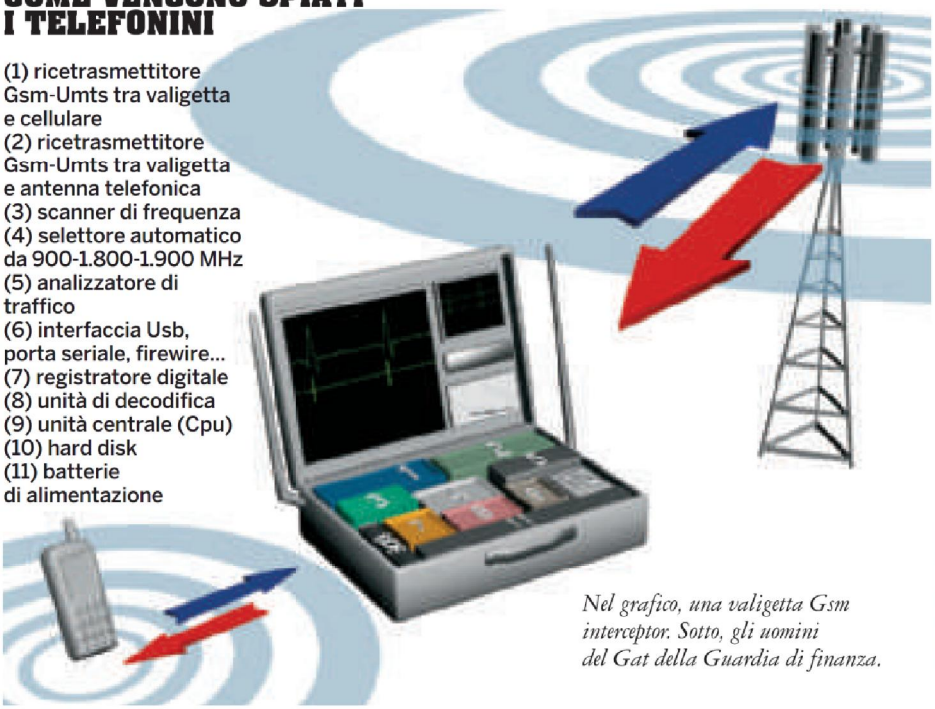
Chi sono i produttori di queste macchine? Roman Korolik che in Australia ha il brevetto per un software antiintercettazione, il SecureGsm, oggi in vendita in tutto il mondo e facilmente installabile su qualsiasi cellulare o palmare che funziona con il Windows Mobile versione 5 e 6, li elenca a *Panorama*: «Ufficialmente producono attrezzature vendute in esclusiva alla polizia. Le società più note sono Verint, Nice, Gss, Endoacustica, Shogi. A volte, per sfuggire alle indagini, creano delle sottounità con nomi più attraenti, come Cyclone in Messico. Fra queste aziende c'è anche la Italiaspy».

Questa piccola società di trading ha sede a Formia, in provincia di Latina, ed è specializzata nell'intelligence elettronica: microspie, bonifiche ambientali, microfoni direzionali. Nel suo catalogo spicca anche il Gsm interceptor. «Lo vendiamo esclusivamente alle forze dell'ordine» mette le mani avanti il direttore commerciale dell'Italiaspy Ettore Gasparini. Un cittadino qualsiasi può entrarne in possesso? «Certo, può andarlo ad acquistare direttamente in India, dove si produce. Sicuramente apparecchi come questi ce ne sono nel nostro Paese a disposizione dei privati».

L'ingegnere torinese Ivanov ricorda il recente caso, rivelato proprio da *Panorama*, che riguardava l'intercettazione telefonica di Marco Tronchetti Provera da parte della Kroll, multinazionale delle agenzie di investigazione. Lo strumento era proprio l'interceptor, magari del tipo più costoso e affidabile.

COME VENGONO SPIATI I TELEFONINI

(1) ricetrasmettitore Gsm-Umts tra valigetta e cellulare
(2) ricetrasmettitore Gsm-Umts tra valigetta e antenna telefonica
(3) scanner di frequenza
(4) selettore automatico da 900-1.800-1.900 MHz
(5) analizzatore di traffico
(6) interfaccia Usb, porta seriale, firewire...
(7) registratore digitale
(8) unità di decodifica
(9) unità centrale (Cpu)
(10) hard disk
(11) batterie di alimentazione



Nel grafico, una valigetta Gsm interceptor. Sotto, gli uomini del Gat della Guardia di finanza.

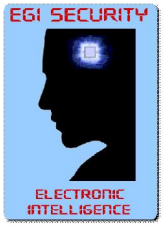
FRANCESCO DE GIORGI

Questi intercettatori sono catalogati sotto la specie dei security-killer, i sicari professionisti dello spionaggio industriale. La loro attrezzatura, rivela il colonnello Rapetto, «è futuristica. Altro che valigetta, girano con il trolley».

Non è una battuta. Un anno fa un gruppo di esperti informatici ha simulato uno spionaggio di questo tipo girando con un trolley ad alto contenuto tecnologico per una settimana intera fra l'aeroporto di Malpensa, la stazione di Milano Centrale e la fermata della metropolitana di Cadorna. Era la cosiddetta Blue bag, la valigia blu, in grado di captare i segnali non del wi-fi, non del cellulare, ma del semplice bluetooth e di rubare di tutto e di più. Al termine della ricognizione sono stati individuati 1.312 cellulari, 39 computer, 21 palmari, 15 navigatori Gps, 5 stampanti e altre 13 periferiche con funzioni bluetooth in azione e facilmente intercettabili.

RETI A RISCHIO

Le più esposte alle incursioni dei pirati informatici sono le connessioni wireless (senza fili). Quindi i sistemi blue tooth e wi-fi.



L'altra categoria di spioni è quella dei «privacy sniper», i cecchini della nostra riservatezza. Lo fanno per mestiere, ma con apparecchi meno costosi. L'indagine giudiziaria sul Laziogate ha mostrato che con 1.000 euro un gruppo di investigatori privati era in grado di fornire la trascrizione delle telefonate di qualsiasi cellulare.

Anche le organizzazioni criminali stanno approfittando dell'alta tecnologia per ricattare e arricchirsi. Nel primo caso operano per lo più con gli interceptor. Nel secondo caso si dedicano alla penetrazione delle reti e dei sistemi informatici. >

L'interceptor non si può vendere in Italia, ma si può facilmente trovare e acquistare in India, dove viene prodotto.

> In pratica rapinano le identità. Possono farlo nei modi più diversi. A Milano l'anno scorso una grossa catena di supermercati ha subito l'attacco di una banda di romeni i quali, con la complicità di un'impiegata, sono riusciti a manomettere le casse inserendovi un gadget elettronico che, con il supporto di una scheda telefonica Gsm, trasferiva i dati delle carte di credito dei clienti ai complici in Romania. Questi a loro volta clonavano i mezzi di pagamento degli ignari clienti ai quali, poco tempo dopo, venivano addebitate spese mai effettuate.

Un altro episodio ha visto come protagonista un'impiegata di un call center che ha utilizzato i codici delle carte di credito di alcuni noti giocatori di calcio per ricaricare i telefoni delle sue amiche. Era convinta che i campioni con redditi milionari non avrebbero mai controllato i conti. A Bologna, sempre nel 2006, un hacker, finito in manette, è stato trovato in possesso di un file contenente 80 mila carte di credito pronte per essere clonate e acquistate online al prezzo di un euro ciascuna.

Ma questa è solo la punta visibile. Ben più rilevanti sono due tecniche recenti che vanno sotto il nome di phishing e di pharming. Con la prima si vanno a pescare all'amo con email provenienti all'apparenza dalla propria banca informazioni riservate come i codici di accesso ai conti bancari personali. Con la seconda, assai più sottile, mediante l'immissione di virus o di cavalli di Troia (Trojans), la vittima della truffa finisce per navigare in uno spazio virtuale clone della pagina web del proprio istituto di credito. Si immettono i dati del conto online e si è deviati immediatamente verso un server gestito dall'organizzazione criminale.

Solo la polizia postale ha in corso mille indagini su queste frodi telematiche. Le menti, un centinaio di ingegneri assunti dalle mafie locali, sono state rintracciate quasi tutte nei paesi dell'ex Unione Sovietica, specialmente in Russia,

NUMERI DI UN FENOMENO IN CRESCITA

60 milioni gli utenti di cellulari

100 mila le intercettazioni legali nel 2006

3 mila le persone denunciate per frodi telematiche dal 2000 a oggi

6,5 milioni: i conti correnti online

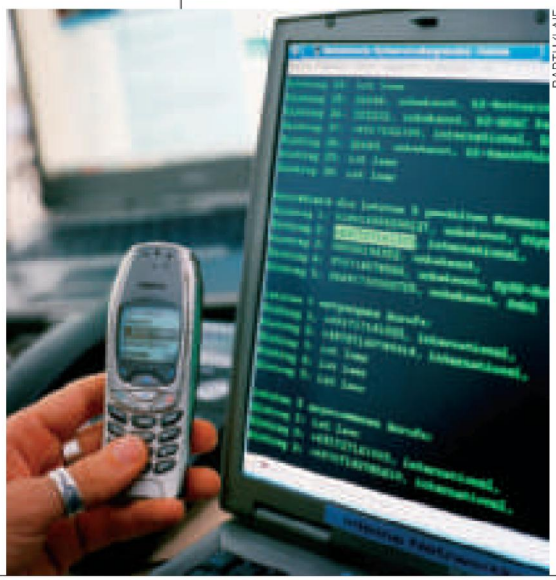
3.135 gli arrestati per truffe informatiche

1.807 le denunce nel 2006 per le carte di credito clonate

Un segnale degli hacker per segnalare una rete wi-fi senza protezioni.

nell'area di San Pietroburgo. Il danno economico è rilevante. «Nel 2005 abbiamo registrato tentativi di truffa per 1 milione di euro, di cui 360 mila euro sono stati incassati. L'anno scorso abbiamo avuto meno tentativi (per 660 mila euro), ma più soldi rubati: quasi 570 mila euro» ha calcolato Antonio Abruzzese, il responsabile del compartimento regionale dell'Emilia-Romagna della polizia postale. «Il tasso di realizzazione si è praticamente triplicato».

La minaccia criminale alla nostra vita digitale non riguarda solo l'Italia. Ormai è un fenomeno esteso a ben 35 paesi. «Quello che abbiamo riscontrato è una diffusa ritrosia da parte dei fornitori di servizi bancari online e di commercio elettronico di denunciare le truffe subite nel timore di un'inevitabile pubblicità negativa» denuncia Domenico Vulpiani, il dirigente della polizia postale. «Si preferisce il ricorso a costosi sistemi assicurativi che garantiscono il cliente e il fornitore dei servizi piuttosto che rivolgersi alla polizia e alla magistratura con un evidente vantaggio per i malviventi che così rimangono impuniti. Per fortuna, da alcuni mesi, la collaborazione sta facendo grandi progressi».



BARTH/LAIF

All'orizzonte si affaccia l'ultimo pericolo che proviene dall'innovazione tecnologica: il furto dei dati che transitano nell'etere attraverso le reti senza fili delle abitazioni private o anche delle aziende. Un test effettuato in alcune zone di Roma dai funzionari della polizia postale ha stabilito che due terzi degli apparati wi-fi individuati risultano facilmente violabili dai malintenzionati appostati con computer e antenne semiartigianali.

«La verità è che in Italia manca completamente la cultura della sicurezza e della protezione dei dati. Questo riguarda sia chi fornisce i servizi sia gli utenti finali» accusa Maurizio Masciopinto, dirigente della divisione operativa della polizia postale e delle comunicazioni. Aver denunciato 85 persone dall'inizio del 2006 a oggi solo per il phishing evidentemente non basta. Bisogna fare di più. Tutti: individui, banche, investigatori.

Il colonnello Rapetto non ammette più mezze misure: «Occorre che anche lo Stato, prendendo atto delle vulnerabilità, investa di più in ricerca e sviluppo. È indispensabile formare specialisti delle indagini hi-tech miscelando la cultura dell'investigazione tradizionale al know-how informatico di più alto livello. Ma fondamentalmente bisogna capire che i soldi impiegati in questo settore costituiscono un investimento e non una spesa». ●

WWW.
www.securegsmitalia.it
www.caspertech.it
www.speeka.it
www.Gat.gdf.it
www.Commissariatodips.it