

CRYPTO-GRAM
15 agosto 2006

Scritta da Bruce Schneier
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

Web: <http://www.schneier.com> oppure <http://www.counterpane.com>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Crypto-Gram in versione originale è anche consultabile in formato RSS:
<http://www.schneier.com/crypto-gram-rss.xml>

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:
<http://www.schneier.com/blog>.

Crypto-Gram è anche consultabile in formato RSS.

** *** ***** ***** ***** ***** ***** *****

In questo numero:

Gli arresti della scorsa settimana legati al terrorismo
Software per il controllo remoto di aerei
Le ristampe di Crypto-Gram
Il doping negli sport professionistici
Furti di iPod
News
Attestati di Sicurezza
Il Canile: Sniper Flash Cards
Un mese di bug dei browser
Sensazionalismi intorno all'insicurezza della HSBC
Le news di Counterpane
Aggiornare il modello di sicurezza tradizionale
I bot network
Commenti dei lettori

** *** ***** ***** ***** ***** ***** *****

Gli arresti della scorsa settimana legati al terrorismo

Ore e ore di attesa ai checkpoint. Ridicoli divieti su ciò che è possibile portare a bordo. Il lavoro compiuto per sventare una seria trama terroristica la scorsa settimana e le conseguenti misure di sicurezza aerea illustrano in maniera molto chiara la differenza fra sicurezza vera e propria e messinscena di sicurezza.

Nessuna delle misure di sicurezza attuate a seguito dell'11 settembre (no-fly list, screening secondario, messa al bando di coltellini tascabili e cavatappi) ha avuto niente a che vedere con gli arresti della scorsa settimana. E non avrebbero evitato gli attacchi pianificati se non fossero stati arrestati i terroristi. Non sarebbe servito nemmeno un documento d'identità nazionale.

Gli arresti rappresentano invece una vittoria delle indagini e dell'intelligence di vecchio stampo. I dettagli sono ancora segreti, ma le forze di polizia in almeno due paesi stavano tenendo d'occhio i terroristi da molto tempo. Hanno seguito degli indizi, hanno scoperto chi stesse comunicando con chi, e hanno pazientemente ricostruito la rete di contatti e il piano terroristico.

Le nuove misure di sicurezza aerea si concentrano su quel piano, perché le autorità ritengono di non aver ancora catturato tutte le persone coinvolte. È ragionevole supporre che alcuni cospiratori solitari, sapendo che i loro compatrioti si trovano in prigione e temendo essi stessi di venire arrestati, possano tentare di finire il lavoro per proprio conto. Le autorità non hanno divulgato pubblicamente i particolari (gran parte della storia sull' "esplosivo liquido" non ha molto senso), ma le misure eccessive di sicurezza sembrano prudenti.

Ma solo temporaneamente. La messa al bando di taglierini a seguito dell'11 settembre, o il doversi togliere le scarpe a seguito di Richard Reid, non ci ha resi più sicuri. E neanche un divieto a lungo termine contro oggetti contenenti liquidi nel bagaglio a mano ci renderà più sicuri. Non è soltanto il fatto che esistano modi per aggirare le regole, è che il focalizzarsi sulla tattica è un progetto destinato a fallire.

È facile difendersi contro ciò che i terroristi hanno pianificato l'ultima volta, ma è imprevedibile. Se investiamo miliardi di dollari nella disposizione di macchine per l'analisi dei liquidi negli aeroporti, e i terroristi impiegano esplosivi solidi, avremo buttato i nostri soldi. Se prenderanno di mira i centri commerciali, avremo buttato i nostri soldi. Il focalizzarsi sulla tattica costringe semplicemente i terroristi a effettuare una lieve modifica ai propri piani. Vi sono troppi obiettivi: stadi, scuole, cinema, chiese, la lunga coda di persone ai checkpoint di un aeroporto - e troppi sistemi per uccidere la gente.

Le misure di sicurezza che cercano di indovinare correttamente non funzionano, perché invariabilmente faremo le supposizioni sbagliate. Non è sicurezza, è messinscena di sicurezza: contromisure ideate per farci sentire più sicuri, ma che non ci rendono effettivamente più sicuri.

La sicurezza aeroportuale è l'ultima linea difensiva, e non difende poi molto bene. Certo, è sufficiente a catturare gli approssimativi e gli stupidi (ed è una buona ragione per non scartarla del tutto) ma non fermerà una trama ben congegnata. Non siamo in grado di tenere le armi fuori dalle prigioni, men che meno dagli aerei.

Lo scopo di un terrorista è di provocare terrore. Gli arresti della scorsa settimana dimostrano come la vera sicurezza non si concentri su probabili tattiche terroristiche, ma sugli stessi terroristi. È una vittoria dell'intelligence e dell'investigazione, e una dimostrazione lampante di come l'investire in queste aree dia ottimi risultati.

E quale può essere il vostro contributo? Non lasciatevi terrorizzare. Ai terroristi basta uccidere un po' di gente per terrorizzarne molta di più, ma qui i morti non c'entrano. Se ci arrendiamo alla paura i terroristi avranno raggiunto il loro scopo anche se vengono arrestati. Se rifiutiamo di farci intimidire allora i terroristi saranno sconfitti, anche se i loro attacchi avranno successo.

Le nuove regole di sicurezza aerea:

http://www.schneier.com/blog/archives/2006/08/new_airline_sec.html

Crypto-Gram è attualmente al suo nono anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare a questo indirizzo:

<http://www.schneier.com/crypto-gram-back.html>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi (le corrispondenti traduzioni in italiano le potete trovare all' indirizzo <http://www.cryptogram.it/crypto-gram.html>, ndt).

Profiling:

<http://www.schneier.com/crypto-gram-0508.html#1>

Cisco e ISS minacciano un ricercatore di sicurezza:

<http://www.schneier.com/crypto-gram-0508.html#2>

Plagio e mondo accademico: un'esperienza personale:

<http://www.schneier.com/crypto-gram-0508.html#8>

Secure Flight:

<http://www.schneier.com/crypto-gram-0508.html#12>

"BOB" a bordo:

<http://www.schneier.com/crypto-gram-0408.html#1>

Gli alibi e la gentilezza degli sconosciuti:

<http://www.schneier.com/crypto-gram-0408.html#3>

I ranger dell'aeroporto di Houston:

<http://www.schneier.com/crypto-gram-0408.html#7>

Siti Web, password e consumatori:

<http://www.schneier.com/crypto-gram-0408.html#8>

Volare con un biglietto aereo altrui:

<http://www.schneier.com/crypto-gram-0308.html#6>

Il testo nascosto nei documenti elettronici:

<http://www.schneier.com/crypto-gram-0308.html#8>

Palladium e il TCPA:

<http://www.schneier.com/crypto-gram-0208.html#1>

Armare i piloti delle linee aeree:

<http://www.schneier.com/crypto-gram-0208.html#8>

Code Red:

<http://www.schneier.com/crypto-gram-0108.html#1>

La protezione del copyright nel Mondo Digitale:

<http://www.schneier.com/crypto-gram-0108.html#7>

Vulnerabilità, divulgazione e risoluzioni basate su virus:

<http://www.schneier.com/crypto-gram-0008.html#2>

Bluetooth:

<http://www.schneier.com/crypto-gram-0008.html#8>

Un cracker hardware DES:

<http://www.schneier.com/crypto-gram-9808.html#descracker>

Sistemi biometrici: Verità e Finzioni:

<http://www.schneier.com/crypto-gram-9808.html#biometrics>

Back Orifice 2000:

<http://www.schneier.com/crypto-gram-9908.html#BackOrifice2000>>

Servizi e-mail basati sul Web e crittografati:

<http://www.schneier.com/crypto-gram-9908.html#Web-BasedEncryptedE-Mail>>

** *** ***** ***** ***** ***** ***** ***** *****

Il doping negli sport professionistici

La grossa novità nel ciclismo professionistico è che è stato annullato il titolo di vincitore del Tour de France a Floyd Landis perché il ciclista è risultato positivo al test antidoping, che ha rivelato l'uso di una droga per aumentare le prestazioni. Lasciando da parte per un momento l'intera questione sul permettere ad atleti professionisti l'uso di droghe per l'aumento di prestazioni, sulla pericolosità di tali droghe, e su cosa sia anzitutto una droga per l'aumento di prestazioni, vorrei parlare della sicurezza e delle questioni economiche legate alla problematica del doping negli sport professionistici.

Il test antidoping è una problematica di sicurezza. Le varie federazioni sportive di tutto il mondo fanno del loro meglio per rilevare il doping illegale, e gli atleti fanno del loro meglio per eludere i test. È il classico braccio di ferro di sicurezza: i progressi delle tecnologie di rilevamento portano a progressi nell'elusione di tali rilevazioni, che a loro volta stimolano lo sviluppo di migliori capacità di rilevamento. Al momento pare che siano le droghe ad avere la meglio; in alcuni contesti i test antidoping vengono anche definiti "test d'intelligenza": se non riesci ad aggirarli, non meriti di giocare.

Ma a differenza di molte altre "gare di forza" di sicurezza, chi effettua i rilevamenti ha la possibilità di esaminare il passato. Lo scorso anno un laboratorio ha analizzato l'urina di Lance Armstrong e ha trovato tracce della sostanza vietata EPO. Il dettaglio interessante è che il campione di urina analizzato non era del 2005, ma del 1999. A quell'epoca non vi erano buoni test per individuare la EPO nelle urine. Oggi sì, e il laboratorio ha preso un campione di urina congelato (e chi lo sapeva che i laboratori conservano i campioni di urina degli atleti?) e lo ha analizzato. Il test fu poi annullato (le procedure di laboratorio sono state approssimative), ma non credo che siano state comprese a fondo le reali implicazioni di quell'episodio. I test possono andare indietro nel tempo.

Questo causa due effetti importanti. Primo: i medici che sviluppano nuove droghe per l'aumento di prestazioni possono conoscere esattamente quali tipi di test verranno condotti dai laboratori antidoping, e possono verificare con anticipo la propria abilità nell'eludere i rilevamenti di tali droghe. Ma non possono sapere quali tipi di test verranno sviluppati in futuro, e gli atleti non possono dare per scontato che, siccome una certa droga non è rintracciabile oggi, continuerà a esserlo anche negli anni a venire.

Secondo: gli atleti accusati di doping in base ad analisi condotte su campioni di urina vecchi di qualche anno non hanno modo di difendersi. Non possono sottoporsi nuovamente alle analisi, è troppo tardi. Se io fossi un atleta preoccupato per tali accuse, farei periodici depositi in garanzia della mia urina, così da poter avere qualche possibilità in più per contestare un'accusa.

Il braccio di ferro del doping continuerà a causa degli incentivi. Si

tratta del classico Dilemma del Prigioniero. Consideriamo due atleti in competizione, Alice e Bob. Sia Alice sia Bob devono decidere individualmente se faranno uso di droghe o meno.

Immaginiamo Alice mentre valuta le proprie due opzioni:

“Se Bob non prende droghe”, pensa, “allora sarò nel mio miglior interesse prenderle, perché mi daranno un margine di prestazioni ai danni di Bob. Avrò maggiori possibilità di vittoria.

“Analogamente, se Bob fa uso di droghe, è anche nel mio interesse accettare di usarle. In questo modo, almeno, Bob non avrà vantaggi su di me.

Perciò, anche se non posso controllare quel che Bob sceglierà di fare, il prendere droghe mi darà comunque un risultato migliore, a prescindere dalle decisioni di Bob”.

Purtroppo Bob farà esattamente lo stesso ragionamento. Risultato: entrambi faranno uso di droghe per l'aumento di prestazioni e nessuno dei due avrà un vantaggio rispetto all'altro. Se potessero fidarsi l'uno dell'altra, potrebbero rifiutarsi di assumere droghe e mantenere la stessa situazione di equilibrio, senza alcun rischio legale o fisico. Ma gli atleti in competizione non possono fidarsi gli uni degli altri, e tutti hanno la sensazione che sia meglio drogarsi (e continuare a cercare droghe sempre più nuove e non rilevabili) per competere. E il braccio di ferro va avanti.

Alcuni sport sono molto più vigili di altri rispetto alla questione doping. Il ciclismo europeo è particolarmente attento, e anche le Olimpiadi. Gli sport professionistici americani sono molto più permissivi, spesso cercano di dare un'immagine di vigilanza mentre in realtà continuano a permettere agli atleti di assumere sostanze che aumentano le prestazioni. Sanno che i loro sostenitori vogliono vedere linebacker muscolosi, battitori vigorosi e scattisti veloci come fulmini. E quindi, con una strizzatina d'occhio e un cenno di assenso, eseguono soltanto i test più semplici.

Si prenda per esempio l'attuale dibattito sull'uso dell'HGH, l'ormone della crescita, nel baseball. Vi sono test e sanzioni molto gravi per l'uso di steroidi, ma tutti sanno che adesso i giocatori stanno prendendo l'HGH perché non vi sono analisi delle urine a riguardo. Si sta sviluppando un esame del sangue per rilevarlo, ma è ancora ben lungi dal funzionare. Il metodo per fermare l'utilizzo di HGH è quello di prendere campioni di sangue oggi e conservarli per analisi future, ma il sindacato dei giocatori si è rifiutato di permettere una cosa del genere, e la commissione del baseball non sta spingendo in questa direzione.

Alla fin fine, il doping è una questione puramente economica. Gli atleti continueranno a drogarsi perché il Dilemma del Prigioniero li costringe a farlo. Le autorità sportive continueranno a migliorare le proprie tecniche di rilevamento oppure a fingere di farlo, a seconda dei propri sostenitori e degli introiti. E con il continuo progresso tecnologico, gli atleti professionisti diventeranno sempre più come auto da corsa volontariamente ideate e plasmate.

<http://www.msnbc.msn.com/id/14059185/>

Il caso Armstrong:

http://www.schneier.com/blog/archives/2005/09/lance_armstrong.html

Il baseball e l'HGH:

<http://sports.yahoo.com/mlb/news?slug=jp-hgh061206&prov=yhoo&type=lgns>
<http://sports.yahoo.com/mlb/news?slug=jp-hgh060706&prov=yhoo&type=lgns>

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/news/columns/0,71566-0.html>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

Furti di iPod

Che cosa succede se si distribuiscono 50 milioni di oggetti piccoli, di valore e facilmente vendibili, nelle mani di uomini donne e bambini in tutto il mondo, dicendo loro di camminare per le strade portandoseli addosso? Beh, la gente li ruba, ovviamente. Ecco i dati:

“Aumento dei reati: colpa degli iPod”, strilla la prima pagina del Metro, a Londra. ‘Gli scippatori prendono di mira chi possiede un iPod’, dice lo ITV. Questa è la reazione alla notizia data dal governo secondo cui i furti nel Regno Unito sono aumentati dell’8% nell’ultimo anno, da 90.747 a 98.204. Il Ministro dell’Interno John Reid attribuisce tutto questo all’esca irresistibile rappresentata da ‘giovani che portano con sé merci costose, come telefoni cellulari e lettori di MP3’. Un distinto sondaggio sul crimine britannico, tuttavia, suggerisce che le rapine siano aumentate del 22%, a 311.000 casi”.

Ciò non dovrebbe sorprendere, così come non c’era da sorprendersi negli anni Novanta quando vi fu un’ondata di furti di scarpe da ginnastica di marca e molto costose. O che vi sia anche un’ondata di furti di computer portatili.

Che cosa si può fare? Sostanzialmente non molto, a parte essere cauti. Gli scippi sono sempre stati reati a basso rischio, per cui è sensato constatarne l’aumento con l’innalzarsi del valore degli oggetti che le persone si portano appresso. E chi ha con sé un lettore musicale portatile è facilmente individuabile grazie a un infallibile indicatore: quegli onnipresenti auricolari.

L’economia legata a questo reato è tale per cui i furti continueranno a meno che non accada una delle tre cose seguenti. Uno: i lettori musicali portatili saranno meno costosi. Due, i costi del reato saranno molto più alti. Tre, la società affronterà il problema della classe povera e le offrirà un’alternativa migliore del furto di iPod.

<http://crave.cnet.co.uk/digitalmusic/0,39029432,49282165,00.htm>
http://www.educatedguesswork.org/movabletype/archives/2006/07/on_ipod_theft.html oppure <http://tinyurl.com/g9ojv>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

News

Uno scandalo nazionale francese con al centro un hacking ai danni di una banca.

<http://www.wired.com/news/technology/0,71363-0.html>

Symantec ha riportato un exploit zero-day di PowerPoint. Al momento, l’entità stimata della minaccia è bassa, ma potrebbe cambiare dall’oggi al domani se qualcuno scrivesse uno worm automatico che approfittasse di tale vulnerabilità. Si noti che la vulnerabilità è apparsa “in the wild”

alcuni giorni dopo il "Martedì delle Patch", presumibilmente per ingrandire il più possibile la finestra di esposizione prima che Microsoft pubblichi una patch.

http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-071212-4413-99&tabid=1 oppure <http://tinyurl.com/zrq6o>

L'elenco dei principali bersagli terroristici fornito dal Dipartimento per la Sicurezza Nazionale è veramente ottuso. Comprende 1.305 casinò, 234 ristoranti, una gelateria, un negozio di attrezzature, un mercato delle pulci e una fabbrica Amish di popcorn; 3.650 siti in totale. Ma che sta succedendo? La politica dello spreco, ecco ciò che sta accadendo. Non saremo mai in grado di comprendere la sicurezza in maniera corretta se continuiamo a farne una parodia di se stessa.

http://seattletimes.nwsourc.com/html/localnews/2003123566_danny13.html
>

Documenti di identità fasulli salvano delle vite in Iraq:

<http://www.cato-at-liberty.org/2006/07/11/fake-ids-save-lives-in-iraq/>>

Dal primo gennaio 2007, chiunque attraversi il confine fra gli Stati Uniti e il Canada è tenuto ad avere un passaporto. Questo a causa del terrorismo, naturalmente. Ma ora ci viene detto che saranno esenti i traghetti e le imbarcazioni private. I casi sono due: o i passaporti sono necessari alla sicurezza, e allora dovremmo bloccare i traghetti. Oppure servono solo per salvare le apparenze, e allora è sufficiente fare quel che è più comodo. Oppure, semplicemente, sappiamo che i terroristi non prendono mai il traghetto. Capisco che la sicurezza sia un compromesso, ma tutto questo è abbastanza sciocco.

<http://www.cbc.ca/story/canada/national/2006/07/18/chertoff-edmonton.html> oppure <http://tinyurl.com/zl5af>

ABN AMRO ha introdotto l'autenticazione vocale nel proprio sistema bancario telefonico. Sembra essere una buona idea, a patto che sia affidabile.

<http://www.abnamro.com/pressroom/releases/2006/2006-07-20-en.jsp>

Firefox 2.0 conterrà funzioni anti-phishing:

<http://redmondmag.com/news/article.asp?EditorialsID=7614>>

Qualcuno ha effettuato hacking ai danni dei computer che servivano annunci pubblicitari a molti siti web, fra cui MySpace. Come risultato sono stati infettati un milione di computer.

http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_ad_ware_to_mo.html oppure <http://tinyurl.com/ehyen>
<http://www.freedom-to-tinker.com/?p=1043>

Nepenthes: uno strumento di raccolta di malware e un'ottima idea per un progetto di ricerca:

<http://nepenthes.mwcollect.org/>>

Questo pare un utilizzo davvero intelligente dell'RFID. L'idea è di incorporare dei chip nelle attrezzature chirurgiche, e poi passare un rilevatore sui pazienti per assicurarsi che i medici non abbiano lasciato accidentalmente qualche strumento nel corpo di un paziente. Finché il sistema automatico si aggiunge, migliorandolo, a quello manuale senza sostituirlo completamente, sono a favore di questa idea.

<http://go.reuters.com/newsArticle.jhtml?type=oddlyEnoughNews&storyID=12877093> oppure <http://tinyurl.com/zrw5h>

Gli sky marshal devono scrivere rapporti su persone innocenti per rientrare in una quota prefissata:

<http://www.thedenverchannel.com/news/9559707/detail.html>>

<http://www.interesting-people.org/archives/interesting-people/200607/ms>

g00156.html> oppure <http://tinyurl.com/k5og2>>

I problemi di chi è corrispondente dalla zona di guerra nel Libano:
<<http://www.cnn.com/CNN/Programs/anderson.cooper.360/blog/2006/07/trying-to-avoid-becoming-target.html>> oppure <http://tinyurl.com/f6k9h>>

Degli agenti della CIA sono stati esposti per aver usufruito delle migliaia accumulate come frequent flyer e per aver commesso altre sviste. Non vedo però dove sia il problema nell'accumulare migliaia come frequent flyer. Se si presume che stiano viaggiando sotto copertura come dirigenti d'azienda, è logico che si comportino come tanti altri dirigenti d'azienda. Non è che non vi sia altro modo di ricostruire i loro viaggi.

<<http://www.chicagotribune.com/news/nationworld/chi-0607240160jul24,1,1064628.story>> oppure <http://tinyurl.com/zlu6a>>

In "Beyond Fear" ho scritto in merito al profiling. Ho parlato a lungo di come un profiling intelligente basato sul comportamento sia molto più efficace di un profiling stupido e meccanico basato su determinate caratteristiche, e di come delle persone ben addestrate siano di gran lunga migliori dei computer. La storia che presi come esempio riguardava l'agente di frontiera statunitense Diana Dean, che catturò Ahmed Ressay nel 1999. In questa vicenda, un attento ufficiale di frontiera ha notato una maglietta da calcio inglese indosso a un senegalese che tentava di entrare a Cipro con un passaporto francese falsificato. Quel dettaglio ha indotto l'ufficiale a controllare il passaporto un po' più da vicino, e ha così notato la falsificazione. Particolari come questi non possono essere notati da un computer, almeno fino a quando l'intelligenza artificiale non produrrà un vero e proprio cervello.

<<http://go.reuters.com/newsArticle.jhtml?type=oddlyEnoughNews&storyID=12953590>> oppure <http://tinyurl.com/zvkhd>>

Quel che ho scritto sul profiling:

<<http://www.schneier.com/blog/archives/2005/07/profiling.html>>

Memorie di uno screener di sicurezza aeroportuale.

Questa persona parla del suo lavoro di screener molti anni prima dell'11 settembre, prima della TSA, per cui si spera che le cose siano cambiate adesso. È una lettura davvero affascinante, però. Due cose mi saltano all'occhio. La prima, come scrissi io stesso, è che si tratta di un compito orrendamente noioso. La seconda: gli screener venivano addestrati non a trovare armi, ma a trovare quelle specifiche armi di esempio che la FAA usava per i test.

<<http://www.kuro5hin.org/story/2006/7/26/1497/94515>>

<http://www.schneier.com/blog/archives/2006/03/airport_passeng.html>

Nel 1994 il Congresso approvò il CALEA (Communications Assistance for Law Enforcement Act). Sostanzialmente si tratta della legge che obbliga le compagnie telefoniche a mettere a disposizione le vostre chiamate (anche quelle da cellulare) per le intercettazioni governative. Ma ora il governo vuole avere accesso anche alle chiamate VoIP, ai messaggi SMS e a tutto il resto. Sta facendo del proprio meglio per interpretare il CALEA nel senso più generale possibile, ma sta anche perseguendo una prospettiva legale.

<<http://arstechnica.com/news.ars/post/20060727-7372.html>>

ScatterChat è un client di messaggia istantanea protetta che si serve del sistema di comunicazione anonima Tor.

<<http://www.scatterchat.com/>>

<<http://www.prweb.com/releases/2006/7/prweb414312.htm?tag=scatterchat>>

Vi sono delle falle nel protocollo, però.

<<http://www.lightbluetouchpaper.org/2006/08/11/>>

<http://www.scatterchat.com/advisories/2006-01_tech.html>

Interessante ricerca sulla sicurezza e la monocoltura:
<<http://www.tmcnet.com/usubmit/2006/07/21/1725091.htm>>

I tre maggiori programmi antivirus, di Symantec, McAfee e Trend Micro, hanno minori probabilità di rilevare nuovi worm e virus rispetto a programmi meno conosciuti perché gli autori di virus collaudano il proprio lavoro specificamente contro quei programmi. È interessante vedere il cambiamento di scenario, con il malware diventare sempre meno il campo di attività degli hacker e sempre più quello dei criminali. Questa è l'ennesima mossa nel continuo braccio di ferro fra aggressori e difensori.

<http://www.zdnet.com.au/blogs/securifythis/soa/Why_popular_antivirus_ap_ps_do_not_work_/0,39033341,39264249,00.htm> oppure
<<http://tinyurl.com/e63uw>>

Questo servomotore computerizzato apre serrature a combinazione facendo un'operazione di forza bruta contro tutte le combinazioni. Non che sia particolarmente sorprendente, ma è interessante vedere che qualcuno ha realizzato davvero un simile strumento.

<<http://www.hackaday.com/entry/1234000507073793/>>

Ecco una descrizione di come aprire una comune serratura Master in 10 minuti circa. La progettazione riduce a 121 le 40^3 possibili combinazioni. È una metafora fisica per illustrare una pessima crittografia.

<<http://www.fusor.us/lockpick.html>>

Prendendo spunto da un'inutile idea americana, il Regno Unito ha annunciato un sistema di livelli di minaccia:

<<http://www.nytimes.com/2006/08/01/world/europe/01cnd-britain.html>>

Ho scritto sulla stupidità di questo tipo di sistema nel 2004:

<<http://www.schneier.com/essay-059.html>>

L'amministrazione Bush si è servita di tale sistema soprattutto come strumento politico. Forse Tony Blair ha in mente la stessa idea.

Le difese antimissilistiche per aerei passeggeri non verranno implementate tanto presto:

<<http://www.washingtonpost.com/wp-dyn/content/article/2006/07/31/AR2006073100922.html>> oppure <<http://tinyurl.com/l9jo4>>

E forse è meglio così. In primo luogo, vi sono maniere molto più efficaci per investire quel denaro nella lotta al terrorismo.

Secondariamente, tali difese funzionano bene soltanto contro un tipo particolare di tecnologia missilistica.

Degli hacker clonano passaporti RFID:

<http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html>

Che cosa fate quando scoprite che qualcuno sta rubando banda alla vostra rete wireless? A me non importa molto, ma a questa persona sì. E allora "fa girare squid con un banale redirector che scarica immagini, utilizza mogrify per ruotarle sottosopra e le serve dal proprio server web locale". Le immagini sono pazzesche. Egli cerca persino di modificarle tutte in modo che appaiano sfocate.

<<http://www.ex-parrot.com/peter/upside-down-ternet.html>>

Open Voting Foundation ha divulgato informazioni su un'enorme vulnerabilità della macchina Diebold per il voto elettronico:

<http://openvotingfoundation.org/tiki-read_article.php?articleId=1>

Una banca ha vietato i telefoni cellulari come misura di sicurezza. È una totale sciocchezza. È facile aggirare il divieto: un auricolare Bluetooth è poco appariscente quanto basta. O anche una coppia di auricolari simili a quelli per iPod. O un dispositivo per SMS. Deve solo

funzionare all'inizio: dopotutto, una volta che si comincia a svaligiare una banca, non vi è alcun divieto che ci impedisca di usare il nostro cellulare.

<http://www.upi.com/NewsTrack/view.php?StoryID=20060803-050428-5727r>

Bell'articolo sul data mining e il terrorismo.

<http://www.cio.com/archive/080106/antiterror.html>

Il mese scorso, al BlackHat, Brendan O'Connor ha messo in guardia sui pericoli delle stampanti insicure: trattatele come fossero computer, non stampanti. Mi ricordo del lavoro svolto anni fa dal L0pht sulle vulnerabilità delle stampanti e sui metodi per attaccare reti attraverso le stampanti. Ma il punto è ancora valido e merita di essere ribadito: le stampanti sono computer e hanno anch'esse delle vulnerabilità, come qualsiasi computer.

http://articles.techrepublic.com.com/2100-1009_11-6102367.html

Ottimo articolo di CATO sui rischi del terrorismo:

<http://www.cato.org/pubs/regulation/regv27n3/v27n3-5.pdf>

Il commento:

http://www.boingboing.net/2006/08/07/only_traitors_try_to.html

Ecco un database esaustivo del malware: il costo è di 13.500 euro all'anno.

<https://www.frame4.net/mdpro/index.php>

http://www.schneier.com/blog/archives/2006/08/malware_distrib.html

Anche il gruppo di hacker Cult of the Dead Cow possiede un archivio di malware, libero e con minori restrizioni d'accesso.

<http://www.offensivecomputing.net/>

AOL rilascia un'enorme quantità di dati di ricerca. Si tratta di dati di ricerca per circa 658.000 utenti (resi anonimi) in un intervallo di più di tre mesi, da marzo a maggio; approssimativamente un terzo dell'un per cento dei loro dati complessivi per quel periodo.

http://www.schneier.com/blog/archives/2006/08/aol_releases_ma.html

<http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/> oppure <http://tinyurl.com/ky6ek>

<http://yro.slashdot.org/yro/06/08/07/2022244.shtml>

<http://www.techmeme.com/060806/p28#a060806p28>

<http://www.techcrunch.com/2006/08/07/aol-this-was-a-screw-up/>

Amnesty International lancia una campagna contro la repressione in Internet:

<http://web.amnesty.org/library/Index/ENGA300162006>

Pare che un gruppo di ladri di carte di credito dello Sri Lanka abbia ricavato e raccolto i dati di una serie di carte di credito inglesi protette da chip. Non potendo clonare i chip, hanno estratto le informazioni dalla striscia magnetica e hanno costruito delle carte senza chip. Ovviamente tali carte non avrebbero funzionato nel Regno Unito, per cui i criminali si sono recati in India, dove gli sportelli Bancomat verificano soltanto la striscia magnetica. La compatibilità all'indietro spesso è incompatibile con la sicurezza. Questo ne è un ottimo esempio, e dimostra come dei criminali possano servirsi dell'"arbitraggio tecnologico" per far leva sulla compatibilità.

<http://www.scottcarneyonline.com/blog/2006/08/crime-syndicate-gets-rfid-savvy.html> oppure <http://tinyurl.com/kuhsu>

Ecco una collezione di 11 coltelli e rasoi fabbricati in prigione e confiscati più di 20 anni fa nel New Jersey. Pensate a questi oggetti e alle avverse condizioni in cui furono realizzati la prossima volta che vedrete la sicurezza aeroportuale confiscare a qualcuno il suo coltellino tascabile.

<http://www.designobserver.com/archives/016492.html>

In questa pagina web, scendendo di circa un quarto dall'inizio, troverete la scansione di un fumetto di Superman degli anni Settanta in cui un ragazzino hacker penetra nel sistema informatico della Fortezza della Solitudine, utilizzando quel che sembra un TRS-80 Model III. La password di Superman era "Kal-El", ovvero il suo nome kryptoniano.

http://community.livejournal.com/scans_daily/2192482.html

Ottimo articolo sulla "finta divulgazione": rendere nota una vulnerabilità senza divulgarla veramente.

<http://software.newsforge.com/software/06/08/08/1351256.shtml?tid=78&tid=138> oppure <http://tinyurl.com/jzvbe>

Ricordate: la divulgazione totale è l'unica cosa che costringe i produttori a sistemare i problemi di sicurezza. Più ci allontaniamo dalla divulgazione totale, meno incentivi avranno i produttori per sistemare i problemi, e saremo tutti maggiormente a rischio.

Questo sofisticato circolo di frodi di carte di credito intercettava le chiamate di autorizzazione per le transazioni delle carte di credito a Phuket, Thailandia. Siamo nel 2006 e quei terminali commerciali ancora non criptano le loro comunicazioni?

http://www.theregister.co.uk/2006/08/04/thai_wiretap_scam/

Dipartimento per la Sicurezza Nazionale, Ufficio dell'Ispettore Generale, "Enhanced Security Controls Needed For US-VISIT's System Using RFID Technology (Redacted)" [Maggiori controlli di sicurezza necessari per il sistema US-VISIT mediante l'utilizzo della tecnologia RFID (Redatto)], OIG-06-39, Giugno 2006.

http://www.dhs.gov/interweb/assetlibrary/OIG_06-39_Jun06.pdf

Dipartimento per la Sicurezza Nazionale, Ufficio dell'Ispettore Generale, "Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry" [Rassegna delle azioni intraprese dal CBP per l'intercettazione di sospetti terroristi nei porti d'entrata], OIG-06-43, Giugno 2006.

http://www.dhs.gov/interweb/assetlibrary/OIG-06-43_June06.pdf

** *** ***** ***** ***** ***** ***** *****

Attestati di Sicurezza

Sono stato per molto tempo avverso agli attestati: ho incontrato troppi professionisti di sicurezza pessimi ma con attestati e qualifiche, e conosco molti ottimi professionisti di sicurezza che non possiedono alcun attestato. Tuttavia sono giunto a ritenere che, se da un lato attestati e qualifiche non sono perfetti, dall'altro rappresentano per un professionista un sistema decente per imparare alcune delle cose che dovrà conoscere; inoltre aiutano un potenziale datore di lavoro a valutare se un candidato possiede o meno le competenze di sicurezza che dovrà avere.

Che cosa è cambiato? Sia i requisiti necessari per la professione, sia i corsi che rilasciano le certificazioni.

Chiunque può inventare un sistema di sicurezza che l'inventore stesso non può espugnare. L'ho sostenuto così tante volte che Cory Doctorow l'ha definita "la Legge di Schneier": quando qualcuno vi affida un sistema di sicurezza e vi dice "Ritengo che sia sicuro", la prima cosa da chiedere è "Chi diavolo è lei?" Mi faccia vedere quali sistemi è riuscito a violare, così mi dimostrerà che la sua asserzione in merito

alla sicurezza del sistema ha un qualche significato.

Quel genere di competenza non si può trovare in un attestato. Si tratta di una combinazione di un feeling innato per la sicurezza, di un'approfondita conoscenza della letteratura accademica sulla sicurezza, di una lunga esperienza con gli attuali sistemi di sicurezza, e di pratica. Quando ho assunto delle persone per progettare e valutare sistemi di sicurezza, non ho prestato la minima attenzione ai loro attestati. Non significano niente; io ho bisogno di una serie diversa di competenze e di capacità.

Ma a moltissime organizzazioni non serve assumere quel tipo di persona. La sicurezza di rete si è standardizzata; le aziende hanno bisogno di un professionista praticante, non di un ricercatore. E questa è una buona cosa, perché vi è così tanta richiesta di tali professionisti che non vi sono abbastanza ricercatori in circolazione. I corsi di formazione sono ottimi per sfornare professionisti praticanti.

E nel corso degli anni questi corsi sono migliorati, e insegnano davvero concetti e nozioni necessari ai professionisti di sicurezza. Probabilmente io non vorrei un neodiplomato per progettare un protocollo di sicurezza o per valutare un criptosistema, ma i diplomati vanno benissimo per ricoprire una delle varie posizioni necessarie a un'organizzazione per la propria sicurezza di rete.

Nella mia azienda incoraggiamo i nostri security analyst a seguire tali corsi. Pensiamo che sia il metodo più efficace economicamente per fornire loro le competenze necessarie a svolgere lavori sempre più complessi.

Ovviamente nulla di tutto questo è perfetto. Continuo a incontrare pessimi praticanti di sicurezza con qualifiche e attestati, e conosco ancora eccellenti professionisti di sicurezza che ne sono privi.

Alla fine, gli attestati sono come il profiling. Funzionano, ma sono approssimativi. Solo perché una persona possiede un certo attestato o qualifica, non significa che egli possieda le competenze in ambito di sicurezza che state cercando (in altre parole, vi sono dei falsi positivi). E solo perché una persona non possiede un attestato di sicurezza, non significa che egli non possieda le competenze di sicurezza richieste (falsi negativi). Ma ci serviamo degli attestati per lo stesso motivo per cui eseguiamo il profiling: non abbiamo il tempo, la pazienza o la capacità di effettuare esplicite valutazioni per la figura che stiamo cercando.

Il profiling basato sugli attestati e le qualifiche di sicurezza è il modo più semplice per un'organizzazione di prendere una buona decisione riguardo a un'assunzione, e il modo più semplice per un'organizzazione di addestrare gli impiegati già occupati. E in tutta onestà, di solito questo è più che sufficiente.

Questo articolo è originariamente apparso come botta e risposta con Marcus Ranum nel numero di luglio 2006 di Information Security Magazine. (Per leggere il "contrappunto" di Marcus è necessario rispondere a un sondaggio un po' seccante, ma 1) potete mentire e 2) ne vale la pena). http://informationsecurity.techtarget.com/magLogin/1,291245,sid42_gci1196098,00.html oppure <http://tinyurl.com/zp7tk>

Una guida agli attestati di Information Security:
<http://dmiessler.com/writing/infosecerts/>

** *** *****

Il Canile: Sniper Flash Cards

Hanno organizzato una competizione di crittanalisi con un premio di 5.000 dollari, ma chiedono una quota di partecipazione di 100 dollari. A me sembra proprio una truffa.

<http://www.sniperflashcards.com/cipher.asp>

I miei commenti sulle gare di cracking:

<http://www.schneier.com/crypto-gram-9812.html#contests>

** *** ***** ***** ***** ***** ***** *****

Un mese di bug dei browser

Per inaugurare il suo nuovo blog Browser Fun, H.D. Moore ha iniziato con "A Month of Browser Bugs" [Un mese di bug dei browser]. Trentun giorni e trentuno hack dopo, il blog elenca gli exploit contro tutti i browser più importanti:

Internet Explorer: 25
Mozilla: 2
Safari: 2
Opera: 1
Konqueror: 1

Immagino che avrebbe potuto andare avanti per un altro mese senza problemi, e forse avrebbe potuto produrre un nuovo bug di browser al giorno indefinitamente.

Qui la morale non è tanto che IE sia meno sicuro degli altri browser, anche se personalmente non ho dubbi a riguardo. La morale è che gli standard di scrittura del codice sono talmente pessimi che le vulnerabilità di sicurezza sono comuni fino a questo punto.

<http://browserfun.blogspot.com>

La teoria di Eric Rescorla sulla scoperta dei bug:

<http://www.rtfm.com/bugrate.pdf>

Un altro commento:

<http://osvdb.org/blog/?p=127>

** *** ***** ***** ***** ***** ***** *****

Sensazionalismi intorno all'insicurezza della HSBC

La storia è del Guardian:

"Il Guardian ha appreso che una delle più grandi banche d'Inghilterra ha esposto milioni di conti correnti online a potenziali frodi a causa di un'evidente falla di sicurezza.

"Il difetto nel sistema bancario online della HSBC è tale che 3,1 milioni di clienti nel Regno Unito che si sono registrati per usufruire del servizio sono stati vulnerabili a eventuali attacchi per almeno due anni. Un esperto di informatica ha definito questa mancanza

'scandalosa'.

"La scoperta è avvenuta grazie a un gruppo di ricercatori della Cardiff University, i quali hanno notato che chiunque avesse sfruttato la vulnerabilità avrebbe sicuramente potuto penetrare in qualsiasi conto corrente in non più di nove tentativi".

Sembra piuttosto grave.

Ma leggete questo:

"La falla, che il Guardian non descrive in dettaglio, riguarda il modo in cui i clienti HSBC accedono al loro servizio di internet banking. Dei criminali, servendosi di cosiddetti 'keylogger' (gingilli hardware di facile reperibilità oppure virus che registrano ogni sequenza di tasti digitata sulla tastiera del computer bersaglio), possono facilmente dedurre i dati necessari per ottenere accesso indiscriminato ai conti correnti in pochi tentativi".

Ah, quindi la "scandalosa" vulnerabilità consisterebbe nel fatto che un aggressore _che ha già installato un keylogger sul computer di qualcuno_ può penetrare nel conto corrente HSBC di questa persona. A me sembra che se un aggressore ha installato un keylogger sul computer di qualcuno, questo malcapitato dovrà affrontare ogni genere di problema di sicurezza.

Se questa è la falla più grande del sistema di autenticazione della HSBC, credo che quella banca stia facendo un ottimo lavoro.

<http://technology.guardian.co.uk/news/story/0,,1841016,00.html>

** **

Le news di Counterpane

Sono ora disponibili le trascrizioni del Counterpane Customer Panel, che ha avuto luogo al Gartner show di qualche mese fa:

<http://www.counterpane.com/transcript>

La Minnesota Public Radio mi ha intervistato mentre girovagavo a Minneapolis alla ricerca di telecamere e di altre forme di sorveglianza di massa.

<http://minnesota.publicradio.org/display/web/2006/05/25/surveillance/>

** **

Aggiornare il modello di sicurezza tradizionale

L'anno scorso, nella mailing list Firewall Wizards, Dave Piscitello ha formulato un'osservazione affascinante. Analizzando il modello di sicurezza tradizionale suddiviso in quattro passaggi:

Autenticazione (chi siete)
Autorizzazione (che cosa vi è permesso fare)
Disponibilità (i dati sono accessibili?)
Autenticità (i dati sono integri?)

Piscitello ha affermato:

“Questo modello non è più sufficiente perché non include l’affermazione della credibilità del dispositivo endpoint da cui un utente (remoto) si autenticherà e da cui conseguentemente accederà ai dati. L’ammissione alla rete e il controllo dell’endpoint sono necessari per determinare se il dispositivo è libero da malware (specialmente i keylogger) prima ancora di poter accettare un solo carattere digitato da un utente. Per cui aggiungiamo “ammissibilità” in testa all’elenco, e realizziamo quindi uno sgabello a cinque gambe; oppure chiamiamolo il Pentagono della Fiducia”.

Ha ragione al 100%.

** *** ***** ***** ***** ***** ***** *****

I bot network

Che cosa si potrebbe fare se si controllasse una rete di migliaia di computer, o se si potesse almeno sfruttare i cicli inutilizzati dei processori di quelle macchine? Si potrebbero effettuare imponenti calcoli paralleli: tracciare i modelli di esplosioni nucleari o pattern meteorologici globali, fattorizzare numeri altissimi o trovare i numeri primi di Mersenne, oppure risolvere problemi crittografici.

Tutte queste sono applicazioni più che legittime. E potete visitare distributed.net e scaricare del software che vi permette di donare i cicli inutilizzati del processore del vostro computer ad alcuni di quei progetti (potete dare il vostro contributo alla ricerca di Optimal Golomb Rulers, per esempio, anche se non sapete cosa sono). Avete molti cicli inutilizzati da spartire. E non c’è ragione perché il vostro computer non possa contribuire alla ricerca di vita extraterrestre mentre, per esempio, se ne sta inoperoso in attesa che voi leggiate questo articolo.

Il motivo per cui queste iniziative funzionano è che sono consensuali: nessuno di tali progetti scarica software sul vostro computer a vostra insaputa. Nessuno di tali progetti controlla il vostro computer senza il vostro permesso. Ma vi sono molti programmi che fanno proprio questo.

Il termine utilizzato per definire un computer controllato a distanza da qualcuno è “bot”. Un gruppo di computer (migliaia o anche milioni) controllati da qualcun altro è un bot network. Secondo alcune stime, oggi su internet milioni di computer fanno parte di bot network, e i bot network più grandi sono costituiti da oltre 1,5 milioni di macchine.

Inizialmente, i bot network venivano usati per un solo scopo: attacchi denial-of-service. Gli hacker se ne servivano per attaccare i computer di altri hacker, una guerra tra feudi hacker nel cyberspazio. Il primo uso largamente pubblicizzato di uno strumento distribuito di intrusione (tecnicamente non si trattava di un botnet, ma era praticamente la stessa cosa) avvenne nel febbraio 2000, quando l’hacker canadese Mafiaboy condusse un esercito di computer compromessi per sopraffare CNN.com, Amazon.com, eBay, Dell Computer e altri siti mediante volumi di traffico di rete assolutamente debilitanti. Quella vicenda finì su tutti i giornali.

Di questi tempi, i bot network sono controllati più probabilmente da criminali che non da hacker. La differenza sostanziale è il movente: il guadagno. I network vengono utilizzati per inviare email di phishing e altro spam. Vengono usati per la frode del clic. Oppure come strumento di estorsione: pagate o vi scagliamo contro un attacco DDoS!

Più che altro vengono utilizzati per raccogliere dati personali a scopo di frode, comunemente chiamata "furto di identità". L'attuale software bot non attacca solamente altri computer, ma anche i suoi host. Nel malware sono compresi dei keylogger per sottrarre password e numeri di conto. Infatti, molti bot ricercano automaticamente informazioni finanziarie, e alcuni botnet sono stati costruiti solamente con questa finalità: raccogliere numeri di carte di credito, password di internet banking, account PayPal, ecc., dagli host compromessi.

Anche i frodatori si stanno servendo di bot network per commettere la cosiddetta frode del clic. I sistemi antifrode di Google sono sufficientemente sofisticati da rilevare migliaia di clic da un solo computer; è molto più arduo stabilire se un solo clic proveniente da ogni computer di un bot network costituito da migliaia di macchine è frode o semplice popolarità.

Inoltre, ovviamente, moltissimi bot sono sempre alla ricerca di altri computer che possono venire infettati e aggiunti al bot network. (Un bot network di 1,5 milioni di unità è stato scoperto nei Paesi Bassi lo scorso anno. Il centro di comando è stato smantellato, ma alcuni bot sono ancora attivi e infettano altri computer per poi aggiungerli a questo network ormai defunto).

Gli attuali bot network sono aggiornabili a distanza, per cui gli operatori possono aggiungere nuove funzionalità ai bot in qualsiasi momento, oppure passare da un programma bot a un altro. Gli autori dei bot aggiornano periodicamente i loro botnet durante lo sviluppo, oppure per eludere i rilevamenti di strumenti antivirus e anti-malware.

Un'applicazione dei bot network che non abbiamo ancora visto con molta frequenza è quella di lanciare un worm a rapida diffusione. È stato scritto molto su "flash worm" che possono saturare Internet in 15 minuti o meno. La situazione può ancora peggiorare se 10 mila bot sincronizzano gli orologi e rilasciano il worm nello stesso preciso istante. Perché non abbiamo visto molte operazioni di questo genere? Secondo me perché non vi è alcun guadagno nel farlo.

Non esiste una soluzione vera e propria al problema botnet perché non vi è un unico problema. Vi sono molti bot network diversi fra loro, controllati in modi diversi, costituiti da computer infettati attraverso le più svariate vulnerabilità. In sostanza un bot network non è altro che un aggressore che trae vantaggio da 1) una o più vulnerabilità software, e 2) dall'economia di scala insita nelle reti di computer. È la stessa cosa di un distributed.net o di SETI@home, solo che l'aggressore non chiede prima il vostro permesso.

Finché i computer in rete avranno vulnerabilità (e continueranno ad averne anche nel prossimo futuro), vi saranno dei bot network. È un effetto collaterale naturale di una rete di computer con dei bug.

Questo articolo è originariamente apparso su Wired.com:
<<http://www.wired.com/news/columns/0,71471-0.html>>

Distributed.net:
<<http://www.distributed.net>>

SETI@home:
<<http://setiathome.berkeley.edu>>

MafiaBoy:
<<http://www.infoworld.com/articles/hn/xml/01/01/18/010118hnmafiaboy.html>>

Il bot network da 1,5 milioni di unità:
<<http://www.techweb.com/wire/security/172303160>>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate la vicenda sulla quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

** *** ***** ***** ***** ***** ***** ***** ***** ***** *****

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.
I numeri arretrati sono disponibili all'indirizzo
<<http://www.schneier.com/crypto-gram.html>>.

Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate:
<<http://www.schneier.com/crypto-gram.html>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

La versione italiana è curata da Communication Valley SpA
<http://www.communicationvalley.it/>.

Per iscriversi o cancellarsi andare all'indirizzo
<http://www.cryptogram.it/>.

I numeri arretrati sono disponibili all'indirizzo
<http://www.cryptogram.it/>.

Per informazioni crypto-gram@communicationvalley.it.

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di Counterpane Internet Security, Inc.

Copyright (c) 2006 by Bruce Schneier.