

<http://www.aeaweb.org/permissions.php>

Copyright © 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 by the American Economic Association.

Permission to make digital or hard copies of part or all of American Economic Association publications for personal or classroom use is granted without fee provided that copies are not distributed for profit or direct commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation, including the name of the author. Copyrights for components of this work owned by others than AEA must be honored. Abstracting with credit is permitted.

The author has the right to republish, post on servers, redistribute to lists and use any component of this work in other works. For others to do so requires prior specific permission and/or a fee. Permissions may be requested from the American Economic Association Business Office.

È permesso fare copie digitali e cartacee di parti o dell'intero contenuto delle pubblicazioni dell'American Economic Association esclusivamente per uso personale o per uso didattico a condizione che le copie siano gratuite e non utilizzate per fini di lucro o per ottenere vantaggi commerciali anche indiretti e che ciascuna copia contenga nella prima pagina, o sulla schermata iniziale, questo avviso con la citazione completa dell'opera e dei suoi autori. Gli eventuali diritti di terze parti, diverse da AEA, richiamate in questo documento devono essere garantiti. Sono permesse sintesi che riportino i corretti riferimenti.

L'autore ha il diritto di ripubblicare, anche elettronicamente, distribuire a liste ed usare qualsiasi parte di questo documento anche in altri lavori; per tutti gli altri tale possibilità richiede una preliminare autorizzazione e/o il pagamento di una fee. Le autorizzazioni possono essere richieste all'American Economic Association Business Office.

Aspetti economici del crimine online

(la versione originale in lingua inglese di questo documento è disponibile, in formato pdf, in

<http://people.seas.harvard.edu/~tmoore/jep09.pdf>. Traduzione italiana a cura di Agatino Grillo,

<http://www.agatinogrillo.it/>, disponibile in <http://www.agatinogrillo.it/content/aspetti-economici-del-crimine-online-tyler-moore-richard-clayton-ross-anderson-italiano>)

Tyler Moore, Richard Clayton e Ross Anderson

Tyler Moore è ricercatore presso il Center for Research on Computation and Society (CRCS), Harvard University, Cambridge, Massachusetts. Richard Clayton è ricercatore in ambito privato e Ross Anderson è professore di Security Engineering presso il Computer Laboratory dell'Università di Cambridge, in Inghilterra. Le loro email sono rispettivamente: tmoore@seas.harvard.edu, Richard.Clayton@cl.cam.ac.uk e Ross.Anderson@cl.cam.ac.uk.

L'economia della sicurezza è diventata, di recente, una disciplina accademica in forte crescita; questo filone di ricerca ha avuto inizio nel 2001 dall'osservazione che errati o insufficienti incentivi economici possono spiegare il fallimento dei sistemi di sicurezza almeno quanto i fattori tecnici (Anderson, 2001). Spesso infatti i sistemi informativi sono controllati da infrastrutture i cui responsabili hanno interessi divergenti per cui l'analisi microeconomica e la teoria dei giochi giocano un ruolo importante nello studio dell'affidabilità dei protocolli di sicurezza e delle tecniche di crittoanalisi. L'approccio "economico" non solo fornisce un modo più semplice ed efficace per analizzare i problemi della sicurezza delle informazioni in ambiti quali la privacy, lo spam ed il *phishing* ma fornisce agli studiosi anche un quadro di riferimento su temi quali l'affidabilità, i conflitti di interesse ed il crimine. Dal 2002 si svolge ogni anno il *Workshop on the Economics of Information Security* (WEIS): oggi questo ambito di ricerca coinvolge oltre 100 ricercatori e riunisce insieme ingegneri della sicurezza, economisti ed anche avvocati e psicologi. Per un'analisi generale ed un *survey* sulla economia della sicurezza in termini generali si veda Anderson e Moore (2006).

Questo studio si focalizza in particolare sugli aspetti del crimine online che, dal 2004, si è trasformato in una vera e propria impresa economica. Prima di tale data la maggior parte delle minacce online era rappresentata da hacker dilettanti che si dedicavano al *defacement* dei siti web ed allo sviluppo di codice pericoloso per lo più per potersi vantare delle proprie azioni. Ai “vecchi tempi”, la frode elettronica era per lo più un’attività da retrobottega, a carattere familiare e molto inefficiente: il tipico “frodatore” gestiva un piccolo business integrato verticalmente. Il criminale, ad esempio, acquistava uno strumento per programmare le carte di credito ed apriva poi un negozio nel quale accettava i pagamenti con carta di credito; in tal modo poteva quindi copiare illegalmente le carte che poi sfruttava facendo acquisti illegali o prelevando somme ai bancomat. Similmente di solito la frode elettronica riguardava gli addetti al *call-center* che rubavano le password e le facevano usare ad un complice. Oggi invece siamo in presenza di veri e propri network criminali – una sorta di nuovo mercato nero nel quale i criminali commerciano tra loro e dove si è creata una netta specializzazione di ruoli (Thomas e Martin, 2006). Proprio come nella fabbrica di spilli di Adam Smith, la specializzazione ha portato ad un incredibile guadagno di produttività anche se in questo caso si parla di codici segreti di bancomat invece che di manufatti in metallo. Come è illustrato nella **tabella 1**, chiunque sia in grado di raccogliere carte bancomat o di credito, PIN e codici di accesso per l’*electronic banking* può adesso rivenderli attraverso broker anonimi con tariffe che vanno dai \$0,40 fino ai \$20,00 per ogni carta e da \$10 fino a \$100 per ogni *account* bancario (Symantec, 2008). Le tariffe richieste per appropriarsi dell’identità digitale di qualcun altro (nominativo, *social security number*, data di nascita) variano da \$1 fino a \$15. I broker a loro volta vendono le credenziali agli specialisti del riciclaggio di denaro sporco che sono in grado di nascondere il denaro e ripulirlo.

Un *modus operandi* comune consiste nel trasferire il denaro dal conto bancario della vittima a quello di un “mulo” (*money mule*). I muli sono di solito persone ingenuie raggirate sulla reale provenienza del denaro, indotte ad accettarlo e poi a trasferirlo a loro volta a qualcun altro. I criminali li assoldano per mezzo di annunci di lavoro via e-mail o su siti specializzati come Craigslist o Monster (Krebs, 2008a), che offrono la possibilità di lavorare da casa come “*transaction processor*” o “*sales executive*”. Ai “muli” viene raccontato che il denaro che riceveranno è la contropartita di merci già vendute o di servizi già resi e che il loro incarico consiste nel trattenere una commissione e girare il resto della somma usando sistemi di pagamenti “non revocabili” quali i sistemi di *money transfer* tipo Western Union. Ma se il mulo ha girato il denaro attraverso tali *money transfer* e la frode viene alla luce allora il mulo diventa personalmente responsabile dei fondi che ha inviato. I “cassieri” criminali (*cashier*) usano il denaro rubato anche per pompare il prezzo delle azioni di piccole società minori nelle quali hanno investito e spesso “ripuliscono” il denaro ricevuto dai “muli” attraverso servizi sul web come il poker online e le aste su Internet.

Anche la raccolta delle password bancarie è diventato un lavoro specializzato. I “*phishermen*” fanno copie dei veri siti web delle banche e inducono i clienti incauti ad autenticarsi con le proprie credenziali autentiche sui falsi siti ed in tal modo si impossessano dei numeri di conto corrente, delle password e delle altre credenziali. Questi *phishermen* si servono a loro volta di “*spammer*” per convincere i clienti incauti a utilizzare i loro siti fasulli attraverso l’invio di e-mail che spacciano come email proveniente dalla vera banca. Sia gli *spammer* sia i *phishermen* usano software maligno come il “*malware*” che è progettato esplicitamente per infettare i computer delle persone che lo usano; per spingere le vittime ad usare questi software dannosi si fa credere loro che si tratti ad esempio di programmi innocui o li si convince a visitare uno dei tre milioni di siti infetti (Provos, Mavrommatis, Rajab e Monrose, 2008). L’emergere di un mercato del *malware* che genera profitti indica che questo software maligno non viene più scritto da *teenager* alla ricerca di notorietà ma da vere e proprie aziende criminali (*firm*) che dispongono di budget per la ricerca, lo sviluppo ed il *testing*. Queste “*firm*” sono in grado addirittura di assicurare ai propri clienti criminali che i loro prodotti non sono intercettabili dai software antivirus ed offrono aggiornamenti quando gli antivirus diventano in grado di intercettarli (Schipka, 2007).

Tabella 1

Dati sulla criminalità informatica

	<i>Stima</i>	<i>Fonte</i>
<i>Prezzo unitario per la commercializzazione nell'economia sommersa</i>		
Credenziali di conto bancario	\$10–\$100	Symantec (2008)
Carta di credito	\$0.40–\$20	Symantec (2008)
Dati per furto di identità (nominativo, SSN, data compleanno, ecc.)	\$1–\$15	Symantec (2008)
Asta di credenziali di conto	\$1–\$8	Symantec (2008)
<i>Numero di computer e siti web compromessi</i>		
Computer facenti parti di <i>botnet</i>	5 milioni	Symantec (2008)
Computer infetti con software maligno per furto di identità	10 milioni	Panda Security (2009)
False pagine web usate per il <i>phishing</i> (banche fasulle)	116,000	Moore and Clayton (2009)
Siti web che infettano i visitatori per mezzo di software maligno (<i>malware</i>)	3 milioni	Provos et al. (2008)
<i>Perdite annue</i>		
Frodi online di banche del Regno Unito (6/2007–5/2008)	£36,5 milioni	APACS (2008)
Perdite dirette dovute a furto di identità negli U.S.A. (2006)	\$2,8 miliardi	Gartner (2006)
Danni in Europa causati dal <i>malware</i> (2006)	€9,3 miliardi	Computer Economics (2007)

Una conseguenza di questo nuovo quadro “industriale” è che mentre il software antivirus in precedenza riusciva ad intercettare la maggior parte del *malware* adesso esso riesce a bloccarne solo una minima parte. I computer infetti sono in grado, inoltre, di registrare i tasti premuti dai loro utilizzatori quando digitano le credenziali per l'*electronic banking*; essi possono anche essere utilizzati per realizzare reti di computer infetti, le *botnet*, di cui parleremo successivamente. Anche se le stime variano, c'è un generale consenso che in ogni istante circa il 5% di tutti i computer del mondo sono soggetti alle infezioni del *malware* (*House of Lords Science and Technology Committee*, 2007); un *security provider* ha stimato che esistono circa 10 milioni di computer infetti da *malware* progettato per rubare le credenziali online (Panda Security, 2009). In questo nuovo ecosistema criminale online si è creata una nuova professione: il “pastore di botnet” (*botnet herder*) – una persona che “gestisce” una *botnet* cioè una rete di personal computer infetti e li affitta a *spammer*, *phishermen* ed altri truffatori. I computer che fanno parte della *botnet* sono stati infettati con *malware* che permette alla *botnet* di controllarli da remoto proprio come se fossero dei robot. Quasi tutto lo spam email è mandato attraverso *botnet*. Molti siti web criminali sono ospitati dalle *botnet*: dalle farmacie online fino alle false banche usate per fare *phishing* ed alle aziende fasulle usate per “assumere” i “*money mule*” (Moore e Clayton, 2008a). Anche coloro che inviano le email (*blackmailer*) affittano le *botnet* e spesso, di solito in occasione di grandi eventi sportivi, minacciano di sovraccaricare i siti dei broker online per mezzo del traffico generato da tali *botnet*; nel 2004, tre Russi sono stati arrestati per aver estorto diverse centinaia di migliaia di dollari in questo modo (Sullivan, 2004). Una *botnet* è stata usata per “spegnere” parti significative dell'infrastruttura ICT dell'Estonia in segno di protesta politica (Lesk, 2007). Solo nella seconda metà del 2007 circa cinque milioni di computer hanno partecipato alle *botnet* senza che i loro

legittimi proprietari se ne accorgessero (Symantec, 2008). I criminali online sono anche coinvolti in molte altri tipi di frodi, dalle false lotterie, al furto di materiale ordinato online, all'alterazione di tariffe fino ad arrivare alla distribuzione di immagini pedopornografiche. I "costi" del crimine online sono stimati secondo quanto riportato nella **tabella 1**.

Contro questa rapida crescita ed industrializzazione della criminalità online i governi, le istituzioni e le imprese devono organizzarsi in modo nuovo.

Oggi di solito le banche nascondono le perdite dovute a truffe o ne danno la colpa ai propri clienti ed esitano nel condividere tali informazioni con le altre banche.

Anche le forze di polizia non si sono ancora organizzate in modo valido.

Il crimine online ha molte similitudini con gli aspetti economici del crimine convenzionale, lo studio dei quali ha avuto origine a partire dai primi determinanti lavori di Becker (1968). Ma ci sono pure alcune differenze interessanti determinate dalla scala globale del crimine online.

Possiamo trovare una interessante analogia storica due generazioni fa quando i criminali hanno iniziato ad utilizzare le automobili. All'improvviso uno svaligiante poteva intrufolarsi in diverse abitazioni in città dove la polizia non lo conosceva e tornare a casa sua in tempo per la colazione. Alla polizia servirono diversi anni per organizzarsi per mezzo di forze di polizia "nazionali" e non solo "locali" ed archivi di impronte digitali. Il crimine online, come il crimine "motorizzato", impone grossi cambiamenti sia perché è per sua natura transnazionale sia perché consiste di delitti di gran volume ma di basso valore unitario. Gli attuali meccanismi per la cooperazione internazionale tra le forze di polizia sono progettati per contrastare crimini poco frequenti e di grande impatto, come l'assassinio ed il terrorismo, mentre viceversa il crimine online è un reato di valore poco significativo ma compiuto su scala globale e industriale. Un'altra differenza è che il crimine convenzionale è in genere commesso da un numero minoritario dei componenti della società, di solito da giovani che soffrono di molteplici privazioni o che abusano di alcool o droga. Al contrario i criminali online di solito hanno avuto un'ottima educazione e formazione anche se vivono in società con poche prospettive di lavoro e polizia poco efficace.

Questo studio comincia da un'analisi dei dati sul crimine online. Poi si esaminano gli aspetti relative alle azioni collettive: persone che connettono personal computer infetti ad Internet e che creano esternalità negative in quanto le loro macchine potrebbero spedire spam, ospitare siti di *phishing* e distribuire contenuti illegali. L'architettura di Internet, globale e distribuita, ha come conseguenza un tipo di sicurezza a "catena" in cui l'anello più debole può compromettere l'intero sistema, anello debole che in questo contesto è lo scarso coordinamento tra istituzioni pubbliche ed attori privati impegnati nel contrastare il crimine.

Nello studio presentiamo evidenze empiriche di come i criminali informatici (gli "attaccanti") riescono a muoversi agilmente tra le frontiere nazionali; il nostro obiettivo è illustrare le tattiche usate dai criminali online e discutere dei modi per migliorare la coordinazione tra le forze dell'ordine.

Infine esaminiamo come gli incentivi economici dei "difensori" della rete possono influenzarne i risultati. Un interessante caso di studio è la misura del tempo medio richiesto per rimuovere da Internet i differenti tipi di contenuto offensivo.

I siti di *phishing* che impersonificano in modo diretto famosi siti di *technology business*, come eBay, sono di solito rimossi in poche ore; siti che impersonificano banche di solito scompaiono dopo pochi giorni; i siti utilizzati per il riciclaggio del denaro rimangono invece in piedi molto più tempo in quanto non prendono di mira una singola banca ma l'intero sistema bancario e così nessuno li contrasta con particolare vigore.

Vedremo anche come il rifiuto delle banche (e dei loro fornitori) di condividere le informazioni sul *phishing* rallenti in modo significativo le attività di bonifica e come un intervento del settore pubblico è improbabile almeno nel breve termine.

Informazioni accurate

Nella maggior parte dei paesi le statistiche relative alle perdite dovute al crimine online sono difficili da ottenere. Ma senza tali statistiche altri dati - quali le vulnerabilità nei sistemi informativi, il numero di *botnet* o la quantità di spam - perdano il loro significato in relazione all'economia reale.

Un primo problema è che molte delle statistiche sui fallimenti della sicurezza sono elaborate da attori che hanno un incentivo di fatto a sovrastimare o sottostimare i dati. Per esempio il gruppo *anti-phishing* PhishTank si è vantato dal gran numero di siti identificati (OpenDNS, 2007) anche se eliminando i dati duplicati i numeri riportati si sarebbero ridotti in modo significativo (Moore e Clayton, 2007). L'associazione delle banche e del commercio del Regno Unito, APACS (*Association for Payment Clearing Services*), fornisce un altro esempio a riguardo; essa asserisce di aver rilevato un aumento del 726% negli attacchi di *phishing* tra il 2005 e il 2006 a fronte però di un aumento delle relative perdite del solo 44% (APACS, 2007).

I governi, al contrario, spesso cercano di minimizzare le statistiche sul crimine.

In un caso particolarmente significativo, il governo del Regno Unito ha cambiato le regole chiedendo che le denunce sulle frodi fossero inoltrate alla banca invece che alla polizia; questo cambiamento ha fatto sì che i dati statistici si siano ridotti fin quasi allo zero e ciò è stato aspramente criticato dal comitato parlamentare (*House of Lords Science and Technology Committee*, 2007). Anche gli ISP - *Internet Service Provider* - sono portati a sottovalutare i dati: essi vogliono minimizzare la quantità di traffico cattivo causato dal loro clienti, per timore che ciò influenzi le relazioni con gli altri *Internet Service Provider*.

Al momento ci sono due approcci "promettenti" per la misurazione del crimine online.

Infatti sebbene le singole banche non siano di solito disponibili a scambiarsi i dati sulle perdite per frodi è tuttavia possibile, in certi paesi, avere una aggregazione a livello nazionale dei dati delle banche. La Banca di Francia e l'APACS hanno infatti pubblicato i dati annuali aggregati relativi alle somme perdute dalle banche a causa degli attacchi di *phishing* rispettivamente in Francia e nel Regno Unito, insieme con il totale dei furti nei bancomat ed altre frodi finanziarie. Dato che le banche raccolgono questi dati per scopi operativi, per il controllo interno e l'audit, aggregarli su base nazionale è piuttosto semplice. In un rapporto sull'economia della sicurezza ed il mercato interno che c'è stato commissionato dalla Commissione Europea (Anderson, Bohme, Clayton e Moore, 2008), abbiamo già raccomandato che altri paesi seguano l'esempio della Gran Bretagna e della Francia e pubblichino questo tipo di dati aggregati nazionali.

Un approccio differente ma complementare è emerso in molti stati USA ed è stato recentemente preso in considerazione anche dal Parlamento europeo: ci riferiamo alle leggi sull'obbligo di dare notizia degli incidenti e violazioni di sicurezza.

Una legge della California emanata nel settembre del 2002 (*California State Senate*, 2002) obbliga infatti le organizzazioni private e pubbliche che operano in California ad avvertire le singole persone interessate quando i loro dati personali sono perduti, rubati o comunque acquisiti da personale non autorizzato. Il senso di questa normativa è garantire che ciascuno abbia la possibilità di proteggere i propri interessi e privacy in caso di furto di dati personali, come quando 45 milioni di numeri di carte di credito sono stati rubati dai sistemi informativi di T.J. Maxx (*Greenemeier*, 2007).

Questa legge voleva anche incentivare le aziende a conservare i dati in modo sicuro; Acquisti, Friedman e Telang (2006) hanno rilevato un impatto statistico significativo in negativo sul valore delle azioni a seguito della comunicazione al pubblico di un incidente di sicurezza. Romanosky, Telang, Acquisti (2008) hanno esaminato il rapporto sul furto di identità ottenuto dalla *Federal Communications Commission* relativo al periodo dal 2002 al 2007: analizzando le differenze temporali nell'adozione da parte di ciascuno stato delle proprie leggi sulla "comunicazione delle violazioni di sicurezza" (*breach disclosure*), si è rilevata una piccola ma significativa riduzione del numero di frodi. Le leggi sulla *breach disclosure* favoriscono inoltre la raccolta e pubblicazione dei

dati sugli incidenti di sicurezza. La legge della California ha ispirato ulteriori leggi in almeno altri 34 stati sebbene essi abbiano dettagli molto diversi.

La notificazione delle violazioni di sicurezza potrebbe essere migliorata con un centro di coordinamento centrale (*clearinghouse*) ed alcune procedure di standardizzazione. Il coordinamento sarebbe di aiuto per assicurare che tutte le violazioni riportate vengano a conoscenza della stampa, dagli investitori, dai ricercatori e dai regolatori di settore. Le future leggi USA ed EU dovrebbero anche definire standard minimi per la notificazione; alcune aziende Usa hanno ad esempio regole per nascondere tali notificazioni nel proprio materiale di marketing. Infine le notificazioni dovrebbero includere avvisi e consigli su quello che gli individui dovrebbero fare; alcune notificazioni da parte delle aziende USA sono incomprensibili o fanno paura ai loro destinatari invece di aiutarli con consigli su come ridurre il rischio.

Alcuni ricercatori infine hanno studiato il nuovo mercato del crimine in modo diretto.

Ricercatori dell'azienda di sicurezza Internet Team Cymru hanno documentato in modo approfondito il crimine online (si veda ad esempio: Thomas and Martin, 2006). Franklin, Perrig, Paxson e Savage (2007) hanno monitorato i canali pubblici di *chat* usati dai criminali online per contattarsi tra di loro, raccogliendo un gran numero di dati sulle frodi di carte di credito, spam, *phishing* e la vendita di *host* compromessi. Kanich ed altri (2008) hanno fatto un passo ulteriore. Si sono infiltrati in una grande *botnet* ed hanno modificato le e-mail di spam che venivano mandate così che puntassero ad un sito web duplicato ma benigno sotto il controllo dei ricercatori. E così hanno potuto per la prima volta fornire una risposta indipendente ad una domanda di lunga data: quante persone rispondono allo spam? È risultato che solo 28 vendite hanno avuto successo a fronte di 350 milioni di e-mail di spam che pubblicizzavano prodotti farmaceutici - un tasso di conversione del 0,00001%. Questo monitoraggio di tipo innovativo continuerà fino a che sarà necessario.

Sfortunatamente in molti paesi (compreso il Regno Unito) questo tipo di ricerche non possono essere portate avanti dalle agenzie di controllo legali in quanto la maggior parte di queste non hanno la necessaria *expertise* tecnica o semplicemente non si curano del problema.

In molti dei paesi che hanno adottato nuove leggi sulla sicurezza informatica molto probabilmente si avrà l'effetto di impedire ai ricercatori di sicurezza di fare il loro mestiere piuttosto che contrastare il crimine reale.

Senza informazioni accurate precise sul crimine online è difficile per i mercati privati fornire incentivi per un software più sicuro. Il modello di Akerlof (1970) del cosiddetto “mercato dei limoni” si applica a molti mercati di prodotti e servizi di *information security*. Per gli sviluppatori è molto difficile e costoso garantire la sicurezza del software prodotto e pertanto la risoluzione del problema viene lasciata alla buona volontà dei propri clienti; i consumatori naturalmente si rifiutano di pagare un prezzo extra per un tipo di qualità che essi non possono valutare direttamente.

La sicurezza interdipendente e la difficoltà del coordinamento

In molti contesti la sicurezza dipende dagli sforzi congiunti di molti attori interdipendenti. Hirshleifer (1983) ci racconta la storia di Anarchia, un'isola le cui difese contro le inondazioni erano affidate alle singole famiglie dei proprietari terrieri e la cui protezione globale dipendeva, pertanto, dall'anello più debole della catena - cioè dalla famiglia che più oziava. Egli ha confrontato questa situazione con quella di una città la cui protezione contro un attacco missilistico dipendeva dal cannone che più degli altri riesce ad intercettare i missili (anello più forte) ed ha dimostrato che il modello "anello più forte" è più efficace rispetto al modello "anello più debole". Varian (2004) ha proposto un terzo modello - nel quale le *performance* dipendono dalla somma degli sforzi di tutti i difensori come in una democrazia dove si pagano le tasse e si assumono i soldati - ed ha dimostrato che questa strategia di difesa basata sulla somma degli sforzi è migliore delle altre due. Contrastare il crimine online è difficile perché la sicurezza di Internet è spesso basata sul modello in cui vi è un "anello più debole" della catena. Milioni di personal computer sono sotto il controllo delle *botnet* e dunque gli "attaccanti" sono favoriti perché possono scegliere tra infiniti computer che utilizzano software non aggiornato, affetti da banchi di sicurezza, facili da compromettere. Inoltre l'insicurezza di Internet assomiglia un certo senso all'inquinamento ambientale: chiunque connetta un computer insicuro alla rete crea una *esternalità* negativa, dato che il computer può essere usato da altri per attaccare terze parti; alcuni hanno anche suggerito un approccio *cap-and-trade* per la qualità del software (Camp and Wolfram, 2004) cioè la possibilità che venga fissato un tetto massimo di non conformità (di sicurezza) oltre il quale le aziende devono pagare per la correzione degli errori. Le attuali caratteristiche dell'industria del software e la sua abilità nel negare ogni responsabilità contrattuali ci dicono però che tali soluzioni non sono oggi oggettivamente realizzabili.

I criminali online comprano infatti servizi da fornitori con deboli politiche di sicurezza e che chiudono un occhio su chi si comporta male.

La tipica natura ad "anello debole" della Internet *security* ci porta al tema fondamentale di questo studio: dove possiamo stabilire efficaci punti di controllo.

La responsabilità della prevenzione degli attacchi può essere addebitata infatti a diversi soggetti: i proprietari dei computer, gli *Internet service provider*, i fornitori di software, le aziende di sicurezza, le banche. Naturalmente ciascuno di questi *stakeholder* vorrebbe che fosse qualcun altro a risolvere il problema. La sicurezza è un classico problema di azione collettiva: come possiamo spingere gli attori del sistema a rispondere dei costi sociali del crimine online e non solo dei loro costi privati?

Un ruolo centrale per gli *Internet Service Provider*

Gli *Internet service provider* (ISP) sono di solito "ben posizionati" per intercettare le infezioni informatiche perché le prime avvisaglie dell'infezione di un utente si manifestano necessariamente sul network di un ISP. I circa 4.000 ISP negli Stati Uniti variano dal punto di vista delle dimensioni da aziende familiari che servono poche centinaia di clienti in avamposti rurali a giganti come AT&T, Verizon, AOL e Comcast ciascuno dei quali fornisce connettività a milioni di abitazioni e aziende. Inoltre i grandi ISP hanno uno staff tecnico che può individuare e "ripulire" i computer infetti mentre gli utenti privati e le piccole medie aziende di solito non sono neanche capaci di riconoscere di essere stati infettati. Gli ISP sono anche gli unici a presidiare i confini di un computer infetto in quanto controllano la sua connessione Internet e potrebbero disconnetterlo in caso di necessità. Le attuali *best practice* sono però meno severe: i computer infetti sono di solito isolati in una sottorete specifica, una sorta di "zona recintata", dalla quale possono accedere alle *patch* di sicurezza software per decontaminarsi e a nient'altro.

Il mercato tuttavia fornisce incentivi di fatto agli *Internet service provider* per intraprendere azioni di contrasto del crimine online. Uno studio dell'OCSE ha rilevato infatti che si sostengono forti

costi per il supporto ai clienti infettati: un ISP di medie dimensioni deve dedicare circa l'1,2% dei suoi ricavi totali per gestire le chiamate relative a problemi di sicurezza (van Eeten e Bauer, 2008). Un altro incentivo è che un ISP i cui clienti inviano traffico maligno potrebbe penalizzare tali clienti in vario modo ad esempio riducendo o isolando questi network maligni; di fatto però gli ISP non ricorrono a queste misure di isolamento: in pratica la maggior parte del traffico maligno del mondo proviene da questi network “troppo grandi per essere bloccati”.

Alcuni ISP particolarmente negligenti attirano quantità sproporzionate di business illegale. Per esempio fino al 2007, una grande quantità del malware mondiale era ospitato dal *Russian Business Network*, che ignorava le richieste da parte delle forze di polizia internazionali (*The Economist*, 2007). Dopo che il *Russian Business Network* fu bloccato alla fine del 2007, la distribuzione del malware si è spostato altrove. Nel novembre 2008, un giornalista del *Washington Post* ha convinto gli ISP ad interrompere la connessione alla società McColo, nei pressi di San Francisco (Krebs, 2008b) il che ha portato alla caduta temporanea di quasi il 70% del volume di spam in tutto il mondo: McColo usava molte *botnet* per tenere i computer sotto controllo. Recentemente *EstDomains*, che fungeva da *primary domain name registrar* per i siti web maligni ospitati dal *Russian Business Network* (Krebs, 2008c), è stato il primo *domain registrar* ad aver revocato il proprio accreditamento da parte dell'*Internet Corporation for Assigned Names and Numbers* (ICANN, 2008), l'ente no profit che gestisce il sistema dei domini Internet.

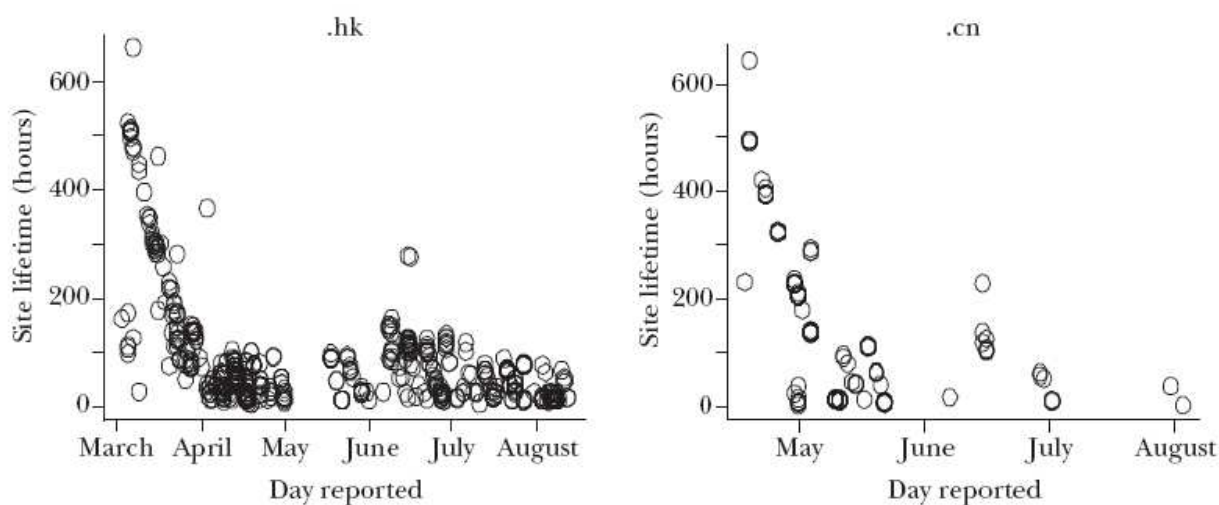
Tuttavia gli “attaccanti”, quando sono respinti su un certo punto, possono rapidamente dedicarsi al successivo anello debole di Internet molto più velocemente di quanto i “difensori” possano chiudere loro la porta. Moore e Clayton (2007) hanno descritto in che modo un gruppo di truffatori online, *the rock-phish gang*, opera. La gang registra innumerevoli domini di siti web maligni, usando nomi falsi e carte di credito rubate, come basi per lanciare propri attacchi; periodicamente cambia *domain name registrar* dei propri domini diventando così un cliente molto attivo e “ricercato”. Dato che i *registrar* possono “sospendere” e rendere irraggiungibile un nome di dominio se a loro avviso esso è abusivo o illegale - ad esempio se usa o copia un nome famoso o leggermente modificato- la *rock-phish gang* sceglie domini che non sembrano violare nessun *trademark*. In tal modo è necessario molto più tempo per convincere il *registrar* che domini apparentemente innocui in realtà sono utilizzati per scopi criminali.

La **figura 1** illustra i diagrammi relativi alla vita dei siti web sulla base dei dati riportati da Moore e Clayton (2007). L'asse orizzontale mostra il momento in cui il sito di *phishing* è stato identificato mentre l'asse verticale mostra quanto tempo il sito è rimasto online.

La gang ha utilizzato all'inizio (marzo 2007) domini di Hong Kong; successivamente dopo che le autorità di Hong Kong li hanno bloccati, sono passati su domini cinesi (maggio 2007). I siti di *phishing* con suffisso .hk (Hong Kong) e .cn (China) hanno avuto una vita molto più lunga nei primi mesi, quando la gang personalizzava ciascun dominio, rispetto agli ultimi mesi quando ciò non accadeva.

Figura 1

Scatter Plot of Phishing Site Lifetimes over Time Based on the Domain Targeted



Fonte: Moore e Clayton (2007)

Anche altri ricercatori hanno documentato come i siti web che contengono codice maligno si muovono da un registrar all'altro (Day, Palmen e Greenstadt, 2008). La “sensibilizzazione” dei registrar su queste problematiche è ancora un *work in progress*. Poche aziende molto grandi fanno numerose registrazioni (per esempio: *GoDaddy*, *Network Solutions*, *register.com*), ma come nel caso degli *Internet service provider*, ci sono anche migliaia di piccole aziende. Il comitato sulle politiche di Internet dell'*Anti-Phishing Working Group* (2008) si è dato l'obiettivo ambizioso di sensibilizzare e formare tutti i registrar sulle minacce più comuni, come la *rock-phish gang*, prima che gli stessi siano coinvolti in tali attività.

Le istituzioni governative dovrebbero dare agli *Internet service provider*, specialmente quelli più grandi, maggiori incentivi per bloccare i computer e le reti da cui partono le infezioni verso gli altri utenti. Per esempio nel nostro rapporto per la Commissione Europea, abbiamo proposto di rendere obbligatorio per legge il rimborso dei danni se un ISP non agisce entro un determinato periodo di tempo dopo che gli sia stato notificato che un sito infetto agisce sulla sua rete (Anderson, Bohme, Clayton e Moore, 2008). Al momento, la velocità di “spegnimento” dei computer infetti può variare in modo significativo: il miglior ISP rimuove siti di phishing in meno di un'ora mentre altri hanno bisogno di quasi una settimana. Un incentivo efficace per gli ISP potrebbe essere l'introduzione di una multa se in un periodo di tempo prestabilito, diciamo tre ore, non si agisce contro i siti che contengono software maligno.

L'obbligo di rifondere i danni in questa forma generale è stato usato in modo efficace per le aerolinee: l'Unione Europea lo ha introdotto per le compagnie che si macchiano di *overbooking*, cancellazioni o eccessivi ritardi. Un passeggero che non può volare può richiedere un rimborso fisso (di solito 250 euro) dalla compagnia senza dover fornire conti di albergo o altre evidenze di spese sostenute. La compagnia aerea a sua volta può rivalersi sulle altre controparti (come gli aeroporti o i fornitori di manutenzione) per recuperare questi danni se ciò è appropriato. In modo analogo gli *Internet service provider* potrebbero recuperare i danni subiti da una terza parte negligente. Un'altra delle nostre raccomandazioni è che i produttori di apparecchiature di rete dovrebbero certificare che esse sono progettate in modo sicuro (*secure by default*) così nel caso poi non si rivelassero tali gli ISP possano chiedere ai produttori i danni senza imbarcarsi in estenuanti battaglie legali.

I film ed i romanzi a volte descrivono gli hacker come geni dell'informatica con capacità mitiche e le bande organizzate in modo efficiente e perfetto. L'analisi dei dati a nostra disposizione ci

suggerisce invece che è successo di molte di queste bande è più strategico che tecnologico: cioè gli “attaccanti” non scrivono software brillante ma invece sfruttano gli errori ed i banchi del software commerciale installato sui computer. Ohm (2008) ha confermato questa analisi in una discussione su “mito del Superuser”. La gente ritiene che gli hacker abbiano grandissime capacità ma gli studi empirici rivelano che la realtà è molto più semplice.

Condividere i dati di sicurezza sulle aziende che vengono “scollegate”

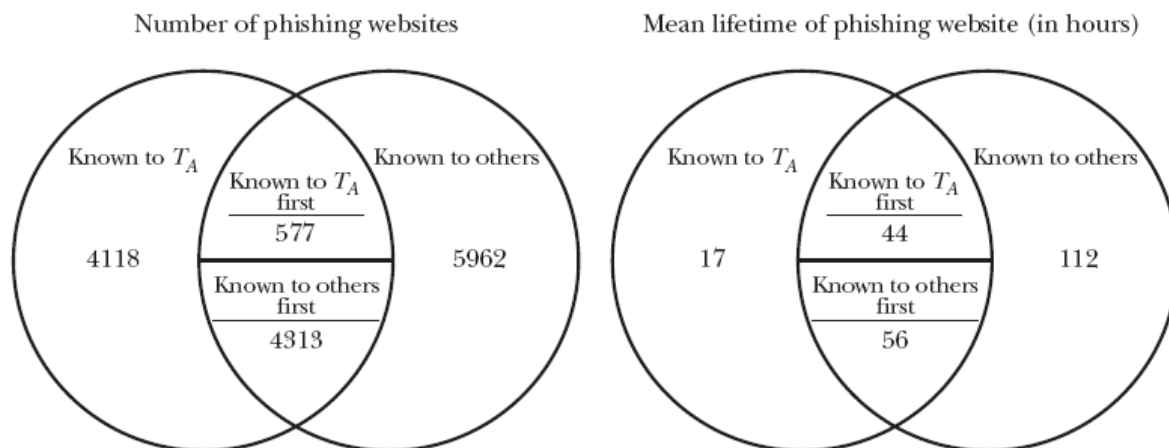
Per proteggere i consumatori è essenziale raccogliere tempestivamente dati completi sulle vulnerabilità più recenti e sui siti web compromessi. Ma molte società di *information security* che provvedono a “scollegare” i siti web maligni a nome delle banche e delle aziende loro clienti non condividono le informazioni su tali siti sostenendo che si tratta di dati che garantiscono loro una posizione competitiva.

Dalle nostre analisi risulta che i consumatori otterrebbero notevoli benefici se tali società di *information security* condividessero tra loro le informazioni. Anche negli anni '80 e '90 le aziende di antivirus non si scambiavano le informazioni sui virus intercettati e si facevano un'accanita concorrenza basata anche su chi pubblicava, sulle riviste di settore, le liste più lunghe di virus bloccati. Le riviste mettevano a confronto i prodotti antivirus indicando, ad esempio, se Dr. Solomon intercettava più virus rispetto a Norton. Ma nel 1993, una serie di comunicati stampa da parte delle maggiori aziende del settore annunciò che virus sarebbero stati valutati congiuntamente: finalmente era diventato chiaro che la mancata condivisione delle informazioni stava danneggiando il comparto industriale dei produttori di antivirus. In quell'anno alla conferenza degli *European Institute for Computer Research* (EICAR), un incontro di ricercatori antivirus, fu siglato l'accordo per cui ciascun produttore di antivirus avrebbe confrontato i propri esempi di virus con quelli dei propri *competitor*. Questo accordo è valido ancor oggi e ha portato un netto miglioramento della qualità dei prodotti e della protezione dei clienti. Il comparto industriale relativo all'*anti-phishing* non ha ancora imparato questa lezione. Al suo interno ci sono fornitori specializzati, come Cyveillance, RSA e MarkMonitor, che sono ingaggiati dalle banche per rimuovere i siti di phishing e per scollegare i *domain name* abusivi. Queste aziende compilano, ognuno per suo conto, liste (*feeds*) di siti di *phishing* aggiornate molto frequentemente ma senza scambiarsi tra loro le informazioni. Moore e Clayton (2008b) hanno analizzato sei mesi di *feeds* da fonti multiple, compresi due fornitori *anti-phishing*. In ciascun caso molti siti di *phishing* erano conosciuti da qualcuno nella *industry*, ma non dalla società che avrebbe tutto “scollegarlo” al nome della banca attaccata dal sito.

La **figura 2** mostra i risultati di uno delle aziende più grandi che si occupano di “scollegamento” di siti di *phishing*, una società chiamata T_A, che ha rimosso 54 siti di false banche in un periodo di sei mesi circa. T_A ha identificato 9.008 siti che “impersonificavano” banche suoi clienti (dato rappresentato dai cerchi sulla sinistra) mentre ulteriori 5.962 siti sono stati identificati dai *competitor* di T_A (il cerchio a destra). È ragionevole ipotizzare, dato che ci potrebbero essere altri siti non identificati né da T_A né dai suoi *competitor*, che T_A ha “mancato” almeno il 40% del suo target.

Figura 2

Diagramma di Venn che rappresenta la “consapevolezza” dell'azienda T_A in relazione alle azioni di risposta ai siti di *phishing* che “impersonificano” le sue 54 banche clienti nel periodo ottobre 2007 – marzo 2008



Fonte: Moore e Clayton (2008b).

Moore e Clayton hanno calcolato in modo approssimativo i costi di questa situazione relativa alla mancata cooperazione esaminando “il tempo di vita” medio dei siti web.

I siti che erano stati identificati solo da T_A sono stati rimossi in una media di 17ore mentre i siti sconosciuti a T_A dopo una media di 112, circa quattro giorni in più. In aggiunta dei 9.008 siti web che T_A conosceva, 4.313 sono stati identificati prima da altri fonti, con 50 di media di meno rispetto a T_A. L’effetto di questi ritardi può essere visto nei dati sul “tempo di vita” medio: questi siti web rimangono in vita per 56 ore di media, 39 ore più a lungo dei siti conosciuti solo da T_A. La vita dei siti di *phishing* potrebbe essere ridotta in modo significativo se le aziende di “scollegamento” condividessero i loro dati così come fanno già le aziende di antivirus da 15 anni. I loro clienti ne guadagnerebbero e anche le aziende ne avrebbero benefici – non solo per l’opportunità di incrementare i ricavi avendo più lavoro da fare ma anche perché offrirebbero al mercato un servizio di maggior valore.

Moore e Clayton (2008b) hanno calcolato che la “vita” di un sito potrebbe essere abbattuto della metà o più grazie alla condivisione delle informazioni e che – sulla base di stime abbastanza grezze – potrebbero essere prevenute circa 330 milioni di dollari l’anno di frodi grazie allo scambio di informazioni.

Come per il comparto delle imprese di antivirus di 15 anni fa, la “condivisione” porterebbe effetti positivi a tutta l’*industry*. Le aziende di “scollegamento” competono su numerosi fattori, tra i quali il prezzo, il servizio alla clientela, la velocità di rimozione dei siti fasulli e la “completezza dei *feed*” – che è il termine di riferimento usato in quest’*industry* per indicare quanto profondamente essi scandagliano il web alla ricerca di siti maligni. Condividere le informazioni eliminerebbe la “completezza dei *feed*” come fattore competitivo; ciò potrebbe avere l’effetto negativo di ridurre gli incentivi in quest’area (Olson, 2008): a questa obiezione si può rispondere prevedendo di “compensare” coloro che forniscono più informazioni alla lista comune dei siti fasulli (Moore, 2008).

Alcune aziende ben organizzate che già presidiano questo mercato temono che la condivisione dei *feed* possa ridurre le barriere all’entrata in questo comparto: inevitabilmente però la competizione alla fine si giocherà sulla velocità di rimozione, sul prezzo, sui servizi accessori, fattori sui quali gli attuali *incumbent* dovrebbero continuare a mantenere un vantaggio competitivo rispetto ai nuovi arrivati.

E aumentando il numero di siti che sono rimossi, il servizio stesso acquisterebbe maggior valore per le banche. Nella nostra visione le attuali aziende di “scollegamento” otterranno maggiori benefici dalla condivisione dei *feed* rispetto ai nuovi arrivati perché la competizione si sposterà sulla qualità del servizio e non più sull’ampiezza delle liste di siti di *phishing*.

Coloro che veramente avrebbero da perderci sono le piccole aziende che sono specializzate principalmente nel produrre *feed*. Per le banche che sono clienti di grandi aziende di “scollegamento” il *feed sharing* offre solo benefici.

Tabella 2

Tempo di vita dei siti web per tipo di contenuto illegale

<i>Phishing</i>				
Free web-hosting	Gen. 2008	240	4.3 0	0
web server compromessi	Gen. 2008	105	3.5	0
Domini sotto il controllo di gang di phishing	Gen. 2008	821	70.3	33
Domini fast-flux	Gen. 2008	314	96.1	25.5
<i>Siti web fraudolenti</i>				
Siti web per il reclutamento di “muli”	Mar. 07–Feb. 08	67	308.2	188
Farmacie online fast-flux	Ott.–Dic. 2007	82	1370.7	1404.5
Immagini pedopornografiche	Gen.–Dic. 2007	2585	719	288

Fonte: Moore e Clayton (2008a).

Come gli incentivi dei difensori hanno influenza sulla velocità di “scollegamento”

Molti tipi differenti di contenuti online illegali – violazioni del *copyright*, pedopornografia, siti di *phishing* – sono soggette a richieste di “scollegamento (*take-down*). Moore e Clayton (2008a) hanno raccolto i dati sulla “vita media” di diversi tipi di siti web, dati sintetizzati nella **tabella 2**.

La vita di un sito “discutibile” è significativamente influenzato da chi ha un incentivo a trovare e reclamare in relazione al materiale “offensivo”. I siti web di *phishing* che sono rimossi in modo più veloce sono le banche che sono fortemente motivate a rimuovere ogni sito web che impersonifichi le loro aziende. Viceversa altre attività illecite come le farmacie online non vengono rimosse per niente.

Ma molte banche si attivano solo per rimuovere i siti che le attaccano direttamente. Le banche ignorano ad esempio una componente chiave nella “catena del *phishing*”: il reclutamento dei “muli”. Come descritto precedentemente, i *phishermen* assoldano i “*money mule*,” gonzi che ripuliscono il denaro rubato di solito usando i sistemi di *money transfer* quali Western Union. Dato che i trasferimenti fraudolenti sono spesso “contestati” il mulo finisce con il rimetterci personalmente e così le banche non hanno un incentivo adeguato per contrastare il reclutamento di “muli”. La loro motivazione è frenata inoltre dal classico dilemma di ogni azione collettiva: è difficile saper in anticipo quale banca sarà messa sotto attacco a causa del reclutamento di un mulo.

Così anche se il reclutamento dei muli danneggia le banche direttamente né le banche né le società di *take-down* combattono i siti di reclutamento. Di solito solo gruppi di “vigilanti” come “*Artists Against 419*” tentano di rimuovere questi siti ed anche essi trattano questi siti web con bassa priorità perché essi considerano i muli solo come complici del *phishing*. Infine le autorità di vigilanza potrebbero obbligare le banche a considerare il riciclaggio di denaro come un tema di *due diligence* invece che un modo per ridurre il rischio; la maggior parte dei controlli antiriciclaggio sono finalizzati infatti a contrastare crimini come il traffico di droga nei quali le banche non sono le vere vittime e la mancanza di incentivi effettivi li spinge verso un impegno minimo e una *compliance* di tipo meccanico. Moore e Clayton (2008a) hanno rilevato che i siti web di *mule-recruitment* vivono 308 ore, molto più a lungo dei siti web che impersonificano direttamente le banche (da 4 a 96 ore). Questo vuol dire lasciar cadere un’opportunità; la crescita molto rapida di spam alla fine del 2008 si

deve proprio al *mule recruitment*, il che suggerisce in modo forte che la scarsità di muli è diventato un importante collo di bottiglia nelle operazioni di *phishing*.

Anche l'infrastruttura usata dagli "attaccanti" ha impatto sui tempi di *take-down* ma con minor importanza rispetto ad altri fattori. I criminali improvvisati affidano i loro siti web a servizi gratuiti o server web compromessi il che rende facile ai "difensori" scollegarli; i criminali più agguerriti come la *rock-phish gang* prima menzionata usano tecniche evasive come il *fast-flux*. Moore e Clayton (2007) hanno descritto questa particolare tecnica: i siti web sono in *host* dinamico su una *botnet*, che risiede per pochi minuti su ciascun computer e si muove da un'altra parte prima che il servizio di rimozione possa fare alcunché. Ma i nostri dati mostrano che la vita di un sito criminale è determinato più dagli incentivi diretti che i "difensori" hanno nello scollegarlo piuttosto che dallo strumento tecnologico usato dai criminali per sferrare l'attacco. Per esempio Moore e Clayton (2008a) hanno trovato che i siti di *phishing fast-flux* sono rimossi in 96 ore mentre le farmacie online *fast-flux* sono rimosse con maggiore difficoltà (fino a raggiungere due mesi di vita).

Coordinamento delle forze dell'ordine

In tutto il mondo ci sono decine di migliaia di "agenzie" legate in un modo o nell'altro alle forze dell'ordine; la maggior parte di esse, anche nei paesi più sviluppati, si comporta in maniera analoga in relazione al *computer crime*. Ciò che è esplicitamente illegale varia da un paese ad un altro: il framework legale che sta diventando dominante, la Convenzione del Consiglio d'Europa sul *Cybercrime*, è stato ratificato dagli Stati Uniti ma non è stato ancora ratificata dalla maggior parte degli stati membri dell'Unione Europea. Tuttavia anche quando i governi si saranno messi d'accordo su cosa è un crimine online, le forze di polizia continueranno ad avere scarsi incentivi per lavorare insieme sulla massa del crimine globalizzato. Supponiamo che uno *phisher* in Russia mandi milioni di e-mail di spam ad indirizzi di e-mail a caso. La più grande forza di polizia in Gran Bretagna, la *London's Metropolitan Police* (MET), si potrebbe trovare con 10.000 di queste email nella sua area – gli *account* di posta "riconducibili" all'area metropolitana di Londra sono infatti circa l'1% del totale. La "Met" potrebbe essere tentata di dire "Che seccatura, lasciamo che se ne occupi l'FBI" e concentrarsi invece sulla repressione dei crimini di strada. Molte delle forze di polizia infatti hanno come priorità il contrasto del crimine sulla base del numero di cittadini che ne sono vittime, sul numero di criminali e sulla gravità dei danni in ambito locale. Usando questi criteri, risultare che i pochi attacchi online valgono poco anche se, nel loro insieme, essi possono avere un effetto enorme. Nel Regno Unito, per esempio, ci sono solo due piccole unità di polizia specializzate nelle frodi online (la *Dedicated Cheque and Plastic Crime Unit* e la *Police Central e-crime Unit*) ed entrambe si basano sulla collaborazione dell'*industry* bancaria per gran parte delle loro attività.

Le barriere alla cooperazione sono ulteriormente alzate dal fatto che il crimine online di solito è transnazionale. Gli attuali meccanismi di cooperazione internazionale delle polizie sono costosi e lenti, disegnati per acchiappare gli occasionali assassini in fuga, non per gestire milioni di frodi del valore di poche centinaia di dollari ciascuna. Il problema è aggravato dalla sensibilità rispetto alla propria sovranità nazionale: ciascun caso è analizzato dalle forze diplomatiche per assicurarsi che non ci siano implicazioni politiche. Il nostro suggerimento qui è che, seguendo i precedenti dello SHAEF (la *Supreme Headquarters Allied Expeditionary Force*) durante la seconda guerra mondiale e della NATO oggi, i diversi paesi dovrebbero mantenere "ufficiali di collegamento" (*liaison officer*) nei centri di comando che decidono effettivamente su quali crimini impegnarsi maggiormente. Devono essere questi *liaison officers* a trasmettere le richieste alle forze dei propri paesi: questa sorta di "joint operation" permanente deve decidere velocemente, sulla base degli accordi internazionali già esistenti, quali sono le priorità. La cosa importante è che ciascun paese abbia fiducia che i propri "ufficiali di collegamento" sappiano valutare quali richieste non abbiano implicazioni politiche e possano essere trattate come semplici casi di polizia.

Abbiamo inoltre bisogno di un meccanismo per elaborare una strategia globale sulle priorità relative al crimine cibernetico: questo richiede sia un *feedback* operativo che una *accountability* democratica.

Azione pubblica contro azione privata

Un tema relativo al *cybercrime* che realmente cattura l'attenzione dei politici e dei e dei mass-media popolari riguarda i siti web che ospitano immagini pedopornografiche. Tuttavia ancora una volta curiosamente abbiamo rilevato che questi siti web sono rimossi molto più lentamente degli altri siti che ospitano contenuti illegali. La loro vita media è di 719 ore, circa 150 volte di più che un normale sito di *phishing* e più del doppio anche dei siti web usati per il reclutamento dei muli. Perché accade ciò?

Negli anni 90 quando Internet è entrata alla pubblica attenzione i *policymaker* hanno stabilito che la “pedopornografia” era il male assoluto di Internet e che tutti i governi dovessero essere d'accordo nel bandirla. In 29 paesi, gli ISP hanno stabilito *hotline* per identificare e scollegare rapidamente questo tipo di materiale offensivo. Nel Regno Unito l'*Internet Watch Foundation* (IWF) svolge questa attività e obbliga alla rimozione delle immagini che riguardano abusi sessuali sui bambini nei siti web in Gran Bretagna entro 48 ore; di conseguenza solo lo 0.2% di questi siti sono oggi ospitati nel Regno Unito (*Internet Watch Foundation*, 2006). Quando questi siti web sono ospitati in altri paesi l'IWF notifica la sua richiesta alla *hotline* locale o a una forza di polizia di quel paese ma non effettua nessun'altra azione.

Le politiche sulle *hotline* e la loro efficacia variano di paese in paese ma di fatto nessuno è efficace come l'*Internet Watch Foundation*. L'U.S *CyberTipline* che opera presso il *National Center for Missing and Exploited Children* (NCMEC) dichiara che comunica i propri avvisi per lo scollegamento a tutti gli *Internet service provider* “nel modo più opportuno e quando appropriato”; ma apparentemente, in tutto il mese di ottobre 2008, NCMEC ha inoltrato le sue richieste di scollegamento solo al sottoinsieme degli ISP che fanno parte del suo network. Una nuova legge USA emanata nell'ottobre 2008, il *Protect Our Children Act*, punta a risolvere questo particolare problema rendendo obbligatorio agli ISP di registrarsi presso il NCMEC.

La capacità e velocità di risposta alle richieste delle autorità sono anch'esse molto varie.

Di solito le richieste di “scollegamento” sono passate all'agenzia nazionale che deve poi passare le informazioni alla giurisdizione locale, che poi contatta l'ISP responsabile.

I budget delle aziende per le attività in risposta alle richieste delle autorità sono sempre ridotti ed i tempi di intervento delle forze di polizia variano molto in relazione a quanto il tema “Internet e sicurezza” è discusso dalle forze politiche locali in quel momento.

Quasi tutti i tipi di materiale online illegale sono trattati in contesti internazionale e le frontiere sono di solito di tipo immateriale: tutto ciò demotiva un'azienda privata che voglia far “scollegare” un sito illegale che la danneggia o che semplicemente è offensivo.

Inoltre in molte giurisdizioni la polizia ha l'esclusiva nella gestione dei casi di pedopornografia.

Nel Regno Unito per esempio, il solo possesso di materiale pedopornografico è considerato un crimine il che effettivamente disincentiva il settore privato nel collaborare con le autorità (una azienda che voglia far scollegare un sito pedopornografico deve “detenere” anche temporaneamente almeno un'immagine di questo tipo anche solo sullo schermo).

Infine dato che solo la polizia ha l'autorità di perseguire questo tipo di reato, la giurisdizione diventa un significativo ostacolo se le forze di polizia non operano in modo internazionale oltre le frontiere sia tra diversi stati sia tra diversi paesi. L'*Internet Watch Foundation* ci insegna che essi dovrebbero “camminare sulle orme delle altre persone” se vogliono contattare gli *Internet service provider* fuori dal Regno Unito e che ad essi “non sono in ogni caso autorizzati a chiedere lo scollegamento dei siti fuori dal Regno Unito”.

In contrasto, con altri tipi di crimine online, le banche, le aziende di *take-down* ed anche i vigilantes mostrano di solito grande flessibilità nel loro impegno di perseguire i materiali oltre frontiera.

Le forze di polizia non hanno quindi un ruolo preciso nel contrasto del crimine online. Per esempio abbiamo notato recentemente un significativo consolidamento nelle *botnet* e nell'industry dello spam; come abbiamo già notato il *takedown* di McColo ha ridotto lo spam in tutto il mondo del 70% quando è stato interrotto il controllo che sei grandi raggruppamenti avevano sulle *botnet*. Nella nostra visione le risorse di polizia dovrebbero concentrarsi sul perseguire queste grandi gang e l'FBI con l'operazione "*Bot Roast*" si sta già muovendo in questa direzione. Le attività di routine, come lo scollegamento dei siti web offensivi, è opportuno invece che siano lasciati ai *contractor* privati opportunamente incentivati.

Osservazioni conclusive

Dal 2004 circa, il crimine online è diventato sempre più organizzato ed industrializzato come nessun'altra forma di criminalità ad eccezione, forse, del commercio della droga. Molti dei problemi che le banche e le forze dell'ordine stanno affrontando per contrastare questo nuovo fenomeno esistevano già nelle tradizionali forme di contrasto del crimine ma sono rese adesso più acuti nel mondo online da nuovi fattori che vanno dalle esternalità del network alla scala globale assunta dal fenomeno.

Sfortunatamente i criminali sembrano essere diventati un attore stabile del nuovo ecosistema online e ciò comporta nuovi e significativi costi per le banche, i cittadini, i *service provider* e tutti gli altri. In questo studio abbiamo presentato i risultati di numerose ricerche recenti che insieme spiegano come lavori l'*industry* del crimine online, perché gli sforzi delle forze dell'ordine siano al momento insufficienti e come essi potrebbero essere migliorati.

Come è successo con le innovazioni criminali a causa dell'arrivo di precedenti tecnologie, a partire dalle frodi sulle carte di credito fino all'uso delle "auto rubate" nelle rapine in banca, ogni volta serve un po' di tempo prima di trovare la combinazione ottimale di risorse pubbliche e private in ambito sicurezza.

La nostra analisi in questo studio suggerisce che cambiamenti significativi sono possibili nel modo attuale di trattare le frodi online. I network criminali hanno le loro particolari vulnerabilità – come ad esempio il momento in cui riciclano il denaro. Tuttavia le banche individualmente non contrastano i riciclatori di denaro perché i riciclatori attaccano il sistema bancario nel loro insieme e non la singola banca. Forse toccherebbe alle associazioni di categoria delle banche perseguire i riciclatori.

Le banche si sono rivelate anche incapaci di obbligare i loro *security contractor* a condividere i dati sugli attacchi anche nei casi in cui ciò potrebbe aiutarle direttamente. Il problema di questa azione collettiva è trovare un accordo sulla condivisione delle informazioni nel settore privato come è accaduto 15 anni fa nell'ambito dei produttori di antivirus per computer.

Infine suggeriamo che la polizia si concentri solo sulle maggiori e più pericolose bande di *phishing*. Per contrastare meglio il crimine online dobbiamo prima conoscerlo meglio. La chiave di questa comprensione non è tanto tecnologica ma consiste piuttosto nell'avere un quadro corretto degli aspetti economici e degli incentivi che intervengono in questo contesto.

- *Gli autori ringraziano Allan Friedman, Steven Murdoch e Andrew Odlyzko che hanno letto questo studio in bozza e hanno fatto utili osservazioni.*

Riferimenti

- Acquisti Alessandro, Allan Friedman, Rahul Telang.** 2006. "Is There a Cost to Privacy Breaches? An Event Study." Paper presented at the International Conference on Information Systems (ICIS), Milwaukee, WI.
- Akerlof, George A.** 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *Quarterly Journal of Economics*, 84(3): 488–500.
- Anderson, Ross.** 2001. "Why Information Security is Hard—An Economic Perspective." *Proceedings of the 17th Annual Computer Security Applications Conference*, 358–65. IEEE Computer Society (**traduzione in italiano**: "Perché la sicurezza delle informazioni è ardua - Una prospettiva economica" in <http://www.isacaroma.it/html/newsletter/node/134>)
- Anderson, Ross, Rainer Bohme, Richard Clayton, Tyler Moore.** 2008. "Security Economics and the Internal Market." European Network and Information Security Agency. http://www.enisa.europa.eu/doc/pdf/report_sec_econ_int_mark_20080131.pdf.
- Anderson, Ross, Tyler Moore.** 2006. "The Economics of Information Security." *Science*, 314(5799): 610–13.
- Anti-phishing Working Group Internet Policy Committee.** 2008. "Anti-Phishing Best Practices Recommendations for Registrars." An APWG Industry Advisory. http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf.
- APACS (Association for Payment Clearing Services).** 2007. "Card Fraud Losses Continue to Fall." Press release, March 14. http://www.apacs.org.uk/media_centre/press/07_14_03.html.
- APACS (Association for Payment Clearing Services).** 2008. "APACS Announces Latest Fraud Figures" Press release, September 25. <http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm>.
- Becker, Gary.** 1968. "Crime and Punishment: An Economic Approach." *The Journal of Political Economy*, 76(2): 169–217.
- California State Senate.** 2002. "Assembly Bill No. 700." http://info.sen.ca.gov/pub/01-02/bill_asm/ab_0651-0700/ab_700_bill_20020929_chaptered.pdf.
- Camp, L. Jean, Catherine D. Wolfram.** 2004. "Pricing Security: A Market in Vulnerabilities." In *Economics of Information Security*, Vol. 12, *Advances in Information Security*, ed. L. Jean Camp and Stephen Lewis, 17–34. Boston: Kluwer Academic Publishers.
- Computer Economics.** 2007. "Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and other Malicious Code." <http://www.computereconomics.com/page.cfm?name=Malware%20Report>
- Day, Oliver, Brandon Palmen, Rachel Greenstadt.** 2008. "Reinterpreting the Disclosure Debate for Web Infections." In *Managing Information Risk and the Economics of Security*, ed. M. Eric Johnson, 179–197. New York: Springer.
- The Economist.** 2007. "A Walk on the Dark Side." August 30.
- Franklin, James, Adrian Perrig, Vern Paxson, Stefan Savage.** 2007. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants." *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, 375–388. ACM Press.
- Gartner.** 2006. "Gartner Says Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years." Press release, November 9. <http://www.gartner.com/it/page.jsp?id=498245>
- Greenemeier.** 2007. "T.J. Maxx Parent Company Data Theft Is The Worst Ever." *Information Week*, March 29. <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=198701100>
- Hirshleifer, Jack.** 1983. "From Weakest-link to Best-shot: The Voluntary Provision of Public

- Goods.” *Public Choice*, 41(3): 371–386.
- House of Lords Science and Technology Committee.** 2007. *Personal Internet Security*, 5th Report of 2006–07. London: The Stationery Office.
- Internet Corporation for Assigned Names and Numbers (ICANN).** 2008. “Termination of Registrar EstDomains to Go Ahead.” November 12.
<http://www.icann.org/en/announcements/announcement-12nov08-en.htm>
- Internet Watch Foundation.** 2006. “Half-yearly Report.” July.
http://www.iwf.org.uk/documents/20060803_2006_bi-annual_report_v7_final4.pdf
- Kanich, Chris, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, Stefan Savage.** 2008. “Spamalytics: An Empirical Analysis of Spam Marketing Conversion.” *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, 3–14. ACM Press.
- Krebs, Brian.** 2008a. “‘Money Mules’ Help Haul Cyber Criminals’ Loot.” *Washington Post*. January 25.
<http://www.washingtonpost.com/wp-dyn/content/story/2008/01/25/ST2008012501460.html>
- Krebs, Brian.** 2008b. “Major Source of Online Scams and Spams Knocked Offline.” Blog titled “Security Fix.” *Washington Post*, November 11.
http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html
- Krebs, Brian.** 2008c. “EstDomains: A Sordid History and a Storied CEO.” *Washington Post*. September 8.
http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html
- Lesk, Michael.** 2007. “The New Front Line: Estonia under Cyberassault.” *IEEE Security and Privacy*, 5(4): 76–79.
- Moore, Tyler.** 2008. “How Can We Cooperate to Tackle Phishing?” October 27.
<http://www.lightbluetouchpaper.org/2008/10/27/how-canwe-co-operate-to-tackle-phishing/>
- Moore Tyler, Richard Clayton.** 2007. “Examining the Impact of Website Take-down on Phishing.” *Proceedings of the Anti-Phishing Working Group eCrime Researchers Summit*, 1–13.
- Moore Tyler, Richard Clayton.** 2008a. “The Impact of Incentives on Notice and Takedown.” In *Managing Information Risk and the Economics of Security*, ed. M. Eric Johnson, 199–223. New York: Springer.
- Moore Tyler, Richard Clayton.** 2008b. “The Consequence of Non-cooperation in the Fight against Phishing.” *Proceedings of the Anti-Phishing Working Group eCrime Researchers Summit*, 1–14. IEEE.
- Moore, Tyler, Richard Clayton.** 2009. “Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing.” *Lecture Notes in Computer Science*, vol. 5628, pp. 256–72.
- Ohm, Paul.** 2008. “The Myth of the Superuser: Fear, Risk and Harm Online.” *UC Davis Law Review*, 41(4): 1327–1402.
- Olson, Eric.** 2008. “A Contrary Perspective - Forced Data Sharing Will Decrease Performance and Reduce Protection.” October 22.
<http://www.cyveillanceblog.com/phishing/a-contraryperspective-%e2%80%93forced-data-sharing-willdecrease-performance-and-reduce-protection>
- OpenDNS.** 2007. “OpenDNS Shares April 2007 PhishTank Statistics.” Press release, May 1.
<http://www.opendns.com/about/announcements/14/>
- Panda Security.** 2009. “More than 10 Million Worldwide Were Actively Exposed to Identity Theft in 2008.” March 10.
<http://www.pandasecurity.com/usa/homeusers/media/press-releases/viewnews?noticia=9602&sitepanda=empresas>
- Provos, Niels, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose.** 2008. “All Your iFRAMES Point to Us.” *Proceedings of the 17th USENIX Security Symposium*, 1–15. USENIX Association.
- Romanosky, Sasha, Rahul Telang, Alessandro Acquisti.** 2008. “Do Data Breach Disclosure Laws Reduce Identity Theft?” Paper presented at the 7th Workshop on the

Economics of Information Security, Hanover, NH. Available at SSRN:

<http://ssrn.com/paper=1268926>

Schipka, Maksym. 2007. "The Online Shadow Economy: A Billion Dollar Market for Malware Authors". MessageLabs White Paper.

http://www.fstc.org/docs/articles/messagelabs_online_shadow_economy.pdf

Sullivan, Bob. 2004. "Experts Fret over Online Extortion Attempts." MSNBC. November, 10.

<http://www.msnbc.msn.com/id/6436834/>

Symantec. 2008. *Symantec Global Internet Security Threat Report*, Vol. 13, Trends for July–December 07.

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

Thomas, Rob, Jerry Martin. 2006. "The Underground Economy: Priceless." *USENIX ;login*, 31(6): 7–16.

van Eeten, Michael J. G., Johannes

M.Bauer. 2008. "The Economics of Malware: Security Decisions, Incentives and Externalities." OECD Science, Technology and Industry Working Paper No. 2008/1.

Varian, Hal. 2004. "System Reliability and Free Riding." *In Economics of Information Security*, Vol. 12, *Advances in Information Security*, ed. L. Jean Camp and Stephen Lewis, 1–15. Boston: Kluwer Academic Publishers.