

CRYPTO-GRAM  
15 settembre 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](mailto: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:

Quel che vogliono i terroristi  
Maggiori dettagli sull'arresto dei terroristi nel Regno Unito  
Più di dieci modi per evitare il prossimo 11 settembre  
Il quinto anniversario dell'11 settembre 2001  
Le ristampe di Crypto-Gram  
Educare gli utenti  
Il compromesso di sicurezza uomini/orsi  
Frode legata alla proprietà terriera  
News  
Esiste del software strategico?  
Sanitizzazione dei media e crittografia  
Che cos'è un hacker?  
Le news di Counterpane  
TrackMeNot  
USB Dumper  
Microsoft e FairUse4WM  
Commenti dei lettori

\*\* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \* \*\* \*

Quel che vogliono i terroristi

Il 16 agosto due uomini sono stati scortati fuori da un aereo diretto a Manchester, Inghilterra, perché ad alcuni passeggeri sembravano asiatici o mediorientali, perché sembrava parlassero in arabo, perché indossavano giacche di pelle e stavano consultando i propri orologi da polso, e i passeggeri si sono rifiutati di volare con questi due uomini a bordo. I due sono stati interrogati per parecchie ore e quindi rilasciati.

Il 15 agosto un intero terminal di un aeroporto è stato evacuato perché i cosmetici di un passeggero hanno innescato un falso positivo al test

di esplosivi. Lo stesso giorno, un musulmano è stato fatto scendere da un aereo a Denver perché stava recitando delle preghiere. La Transportation Security Administration ha stabilito che il personale di volo ha reagito in maniera esagerata, tuttavia l'uomo ha dovuto ugualmente passare la notte a Denver prima di poter ritornare a casa il giorno seguente. Il giorno dopo, un terminal dell'aeroporto di Seattle è stato evacuato perché due cani antibomba hanno dato un falso allarme esplosivi.

Il 19 agosto un aereo ha effettuato un atterraggio di emergenza a Tampa, Florida, dopo che l'equipaggio si è insospettito nel constatare che due delle porte dei servizi igienici erano chiuse a chiave. L'aereo è stato esaminato da cima a fondo, ma non è stato trovato nulla. Nel frattempo, un individuo che ha manomesso un rilevatore antincendio in uno dei servizi su un volo diretto a San Antonio è stato liberato dalle accuse di terrorismo, ma solo dopo una perquisizione di casa sua.

Il 16 agosto, durante un volo Londra-Washington, una donna ha avuto un attacco di panico che l'ha resa violenta, per cui l'aereo è stato scortato all'aeroporto di Boston da caccia militari. "La donna aveva con sé della crema per mani e dei fiammiferi, ma non si è trattato di una minaccia terroristica", ha dichiarato il portavoce della TSA dopo l'incidente.

E il 18 agosto un aereo in volo da Londra e diretto in Egitto ha dovuto effettuare un atterraggio di emergenza in Italia dopo che qualcuno ha trovato una minaccia dinamitarda scribacchiata su un sacchetto per il mal d'aria. Sull'aereo non è stato trovato nulla, e nessuno sa da quanto tempo quella nota era presente a bordo.

Adesso fate tutti un bel respiro e ascoltatevi un minuto.

Il fine del terrorismo è provocare terrore, a volte per perpetrare un obiettivo politico, altre volte da puro e semplice odio. Le persone che vengono uccise dai terroristi non sono i bersagli veri e propri, sono danni collaterali. E far saltare aerei, treni, mercati o autobus non è l'obiettivo principale; quella è semplicemente tattica. I veri bersagli del terrorismo siamo tutti noi, i miliardi di persone che non vengono uccise ma che rimangono terrorizzate a causa delle uccisioni. Il vero fine del terrorismo non è l'atto in sé, ma la nostra reazione a esso.

E stiamo facendo esattamente quel che vogliono i terroristi.

Siamo tutti un po' nervosi dopo l'arresto dei 23 sospetti terroristi in Gran Bretagna. Da quanto viene riferito, questi uomini stavano progettando un attacco basato su esplosivo liquido, e sia la stampa che i politici hanno strombazzato la storia fin da subito.

In verità, è piuttosto dubbio che tale piano terroristico avrebbe avuto successo; diversi chimici hanno smontato l'idea sin da quando è diventata di pubblico dominio. Di sicuro i sospettati erano ben lungi dal mettere in pratica il loro piano: nessuno di loro aveva acquistato biglietti aerei, e alcuni non possedevano nemmeno un passaporto.

A prescindere dalla minaccia, nella prospettiva degli aspiranti attentatori gli esplosivi e gli aeroplani erano semplicemente una tattica. Il loro obiettivo era provocare terrore, e vi sono riusciti.

Immaginiamo per un istante che cosa sarebbe successo se avessero fatto saltare dieci aerei. Ci sarebbero stati voli cancellati, un gran caos negli aeroporti, nuovi divieti per quanto concerne il bagaglio a mano, leader mondiali a proporre nuove e più aspre misure di sicurezza, vari atteggiamenti politici e ogni genere di falsi allarmi non appena qualche

individuo un po' teso fosse andato nel panico. In una forma più attenuata, è praticamente quel che sta avvenendo proprio ora.

I nostri uomini politici danno una mano ai terroristi ogni volta che si servono della paura come tattica elettorale. La stampa dà il proprio contributo ogni volta che scrive storie di terrore riguardanti il complotto e la minaccia terroristica. E se ci spaventiamo, se ci facciamo contagiare da quella paura, anche noi contribuiamo. Tutte queste azioni intensificano e ripetono l'operato dei terroristi, e finiscono con l'aumentare l'effetto del loro terrore.

(Non sto affermando che i politici e la stampa sono terroristi, o che sono in parte colpevoli degli attentati terroristici. Non sono così stupido. Ma il terrorismo è un argomento molto più complesso di quel che sembra, e comprenderne le varie cause ed effetti è cruciale per capire come affrontarlo.)

I complotti tutt'altro che plausibili e i falsi allarmi ci danneggiano davvero, in due modi. Non solo innalzano il livello di paura, ma fanno sprecare tempo e risorse che sarebbero meglio spesi contrastando le minacce vere e proprie e aumentando la vera sicurezza. Scommetto che i terroristi stanno ridendo di noi.

Facciamo un altro esempio. Supponiamo per un momento che il governo britannico avesse arrestato i 23 sospettati senza grandi fanfare. Supponiamo che la TSA e le sue controparti europee non avessero attivato sciocche misure di sicurezza aerea come vietare i liquidi. E supponiamo che la stampa non avesse scritto sulla vicenda interminabili fiumi di parole, e che i politici non avessero utilizzato tale evento per ricordare a tutti noi quanto spaventati dovremmo essere. Se avessimo davvero reagito in questo modo, allora i terroristi avrebbero fallito completamente.

È ora di darsi una calmata e di combattere il terrore con anti-terrore. Ciò non significa accettare passivamente il terrorismo. Vi sono cose che il nostro governo può e dovrebbe fare per contrastare il terrorismo, la maggior parte di esse riguarda intelligence e investigazione, e soprattutto non concentrarsi su specifiche trame terroristiche.

Ma il nostro compito è quello di rimanere fermi e risoluti di fronte al terrore, di rifiutare di farci terrorizzare. Il nostro compito è quello di non farci prendere dal panico ogni volta che due musulmani si trovano insieme e consultano i propri orologi. Nel mondo vi sono circa un miliardo di musulmani, dei quali una gran percentuale non è araba, e circa 320 milioni di arabi nel Medio Oriente, e la stragrande maggioranza di essi non sono terroristi. Il nostro compito è quello di pensare in modo critico e razionale, e di ignorare la cacofonia di altri interessi che cercano di sfruttare il terrorismo per far progredire carriere politiche o aumentare l'audience di un certo show televisivo.

La difesa più sicura contro il terrorismo è rifiutare di farsi terrorizzare. Il nostro compito è quello di riconoscere che il terrorismo è solo uno dei rischi che affrontiamo, e non è uno dei più comuni. E il nostro compito è quello di combattere quegli uomini politici che utilizzano la paura come scusa per privarci delle nostre libertà e promuovere messinscene di sicurezza che sprecano solo denaro e non ci rendono affatto più sicuri.

Vari incidenti:

[http://www.dailymail.co.uk/pages/live/articles/news/news.html?in\\_article\\_id=401419&in\\_page\\_id=1770](http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=401419&in_page_id=1770) oppure <http://tinyurl.com/k5njg>  
[http://news.bbc.co.uk/2/hi/uk\\_news/england/5267884.stm](http://news.bbc.co.uk/2/hi/uk_news/england/5267884.stm)  
<http://www.cbsnews.com/stories/2006/08/17/national/main1906433.shtml>





È difficile da organizzare, da pianificare e da eseguire, ed è facilissimo commettere un piccolo errore ed essere presi. Si combini tutto questo con il lavoro della nostra intelligence, che rileva celle terroristiche e blocca i finanziamenti terroristici, e si otterrà una situazione in cui attacchi di grande rilevanza sono assai rari. Per molti versi, il successo dell'11 settembre è stato un'anomalia; vi erano molti punti in cui avrebbe potuto fallire. La ragione principale per cui non si è ancora visto un secondo 11 settembre è che non è così facile come sembra.

Molto del nostro impegno antiterroristico è poco più che una messinscena di sicurezza: contromisure inefficaci che sembrano buone. Dimentichiamoci della guerra al terrore; la difficoltà non sta nell'uccidere o nell'arrestare i terroristi: è nel trovarli. Il terrorismo è un problema delle forze dell'ordine, e deve essere trattato come tale. Per esempio, nessuna delle nostre misure di sicurezza aerea post-11 settembre avrebbe fermato i terroristi dinamitardi londinesi. La lezione di quanto è accaduto a Londra è che le nostre migliori difese sono l'intelligence e l'investigazione. Invece di spendere denaro in sicurezza aerea o nella sicurezza degli stadi (contromisure che ci obbligano a indovinare correttamente un complotto per essere davvero efficaci), faremmo meglio a investire in misure efficaci intrinsecamente, a prescindere da un complotto specifico.

L'intelligence e l'investigazione ci hanno difesi dal terrorismo in passato, e continueranno a farlo in futuro. Se nel 2001 la CIA e l'FBI avessero lavorato meglio nel coordinarsi e nel passarsi informazioni, l'11 settembre sarebbe stato un altro tentativo fallito. La coordinazione è migliorata, e le due agenzie ricevono ora maggiori finanziamenti, ma non basta ancora. Ogni volta che leggiamo dei miliardi spesi per documenti di identità nazionali, o per giganteschi programmi di data mining, o per nuove misure di sicurezza aeroportuale, pensiamo alla quantità di agenti dell'intelligence che quel denaro potrebbe stipendiare. È proprio lì che avremo il maggiore guadagno dal nostro investimento sulla sicurezza.

<http://www.nytimes.com/2006/08/29/business/media/29times.html?ex=1314504000&en=d2eb8d24ef801b5f&ei=5090&partner=rssuserland&emc=rss>  
oppure <http://tinyurl.com/n3lxo>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Il quinto anniversario dell'11 settembre 2001

Mi sono reso conto che molte persone non hanno letto ciò che scrissi alcuni giorni dopo l'11 settembre, né quel che ho scritto un paio di settimane dopo l'evento.

<http://www.schneier.com/crypto-gram-0109.html#1>  
<http://www.schneier.com/crypto-gram-0109a.html>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Le ristampe di Crypto-Gram

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).

Le minacce da trama cinematografica:  
<http://www.schneier.com/crypto-gram-0509.html#1>>

L'uragano Katrina e la sicurezza:  
<http://www.schneier.com/crypto-gram-0509.html#2>>

Le buone pratiche del Trusted Computing:  
<http://www.schneier.com/crypto-gram-0509.html#13>>

La sicurezza alle Olimpiadi:  
<http://www.schneier.com/crypto-gram-0409.html#2>>

Il programma Trusted Traveler:  
<http://www.schneier.com/crypto-gram-0409.html#5>>

La cosiddetta "No-Fly List":  
<http://www.schneier.com/crypto-gram-0409.html#10>>

Incidenti fortuiti e incidenti di sicurezza:  
<http://www.schneier.com/crypto-gram-0309.html#1>>

Worm benigni:  
<http://www.schneier.com/crypto-gram-0309.html#8>>

Numero speciale sull'11 settembre, comprendente articoli sulla sicurezza negli aeroporti, sulla biometrica, sulla crittografia, la steganografia, gli insuccessi dell'intelligence, e sulla protezione della libertà:  
<http://www.schneier.com/crypto-gram-0109a.html>>

L'Esposizione Totale e la Finestra di Esposizione:  
<http://www.schneier.com/crypto-gram-0009.html#1>>

Open Source e sicurezza:  
<http://www.schneier.com/crypto-gram-9909.html#OpenSourceandSecurity>>  
oppure <http://makeashorterlink.com/?U25716849>>

Fattorizzare un numero a 512 bit:  
<http://www.schneier.com/crypto-gram-9909.html#Factoringa512-bitNumber>>  
oppure <http://makeashorterlink.com/?J17752849>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Educare gli utenti

Ho incontrato parecchi utenti, e non sono molto pratici di sicurezza. Potranno essere pratici di fogli di calcolo, di eBay, o di inviare scherzi e barzellette via email, ma non sono dei tecnologi, men che meno esperti in sicurezza. È ovvio che commettano ogni genere di errori di sicurezza. Anch'io ho tentato di educare gli utenti, e concordo sul fatto che sia in gran parte inutile.

Parte del problema è di ordine generazionale. Lo abbiamo visto con ogni tipo di tecnologia: l'elettricità, i telefoni, i forni a microonde, i videoregistratori, i videogiochi. Le generazioni più vecchie si accostano alle tecnologie più recenti con trepidazione, diffidenza e confusione, mentre i bambini che sono cresciuti insieme a queste

tecnologie le comprendono intuitivamente.

Mentre la generazione "più dura a comprendere" alla fine sparirà, noi non entreremo all'improvviso in un'era di sicurezza informatica senza precedenti. Oggi la tecnologia si muove troppo rapidamente: nessuna generazione ha tempo sufficiente a impratichirsi rapidamente in qualcosa.

Qualche mese fa, alcuni ricercatori hanno messo in pratica un esperimento nel distretto finanziario di Londra. Qualcuno, all'angolo di una strada, si è messo a distribuire CD dicendo che si trattava di una promozione speciale per la giornata di San Valentino". Molte persone, fra cui alcune impiegate in importanti workstation bancarie, hanno avviato il programma contenuto nei CD sul loro computer di lavoro. Il programma era benigno: tutto quel che faceva era informare alcuni computer via Internet della propria attivazione, ma avrebbe potuto benissimo essere malevolo. I ricercatori hanno concluso che agli utenti la sicurezza non importa. Non è affatto vero. Agli utenti la sicurezza importa eccome, solo che non la comprendono.

Non vedo un fallimento nell'educazione, se mai nella tecnologia. Non avrebbe dovuto essere possibile per quegli utenti far girare quel CD, né per un programma qualsiasi inserito nel computer di una banca "chiamare casa" attraverso Internet.

Il vero problema è che i computer non funzionano bene. L'industria ha convinto tutti del fatto che oggi sia necessario un computer per sopravvivere, e allo stesso tempo ha creato computer talmente complicati che soltanto un esperto può effettuare la manutenzione.

Se provo a riparare il sistema di riscaldamento di casa mia, probabilmente violerò ogni genere di norma di sicurezza. Non ho esperienza per queste cose, e onestamente cercare di educarmi in questi ambiti è inutile. Ma il sistema di riscaldamento di casa mia funziona benissimo senza che io debba imparare ogni cosa sul suo funzionamento. So come regolare il termostato, e so di dover chiamare un tecnico nel caso qualcosa si guasti.

La punizione non è un'alternativa all'educazione; è una forma di educazione, molto molto primitiva che si può applicare ai bambini e agli animali (e gli esperti non sono molto convinti della sua applicazione sui bambini). Io dico, smettiamola di punire le persone per errori e fallimenti della tecnologia. Occorre esigere che le aziende mettano sul mercato hardware e software sicuri.

Questo articolo è originariamente apparso nel numero di aprile 2006 di Information Security Magazine come seconda parte di un "botta e risposta" con Marcus Ranum. Potete leggere la parte di Marcus qui: [http://www.ranum.com/security/computer\\_security/editorials/point-counte](http://www.ranum.com/security/computer_security/editorials/point-counte) [rpoint/users.html](http://www.ranum.com/security/computer_security/editorials/point-counte/rpoint/users.html) oppure <http://tinyurl.com/pgyp4>

\*\* \*\* \*

Il compromesso di sicurezza uomini/orsi

Mi piace questo esempio tratto da SlashDot: "Negli anni Ottanta, lo Yosemite National Park stava avendo un grosso problema con gli orsi: vagavano nei campeggi e si mettevano a rovistare nei bidoni dell'immondizia. Questo rappresentava un rischio per gli orsi e per le persone. Allora il Servizio del Parco cominciò a installare bidoni dell'immondizia corazzati e difficili da aprire: bisognava far ruotare



tm>

oppure <http://tinyurl.com/mgjyd>

Un libro del 1963 dell'FBI sull'acquisizione di impronte digitali, con un'introduzione di J. Edgar Hoover, è online sul sito Project Gutenberg. <http://www.gutenberg.org/files/19022/19022-h/19022-h.htm>

È possibile comprarne una copia cartacea qui:

<http://www.antiqubook.com/boox/cro/7958.shtml>

Una storia che risale al 2001: individui travestiti da addetti al censimento australiano raccolgono informazioni personali per scopi fraudolenti.

<http://www.abs.gov.au/AUSSTATS/abs@.nsf/mediareleasesbyReleaseDate/3E186C63E6E7F176CA256AA200237AF8?OpenDocument> oppure

<http://tinyurl.com/qftxy>

L'età di questa vicenda è ciò che la rende ancor più interessante.

Questo è il tipo di tattica per un furto di identità che mi sarei aspettato di vedere in atto quest'anno, dato che i criminali sono diventati sempre più sofisticati. Mi sorprende che stessero facendo cose del genere anche cinque anni fa.

"Ten Worst Privacy Debacles of All Time" [I dieci peggiori disastri in ambito di privacy che la storia ricordi]. Come elenco non è male.

<http://www.wired.com/news/politics/privacy/0,71622-0.html>

I commenti di Daniel Solove:

[http://www.concurringopinions.com/archives/2006/08/the\\_ten\\_greates.html](http://www.concurringopinions.com/archives/2006/08/the_ten_greates.html)  
>

"You are what you say: privacy risks of public mentions" [Sei ciò che dici: i rischi di privacy delle citazioni pubbliche], Atti della XXIX Annual International ACM SIGIR Conference on Research and Development in Information Retrieval [Ricerca e Sviluppo nella Raccolta di Informazioni], 2006.

<http://portal.acm.org/citation.cfm?doid=1148170.1148267>

<http://www-users.cs.umn.edu/~dfrankow/files/privacy-sigir2006.pdf>

Kobi Alexander ha abbandonato gli Stati Uniti dieci giorni fa. È stato individuato nello Sri Lanka per una chiamata telefonica effettuata con Skype. Ars Technica spiega: "L'ex CEO fuggiasco probabilmente si era fatto convincere di essere irrintracciabile utilizzando Skype, ma egli (e tutti quelli che credono che il VoIP sia intrinsecamente più sicuro di una normale linea telefonica terrestre) si sbagliava. Tracciare traffico VoIP peer-to-peer anonimo su Internet è possibile. Lo si può fare persino se i due interlocutori hanno preso qualche precauzione per mascherare il traffico". Che questo serva da monito a tutti coloro che credevano che Skype fosse anonimo.

<http://www.haaretz.com/hasen/spages/754476.html>

<http://arstechnica.com/news.ars/post/20060824-7582.html>

<http://ise.gmu.edu/~xwangc/Publications/CCS05-VoIPTracking.pdf>

Intervento di Stepher Colbert sul proteggere il proprio computer:

[http://www.comedycentral.com/shows/the\\_colbert\\_report/videos/season\\_2/index.jhtml?playVideo=72869&rspartner=rssfofReduxx](http://www.comedycentral.com/shows/the_colbert_report/videos/season_2/index.jhtml?playVideo=72869&rspartner=rssfofReduxx) oppure

<http://tinyurl.com/pz4o4>

[http://www.comedycentral.com/shows/the\\_colbert\\_report/videos/season\\_2/index.jhtml?playVideo=72870&rspartner=rssfofReduxx](http://www.comedycentral.com/shows/the_colbert_report/videos/season_2/index.jhtml?playVideo=72870&rspartner=rssfofReduxx) oppure

<http://tinyurl.com/qjq4w>

Sono aperte le nomination per lo Stupid Security Award:

[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-541996](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-541996)  
>

oppure <http://tinyurl.com/hhgzf>

Una truffa per ottenere numeri di carte di credito grazie alla deviazione di chiamata:

[http://www.schneier.com/blog/archives/2006/08/call\\_forwarding\\_1.html](http://www.schneier.com/blog/archives/2006/08/call_forwarding_1.html)

Una storia di statistica e sicurezza sulla Seconda Guerra Mondiale: stimare il numero di carri armati prodotti dai tedeschi.

<http://www.guardian.co.uk/g2/story/0,,1824525,00.html>

"Il Temibile Pirata Bin Ladin" sostiene che, legalmente, i terroristi dovrebbero essere trattati come pirati per quanto concerne la legge internazionale:

[http://www.legalaffairs.org/issues/July-August-2005/feature\\_burgess\\_jul\\_aug05.msp](http://www.legalaffairs.org/issues/July-August-2005/feature_burgess_jul_aug05.msp) oppure <http://tinyurl.com/am9a9>

"Security Engineering" di Ross Anderson è un gran libro. E non sto dicendo questo perché ho scritto la prefazione. Da quando è stato pubblicato nel 2001, l'ho sempre consigliato agli ingegneri interessati alla sicurezza. E fin qui nessuna novità. La novità è che ora è possibile scaricare il libro, gratuitamente e legalmente.

<http://www.cl.cam.ac.uk/~rja14/book.html>

Alcune notizie sul profiling comportamentale come misura antiterrorismo:

[http://www.schneier.com/blog/archives/2006/08/behavioral\\_prof.html](http://www.schneier.com/blog/archives/2006/08/behavioral_prof.html)

E il profiling comportamentale ha reso possibile la cattura di Warren Jeffs:

[http://www.schneier.com/blog/archives/2006/08/behavioral\\_prof\\_2.html](http://www.schneier.com/blog/archives/2006/08/behavioral_prof_2.html)

Non usate Browzar:

<http://web3.0log.org/2006/09/01/new-secure-browser-browzar-is-fake-and-full-of-adware/> oppure <http://tinyurl.com/q7pxy>

Un esperto di antiterrorismo ha dichiarato di aver introdotto di nascosto una bomba su un aereo, per due volte. Poi ha ritrattato. Per quanto posso dire, è un idiota.

[http://www.schneier.com/blog/archives/2006/09/man\\_claims\\_to\\_h.html](http://www.schneier.com/blog/archives/2006/09/man_claims_to_h.html)

Moltissime vignette sulla sicurezza negli aeroporti:

[http://www.schneier.com/blog/archives/2006/09/airport\\_securit\\_1.html](http://www.schneier.com/blog/archives/2006/09/airport_securit_1.html)

Questa è una lettura assolutamente fondamentale per chiunque sia interessato alle modalità con cui gli Stati Uniti stanno perseguendo il terrorismo. Retorica e pose a parte, questo è ciò che sta realmente accadendo. Il TRAC (Transactional Records Access Clearinghouse) raccoglie tali informazioni osservando i registri del Dipartimento di Giustizia. Questa organizzazione di ricerca dati è connessa alla Syracuse University, e sta portando avanti tale compito (tener traccia di ciò che le agenzie federali fanno davvero, e non di quel che dicono di fare) da più di quindici anni.

<http://trac.syr.edu/tracreports/terrorism/169/>

Mi diverte soprattutto la risposta del Dipartimento di Giustizia, che sostanzialmente scredita lo studio senza offrire critiche reali:

<http://www.detnews.com/apps/pbcs.dll/article?AID=/20060904/NATION/609040358/> oppure <http://tinyurl.com/r3s2b>

Le persone vendono, regalano e buttano i propri telefoni cellulari senza nemmeno pensare ai dati che ancora contengono:

<http://www.cnn.com/2006/TECH/ptech/08/30/betrayed.byacellphone.ap/index.html>

oppure <http://tinyurl.com/z5a73>

In misura sempre maggiore, le nostre informazioni non sono realmente sotto il nostro controllo. Le archiviamo in dispositivi e siti web di terze parti, o nel nostro computer. Cerchiamo di cancellarle, ma non vi riusciamo davvero. Cerchiamo di controllarne la diffusione, ma è sempre

più difficile.

La California sta per proteggere le reti wireless mediante etichette informative:

[http://www.theregister.co.uk/2006/09/04/wi-fi\\_warnings\\_legislated/](http://www.theregister.co.uk/2006/09/04/wi-fi_warnings_legislated/)

Un servizio di prima pagina di Business Week dell'agosto 2005 sullo "Stato della Sorveglianza":

[http://www.businessweek.com/magazine/content/05\\_32/b3946001\\_mz001.htm](http://www.businessweek.com/magazine/content/05_32/b3946001_mz001.htm)

Un articolo di CIO Insight sulla fine della privacy:

<http://www.cioinsight.com/article2/0,1540,2012398,00.asp>

Ed ecco il mio intervento sul futuro della privacy ("The Future of Privacy").

[http://www.schneier.com/blog/archives/2006/03/the\\_future\\_of\\_p.html](http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html)

Bomba o no? Potete individuare la bomba?

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

Per restare in argomento, ecco un tizio che è riuscito a passare il checkpoint di sicurezza con un vibratore in funzione nascosto nei pantaloni.

[http://www.zug.com/gab/index.cgi?func=view\\_thread&thread\\_id=68619](http://www.zug.com/gab/index.cgi?func=view_thread&thread_id=68619)

Vi è anche un video divertente su Dutch TV. Uno screener esamina la borsa di un passeggero, mettendo da parte svariati sacchetti chiaramente contenenti cocaina, per ammonirlo in merito a una piccola limetta per le unghie.

<http://ul.peersphere.net/cas/controller/Luchthaven.mpg?livelinkDataID=1446471>

oppure <http://tinyurl.com/zlqrv>

Qui è possibile comprare materiale confiscato al Boston Logan Airport.

Ho anche letto da qualche parte che molti oggetti finiscono su eBay.

[http://www.boston.com/business/articles/2006/09/04/banned\\_items\\_find\\_new\\_home\\_in\\_discount\\_bin/](http://www.boston.com/business/articles/2006/09/04/banned_items_find_new_home_in_discount_bin/) oppure <http://tinyurl.com/gS735>

E infine Quinn Norton ha detto: "Credo che qualcuno dovrebbe provare a far saltare un aereo con un frammento di tessera di identità, solo per veder implodere la mente della TSA".

<http://www.ambiguous.org/archive.php3/2006/08/31#quinn2006831.1>

Il presidente della Hewlett-Packard, sempre più infastidito dalle fughe di notizie, ha assunto degli investigatori per intercettare i registri delle chiamate telefoniche (comprese quelle dal telefono di casa e dal cellulare) degli altri membri della dirigenza HP. Uno di essi si è dimesso a seguito di questo provvedimento. Il responsabile delle fughe di notizie si è rifiutato di dimettersi, malgrado sia stato espulso. Si noti che l'articolo riporta che gli investigatori si sono serviti del "pretexting", che è un metodo illegale.

<http://www.msnbc.msn.com/id/14687677/site/newsweek/>

[http://riskman.typepad.com/perilocity/2006/09/does\\_hp\\_have\\_an.html](http://riskman.typepad.com/perilocity/2006/09/does_hp_have_an.html)

[http://news.com.com/Leak+scandal+costs+HPs+Dunn+her+chairmans+job/2100-1014\\_3-6114655.html](http://news.com.com/Leak+scandal+costs+HPs+Dunn+her+chairmans+job/2100-1014_3-6114655.html) oppure <http://tinyurl.com/pu286>

La polizia perde del Semtex durante una prova. Oops. Sono soltanto otto onces (circa 230 grammi), certo, però...

[http://www.boston.com/news/globe/city\\_region/breaking\\_news/2006/09/state\\_police\\_lo.html](http://www.boston.com/news/globe/city_region/breaking_news/2006/09/state_police_lo.html) oppure <http://tinyurl.com/r9ak5>

Spionaggio digitale per le masse:

<http://www.nytimes.com/2006/09/07/fashion/07spy.html?ex=1315281600&en=c48cca6a35e9bd22&ei=5090&partner=rssuserland&emc=rss>

oppure <http://tinyurl.com/ovoyu>

Appunti dallo Hash Function Workshop:

[http://www.schneier.com/blog/archives/2006/09/notes\\_from\\_the.html](http://www.schneier.com/blog/archives/2006/09/notes_from_the.html)

La "Casa più sicura in assoluto". Uno scherzo oppure no?

[<http://ultimatesecurehome.com/>](http://ultimatesecurehome.com/)

[<http://www.schneier.com/blog/archives/2006/09/ultimate\\_secure.html>](http://www.schneier.com/blog/archives/2006/09/ultimate_secure.html)

Pare che gli ufficiali di dogana del Sudan stiano sequestrando i computer portatili di chiunque entri nel paese e controllino i dati contenuti nell'hard disk. Malgrado la motivazione addotta sia la pornografia, chiunque porti un computer all'interno del paese dovrebbe preoccuparsi di eventuali informazioni personali, di scritti che possano essere considerati politici dalle autorità sudanesi, informazioni di lavoro confidenziali, e così via.

[<http://edition.cnn.com/2006/WORLD/africa/08/30/sudan.crackdown.reut/index.html>](http://edition.cnn.com/2006/WORLD/africa/08/30/sudan.crackdown.reut/index.html)

oppure [<http://tinyurl.com/pdag7>](http://tinyurl.com/pdag7)

[<http://ngosecurity.blogspot.com/2006/09/incident-laptop-seizures-sudan.html>](http://ngosecurity.blogspot.com/2006/09/incident-laptop-seizures-sudan.html)

oppure [<http://tinyurl.com/lla8b>](http://tinyurl.com/lla8b)

Questo dovrebbe essere motivo di preoccupazione a prescindere dalla frontiera che si oltrepassa. I nostri diritti di privacy quando si entra in un paese straniero sono assai ridotti, e questo genere di cose potrebbe accadere ovunque. (Ho sentito vari aneddoti secondo cui Israele farebbe altrettanto, ma non ci sono conferme). Se avete con voi un portatile quando giungete a una frontiera internazionale, dovrete cancellare i file non strettamente necessari e criptare tutto il resto.

La Turing Bombe ricreata a Bletchley Park:

[<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/09/07/nbletchley07.xml>](http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/09/07/nbletchley07.xml) oppure [<http://tinyurl.com/mg6fw>](http://tinyurl.com/mg6fw)

Dei ladri aggirano un sistema d'allarme. Tattica intelligente di cui ho parlato in "Beyond Fear":

[<http://www.schneier.com/blog/archives/2006/09/burglars\\_foil\\_a.html>](http://www.schneier.com/blog/archives/2006/09/burglars_foil_a.html)

Uno studio del CATO Institute: "Doublespeak and the War on Terrorism" [Il 'doublespeak' e la guerra al terrorismo] (il termine doublespeak indica un linguaggio deliberatamente costruito per camuffare o distorcere il suo reale significato, ndt):

[<http://www.cato.org/pub\\_display.php?pub\\_id=6654>](http://www.cato.org/pub_display.php?pub_id=6654)

Manomettere una fotocopiatrice a monete con un fermaglio:

[<http://www.instructables.com/id/EW8JTRWKO9ERIE1UQD/>](http://www.instructables.com/id/EW8JTRWKO9ERIE1UQD/)

Un articolo sullo spionaggio industriale. Molti sensazionalismi, ma comunque interessante:

[<http://news.bbc.co.uk/2/hi/technology/5313772.stm>](http://news.bbc.co.uk/2/hi/technology/5313772.stm)

Ed Felten e il suo team a Princeton hanno analizzato una macchina per il voto elettronico Diebold AccuVote-TS, e hanno scoperto ogni genere di vulnerabilità. Sono stati in grado di introdurre un virus che cambia i voti e che si propaga automaticamente da macchina a macchina. Sorprendente. Diebold, com'è ovvio, finge che non vi sia alcun problema.

[<http://itpolicy.princeton.edu/voting/>](http://itpolicy.princeton.edu/voting/)

Video della dimostrazione:

[<http://itpolicy.princeton.edu/voting/videos.html>](http://itpolicy.princeton.edu/voting/videos.html)

[<http://www.salon.com/opinion/feature/2006/09/13/diebold/index.html>](http://www.salon.com/opinion/feature/2006/09/13/diebold/index.html)

[<http://arstechnica.com/news.ars/post/20060913-7735.html>](http://arstechnica.com/news.ars/post/20060913-7735.html)

[<http://www.msnbc.msn.com/id/14825465/>](http://www.msnbc.msn.com/id/14825465/)

[<http://www.computerworld.com/blogs/node/3475>](http://www.computerworld.com/blogs/node/3475)

"The Onion" sulle sviste della sicurezza negli aeroporti:

[<http://www.theonion.com/content/node/52333>](http://www.theonion.com/content/node/52333)

E una vignetta sulla crittografia:

<http://xkcd.com/c153.html>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Esiste del software strategico?

Se si definisce "infrastruttura critica" come "insieme di cose essenziali per il funzionamento di una società e di una economia", allora il software è un'infrastruttura critica. Per molte aziende e singoli individui, se i loro computer smettono di funzionare, loro smettono di lavorare.

È una situazione in cui siamo finiti quasi senza accorgercene. Tutti sapevano che il software che pilota i 747 o che intercetta i missili era critico, ma chi pensava ai computer di peso e bilanciamento delle linee aeree, o al sistema operativo in cui girano i database e i fogli di calcolo che determinano quali missili vengano trasportati dove?

E negli anni, del software comune, pronto all'uso, di livello personale o aziendale è stato utilizzato per applicazioni sempre più critiche. Oggi ci troviamo in una situazione per cui una falla ben posizionata in Windows, nei router Cisco o in Apache potrebbe danneggiare seriamente l'economia.

È perfettamente razionale presupporre che alcuni programmatori, una ridotta minoranza, ne sono certo, aggiungano intenzionalmente delle vulnerabilità e delle backdoor nel codice che scrivono. In effetti sono piuttosto sorpreso dal fatto che le backdoor aggiunte segretamente da CIA/NSA, MI5, dai cinesi, dal Mossad, e da altri non entrino in conflitto tra loro. Anche se questi gruppi non stanno infiltrandosi in aziende di software con backdoor, potete star certi che stanno setacciando i prodotti cercando vulnerabilità che possono sfruttare, se necessario. D'altro canto, stiamo già vivendo in un mondo dove decine di nuove vulnerabilità vengono scoperte in comuni prodotti software con cadenza settimanale, e tuttavia l'economia procede tranquillamente. Ma non stiamo parlando del worm del mese proveniente dall'Asia o di un nuovo software di phishing creato dalla Mafia russa: qui si parla di organizzazioni di intelligence nazionali. "Infowar" è un termine ormai abusato, ma la prossima guerra avrà una componente cyberspaziale, e queste organizzazioni non starebbero facendo il proprio mestiere se non si stessero preparando per un tale scenario.

Marcus [Ranum] ha ragione al 100% quando dice che è semplicemente troppo tardi per farci qualcosa. L'industria del software è internazionale, e nessun paese può iniziare a esigere software solamente locale e sperare di ottenere qualche risultato. Né sarebbe una soluzione al problema, che ha più a che vedere con la fedeltà di milioni di singoli programmatori che non con il paese in cui vivono.

Che fare, dunque? Il punto chiave qui è tener presente il problema vero: le attuali pratiche relative al software commerciale non sono sufficientemente sicure per rilevare in maniera affidabile e cancellare eventuale codice malevolo inserito intenzionalmente. Una volta compreso questo, si lasceranno perdere gli argomenti fuorvianti che hanno portato CheckPoint a non essere in grado di comprare Sourcefire e ci si concentrerà sulla soluzione vera e propria: una difesa in profondità.

In teoria, il software di sicurezza è una soluzione improvvisata post factum, perché il sistema operativo e le applicazioni sottostanti sono pieni di vulnerabilità. Se il vostro software fosse scritto in maniera appropriata, non avreste bisogno di un firewall, no?

Se prendessimo sul serio la questione dell'infrastruttura critica, riconosceremmo che ogni cosa è critica e inizieremmo a costruire del software di sicurezza per proteggerla. Realizzeremmo la nostra sicurezza basandoci sui principi del fallimento protetto, ovvero assumere che la sicurezza può venir meno e assicurarsi che tutto vada per il meglio quando ciò accade. Ci serviremmo della difesa in profondità e della divisione in compartimenti per ridurre gli effetti di un eventuale fallimento. Sostanzialmente, faremmo tutto ciò che dovremmo fare ora per proteggere le nostre reti.

Sarebbe molto costoso, forse a livelli proibitivi. Forse sarebbe più facile ignorare il problema, o per lo meno gestire la geopolitica in modo che nessun esercito nazionale voglia abbatteerci.

Questo articolo è originariamente apparso nel numero di settembre 2006 di Information Security Magazine come seconda parte di un "botta e risposta" con Marcus Ranum. Potete leggere la parte di Marcus qui: [http://www.ranum.com/security/computer\\_security/editorials/point-counterpoin/strategic.html](http://www.ranum.com/security/computer_security/editorials/point-counterpoin/strategic.html) oppure <http://tinyurl.com/nmask>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

#### Disinfezione dei media e crittografia

La scorsa settimana il NIST ha pubblicato la Special Publication 800-88, "Guidelines for Media Sanitization" [Linee guida per la disinfezione dei media].

Vi è un nuovo paragrafo in questo documento (pagina 7) che non era presente nella bozza originale: "La crittografia non è un mezzo di disinfezione generalmente accettato. La potenza sempre maggiore dei computer riduce il tempo necessario a decifrare il testo cifrato e perciò non è possibile assicurare l'impossibilità di recuperare informazioni crittografate".

Devo ammettere che per me tutto questo non ha senso. Se la crittografia viene effettuata in modo appropriato, e se la chiave viene adeguatamente scelta, allora cancellare la chiave e tutte le copie equivale a cancellare i file. E se si sta utilizzando una crittografia estesa a tutto il volume, allora cancellare la chiave equivale a disinfettare il disco. Se ciò non è vero, vuol dire che il programma di crittografia non è sicuro.

Credo che il NIST sia solo un po' confuso.

<http://csrc.nist.gov/publications/nistpubs/#sp800-88>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

#### Che cos'è un hacker?

Un hacker è una persona che pensa in modo creativo. È una persona che rigetta le credenze convenzionali per fare qualcosa di completamente diverso. È un individuo che osserva un limite e si chiede che cosa vi è oltre. È un individuo che considera un insieme di regole e si chiede che cosa succede a non seguirle. Un hacker è qualcuno che sperimenta i limiti dei sistemi per curiosità intellettuale.

Ho scritto quest'ultima frase nel 2000, nel mio libro "Beyond Fear", e confermo tale definizione.

In "Beyond Fear" ho anche scritto:

"Gli hacker sono vecchi quanto è vecchia la curiosità, anche se il termine è moderno. Galileo era un hacker. Anche Madame Curie lo era. Aristotele no. (Aristotele aveva una qualche prova teorica per cui le donne avevano meno denti degli uomini. Un hacker avrebbe semplicemente contato i denti di sua moglie. Un buon hacker avrebbe contato i denti di sua moglie senza che lei se ne accorgesse. Un buon pessimo hacker ne avrebbe estratti alcuni, per provare il suo punto di vista).

"Quando ero al college, conoscevo un gruppo di ragazzi simili agli hacker: i cosiddetti 'key freaks'. Ricercavano l'accesso totale, e il loro obiettivo era avere una chiave per ogni serratura del campus. Studiavano le tecniche di manomissione delle serrature e ne imparavano di nuove, si scambiavano le mappe dei condotti di aerazione e di dove conducevano, nonché copie delle chiavi che ottenevano. Una porta chiusa era una sfida, un affronto personale alla loro abilità. Queste persone non avevano intenzione di fare danni o torti, il loro scopo non era rubare, anche se avrebbero potuto farlo. Il loro hobby consisteva nel poter andare dovunque volessero.

"Si ricordino i 'phone phreaks' di qualche tempo fa, quelli che potevano fischiare in un telefono pubblico ed effettuare chiamate gratis. Certo, rubavano servizio telefonico. Ma non è che avessero bisogno di fare chiamate di otto ore a Manila o McMurdo. Il loro vero obiettivo era la conoscenza segreta: la rete telefonica era un enorme labirinto di informazioni. Volevano conoscere il sistema meglio di chi lo aveva progettato, e volevano avere la capacità di modificarlo a piacimento. Comprendere il funzionamento del sistema telefonico, quello era il vero trofeo. Altri fra i primi hacker erano gli appassionati di radiocomunicazioni e di trenini elettrici.

"Richard Feynman era un hacker: leggete i suoi libri.

"Gli hacker informatici seguono questa direzione evolutiva. O meglio, sono lo stesso gene che opera in un sistema nuovo. I computer, e le reti in particolare, sono il nuovo territorio da esplorare. Le reti offrono il più grande labirinto di condotti di aerazione, in cui una nuova tecnica di hacking diventa una chiave che può aprire un computer dopo l'altro. E al suo interno vi è la conoscenza, la sapienza. L'accesso. Come funzionano le cose. Perché funzionano. È tutto là fuori, in attesa di essere scoperto".

I computer sono il luogo di svago perfetto per gli hacker. I computer e le reti di computer sono tesori di conoscenza segreta. Internet è un immenso territorio di informazioni da scoprire. Più si conosce, più cose si possono fare.

E non dovrebbe sorprendere che molti hacker abbiano concentrato le proprie abilità sulla sicurezza informatica. Non solo è spesso l'ostacolo che separa un hacker dalla conoscenza, e quindi qualcosa da sconfiggere, ma occorre aggiungere che la forma mentis necessaria per eccellere nella sicurezza è proprio la stessa che possiedono gli hacker: pensare in modo creativo, non rispettare le regole, esplorare i limiti di un sistema. Il modo più semplice per sconfiggere un sistema di sicurezza è scoprire ciò a cui non hanno pensato i progettisti di quel sistema. Questo è lo hacking nell'ambito della sicurezza.

Gli hacker giocano sporco. E per violare la sicurezza si gioca sempre sporco. Scoprire la chiave RSA di una smart card osservando le

fluttuazioni di energia, perché chi ha ideato la card non si è mai reso conto che qualcuno avrebbe potuto fare una cosa del genere. Auto-firmare una porzione di codice, perché il sistema di verifica della firma non pensava che qualcuno avrebbe potuto fare un simile tentativo. Utilizzare una parte di un protocollo per violarne uno completamente diverso, perché tutte le precedenti analisi di sicurezza hanno sempre considerato i protocolli individualmente invece che a coppie.

Questo è hacking nella sicurezza: penetrare in un sistema pensando in modo differente.

Suona tutto assai criminoso: recuperare testo crittografato, ingannare algoritmi di firma, violare protocolli. Ma onestamente è soltanto il gergo di noi esperti di sicurezza. Lo hacking non è criminoso. Tutti gli esempi elencati nel paragrafo precedente sono stati effettuati da rispettati professionisti di sicurezza, e sono stati tutti presentati a conferenze di sicurezza.

Ricordo una conversazione a una Crypto conference, agli inizi della mia carriera. Avvenne fuori, fra gamberoni, fragole ricoperte di cioccolato e altre golosità. Un gruppo di noi esperti stava parlando di un certo sistema crittografico, e fra i presenti c'era Brian Snow della NSA. Qualcuno descrisse un attacco non convenzionale, che non seguiva affatto le solite regole della crittanalisi. Non ricordo i particolari, ma ricordo come reagii dopo aver sentito la descrizione dell'attacco.

"Così vuol dire imbrogliare", dissi.

Perché era proprio così.

Ricordo anche come Brian si girò verso di me. Non disse nulla, ma il suo sguardo parlava chiaramente. "In questo lavoro non esiste il concetto di imbrogliare".

Perché davvero non esiste.

Hacking significa imbrogliare, giocare sporco, ed è il sistema per migliorare nel campo della sicurezza. È solo quando qualcuno inventa un nuovo attacco che il resto di noi può scoprire come difendersi contro di esso.

Per anni mi sono rifiutato di giocare con la semantica di "hacker" contro "cracker". Vi sono ottimi hacker e pessimi hacker, proprio come vi sono ottimi elettricisti e pessimi elettricisti. "Hacker" è una forma mentale e un insieme di capacità; come si impiegano tali capacità è un altro discorso.

E credo che i migliori esperti di sicurezza informatica possiedano la forma mentis dell'hacker. Quando devo assumere nuovi impiegati, cerco qualcuno che, entrando in un negozio, non possa fare a meno di pensare a un modo per rubacchiare. Cerco qualcuno che non possa fare a meno di testare un programma di sicurezza informatica senza provare ad aggirarlo. Cerco qualcuno che, quando gli si dice che le cose funzionano in un certo modo, mi chieda immediatamente in che modo le cose smettono di funzionare se si fa qualcos'altro.

Abbiamo bisogno di queste persone nel campo della sicurezza, e abbiamo bisogno che stiano dalla nostra parte. I criminali sono sempre alla ricerca di nuovi metodi per violare i sistemi di sicurezza. Si implementi un nuovo sistema (uno sportello bancomat, un sistema di internet banking, una macchina per il gioco d'azzardo) e i criminali cercheranno di trarne profitti illeciti. E alla fine scopriranno come farlo, perché alcuni hacker sono anche dei criminali. Ma se abbiamo

degli hacker che lavorano per noi, lo scopriranno per primi e quindi potremo difenderci.

È la nostra unica speranza per la sicurezza in questo modo tecnologico che si muove sempre più velocemente.

Questo intervento è apparso nel numero dell'estate 2006 di "2600".

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Le news di Counterpane

Counterpane ha un nuovo servizio di application security assessment:  
<<http://www.counterpane.com/application-security-assessment.html>>

Schneier interverrà in teleconferenza alla Hack-in-the-Box Conference, a Kuala Lumpur in Malaysia il 20 settembre:  
<<http://conference.hitb.org/hitbsecconf2006kl/>>

Schneier parlerà alla University of Southern California a Los Angeles il 26 settembre:  
<<http://netzoo.net/cpd/schneier.html>>

Schneier interverrà alla cena del Presidente del Consiglio della ACLU National Capital Area a Washington DC il 27 settembre.

Schneier parlerà alla Michigan Technical University, a Houghton, Michigan, il 2 ottobre.  
<<http://www.greatevents.mtu.edu/geseason/04.html>>

Schneier parlerà ai Sandia National Laboratories a Livermore, California, il 5 ottobre.

Schneier interverrà a "Security Takes Off" a Malmoe, Svezia, il 9 ottobre.  
<<http://www.dfs.se/kretsar/sodra>>

Schneier interverrà all'Information Security Solutions Europe a Roma il 10 ottobre.  
<<http://www.eema.org/static/isse/budapest.htm>>

Schneier è stato intervistato per il podcast di Martin McKeay sulla sicurezza.  
<[http://www.mckeay.net/secure/2006/08/network\\_security\\_podcast\\_episo\\_35.html](http://www.mckeay.net/secure/2006/08/network_security_podcast_episo_35.html)>  
oppure <<http://tinyurl.com/mxkfe>>

"Cose da sapere su Bruce Schneier":  
<<http://geekz.co.uk/schneierfacts/>>  
Alcune sono molto divertenti. E no, non ho contribuito alla loro realizzazione.

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

TrackMeNot

A seguito della pubblicazione di informazioni di ricerca da parte di AOL e dell'articolo del New York Times che dimostra quanto sia semplice scoprire chi ha effettuato le ricerche, ecco TrackMeNot:

"TrackMeNot gira in Firefox come processo in background a bassa priorità e periodicamente avvia delle query di ricerca assolutamente casuali nei motori di ricerca più diffusi: AOL, Yahoo!, Google e MSN. Nasconde le vere ricerche dell'utente in una nuvola di ricerche 'fantasma' indistinguibili, rendendo difficile, se non impossibile, aggregare tali informazioni per definire il profilo accurato e inequivocabile di un determinato utente. TrackMeNot si integra nel menu 'Tools' di Firefox e comprende svariate opzioni configurabili dall'utente".

Facciamo una lista dei modi per cui tutto ciò non funziona.

1) Non nasconde le vostre ricerche. Se il governo vuole sapere chi ha cercato i "centri di arruolamento di al Qaeda", non importa che voi abbiate effettuato altre diecimila ricerche: verrete individuati.

2) È troppo facile da individuare. Vi sono solamente 1.673 termini di ricerca nel dizionario del programma. Ecco, a titolo di esempio, le parole che iniziano per "G": gag, gagged, gagging, gags, gas, gaseous, gases, gassed, gasses, gassing, gen, generate, generated, generates, generating, gens, gig, gigs, gillion, gillions, glass, glasses, glitch, glitched, glitches, glitching, glob, globed, globing, globs, glue, glues, gnarlier, gnarliest, gnarly, gobble, gobbled, gobbles, gobbling, golden, goldener, goldenest, gonk, gonked, gonking, gonks, gonzo, gopher, gophers, gorp, gorps, gotcha, gotchas, gribble, gribbles, grind, grinding, grinds, grok, grokked, grokking, groks, ground, grovel, groveled, groveling, grovelled, grovelling, grovels, grue, grues, grunge, grunges, gun, gunned, gunning, guns, guru, gurus.

Gli autori del programma sostengono che questo elenco è temporaneo, e che vi sarà presto un server TrackMeNot con una lista di termini in continuo cambiamento. Ovviamente, tale lista può essere monitorata da qualsiasi programma di analisi; stesso dicasi delle query effettuate verso tale server.

In ogni caso, ogni dodici secondi (puntualmente) il programma sceglie a caso una coppia di termini e la invia ad AOL, o a Yahoo, o a MSN, o a Google. Secondo me le vostre ricerche contengono più di due parole, non le inviate a intervalli precisi di dodici secondi, e utilizzate un solo motore di ricerca preferito.

3) Alcune delle ricerche del programma sono persino peggiori di quelle che potreste effettuare voi. Altre parole comprese nel dizionario sono infatti: HIV, atomic, bomb, bible, bibles, bombing, bombs, boxes, choke, choked, chokes, choking, chain, crackers, empire, evil, erotics, erotices, fingers, knobs, kicking, harier, hamster, hairs, legal, letterbomb, letterbombs, mailbomb, mailbombing, mailbombs, rapes, raping, rape, raper, rapist, virgin, warez, warezes, whack, whacked, whacker, whacking, whackers, whacks, pistols.

C'è qualcuno che crede veramente che ricerche su "erotic rape" [violenza sessuale erotica], "mailbombing bibles" e "choking virgins" [soffocare vergini] riusciranno a far passare inosservate le vere ricerche fatte dall'utente?

4) Vi è un enorme spreco di banda. Una query effettuata ogni dodici secondi significa 2.400 query al giorno assumendo giornate lavorative di otto ore. Una classica risposta di Google è di circa 25K, il che vuol dire 60 megabyte di traffico ulteriore ogni giorno. Immaginatevi se tutti gli impiegati di un'azienda lo utilizzassero.

Suppongo che questo genere di soluzione possa essere un deterrente per chi sta analizzando manualmente una stampa su carta delle vostre

ricerche, ma non costituisce un grosso ostacolo per l'analisi computerizzata, né per chi non si fa cogliere dalla pigrizia. Ma sarebbe difficile, per un programma di profiling computerizzato, ignorare queste ricerche.

Come ha detto un commentatore: "Supponiamo che un poliziotto vi faccia accostare per eccesso di velocità. Mentre si sta avvicinando alla vostra auto, vi rendete conto di aver dimenticato a casa il portafoglio. Senza patente, potreste essere nei guai. Allora, quando il poliziotto si avvicina, abbassate il finestrino e gridate: 'Salve agente! Questo veicolo non è assicurato! Quest'auto è rubata! Ho dell'erba nel portaoggetti! Non ho la patente! Poco fa ho investito una vecchietta! È tutta mattina che passo i semafori con il rosso! Ho un cadavere nel bagagliaio! Quest'auto non ha passato la revisione! Non mi è permesso guidare perché sono agli arresti domiciliari!'. Poi vi fermate a prendere fiato, certi di aver fornito un tale surplus di informazioni al poliziotto che è praticamente impossibile scoprire che siete senza patente in questo momento".

Certo, il data mining è un problema segnale-rumore. Ma rumore artificiale come questo non è di grande aiuto. Se dovessi migliorare quest'idea, farei in modo che il plug-in osservasse i pattern di ricerca dell'utente. Farei in modo che inviasse query solo ai motori di ricerca utilizzati dall'utente, e solo quando si trova online. Farei scegliere a caso gli intervalli di tempo in cui agire (a questo proposito il codice contiene un commento, per cui è probabile che la cosa venga sistemata in una futura versione del programma). Farei in modo che controllasse le pagine web che l'utente visita e realizzasse delle query basandosi su parole chiave trovate in quelle pagine. Farei in modo che inviasse query nel formato che l'utente utilizza più spesso, che sia una parola sola, due parole, o qualsiasi altra cosa.

Ma onestamente non saprei se, anche con queste modifiche, mi servirei di questo programma. Il sistema utilizzato dalle persone serie per proteggere la privacy delle loro ricerche è l'anonimizzazione. Usate Tor per una anonimizzazione web efficace. O Black Box Search per semplici ricerche anonime (vi è un'estensione Greasemonkey che lo fa automaticamente). E impostate il vostro browser in modo che cancelli periodicamente i cookie dei motori di ricerca.

TrackMeNot:

<http://mrl.nyu.edu/~dhowe/TrackMeNot/>

Un altro commentatore:

<http://blog.air0day.com/2006/08/21/worst-security-tool-ever/>

Altri strumenti:

<http://tor.eff.org/>

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

<http://blog.nemik.net/2006/08/21/dont-leave-traces/>

L'abuso della privacy da parte di AOL:

[http://www.schneier.com/blog/archives/2006/08/aol\\_releases\\_ma.html](http://www.schneier.com/blog/archives/2006/08/aol_releases_ma.html)

[http://mrl.nyu.edu/~dhowe/TrackMeNot/NYTimes\\_AOL\\_Exposed.htm](http://mrl.nyu.edu/~dhowe/TrackMeNot/NYTimes_AOL_Exposed.htm)

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

USBDumper

USBDumper è una piccola utility che copia silenziosamente su disco fisso i contenuti di una chiave USB inserita nel computer. L'idea è quella di

installare questo programmino sul vostro computer o su un PC pubblico, e poi raccogliere i file (alcuni di essi personali e confidenziali) di chiunque inserisca la propria chiavetta USB in quel computer. (Esiste una simile applicazione che scarica un'immagine del disco, permettendo di recuperare persino i file cancellati).

Non è niente di straordinario per chi lavora nella sicurezza informatica, ma forse può essere un brutto colpo per rappresentanti commerciali, presentatori di conferenze, persone che condividono file e molti altri che periodicamente inseriscono le proprie chiavette USB in computer sconosciuti.

[http://www.secuobs.com/news/07062006-sstic\\_usbduimper.shtml](http://www.secuobs.com/news/07062006-sstic_usbduimper.shtml)  
<http://www.secuobs.com/USBdumper.rar>  
<http://www.rfc1149.net/blog/2006/08/23/wiping-unused-space-in-a-file-system/>  
oppure <http://tinyurl.com/m757a>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Microsoft e FairUse4WM

Se volete vedere Microsoft affrettarsi ad applicare una patch a una vulnerabilità di un suo software, non dovete guardare quelle falle che danneggiano innumerevoli utilizzatori di Internet Explorer o che offrono agli intrusi il controllo di migliaia di macchine Windows. Basta craccare il DRM di Redmond.

Le patch di sicurezza, una volta, erano rare. I produttori di software erano contenti di fingere che le vulnerabilità nei loro prodotti fossero qualcosa di illusorio, e sistemavano quietamente il problema nella release successiva di quel software.

Tutto questo è cambiato grazie al movimento per l'esposizione totale. Ricercatori di sicurezza indipendenti hanno iniziato a rendere pubbliche le falle da loro trovate, costringendo i produttori di software a smettere di ignorarle. Poi i worm si sono diffusi sempre più; realizzare patch, e velocemente, è diventata la norma.

Ma ancora oggi a nessun produttore di software piace rilasciare patch. Ogni patch è una pubblica ammissione di un errore commesso dalla compagnia. Inoltre questo processo dirotta risorse ingegneristiche dal nuovo sviluppo. Le patch irritano gli utenti perché li costringono ad aggiornare il software, e li fanno infuriare ancor più se l'aggiornamento non funziona come dovrebbe.

Dal punto di vista del produttore, vi è un atto di bilanciamento economico: quanto più sarà irritata la propria utenza da software senza patch rispetto a quanto lo sarà a causa della patch, e tale "riduzione di seccatura" varrà il costo della realizzazione della patch?

Dal 2003 in avanti, la strategia di Microsoft per bilanciare tali costi e benefici è stata quella di raggruppare le patch: invece di pubblicarne una alla volta, le ha pubblicate tutte insieme il secondo martedì di ogni mese. Ciò diminuisce i costi di sviluppo per Microsoft e aumenta l'affidabilità delle sue patch.

Il prezzo pagato dall'utente per questa strategia è quello di rimanere aperto a vulnerabilità conosciute per quasi un mese. D'altra parte gli utenti beneficiano di una programmazione prevedibile: Microsoft può verificare tutte le patch che verranno pubblicate allo stesso tempo, il

che significa che le patch sono più affidabili e gli utenti possono installarle più velocemente e con maggiore sicurezza.

In assenza di leggi, di responsabilità per il software, o di qualche altro meccanismo che renda un software non 'patchato' costoso per il produttore, il Martedì delle Patch è la cosa migliore che possono aspettarsi gli utenti.

Perché? Perché per Microsoft ha senso nel breve periodo, da un punto di vista finanziario. L'azienda non è un'istituzione benefica pubblica, e se Internet soffre o se i computer vengono compromessi en masse, l'impatto economico per Microsoft continua a essere minimo.

Microsoft è nel business per fare soldi, e proteggere i suoi utenti realizzando patch per il proprio software è un elemento secondario a tale scopo.

Non vi è esempio migliore per constatare questo principio in azione, del comportamento di Microsoft per quanto riguarda la vulnerabilità nel suo software di gestione dei diritti digitali (DRM) PlaysForSure.

In agosto, un hacker ha sviluppato un'applicazione chiamata FairUse4WM che elimina la protezione anticopia dai file Windows Media DRM 10 e 11.

Ora, questa non è una "vulnerabilità" nel senso comune del termine: la gestione dei diritti digitali non è una funzionalità che gli utenti desiderano. Essere in grado di eliminare la protezione anticopia è una buona cosa per alcuni utenti, e qualcosa di totalmente irrilevante per tutti gli altri. Nessun utente dirà mai: "Oh no. Ora posso riprodurre la musica che ho comprato per il mio computer anche sulla mia auto! Devo installare una patch che mi impedisca di farlo".

Ma tale vulnerabilità, per Microsoft, è qualcosa di grosso. Va a influire sui rapporti che l'azienda ha instaurato con le maggiori etichette discografiche. Influisce sulle offerte dei prodotti della compagnia. Influisce sui profitti e le perdite della compagnia. È nei migliori interessi della compagnia sistemare questa "vulnerabilità"; l'utente non importa.

E allora Microsoft non ha sprecato tempo: ha pubblicato una patch tre giorni dopo aver appreso dell'hack. Non vi sono attese di un mese per i possessori di copyright che si affidano al DRM di Microsoft.

Questo dimostra chiaramente che il fattore economico è un incentivo molto più forte rispetto alla sicurezza.

Non c'è da sorprendersi che il sistema non sia rimasto protetto per molto. FairUse4WM 1.2 aggira la patch di Microsoft, e anche il sistema anticopia dei file Windows Media DRM 9 e 11beta2. Quattro giorni dopo, Microsoft ha pubblicato un'altra patch.

Le cose stanno a questo punto. Qualche ipotesi su quanto tempo impiegheranno i tipi di FairUse4WM ad aggiornare il loro software? E su quanto tempo passerà prima che Microsoft rilascerà l'ennesima patch?

Sicuramente molto meno tempo di quel che servirà a Microsoft e all'industria discografica per rendersi conto di star giocando una partita persa in partenza, e che cercare di rendere dei file incopiabili è come cercare di rendere l'acqua non bagnata.

Se Microsoft lasciasse perdere questo sforzo interminabile e impiegasse le medesime energie di sviluppo nella realizzazione di un sistema di patching veloce e affidabile, sarebbe un beneficio per tutta Internet.



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.