

CRYPTO-GRAM
15 giugno 2007

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA

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

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0703.html>>.

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

Crypto-Gram è anche consultabile in formato RSS.

** ** ** * * * * *

In questo numero:

Rischi rari e reazioni eccessive

Tattiche, bersagli e obiettivi

News

Ritratto del Terrorista Moderno da Idiota

L'insegnamento dei virus

Rubato l'orologio di Bush?

Le news su Schneier/BT Counterpane

Il vincitore della seconda edizione del Concorso "Minaccia da Trama Cinematografica"

Il Canile Perpetuo: Meganet

Considerazioni estranee alla sicurezza nelle decisioni di sicurezza

Commenti dei lettori

** ** ** * * * * *

Rischi rari e reazioni eccessive

Tutti hanno reagito agli orribili eventi della sparatoria alla Virginia Tech University. Alcune di tali reazioni sono state razionali, altre no.

Uno studente della high school è stato sospeso per aver personalizzato un videogioco in stile sparattutto in prima persona utilizzando una mappa della propria scuola. Un fornitore è stato licenziato dal suo posto di lavoro governativo per aver parlato di una pistola, e ha perfino ricevuto una visita della polizia quando ha creato una vignetta sull'incidente. Un preside a Yale ha proibito l'uso di armi finte nei teatri dell'università, un provvedimento che è stato annullato nel giro di un giorno. E alcuni insegnanti hanno terrorizzato gli alunni di sesta classe inscenando un'aggressione a mano armata senza dire ai ragazzi che si trattava di una dimostrazione.

Tutte queste cose sono accadute, anche se sparatorie come quella della Virginia Tech sono incredibilmente rare; anche se, secondo la stampa, meno dell'uno per cento degli omicidi e dei suicidi di bambini e ragazzi fra i 5 e i 19 anni avvengono nelle scuole. Infatti, tali reazioni eccessive hanno avuto luogo non a dispetto di questi fatti, ma a causa di essi.

Il massacro della Virginia Tech è precisamente il genere di evento che tende a scatenare reazioni esagerate in noi umani. La nostra mente non è molto brava in materia di analisi delle probabilità e dei rischi, specialmente di fronte ad accadimenti rari. Tendiamo a esagerare eventi spettacolari, strani e insoliti, e minimizziamo quelli ordinari, familiari e comuni. Vi è molta ricerca nella comunità psicologica su come il cervello risponde al rischio (argomento di cui ho già parlato, almeno in parte), ma il nocciolo della questione è che il nostro cervello funziona molto bene nell'analisi dei rischi semplici con i quali l'uomo si è confrontato durante gran parte della sua esistenza, ma è decisamente scarso nella valutazione dei rischi complessi che la società di oggi ci costringe ad affrontare.

Novità più terrore uguale reazione eccessiva.

Possiamo vederne gli effetti in continuazione. Abbiamo paura di essere uccisi, rapiti, violentati e assaliti da estranei, quando è molto più probabile che a commettere quei reati sia un parente o un amico. Abbiamo paura di eventuali disastri aerei e di tiratori scatenati invece di preoccuparci di incidenti d'auto e di violenza domestica, due evenienze molto più comuni.

Negli Stati Uniti, cani, serpenti, api e maiali uccidono ogni anno molte più persone che non gli squali. Anzi, i cani uccidono più esseri umani di ogni altro animale (a eccezione dell'uomo). Certo, gli squali sono molto più pericolosi dei cani, ma nella vita quotidiana è molto più probabile incontrare un cane, non uno squalo.

La nostra più grande reazione eccessiva nei confronti di un evento raro e insolito è stata la risposta agli attacchi terroristici dell'11 settembre. Ricordo l'allora Procuratore Generale John Ashcroft, che tenne un discorso nel 2003 nel Minnesota (dove vivo), in cui dichiarò che il fatto che non ci fossero stati nuovi attacchi terroristici dopo l'11 settembre dimostrava che i suoi metodi stavano funzionando. Ricordo che pensai: "Non ci sono stati attacchi terroristici neanche i due anni precedenti l'11 settembre, e a quell'epoca tu non avevi instaurato alcuna linea di condotta o contromisura. Questo che cosa prova?".

Quel che prova è che gli attacchi terroristici sono molto rari, e che forse la nostra reazione non valeva l'enorme quantità di denaro sprecato, la perdita delle libertà civili,

gli attacchi alla Costituzione americana e i danni alla nostra credibilità di fronte al mondo intero. Ma comunque il reagire in modo esagerato è stata la cosa più naturale da parte nostra. Certo, è tutta messinscena di sicurezza, ma ci fa sentire più al sicuro.

Le persone tendono a basare l'analisi dei rischi più sulla loro storia personale che non sui dati concreti, a dispetto della vecchia battuta "il plurale di aneddoto non è dati". Se un amico viene derubato in un paese straniero, quell'episodio avrà probabilmente più peso su quanto sicuri ci sentiremo viaggiando in quello stesso paese, che non degli astratti dati statistici sulla criminalità.

Diamo più credibilità ai "cantastorie" che conosciamo personalmente che non a degli estranei, e le storie a noi più prossime acquistano un peso maggiore rispetto a quelle di paesi lontani. In altre parole, la prossimità di rapporto influisce sulla nostra valutazione dei rischi. E chi è il più grande "cantastorie" di oggi? La televisione. (L'ottimo libro di Nassim Nicholas Taleb, "The Black Swan: The Impact of the Highly Improbable", tratta questo argomento).

Consideriamo la reazione a un altro evento accaduto il mese scorso: il giocatore di baseball Josh Hancock si è ubriacato ed è morto in un incidente d'auto. Come conseguenza, molte squadre di baseball ora proibiscono l'alcool nelle loro sedi di ritrovo dopo le partite. A parte il fatto che si tratta di una reazione ridicola a un fatto incredibilmente raro (2.430 partite di baseball ogni stagione, 35 persone per sede di ritrovo, due sedi di ritrovo per partita. E quanto spesso è accaduta una cosa del genere?), questa soluzione non ha alcun senso. Hancock non si è ubriacato nella sede di ritrovo, ma in un bar. Ma è necessario che la Major League di baseball venga vista "prendere provvedimenti", anche se quei "provvedimenti" sono insensati, anche se quei "provvedimenti" finiscono in realtà con l'aumentare il rischio, costringendo i giocatori a bere fuori e non nei luoghi di ritrovo, dove c'è maggior controllo.

Di solito dico alla gente che se una cosa è nelle news, non devono preoccuparsi. La definizione stessa di "news" (le "novità", le "nuove") è "qualcosa che capita molto raramente". È quando una cosa non è nelle news, quando è talmente comune che non fa più notizia (incidenti d'auto, violenza domestica) che ci si deve preoccupare.

Ma non è la nostra forma di pensare. Lo psicologo Scott Pious lo ha descritto molto efficacemente in "The Psychology of Judgment and Decision Making" [La psicologia del giudizio critico e del processo decisionale]: "In termini molto generali: (1) Più un evento è ACCESSIBILE, più frequente o probabile apparirà; (2) Più un'informazione è INTENSA, più sarà convincente e memorabile; (3) Più qualcosa è NOTEVOLE, maggiore sarà la probabilità che appaia causale, in un rapporto di causa ed effetto".

Perciò, di fronte a un evento molto accessibile ed estremamente intenso come l'11 settembre o come la sparatoria della Virginia Tech, noi reagiamo in maniera eccessiva. E di fronte a tutti gli eventi notevoli associati a queste tragedie, noi presumiamo la causalità. E approviamo il Patriot Act. E pensiamo che mettendo delle armi in mano ai nostri studenti, o magari rendendo più arduo per uno studente ottenere una pistola, avremo risolto il problema. E non lasciamo andare i nostri figli a fare ricreazione senza qualcuno che li controlli. E stiamo alla larga dall'oceano perché abbiamo letto da qualche parte che uno squalo ha attaccato delle persone.

È la nostra mente al lavoro, ancora una volta. Dobbiamo “fare qualcosa”: non importa se quel qualcosa non ha senso o è totalmente inefficace. E dobbiamo fare qualcosa direttamente collegato con i particolari dell’evento. Pertanto, invece di implementare misure di sicurezza efficaci, ma più generiche, per ridurre il rischio terrorismo, preferiamo vietare i taglierini sugli aerei. E ritorniamo al massacro della Virginia Tech con la facilità del senno di poi e recriminiamo sulle cose che “avremmo dovuto fare”.

Infine la nostra mente deve trovare a tutti i costi qualcuno o qualcosa a cui attribuire la colpa. (Jon Stewart ha un ottimo pezzo sulla caccia al capro espiatorio alla Virginia Tech e sulla copertura dei mass media in generale). Ma a volte non esiste alcun capro espiatorio; a volte abbiamo fatto tutto nel modo migliore e si è trattato di pura sfortuna. Semplicemente non è possibile impedire a un pazzo di sparare alla gente a casaccio, non è qualcosa di prevedibile e non esistono misure di sicurezza che funzionerebbero.

Suonerà come un circolo vizioso, ma un evento raro è raro principalmente perché non accade molto spesso, e non perché vi siano in atto delle misure di sicurezza preventive. E implementare misure di sicurezza per rendere questi rari eventi ancora più rari è un procedimento analogo alla barzelletta del tizio che pesta i piedi tutt’intorno a casa sua per tener lontani gli elefanti.

“Gli elefanti? Ma non ci sono elefanti in questa zona”, dice uno dei vicini.

“Visto come funziona bene il mio sistema?!”

Se si vuole fare qualcosa che abbia un senso dal punto di vista della sicurezza, è necessario individuare l’elemento che accomuna una serie di eventi rari e concentrare le contromisure intorno a quell’elemento. Occorre concentrarsi sul rischio generale del terrorismo, non sulla minaccia specifica di far saltare un aereo con esplosivo liquido, non sulla minaccia specifica di un pazzo tiratore che si aggira per un campus universitario. Occorre ignorare le minacce da trama cinematografica e concentrarsi sui rischi reali.

Reazioni irrazionali:

<<http://arstechnica.com/news.ars/post/20070502-student-creates-counter-strike-map-gets-kicked-out-of-school.html>>

oppure <<http://tinyurl.com/2dbl67>>

<http://www.boingboing.net/2007/05/03/webcomic_artist_fire.html>

<<http://www.yaledailynews.com/articles/view/20843>>

<<http://yaledailynews.com/articles/view/20913>>

<<http://www.msnbc.msn.com/id/18645623/>>

Rischi di sparatorie nelle scuole (del 2000)

<<http://www.cdc.gov/HealthyYouth/injury/pdf/violenceactivities.pdf>>

Statistiche dei reati -- estranei vs. persone conosciute:

<http://www.fbi.gov/ucr/05cius/offenses/expanded_information/data/shrtable_09.html

>

oppure <<http://tinyurl.com/2qbtae>>

Il mio pezzo sulla psicologia del rischio e la sicurezza:

<<http://www.schneier.com/essay-155.html>>

Rischi di attacchi da parte di squali:

<<http://www.oceanconservancy.org/site/DocServer/fsSharks.pdf>>

Il discorso di Ashcroft:

<<http://www.highbeam.com/doc/1G1-107985887.html>>

Il mio pezzo sulle messinscene di sicurezza:

<<http://www.schneier.com/essay-154.html>>

La birra bandita dal Baseball:

<http://blogs.csoonline.com/baseballs_big_beer_ban>

Il saggio di Nicholas Taleb:

<<http://www.fooledbyrandomness.com/nyt2.htm>>

<<http://www.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2007/04/22/do2201.xml>>

oppure <<http://tinyurl.com/3bewfy>>

La Virginia Tech e il controllo delle armi:

<<http://abcnews.go.com/International/wireStory?id=3050071&CMP=OTC-RSSFeeds0312>>

oppure <<http://tinyurl.com/25js4o>>

<<http://www.cnn.com/2007/US/04/19/commentary.nugent/index.html>>

La Virginia Tech e il senno di poi:

<<http://news.independent.co.uk/world/americas/article2465962.ece>>

<http://www.mercurynews.com/charliemccollum/ci_5701552>

Il video di Jon Stewart:

<http://www.comedycentral.com/motherload/player.jhtml?ml_video=85992>

Il mio pezzo sulle minacce da trama cinematografica:

<<http://www.schneier.com/essay-087.html>>

Un altro parere:

<<http://www.socialaffairsunit.org.uk/blog/archives/000512.php>>

Questo articolo è originariamente apparso su Wired.com. È il mio quarantaduesimo intervento su quel sito.

<http://www.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0517>

oppure <<http://tinyurl.com/26cxcs>>

Traduzione francese:

<<http://archiloque.net/spip.php?rubriques2&periode=2007-06#>>

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

Tattiche, bersagli e obiettivi

Se incontrate un leone aggressivo, fissatelo negli occhi. Ma non fatelo con un leopardo: evitate il suo sguardo a tutti i costi. In entrambi i casi, indietreggiate lentamente e non correte. Se vi imbattete in un branco di iene, invece, correte e arrampicatevi su un albero: le iene non sanno arrampicarsi sugli alberi. Ma non fatelo se un elefante vi sta seguendo, perché un elefante butterà giù l'albero (e voi). State fermi e aspettate che si dimentichi della vostra presenza.

Ho passato i giorni scorsi facendo un safari in un parco divertimenti in Sudafrica, e questi sono solo alcuni esempi dei suggerimenti di sicurezza che venivano dati ai visitatori. La cosa interessante di questi consigli è il livello di precisione. Magari le difese non saranno terribilmente efficaci, e potreste finire comunque sbranati, dilaniati o calpestati, ma rappresentano la speranza migliore. Non è consigliabile agire diversamente perché gli animali ripetono costantemente le stesse dinamiche. Queste sono contromisure di sicurezza contro tattiche specifiche.

I leoni e i leopardi apprendono delle tattiche che funzionano per loro, e a me sono state insegnate delle tattiche per difendermi. Gli esseri umani sono intelligenti, e ciò significa che siamo più adattabili degli animali. Però siamo anche pigri e stupidi, generalmente parlando; e, come un leone o una iena, ripeteremo continuamente le tattiche che funzionano. I borseggiatori si servono sempre degli stessi trucchi. Stesso dicasi per i phisher e per chi va a sparare nelle scuole. Se gli ordigni esplosivi improvvisati non funzionassero così spesso, gli insorgenti iracheni si inventerebbero qualcos'altro.

Pertanto anche la sicurezza contro le persone generalmente si concentra sulle tattiche.

Una mia amica mi ha chiesto di recente dove dovrebbe nascondere i gioielli nel suo appartamento, per fare in modo che non vengano scoperti dai ladri. I ladri tendono a guardare sempre negli stessi posti: sopra il comò, nei comodini, nei cassetti del guardaroba, negli armadietti del bagno, pertanto nascondere i gioielli in un altro posto sarà probabilmente più efficace, specialmente in quei casi in cui il ladro è in lotta contro il tempo. Il consiglio è lasciare in vista un po' di soldi e qualche oggetto di valore come esca: il ladro crederà di aver trovato il bottino e se ne andrà. Anche qui, non vi è alcuna certezza che lo stratagemma funzioni, ma è la speranza migliore.

La chiave di queste contromisure è scoprire il pattern, lo schema ricorrente: la tattica comune di attacco dalla quale vale la pena difendersi. Per fare questo occorrono i dati. Un'unica istanza di un attacco che non ha funzionato (esplosivi liquidi, esplosivi nascosti nelle scarpe), o una sola istanza di un attacco che ha avuto successo (l'11 settembre) non è un pattern. Mettere in atto tattiche di difesa contro questi attacchi è come se la mia guida del safari mi dicesse: "Finora, a quanto ci hanno riferito, è capitato una sola volta che un turista incontrasse un leone. Lo ha guardato negli occhi ed è sopravvissuto. Un altro turista ha provato a fare lo stesso con un leopardo ed è stato sbranato. Per cui, se lei dovesse incontrare un leone...". Invece, il consiglio che mi è

stato dato era basato su un'esperienza collettiva millenaria, l'esperienza di persone che hanno incontrato animali africani più e più volte.

Paragonate tutto questo con l'approccio della Transportation Security Administration. Di fronte a ogni minaccia particolare, la TSA implementa una contromisura senza alcun fondamento per dimostrare che funzioni, o che impedirà il ripresentarsi della minaccia.

Inoltre, aggressori umani possono adattarsi molto più rapidamente dei leoni. Un leone non imparerà che deve ignorare le persone che lo fissano negli occhi e divorarle lo stesso. Ma le persone apprenderanno. I ladri ora conoscono i posti "segreti" più comuni dove la gente nasconde i propri oggetti di valore (il serbatoio del water, le confezioni di cereali, il frigorifero, il freezer, l'armadietto dei medicinali, sotto il letto...) e andranno a vedere. Alla fine ho consigliato alla mia amica di trovare un nuovo posto segreto e di mettere pochi oggetti di valore come esca in un luogo più banale.

Questo è il braccio di ferro della sicurezza. A tattiche di attacco comuni corrispondono contromisure altrettanto comuni. Alla fine quelle contromisure saranno aggirate e verranno così sviluppate nuove tattiche d'attacco, che a loro volta richiederanno nuove contromisure. Questo fenomeno è facilmente riscontrabile nella lotta continua che è la frode delle carte di credito, dei bancomat, o i furti d'auto.

Il risultato di queste contromisure di sicurezza mirate a tattiche specifiche è di spingere l'aggressore altrove. Nella maggior parte dei casi, all'aggressore non importa il bersaglio in sé. Ai leoni non importa l'aspetto di chi o cosa divorano: per un leone siamo semplicemente delle proteine in un pratico involucre. Ai ladri non importa molto quale casa derubare, e ai terroristi non importa chi uccidono. Se le vostre contromisure fanno in modo che un leone attacchi un impala e non voi, o se il vostro allarme antifurto spinge il ladro a derubare la casa del vicino e non la vostra, per voi è una vittoria.

Le tattiche hanno meno importanza se l'aggressore vi ha personalmente presi di mira. Se, per esempio, avete un quadro di grandissimo valore appeso in soggiorno e il ladro lo sa, non andrà a derubare la casa accanto, anche se avete un antifurto. Invece, il ladro cercherà di trovare il modo per battere le vostre difese. Oppure vi punterà la pistola e vi costringerà ad aprire la porta di casa. Oppure farà finta di essere il tecnico venuto a riparare l'aria condizionata. Ciò che importa è il bersaglio, e un valido aggressore considererà tutta una serie di tattiche per raggiungerlo.

Questo approccio richiede un tipo diverso di contromisura, ma è una cosa ben compresa nell'universo della sicurezza. Per le persone, è ciò in cui si specializzano le aziende produttrici di allarmi, le compagnie di assicurazione, e le guardie del corpo. Il presidente Bush necessita di un livello di protezione contro attacchi mirati diverso da quello di Bill Gates, e io necessito di un livello di protezione diverso da quello di entrambi. Sarebbe sciocco da parte mia assumere delle guardie del corpo nel caso qualcuno mi prendesse di mira per derubarmi o sequestrarmi. Certo, sarei molto più sicuro, ma non si tratterebbe di un buon compromesso di sicurezza.

Il terrorismo di Al-Qaeda è ancora un'altra questione. L'obiettivo è terrorizzare. Il bersaglio non ha importanza, ma non esiste nemmeno una tattica specifica o un pattern. Data questa premessa, il modo migliore per investire il nostro denaro contro il

questo tipo di cosa. Si tratta di un esempio perfetto di messinscena di sicurezza: una contromisura che funziona se si indovinano per caso i dettagli della trama terroristica; totalmente inutile in tutti gli altri casi. Se non altro verrà disattivata solo una zona molto ridotta.

<<http://www.smh.com.au/news/NATIONAL/Mobiles-to-drop-out-during-Bush-visit/2007/05/16/1178995171116.html>>

oppure <<http://tinyurl.com/2e8nbo>>

<http://www.schneier.com/blog/archives/2007/04/triggering_bomb.html>

<<http://it.slashdot.org/it/07/05/17/1221255.shtml>>

<http://www.theregister.co.uk/2007/05/18/black_helicopter_george_bush_down_under/>

oppure <<http://tinyurl.com/2p266j>>

Dan Geer parla di compromessi di sicurezza, monocultura, e diversità genetica nelle api domestiche:

<<http://geer.tinho.net/acm.geer.0704.pdf>>

L'email EPIC Alert viene inviata due volte alla settimana dall'Electronic Privacy Information Center. È un'ottima risorsa per quanto riguarda la privacy e le policy, sia negli Stati Uniti che all'estero.

<<http://www.epic.org/alert/>>

Dei ricercatori di attacchi WEP spiegano come funziona il loro attacco al protocollo di sicurezza wireless 802.11.

<http://www.theregister.co.uk/2007/05/15/wep_crack_interview/>

<http://www.schneier.com/blog/archives/2007/05/interview_with_5.html>

Una vignetta sulla sicurezza delle linee aeree: qui il "pararsi il didietro" è letterale:

<http://www.clarionledger.com/misc/blogs/mramsey/uploaded_images/bilde-2-780665.jpg>

oppure <<http://tinyurl.com/2as767>>

Divertente parodia della TSA a "Saturday Night Live":

<http://www.youtube.com/watch?v=ykzqFz_nHZE>

Ecco uno scherzo che vi farà arrestare:

<http://www.schneier.com/blog/archives/2007/05/joke_thatll_get_1.html>

Londra sta effettuando una esercitazione "bomba sporca". Si tratta per lo più di una minaccia da trama cinematografica, ma questo genere di esercitazioni è utile, a prescindere dagli scenari. Onestamente, però, gli esplosivi classici rappresentano un rischio molto maggiore rispetto a questi ordigni esotici. Anche se con una bomba sporca, il panico ispirato dai media sarebbe certamente un fattore importantissimo.

<http://www.theregister.co.uk/2007/05/18/dirty_bomb_test_in_marylebone/>

Abbiamo un nuovo record di fattorizzazione: 307 cifre (1023 bit). È un numero speciale, $2^{1039} - 1$, ma le tecniche possono essere generalizzate. C'è da aspettarsi che presto verranno fattorizzati i numeri a 1024 bit. Spero che gli utenti di applicazioni RSA abbiano già abbandonato la sicurezza a 1024 bit da anni, ma per chi non lo ha ancora fatto: svegliatevi.

<<http://www.physorg.com/news98962171.html>>

Sulla futilità di combattere i pirati online:

<http://www.forbes.com/2007/05/04/youtube-piratesbay-piracy-tech-cx_ag_0507pirates.html<http://yro.slashdot.org/yro/07/05/17/1749259.shtml>>

oppure <<http://tinyurl.com/28rwnm>>

Un buon articolo sullo spam grafico:

<http://csoonline.com/read/040107/fea_spam.html>

Da visitare la pagina con le immagini interattive:

<http://csoonline.com/read/040107/fea_spam_by_the_numbers.html>

Dal GAO: "Aviation Security: Efforts to Strengthen International Prescreening are Under Way, but Planning and Implementation Issues Remain" [Sicurezza aerea: si stanno compiendo molti sforzi per rafforzare il pre-screening internazionale, ma permangono problematiche di pianificazione e implementazione], maggio 2007. Vale la pena leggere almeno il sommario.

<<http://www.gao.gov/new.items/d07346.pdf>>

Gli screener di sicurezza aeroportuale hanno fermato un tizio che indossava un'uniforme finta. Sembra una barzelletta. Spendiamo miliardi in sicurezza aeroportuale, e abbiamo da dimostrare così poco in cambio che la TSA deve ingigantire a tal punto un reato come l'impersonare un membro dell'esercito?

<http://www.tsa.gov/press/happenings/florida_uniform.shtm>

La polizia britannica utilizza mezzi militari telecomandati: un altro passo verso la militarizzazione della polizia.

<<http://news.bbc.co.uk/1/hi/england/merseyside/6676809.stm>>

Dei criminali attaccano una grande azienda di web hosting: "La compagnia dichiara di avere più di 700.000 clienti. Se assumiamo per il momento che il ridotto segmento di server IPOWER analizzato da Security Fix sia in un certo qual modo indicativo di un problema più esteso, IPOWER potrebbe essere benissimo la dimora di quasi un quarto di milione di siti web malevoli".

<http://blog.washingtonpost.com/securityfix/2007/05/cyber_crooks_hijack_activities_1.html>

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

Secondo un rapporto del GAO, l'FBI è dotata di una pessima sicurezza contro gli attacchi dall'interno.

<<http://www.pcworld.com/article/id,132250-c,privacysecurity/article.html>>

oppure <<http://tinyurl.com/yt86mg>>

Interessante attacco di spoofing:

<http://www.theregister.co.uk/2007/05/25/strange_spoofing_technique/>

Pensavo che fosse il terrorismo la ragione per cui abbiamo un Dipartimento per la Sicurezza Nazionale, ma pare che vi siano altre cose che preoccupano il Dipartimento: "Delle 814.073 persone accusate dal Dipartimento per la Sicurezza Nazionale in tribunali per l'immigrazione negli ultimi tre anni, 12 sono state imputate di terrorismo,

ha dichiarato il TRAC". Il TRAC è un ottimo gruppo, e consiglio una visita al loro sito web a chi è interessato in ciò che il governo statunitense sta realmente facendo.

<<http://www.cnn.com/2007/POLITICS/05/27/homeland.security.record/index.html>>

oppure <<http://tinyurl.com/3xre8e>>

<<http://trac.syr.edu/>>

Il novembre scorso, il Data Privacy and Integrity Advisory Committee (Commissione consultiva sulla privacy e integrità dei dati) del Dipartimento per la Sicurezza Nazionale ha fortemente sconsigliato l'inserimento di chip RFID nelle carte di identità. Il Dipartimento per la Sicurezza Nazionale lo ha ignorato e ha portato avanti il progetto ugualmente. Ora la Smart Card Alliance sta criticando il programma RFID del Dipartimento per la Sicurezza Nazionale in merito all'identificazione cross-border (il PASS - People Access Security Services), affermando sostanzialmente che si stanno commettendo proprio quegli errori che aveva previsto il Data Privacy and Integrity Advisory Committee.

<http://www.gcn.com/online/vol1_no1/44338-1.html>

<http://www.schneier.com/blog/archives/2006/11/dhs_privacy_com.html>

<http://www.schneier.com/blog/archives/2007/05/rfid_in_people.html>

Questa è una vicenda surreale che risale al 2005, e riguarda un individuo che è stato legato per ore per aver tentato di spendere banconote da 2 dollari. I commessi di Best Buy hanno creduto che le banconote fossero contraffatte e hanno fatto arrestare il tizio. L'estratto più surreale dell'articolo è l'ultima frase: "Commentando l'incidente, il portavoce della polizia di Baltimore County, Bill Toohey, ha detto al Sun: 'È segno del fatto che siamo tutti un po' nervosi nell'era post-11 settembre'". Che cosa diavolo c'entrano gli attacchi terroristici dell'11 settembre con la contraffazione di denaro? Che cosa ha a che vedere l'essere "un po' nervosi nell'era post-11 settembre" con questo incidente? La contraffazione non è terrorismo, non gli assomiglia nemmeno un po'.

<http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=43685>

Difese portuali contro i terroristi a nuoto: scienza e ingegneria davvero interessanti, ma si tratta decisamente di una minaccia da trama cinematografica.

<http://blog.wired.com/defense/2007/05/how_to_stop_a_s.html>

Il Dipartimento per la Sicurezza Nazionale si serve di scrittori di fantascienza per contribuire allo sviluppo di minacce da trama cinematografica. Almeno questa volta sono onesti a riguardo.

<http://www.usatoday.com/tech/science/2007-05-29-deviant-thinkers-security_N.htm>

oppure <<http://tinyurl.com/3cys5h>>

Telecamere della polizia montate sulla testa nel Regno Unito:

<http://www.manchestereveningnews.co.uk/news/s/1007/1007600_super_wardens_g_o_on_patrol.html>

oppure <<http://tinyurl.com/29tdzr>>

Non ho scritto nulla in merito alla guerra cibernetica fra Russia ed Estonia perché... beh, perché non ho creduto vi fosse qualcosa di nuovo da dire. Sappiamo che questo genere di cosa è possibile. Non abbiamo alcuna prova definitiva che dimostri che ci sia stata la Russia dietro a tutto questo. Ma sarebbe sciocco pensare che i vari eserciti del

mondo non abbiano tali capacità. E in ogni caso ho parlato della guerra cibernetica nel gennaio 2005.

<<http://www.schneier.com/crypto-gram-0501.html#10>>

Fuga di informazioni in Slingbox:

<<http://www.freedom-to-tinker.com/?p=1163>>

<<http://www.cs.washington.edu/research/security/usenix07devices.html>>

Inserire sensori nelle falene e in altri insetti:

<<http://government.zdnet.com/?p=3189>>

Insegnare ai computer a dimenticare: un articolo sull'enorme quantità di dati che ora ci seguono per tutta la vita; ci si chiede se non staremmo meglio se i computer "dimenticassero" le cose dopo un determinato periodo di tempo:

<http://arstechnica.com/news_ars/post/20070509-escaping-the-data-panopticon-teaching-computers-to-forget.html>

oppure <<http://tinyurl.com/272629>>

<[http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP07-022/\\$File/rwp_07_022_mayer-schoenberger.pdf](http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP07-022/$File/rwp_07_022_mayer-schoenberger.pdf)>

oppure <<http://tinyurl.com/yq8llf>>

Altri link sull'argomento:

<http://www.concurringopinions.com/archives/2007/05/the_right_to_de.html>

oppure <<http://tinyurl.com/2fhlgb>>

<<http://www.harvardlawreview.org/forum/issues/119/dec05/ohm.shtml>>

<<http://www.lcs.gov.bc.ca/privacyaccess/Conferences/Feb2007/ConfPresentations/Perlman-Radia-keynote.pdf>>

oppure <<http://tinyurl.com/345rte>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051501873.html>>

oppure <<http://tinyurl.com/2o9kw5>>

Anch'io ne ho parlato:

<<http://www.schneier.com/essay-109.html>>

<<http://www.schneier.com/essay-129.html>>

Vi sono state delle interessanti controversie legali negli Stati Uniti in merito alle ricerche via computer e al consenso di terze parti:

<<http://www.law.com/jsp/article.jsp?id=1179092588804>>

<http://www.wired.com/politics/law/commentary/circuitcourt/2007/05/circuitcourt_0523>

oppure <<http://tinyurl.com/2gr7om>>

Interessanti statistiche sul terrorismo: "La maggioranza degli attacchi terroristici non provoca morti, e solo l'1% di tali attacchi provoca la morte di 25 o più persone. [...] Il database identifica più di 30.000 attentati dinamitardi, 13.400 assassinii e 3.200 sequestri. Inoltre tratta in dettaglio più di 1.200 attacchi terroristici all'interno degli Stati Uniti". Molto di questo dipende dalla definizione che ognuno dà al "terrorismo", ma è materiale davvero interessante.

<http://www.livescience.com/history/070524_terrorism_database.html>

<<http://www.start.umd.edu/data/gtd/>>

Il Dipartimento per la Sicurezza Nazionale sta sollecitando proposte di ricerca in merito alla sicurezza informatica e di rete. Vi sono nove aree di ricerca: Botnet e altro malware: Rilevamento e attenuazione, Sistemi sicuri componibili e scalabili, Metrica di sicurezza cibernetica, Visualizzazione dei dati di rete per l'Information Assurance, Topografia/tomografia di Internet, Routing Security Management Tool, Sicurezza dei sistemi di controllo dei processi, Strumenti e tecniche di Data Anonymization, e Rilevamento e attenuazione delle minacce interne.

<http://www.hsarpabaa.com/Solicitations/BAA07-09_CyberSecurityRD_Posted_05162007.pdf>

oppure <<http://tinyurl.com/yv85ne>>

Sensori metallici remoti impiegati per rilevare i bracconieri. Sono sicuro che questa tecnologia ha molto più valore sul campo di battaglia.

<<http://www.technologyreview.com/Biotech/18722/>>

Il Data Privacy and Integrity Advisory Committee (Commissione consultiva sulla privacy e integrità dei dati) del Dipartimento per la Sicurezza Nazionale ha pubblicato un eccellente rapporto su REAL ID:

<http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_05-2007_realid.pdf>

oppure <<http://tinyurl.com/2bbyqv>>

Un ottimo articolo sui rischi percepiti di contro ai rischi reali per i bambini e su come l'eccessiva protezione possa veramente danneggiarli.

<<http://news.bbc.co.uk/1/hi/education/6720661.stm>>

Commento:

<http://www.timesonline.co.uk/tol/comment/columnists/alice_miles/article1890234.ece>

oppure <<http://tinyurl.com/3bthca>>

Rivestimenti protettivi, due storie:

1. Una speciale biancheria intima protegge chi la indossa dalla fotografia a infrarossi.

<http://inventorspot.com/new_shot_guard_underwear_infrared_protection_photographers>

oppure <<http://tinyurl.com/2mjap4>>

2. Un filtro per finestre che blocca le radiazioni elettromagnetiche ma lascia passare la luce:

<<http://www.stltoday.com/stltoday/business/stories.nsf/0/F1B4A7E978173C10862572E7000AA32B?OpenDocument>>

oppure <<http://tinyurl.com/2ax9gd>>

Non credo che nessuno di questi prodotti diventerà un oggetto da mercato di massa, anche se posso immaginare un impiego del secondo in molte installazioni militari.

Il Dipartimento per la Sicurezza Nazionale vuole che le università facciano un inventario di una lunga lista di sostanze chimiche. Nell'articolo si possono leggere notizie interessanti su alcune di queste sostanze.

<http://www.theregister.co.uk/2007/06/02/dhs_dud_interesting_chemicals/>

Filigrane basate sul DNA. Non è crittografia, malgrado il nome, ma è comunque affascinante.

<<http://www.biomedcentral.com/1471-2105/8/176/abstract>>

era ridicolo. I serbatoi di carburante sono molto spessi, rendendoli difficilmente danneggiabili. I serbatoi dell'aeroporto sono separati dalle condutture mediante valvole d'arresto, pertanto anche se scoppiasse un incendio nelle loro vicinanze, le fiamme non entrerebbero nelle tubazioni. E la conduttura non esploderebbe comunque, dato che non vi è ossigeno che possa favorire la combustione. Non che i terroristi siano arrivati (o abbiano dimostrato di poter arrivare) al punto di procurarsi gli esplosivi. O una pianta aggiornata dell'infrastruttura dell'aeroporto, se è per questo.

Ma leggete quel che aveva da dire Russel Defreitas, il leader dei terroristi: "Tutte le volte che si colpisce Kennedy, è la cosa più offensiva che si possa fare agli Stati Uniti. Colpire l'aeroporto John F. Kennedy... wow... Tutti amano il JFK, è come Kennedy in persona. Se colpisci quello, tutto il paese è in lutto. È come se potessi uccidere Kennedy due volte".

Se questi sono i terroristi che stiamo combattendo, abbiamo di fronte un nemico del tutto incompetente.

Non si poteva dedurlo leggendo quanto riportato dalla stampa, però. "Se questo complotto fosse andato a buon fine, la devastazione che avrebbe causato è semplicemente inconcepibile", ha dichiarato il procuratore statunitense Roslynn R. Mauskopf a una conferenza stampa, definendolo "uno dei più agghiaccianti complotti immaginabili". Il senatore Arlen Specter (R-Pennsylvania) ha aggiunto "Aveva il potenziale di essere un altro 11 settembre".

Queste persone sono fuori strada tanto quanto Defreitas.

L'unica voce ragionevole pare sia stata il Sindaco di New York Michael Bloomberg, che ha detto: "Esistono moltissime minacce nel mondo. La minaccia di un attacco cardiaco dovuto a cause genetiche, per esempio. Non ci si può mettere lì a preoccuparsi di ogni cosa. Ma trovatevi una vita... È più probabile che vi colpisca un fulmine che un terrorista".

Ed è stato ampiamente criticato per questo.

Questa non è la prima volta che un gruppo di terroristi incompetenti con un piano irrealizzabile è stato dipinto dai media come gente pronta a fare ogni genere di danno all'America. A maggio si è saputo di un complotto di sei uomini per attaccare Fort Dix penetrando travestiti da fattorini per la consegna di pizze, sparando a quanti più soldati e Humvee possibili, quindi ritirandosi incolumi per riprendere l'attacco un altro giorno. Il loro piano, così com'era, è andato in fumo quando hanno portato la videocassetta con un filmato delle loro esercitazioni armate in un negozio per essere riversata su DVD. Il commesso del negozio ha contattato la polizia, che a sua volta ha contattato l'FBI. (I miei ringraziamenti al commesso per non avere reagito in modo eccessivo, e all'agente dell'FBI che si è infiltrato nel gruppo).

I "Miami 7", fermati lo scorso anno per aver pianificato, fra le altre cose, di far saltare la Sears Tower, erano un altro gruppo di incompetenti: niente armi, niente bombe, nessuna esperienza, niente soldi e nessuna abilità operativa. E non dimentichiamoci Lyman Faris, il camionista dell'Ohio, condannato nel 2003 per la trama risibile di

distruggere il ponte di Brooklyn con una fiamma ossidrica. Almeno alla fine ha concesso che il piano non aveva buone probabilità di riuscita.

Non penso nemmeno che questi pazzoidi, con le loro minacce da trama cinematografica, si meritino l'appellativo di "terrorista". Ma in questo paese, se da un lato occorre essere competenti per compiere un attacco terroristico, dall'altro non è necessario essere competenti per provocare terrore. Tutto quel che si deve fare è cominciare a perpetrare un attacco e, a prescindere che si abbiano o meno un piano realizzabile, delle armi, o persino la più vaga idea di ciò che si sta facendo, i mass media vi aiuteranno a terrorizzare l'intera popolazione.

Il premio per la storia più ridicola legata alla vicenda dell'aeroporto JFK va al New York Daily News, con la sua intervista a una cameriera che aveva servito del salmone a Defreitas; il titolone in prima pagina strillava: "Il maligno pranzava al tavolo 8".

Seguendo una di queste fallite disavventure del terrore, l'amministrazione invariabilmente assalta le news per strombazzare qualsiasi inefficace misura di "sicurezza" stia cercando di promuovere, che siano documenti d'identità nazionale, spionaggio di massa a cura della National Security Agency oppure un data mining sterminato. Non importa che in tutti quei casi ciò che ha permesso di fermare i malviventi sia stato lavoro di polizia alla vecchia maniera, quel genere di cose che si vedono nei film di spionaggio di qualche decennio fa.

L'amministrazione ha ripetutamente attribuito la cattura di Faris ai programmi di intercettazione senza mandato della NSA, anche se ciò è semplicemente falso. Discorso analogo per i terroristi dell'11 settembre: hanno avuto successo in parte perché l'FBI e la CIA non hanno seguito gli indizi prima degli attacchi.

Anche a Londra, i dinamitardi con esplosivi liquidi sono stati catturati grazie a metodi tradizionali di investigazione e intelligence, ma questo non impedisce al Segretario della Sicurezza Nazionale Michael Chertoff di usarlo come pretesto per giustificare l'accesso alle informazioni personali dei passeggeri delle linee aeree.

Naturalmente anche i terroristi incompetenti possono combinare guai. È stato provato più di una volta in Israele, e se il bombarolo Richard Reid fosse stato un poco meno stupido e avesse innescato le scarpe nella toilette, avrebbe potuto far saltare un aeroplano.

Pertanto queste persone dovrebbero essere incarcerate... beh, assumendo che siano veramente colpevoli. Malgrado la frenesia iniziale della stampa, molto spesso i dettagli veri e propri di questi casi si rivelano essere molto meno incriminanti. Troppo spesso non è chiaro se gli imputati sono davvero colpevoli, o se la polizia ha creato un crimine dal nulla.

I cospiratori dell'aeroporto JFK pare siano stati incitati da un informatore, uno spacciatore di droga già detenuto un paio di volte. Un informatore dell'FBI ha quasi certamente spinto i cospiratori di Fort Dix a fare cose che non avrebbero normalmente fatto. La trama della Sears Tower è stata suggerita alla gang di Miami da un agente dell'FBI sotto copertura che aveva infiltrato il gruppo. E nel 2003 ci è voluta una trappola molto elaborata che ha coinvolto tre paesi per arrestare un trafficante di armi

per la vendita di un missile superficie-aria a un sedicente estremista musulmano. È molto probabile che in tutti questi casi vi sia stata induzione al reato.

E il resto puzza di esagerazione. Jose Padilla non era esattamente pronto a far saltare una bomba sporca negli Stati Uniti, malgrado le istrioniche dichiarazioni dell'amministrazione sostengano il contrario. Ora che il processo sta andando avanti, l'imputazione maggiore che può chiedere il governo è cospirazione in omicidio, sequestro e mutilazione, e sembra difficile che le accuse verranno sostenute. Le accuse di terrorismo nei confronti di Rashid Rauf, presunto capobanda dei "dinamitardi liquidi" del Regno Unito, furono ritirate per mancanza di prove (dei 25 arrestati, solo 16 sono stati accusati). E ora sembra che anche lo stratega del JFK sia tutto chiacchiere e niente azione.

Vi ricordate i "Sei di Lackawanna", quei terroristi dell'upstate New York che nel 2003 si dichiararono colpevoli di "fornire supporto o risorse a un'organizzazione terroristica straniera"? Si costituirono poiché vennero minacciati di venire rimossi completamente dal sistema legale. Non sappiamo se fossero davvero colpevoli, né di cosa.

Anche nelle migliori delle circostanze, si tratta di processi difficili. Arrestare delle persone prima che abbiano compiuto il loro piano significa cercare di provare l'intento, e questo scivola rapidamente nell'ambito dello psicoreato. Regolarmente l'accusa si serve di ottusa letteratura religiosa nelle abitazioni degli imputati per provare ciò in cui credono, e questo può sfociare in dibattiti sulla teologia islamica in un'aula di tribunale. E poi c'è la questione di dimostrare una connessione fra un libro su uno scaffale e un'idea nella mente dell'imputato, come se il fatto che stiate leggendo questo articolo o che abbiate acquistato un mio libro dimostri che siete d'accordo con tutto quel che dico. (The Atlantic ha recentemente pubblicato un articolo affascinante sull'argomento).

Sarò il primo ad ammettere di non avere in mano tutti i fatti relativi a ognuno di questi casi. Nessuno di noi li ha. Pertanto facciamoci venire un sano scetticismo. Scetticismo, quando leggiamo di questi terroristi geni del crimine che erano sul punto di uccidere migliaia di persone e causare danni incalcolabili. Scetticismo, quando ci viene detto che il loro arresto è la dimostrazione che dobbiamo rinunciare alle nostre libertà e ai nostri diritti. Scetticismo, sul fatto che gli individui arrestati siano davvero colpevoli.

Esiste una minaccia terroristica reale. E se da un lato sono pienamente favorevole alla continua incompetenza dimostrata dai "terroristi", so che ve ne sono altri che si dimostreranno molto più capaci. Abbiamo bisogno di una sicurezza vera, che non ci richieda di indovinare la tattica o il bersaglio: l'intelligence e l'investigazione, proprio ciò che ha permesso di catturare tutti questi aspiranti terroristi, e la risposta alle emergenze. Ma la retorica della "guerra al terrore" è fatta di politica più che di razionalità. E non dovremmo permettere alla politica della paura di renderci tutti meno sicuri.

Vi sono un'infinità di link associati a questo articolo. Potete trovarli nella versione online:

<http://www.schneier.com/blog/archives/2007/06/portrait_of_the.html>

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/politics/security/commentary/securitymatters/2007/06/securitymatters_0614>

oppure <<http://tinyurl.com/29mxc5>>

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

L'insegnamento dei virus

Più di due anni fa, George Ledin scrisse un articolo in "Communications of the ACM" in cui sosteneva l'insegnamento di worm e virus agli specializzandi in informatica: "Gli studenti di informatica dovrebbero imparare a riconoscere, analizzare, disabilitare ed eliminare il software malevolo. Per farlo, devono studiare i virus e i worm attualmente in circolazione, e programmarne di propri. La programmazione è per l'informatica quel che l'esercitazione sul campo è per la polizia e l'esperienza clinica per la chirurgia. Leggere un libro non basta. Perché l'industria recluta hacker criminali come consulenti di sicurezza? Perché non siamo stati in grado di istruire adeguatamente i nostri studenti".

Questo semestre ha tenuto il corso alla Sonoma State University. Ha ottenuto parecchia copertura da parte della stampa. Nessuno ha scritto un virus come progetto di classe. Nessun nuovo malware è finito "in the wild". Nessuna nuova specie di supercattivo si è diplomato.

Insegnare queste cose è semplicemente brillante.

L'articolo:

<<http://www.csl.sri.com/neumann/insiderisks05.html#175>>

<<http://www.sonoma.edu/pubs/newsrelease/archives/001090.html>>

<<http://www1.pressdemocrat.com/apps/pbcs.dll/article?AID=/20070522/NEWS/705220312/1033/NEWS01>>

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

<<http://blogs.pcworld.com/staffblog/archives/004452.html>>

<<http://www1.pressdemocrat.com/apps/pbcs.dll/article?AID=/20070526/NEWS/705260309/1043/OPINION01>>

oppure <<http://tinyurl.com/2e2anv>>

<<http://www.hardocp.com/news.html?news=MjU5NzgsLCxoZW50aHVzaWFzdCwsLDE>>

<<http://technews.acm.org/archives.cfm?fo=2007-05-may/may-25-2007.html#313412>>

oppure <<http://tinyurl.com/yuur5l>>

<<http://www.calstate.edu/pa/clips2007/may/22may/virus.shtml>>

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

Rubato l'orologio di Bush?

Schneier interverrà alla I-4 Conference il 25 giugno a Milano.

<https://i4online.com/>

Schneier parlerà al Secure 2007 il 26 giugno a Bad Homburg (Germania).

<<http://www.secure2007.de/>>

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

Il vincitore della seconda edizione del Concorso "Minaccia da Trama Cinematografica"

Il primo aprile ho annunciato la seconda edizione del Concorso "Minaccia da Trama Cinematografica":

"Il vostro obiettivo: inventare una trama terroristica per dirottare o far saltare un aereo utilizzando come componente chiave un comune oggetto che viene solitamente portato a bordo. Tale componente dovrà essere talmente essenziale per la riuscita del piano che la TSA non avrà altra scelta che vietare l'oggetto in questione una volta scoperto il piano terroristico. Voglio vedere una trama impressionante e assurda, ma abbastanza plausibile da venire presa sul serio.

"Fate in modo che la TSA proibisca gli orologi da polso. O i computer portatili. O il poliestere. O gli accendini più lunghi di sette centimetri. Insomma, avete capito il concetto.

"La vostra proposta verrà giudicata in base all'oggetto scelto (che la TSA non potrà far altro che vietare) e all'ingegnosità della trama. Deve inoltre essere realistica: niente fantascienza, grazie. E il resoconto è essenziale: l'anno scorso le proposte migliori erano anche le più divertenti e piacevoli da leggere".

Il 5 giugno ho scelto tre semifinalisti fra i 334 commenti pervenuti:

* Farfalle e bevande: occorre vietare l'acqua.

* Dimetilmercurio: i checkpoint di sicurezza devono essere proibiti, ma ovviamente non si possono eliminare. Ah, che fare?!

* Bomba all'ossidrogeno: si devono vietare i fili: auricolari, cavi di alimentazione, ecc.

Bene, abbiamo un vincitore. Non posso divulgare la formula esatta (perché tutti sabotereste il sistema l'anno prossimo), ma posso dire che è stata una combinazione del mio giudizio, del consenso espresso nei commenti sul blog, e della opinione di Tom Grant (il vincitore dello scorso anno -- Non è il suo vero nome).

Il vincitore è... "Farfalle e bevande", inviato da Ron. (Ron riceve copie autografate dei miei libri, un certificato regalo Amazon del valore di 50 dollari messo a disposizione da un lettore e, se riesco a trovarne uno, un'intervista con un vero regista

cinematografico. Qualcuno ne conosce uno? Spero che uno dei premi non sia una visita dell'FBI).

Ecco il contributo vincente:

Il giorno prima doveva essere stato un bel prato, pensò Wilkes. Cercò di immaginarsi com'era, senza quella ferita lunga e ampia che squarciava la terra, senza la fusoliera spezzata e carbonizzata dell'aereo che l'aveva scavata prima che il suolo fosse cosparso di carte, cuscini, frammenti di plastica e tessuto di ogni genere, e di tutte le cose all'interno dell'aereo che ora giacevano come coriandoli di un corteo brevissimo e impetuoso.

Sì, proprio un bel posticino, abbastanza lontano dalle piste dell'aeroporto da non essere troppo rumoroso, ma abbastanza vicino da poter osservare gli aerei atterrare e decollare. Fortunatamente un po' troppo vicino all'aeroporto per essere urbanizzato. Quando l'aereo si rivoltò e puntò verso il basso, neanche un miglio oltre la fine della pista, almeno le sole persone a rischio erano i passeggeri. Per loro, grazie al cielo, tutto è accaduto velocemente: l'impatto li ha uccisi prima che i serbatoi dell'ala schiantata si incendiassero. I corpi carbonizzati erano ancora seduti ai loro posti.

Notò il tizio della NTSB, in piedi accanto alla metà anteriore della fusoliera. Facile notarlo fra quelli della FAA e il personale dell'aeroporto della zona: gli uomini della NTSB erano sempre gli unici in giacca e cravatta in mezzo alla folla. Avvicinandosi, Wilkes considerò che il caso non sarebbe stato troppo difficile: quando gli aerei arrivano a terra così intatti, frammentandosi soltanto in pochi pezzi dopo l'impatto, la causa è sempre più facile da trovare. E quella situazione non sembrava molto diversa.

"Wilkes", mormorò rivolto al tizio elegante, indicando il badge attaccato alla camicia. Non c'era bisogno di diventare troppo amichevoli, avrebbero comunque stilato due rapporti distinti. Finché c'era il benché minimo vago accordo fra loro, non era necessario parlare direttamente al tizio. "E questo piccolo capolavoro?", si chiese ad alta voce, osservando la breccia sul fianco del jet abbattuto.

"Esplosione", biascicò l'uomo della NTSB. Aveva quel tono alla Chuck Yeager un po' rallentato, pensò Wilkes, come di qualcuno che potrebbe starsene calmo e rilassato descrivendo l'Armageddon. "Pare che sia avvenuta dall'interno, un oggetto abbastanza grande da strappar via qualche metro quadrato dalla fiancata. Abbastanza per buttare l'aereo su un fianco".

"E se l'aereo è sufficientemente basso, ancora in fase di decollo, con i motori prossimi alla spinta massima, si rovescia e precipita troppo velocemente...", lasciò sfumare le parole, immaginando il risultato.

"Già, tutto in un paio di secondi. Troppo veloce per dar tempo all'equipaggio di riportarlo indietro". Il tizio della NTSB scosse la testa, la tessera di identificazione attaccata alla giacca prese a ondeggiare seguendo il movimento. "Sempre il momento migliore quando vuoi tirar giù un uccellino: il decollo o l'atterraggio... Mi sa che chiunque abbia fatto questo scherzetto voleva sbrigarcela in fretta". Sbuffò e con tono

di schermo aggiunse, "Qualcuno ha introdotto un esplosivo a bordo; forse uno degli screener stava avendo una giornataccia".

"Forse", disse Wilkes, che non era così propenso a imputare il tutto al semplice errore di uno screener. Quelli della NTSB erano sempre pronti a trovare una decisione sbagliata, un errore umano, e da lì spiegare tutta la faccenda. Ma il lavoro di Wilkes era quello di trovare le vulnerabilità nei sistemi, le procedure, e il pensare a misure preventive. Forse era andata proprio così, nient'altro che uno screener che si era lasciato sfuggire una granata o una barretta di dinamite, qualcosa di talmente ovvio che non restava altro da fare che attribuire la morte di 183 persone a un folle e a un mediocre impiegato della TSA.

Ma forse no. Fu a quel punto che Wilkes notò le prime due farfalle. Di color giallo brillante contro il nero carbonizzato della carcassa bruciata, sembravano gli elementi più incoerenti di tutta la situazione. E mentre stava pensando a questo, ne apparve un'altra.

Mentre venivano scattate foto ed effettuati i rilevamenti, altre farfalle iniziarono a comparire, una alla volta, o a coppie, altre si allontanavano, ma gradualmente aumentavano di numero, arrivando ad esservene decine e decine nel corso della mattinata. Un dettaglio strano, il rappresentante della NTSB non poteva negarlo, ma nulla che dicesse qualcosa sul terrorista che ha abbattuto quell'aereo.

Wilkes non era così sicuro. Di una cosa era certo, che madre natura stava lasciando una traccia grossa come una casa davanti ai loro occhi. Ma che cosa diavolo poteva significare?

Si avvicinò con la fotocamera del cellulare, scattando qualche buona immagine ravvicinata di quegli insetti colorati, e inviandola all'ufficio via email, con la richiesta di contattare un esperto. Aveva bisogno di una consulenza telefonica, di qualcuno che conoscesse il comportamento di questa particolare farfalla, qualcuno che potesse metterlo sulla pista giusta.

Nel giro di pochi minuti, il suo cellulare suonò, una chiamata in audioconferenza già impostata con un professore di entomologia; ancora meglio, un professore della zona, che quindi poteva conoscere questo insetto meglio di qualche altro accademico di un'università più prestigiosa, ma anche più lontana.

Durante le presentazioni, Wilkes non stava realmente ascoltando. Non gli importava sapere chi era quel tizio nei dettagli, la squadra regionale avrebbe avuto tutti i particolari a disposizione se gli fossero serviti più tardi. Adesso voleva semplicemente delle risposte.

"Pieridi", suggerì il professore, "e tutti maschi, ci scommetto".

"Okay", rispose Wilkes, chiedendosi se fosse davvero un indizio rivelatore. "Perché se ne stanno tutte sulla mia breccia?"

“Non posso esserne certo, ma deve trattarsi di qualcosa che le attira. Questi insetti vengono comunemente chiamati ‘farfalle dello zolfo’... Che ci sia dello zolfo sulla carcassa?”

Sicuro, Wilkes pensò; questo sembra sempre più un vicolo cieco. “Niente zolfo, abbiamo già effettuato un veloce test chimico a riguardo. C’è qualche altra cosa che può piacere a queste piccoline?”

“Ah sì, ma dubito che si tratti di qualcosa che troverebbe in un ordigno: il sodio. Lo avvolgono insieme al loro sperma e lo mandano alla femmina come un piccolo dono, un po’ come i fiori e i cioccolatini del mondo delle farfalle”.

“Okay, è incredi... wow, le cose che si imparano in questo lavoro. Scusi se l’ho disturbata, professore, immagino che sia solo... beh, sì, grazie”.

Sperma di farfalla: questo potrebbe segnare un nuovo record come sciocchezza più inutile appresa durante l’indagine di un disastro aereo. Roba da non credere.

Il tizio della NTSB si fece più vicino vedendo che Wilkes aveva finito di parlare al telefono. “Ha ottenuto qualcosa dall’esperto?”, domandò, cercando di mascherare un sorrisino senza riuscirci. Wilkes già si immaginava che presto sarebbe circolata una nuova storiella negli uffici della NTSB, quella dell’“uomo farfalla” della FAA. Ah, beh, meglio così che del tutto anonimi.

“Nah, non molto. Alle farfalline piace lo zolfo...”, Wilkes buttò lì, vedendo che il suo interlocutore accolse l’informazione con una risatina sarcastica. “...E il sodio. A meno che non ci fosse una gran quantità di sale tutt’intorno all’esplosivo del nostro terrorista, queste piccole amiche gialle rimangono un mistero”.

L’uomo della NTSB cambiò espressione, e il suo sguardo si fece assorto. “Sodio. Un esplosivo che lascia tracce di sodio... Beh, potrebbe essere...”

Si guardarono, entrambi diretti verso la medesima conclusione, entrambi restii ad arrivarci. Wilkes lo disse per primo: “Sodio metallico. Economico, facile da ottenere, dev’essere lui: sodio metallico”.

“E molto facile da introdurre su un aereo”, biascicò il rappresentante della NTSB. “Il materiale è tenero, ma si può modellarlo e inserirlo in qualsiasi cosa: montature di occhiali, fibbie di cintura, bottoni, cose semplici che non attirerebbero mai l’attenzione degli screener”.

“E ne basta una piccola quantità”, aggiunse Wilkes ricordando una vecchia burla del corso di chimica al college. “50-60 grammi, sufficienti a far saltare la fiancata di un aereo, sufficienti per spiegare quel che abbiamo qui davanti agli occhi”.

“Con il detonatore più comune del mondo”, continuò l’uomo della NTSB, verbalizzando l’immagine che stava formandosi nella mente di Wilkes. Un bicchiere d’acqua e nulla più, basta lasciarvi cadere il sodio metallico e la reazione chimica rilascia rapidamente gas idrogeno, con abbastanza calore generato come effetto collaterale della reazione

bit...’ Ma di che stanno parlando? Vi fidereste di un crittografo che non conosce la differenza fra crittografia simmetrica e a chiave pubblica? ‘La nostra tecnologia [...] è l'unico sistema di criptazione inviolabile disponibile in commercio’. Il fondatore della compagnia viene citato in un articolo: ‘Tutti gli altri metodi di criptazione sono stati compromessi negli ultimi cinque-sei anni’. Forse nella loro realtà alternativa, ma non in quella in cui tutti viviamo.

“La loro soluzione prevede di non criptare affatto i dati. ‘Noi crediamo vi sia una sola semplice regola nella criptazione: se qualcuno può criptare dei dati, qualcun altro sarà in grado di decifrarli. L'idea che sta alla base di VME è che i dati non vengano né criptati né trasferiti. E se essi non vengono criptati e non vengono trasferiti, non vi è nulla da violare. E se non vi è nulla da violare, il sistema è inviolabile’. Ha ha: è uno scherzo. In realtà i dati vengono criptati, ma loro danno un altro nome al processo”.

Andate a leggerlo tutto, è davvero forte.

Sono ancora in circolazione, e stanno ancora pubblicizzando la loro fantasmagorica “virtual matrix encryption” (il brevetto è finalmente pubblico, e se qualcuno può fare del reverse-engineering sulla combinazione del linguaggio da ufficio brevetti e del burocratese per trasformarlo in un algoritmo, potremo vedere tutti quanto orribile esso sia). La parte tecnica sul loro sito è migliore rispetto al 2003, ma è ancora piuttosto sforzata.

Nel 2005 hanno ottenuto la certificazione del loro prodotto FIPS 140-1. La certificazione riguardava la loro implementazione AES, ma cercano di insinuare che sia stata la VME a essere certificata. Dal loro sito: “La forza di una crittografia al megabit (VME). La garanzia di uno standard a 256 bit (AES). Entrambe le tecnologie insieme in un modulo certificato! FIPS 140-2 CERTIFICATO #505”.

Questo per dimostrare che con un po’ di giochi di prestigio è possibile avere qualsiasi cosa certificata FIPS 140.

<<http://www.meganet.com/>>
<<http://www.meganet.com/Technology/intro.asp>>
<<http://www.meganet.com/Technology/explain.asp>>
<<http://www.meganet.com/challenges/default.asp>>

Il mio articolo del “Canile”:

<<http://www.schneier.com/crypto-gram-0302.html#4>>

Il mio articolo sullo ‘snake oil’:

<<http://www.schneier.com/crypto-gram-9902.html#snakeoil>>

Il brevetto:

<<http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetacgi%2FPTO%2Fsrchnu m.htm&r=1&f=G&l=50&s1=6219421.PN.&OS=PN/6219421&RS=PN/6219421>>
oppure <<http://tinyurl.com/28stql>>

La certificazione FIPS (#505 su questa pagina):

** *** *****

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul 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 sempre <<http://www.schneier.com/crypto-gram.html>>

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>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

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>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane

protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

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

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2007 - Bruce Schneier.