

# McAfee®



Protect what you value.

## Spyware: una strategia mutante

---

# Sommario

Un po' di storia ..... 3

Considerazioni economiche ..... 4

A che punto siamo oggi? ..... 5

Chi vincerà? ..... 6

Aspetti sociali dello spyware ..... 6

Problemi legali ..... 7

Conclusioni ..... 7

Informazioni sull'autore ..... 7

# Spyware: una strategia mutante

Di Anna Stepanov

*"In genere, gli uomini temono ciò che non possono vedere più di quello che hanno di fronte agli occhi."*

—Giulio Cesare

Durante le guerre galliche, Giulio Cesare ha sistematicamente sfruttato la conoscenza delle caratteristiche e delle debolezze delle tribù avversarie per sconfiggerle. Egli, come tutti i grandi condottieri, si è sforzato di comprendere i propri nemici per poterli battere. Oggi, sembra che i creatori di malware stiano utilizzando questa stessa strategia contro di noi.

Nel mondo informatico di oggi, dove tutto, dagli sportelli bancari ai seggi elettorali fino alle partite di poker, può diventare virtuale, corriamo sempre di più il rischio di diventare vittime di ciò che non possiamo vedere. In tutto il mondo, la nostra esistenza quotidiana si affida a server invisibili, procedure nascoste e al trasferimento occulto di informazioni. Ci siamo talmente abituati all'automatizzazione dei processi che spesso ci dimentichiamo di chiederci che cosa accade all'interno dei nostri sistemi. Tutto ciò porta a un falso senso di sicurezza o, perlomeno, all'assenza di un ragionevole dubbio circa l'infalibilità di tale sicurezza. E qui entrano in scena gli spyware, senza preavviso.

Nel corso dei quasi otto anni trascorsi dall'apparizione del primo programma spyware, il panorama è cambiato sensibilmente. Lo spyware è diventato un modello di business e un'importante fonte di reddito per i criminali informatici. Allo stesso tempo, a causa della proliferazione di strumenti anti-spyware sempre più sofisticati, i meccanismi di distribuzione ed esecuzione di spyware e altri programmi indesiderati si sono progressivamente evoluti da vistosi adware per la generazione di pop-up a strumenti di spionaggio e trojan estremamente furtivi.<sup>1</sup> Inoltre, la presenza sempre più massiccia di rootkit segnala un cambiamento fondamentale nella battaglia per la sicurezza dei sistemi.<sup>2</sup>

1 Trojan: programma che apparentemente esegue una determinata operazione, ma che in realtà ne effettua un'altra (conosciuto anche come Trojan horse). Glossario della Anti-Spyware Coalition (ASC) del Center for Democracy and Technology: <http://www.antispywarecoalition.org/index.htm>

2 Rootkit: programma in grado di ottenere o gestire in modo fraudolento l'accesso a un computer di livello amministratore. Tale programma può essere eseguito in modo da non essere rilevato. Una volta che il rootkit ha ottenuto l'accesso a un sistema, questo può essere utilizzato per monitorare il traffico dei dati e le sequenze di tasti battute sulla tastiera, creare un varco per consentire all'hacker di introdursi clandestinamente nel sistema, alterare file di registro, attaccare altre macchine della rete e modificare gli strumenti del sistema per evitare di essere rilevato. I rootkit sono una variante estrema del "software di modifica dei sistemi". Glossario ASC: <http://www.antispywarecoalition.org/index.htm>

In questo documento, si analizzerà come i creatori di spyware hanno modificato la propria strategia di attacco. L'attuale evoluzione dello spyware dovrebbe farci riflettere sulla necessità di preoccuparci maggiormente di ciò che non possiamo vedere.

## Un po' di storia

Gli spyware e i PUP, o programmi potenzialmente indesiderati, sono un concetto relativamente nuovo, anche se in rapida espansione, nella storia di Internet. L'adware e lo spyware si sono rapidamente sviluppati come una naturale evoluzione della pubblicità su Internet, nonché come una forma di sfruttamento di vari "buchi" presenti nei browser e nei sistemi di sicurezza in genere. Nei primi anni novanta, alcune società lecite hanno iniziato a fare pubblicità online. Annunci pop-up con slogan di aziende quali Sprint, Volvo, MCI e altri importanti gruppi erano cosa comune. In breve tempo, l'idea della pubblicità via Web venne applicata su larga scala e la fastidiosa apparizione dello spam la seguì a ruota. Immediatamente dopo entrò in scena il cosiddetto marketing di affiliazione ("metodo per promuovere la propria attività sul Web in cui un affiliato viene ricompensato per ogni visitatore, abbonato, cliente e/o vendita procacciato attraverso le proprie iniziative"<sup>3</sup>). Con lo sviluppo di nuove metodologie di monitoraggio, la prospettiva di trarre profitto dalle abitudini di navigazione delle persone passò da un semplice concetto innovativo a una strategia di marketing intelligente.

Con la crescente insistenza, da parte delle forze di mercato, a incorporare il messaggio pubblicitario all'interno del prodotto stesso, i meccanismi di promozione si fecero sempre più intrusivi. La trasmissione di messaggi pubblicitari in forma trasparente e non importuna ha progressivamente portato allo sviluppo dello spyware.<sup>4</sup> Lo spyware può essere definito anche come "tecnologia in grado di raccogliere informazioni su un individuo e/o sul suo computer e di trasmetterle ad altri: pubblicitari, forze dell'ordine, hacker, ecc. Tali informazioni vengono quindi restituite ai server di provenienza e possono includere indirizzi IP, indirizzi e-mail, configurazioni di sistema e, in alcuni casi, informazioni personali e dati delle carte di credito."<sup>5</sup> È stato il desiderio di guadagno, sia mediante lo sfruttamento delle informazioni raccolte dallo spyware che mediante la trasmissione di

3 Definizione di Wikipedia: [http://en.wikipedia.org/wiki/Affiliate\\_marketing](http://en.wikipedia.org/wiki/Affiliate_marketing)

4 In senso stretto, lo spyware è uno strumento per il monitoraggio del software utilizzato senza il consenso o il controllo dell'utente. Glossario ASC: <http://www.antispywarecoalition.org/documents/glossary.htm>

5 Definizione di Wikipedia: <http://en.wikipedia.org/wiki/Spyware>

messaggi pubblicitari tramite adware, il principale incentivo allo sviluppo dello spyware e di altri PUP.

### Considerazioni economiche

Che cosa ha alimentato la crescente diffusione di spyware, adware e altri programmi PUP negli ultimi anni? La risposta è semplice: il profitto. Le iniziative di adware e spyware sono guidate da una forza trainante molto tangibile, a differenza degli effetti spesso molto meno tangibili di altre dannose minacce alla sicurezza. È il denaro a spingere gli individui a investire tempo e risorse significative nello sviluppo di varie tecniche e metodi di diffusione di spyware, adware e altri programmi PUP. Secondo il commissario della FTC Jonathan Leibowitz, il "piccolo segreto" di adware e PUP dannosi è che alle spalle del problema ci sono grandi gruppi leciti e "rispettabili" che pagano per trasmettere i propri annunci pubblicitari attraverso questi programmi adware malevoli.<sup>6</sup>

Il modello adware funziona in questo modo. I pubblicitari progettano un annuncio per il prodotto o il servizio che devono vendere. Quando l'annuncio è pronto, la società fornitrice di adware entra in scena e realizza il software destinato a trasmettere l'annuncio. La fetta di torta destinata alla società fornitrice di adware viene calcolata in commissioni per singola installazione. A questo punto, potrebbe entrare in gioco anche un distributore che realizza un pacchetto software, spesso gratuito, per distribuire ai consumatori il programma adware in esso contenuto.

L'ignaro consumatore, alla ricerca di un software gratuito, installa il pacchetto sulla propria macchina e attiva la reazione a catena in modo inconsapevole e indesiderato. Nonostante sia spesso molto difficile individuare esattamente chi sponsorizza chi, il risultato finale è sempre lo stesso: i pubblicitari pagano le società fornitrici di adware e i distributori inseriscono l'adware nelle macchine dei consumatori. La funzionalità di monitoraggio dell'adware, se fosse chiara all'utente, sarebbe sicuramente indesiderata ed è compito delle aziende operanti nel settore della sicurezza garantire che gli utenti vengano avvisati di questa funzionalità. Spesso non si considera il comportamento dell'adware malevolo in quanto il suo fine non è distruggere o danneggiare la macchina. Tuttavia, l'installazione stessa del software adware può provocare modifiche all'interno del browser e la trasmissione degli annunci pubblicitari generalmente influisce sulle prestazioni del sistema. Ciononostante, la caratteristica più dannosa dell'adware è la trasmissione di informazioni sulle abitudini di navigazione dell'utente e l'acquisizione di altri dati personali senza il suo consenso. Dati che vanno ad avvantaggiare economicamente una o più parti coinvolte.

<sup>6</sup> [http://www.truste.org/pdf/quote\\_leibowitz.pdf](http://www.truste.org/pdf/quote_leibowitz.pdf)

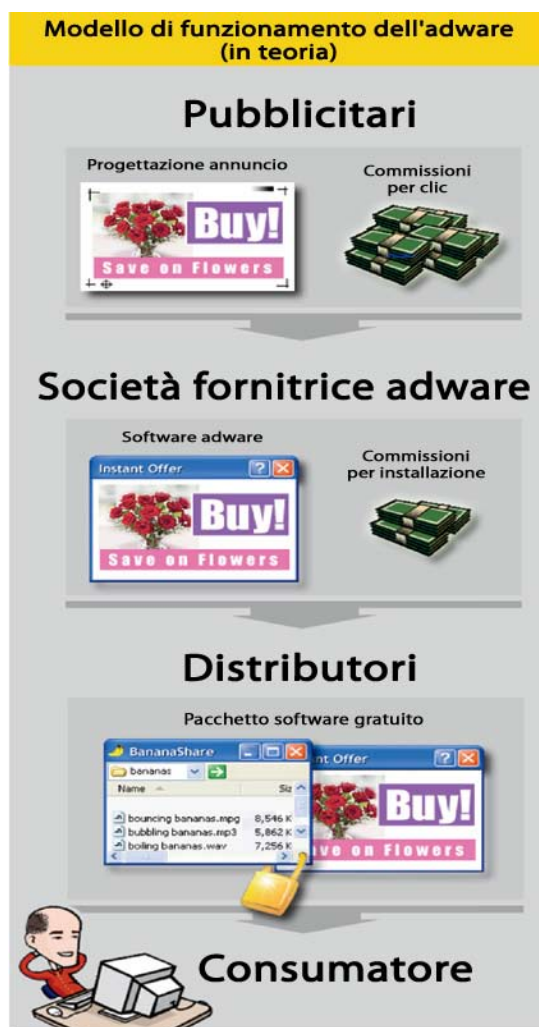


Figura 1: Modello di funzionamento dell'adware<sup>7</sup>

Questo è l'adware in poche parole.<sup>8</sup> Sfortunatamente, però, esiste anche un'altra forma di PUP che è addirittura peggiore: lo spyware. Secondo un'indagine condotta dalla Cyber Security Industry Alliance, il 67 per cento degli intervistati considera lo spyware un problema serio.<sup>9</sup> Nel senso più stretto del termine, lo spyware è un software in grado di monitorare e tracciare il comportamento degli utenti, raccogliendo spesso anche informazioni personali d'identificazione.<sup>10</sup> Sotto molti aspetti, la tracciabilità rappresenta la minaccia più insidiosa.

<sup>7</sup> Diagramma fornito da CDT: <http://www.cdt.org/privacy/20060320adware.pdf>

<sup>8</sup> Adware: tipo di software per la visualizzazione di annunci pubblicitari; in particolare, applicazioni eseguibili il cui scopo primario è trasmettere contenuto pubblicitario in un modo o in un contesto potenzialmente inatteso o indesiderato per l'utente. Numerose applicazioni adware presentano anche funzionalità di tracciamento e, di conseguenza, possono essere considerate tecnologie di tracciamento. Glossario ASC: <http://www.antispywarecoalition.org/documents/glossary.htm>

<sup>9</sup> <https://www.csalliance.org/issues/spyware/>

<sup>10</sup> Le informazioni personali di identificazione sono "informazioni personali su un individuo identificato o identificabile, la cui raccolta, uso o divulgazione dovrebbe essere controllata e autorizzata dall'individuo stesso." Glossario ASC: <http://www.antispywarecoalition.org/documents/GlossaryJune292006.htm>

Lo spyware comprende una categoria di programmi occulti e difficili da rilevare che vengono impiegati sia per finalità innocue (come affermerebbero i loro sostenitori) che malevoli. Si tratta di programmi utilizzati per registrare le sequenze di tasti battute sulla tastiera, le sessioni di chat e addirittura il contenuto di e-mail nel momento in cui vengono scritte. Questa forma di spyware è stata definita dalla ASC (Anti-Spyware Coalition) "un sistema per monitorare il software installato senza preavviso per l'utente, senza il suo consenso e fuori del suo controllo."<sup>11</sup> Lo spyware di sorveglianza, come il software eBlaster, è in grado di monitorare praticamente tutto ciò che avviene nel sistema, dai programmi eseguiti alle attività di file-sharing, fino all'accesso e all'uscita dell'utente dal sistema. Nonostante la maggior parte dei programmi anti-spyware sia in grado di rilevare questi pericolosi software, eBlaster opera in modo da occultare la propria attività, anche quando invia file di registro dalla macchina della vittima alla macchina host. Questo tipo di spyware viene generalmente installato sui PC delle vittime mediante un semplice clic su un annuncio pubblicitario o su un link contenuto in un'e-mail spam o, addirittura, mediante un programma software lecito. Questo tipo di spyware non può essere rilevato o rimosso dall'utente senza l'ausilio di un prodotto anti-spyware affidabile.

Le aziende fornitrici di adware e i creatori di spyware impiegano meccanismi differenti. O tentano di aggirare i prodotti anti-spyware fingendosi innocui, oppure provano a violare le applicazioni di sicurezza servendosi di metodi occulti dall'elevato contenuto tecnologico, quali i rootkit.

Più avanti nel documento verranno prese in esame le conseguenze sociali dei vari tipi di spyware e verranno analizzati i motivi per cui, nonostante il problema dello spyware appaia complessivamente declino, l'esperienza degli utenti nell'uso del computer e di Internet continui a esserne affetta su vasta scala.

### A che punto siamo oggi?

Gli spyware e gli altri programmi PUP sono ancora in aumento? Nonostante la capacità di rilevamento dei PUP sembri migliorare in modo costante anno dopo anno, i tipi di rilevamento univoci sono in diminuzione. Questo fenomeno potrebbe avere due cause: o il numero dei programmi è effettivamente in declino o la modalità di classificazione degli stessi da parte dei fornitori di sistemi di sicurezza è leggermente cambiata. Ad esempio, a causa delle caratteristiche simil-trojan di molti dei più recenti PUP e spyware (o di alcuni vecchi programmi ora aggiornati), ormai si tende a classificarli come trojan anziché come spyware. In ogni caso, i campioni che si trovano in giro si comportano effettivamente più come trojan che come PUP. Di conseguenza, rientrano nella categoria dei programmi dannosi. Inoltre, i creatori di spyware stanno mutando le

11 Glossario ASC: <http://www.antispywarecoalition.org/documents/glossary.htm>

loro strategie di diffusione e installazione del software per renderle più sofisticate e camuffate, come avviene per i rootkit, che stanno diventando una minaccia sempre più reale. I rootkit costituiscono una seria minaccia alla sicurezza, in quanto estremamente difficili da rilevare e rimuovere.<sup>12</sup>

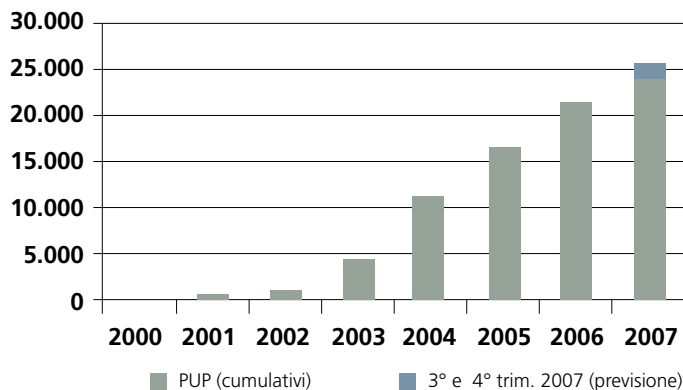


Figura 2: Secondo le statistiche dei McAfee Avert Labs, la diffusione dei programmi indesiderati è cresciuta molto rapidamente negli ultimi cinque anni.

I fornitori di adware, in particolare, stanno apparentemente rimettendosi in carreggiata mediante una correzione del loro comportamento scorretto, anche se a livelli non ancora accettabili. Questa mezza soluzione rende ancora più difficile per le aziende di sicurezza individuare i comportamenti effettivamente "indesiderati", almeno dal punto di vista del consumatore. Per l'amministratore IT, tuttavia, la maggior parte di questo "grayware" indefinito resta sempre indesiderato nell'ambito della rete aziendale e continuerà a essere rilevato come tale. In ogni caso, il confine tra una divulgazione corretta e l'effettiva consapevolezza da parte dell'utente di ciò che ha scelto di vedere rimane sempre molto indistinto. In generale, le aziende che si occupano di sicurezza sostengono che il fattore discriminante è costituito dall'effettivo comportamento del programma e non da ciò che il programma segnala o non segnala all'utente circa il suo comportamento. La lettura di un contratto di licenza di cinque pagine prima dell'installazione di un programma non costituisce per l'utente una rivelazione sufficiente né rilevante, perciò, quando si tratta di classificare un particolare software è opportuno dare la precedenza al suo reale comportamento.

Lo spyware e l'adware possono anche danneggiare in modo significativo i sistemi intaccati da questo tipo di programmi. Un importante aspetto della remediation è l'efficacia con la quale i prodotti anti-spyware riescono a ripulire il sistema da file, chiavi di registro e processi che possono compromettere le prestazioni di una macchina.

12 Per maggiori informazioni sui rootkit si possono leggere i nostri articoli dell'aprile 2006 e aprile 2007 all'indirizzo [http://www.mcafee.com/us/threat\\_center/white\\_paper.html](http://www.mcafee.com/us/threat_center/white_paper.html).

La procedura di rimozione dei file PUP può risultare estremamente complessa, in particolare nel caso dei rootkit, e, talvolta, anche rischiosa. Spyware e adware vengono sempre più spesso progettati per nascondersi perfettamente all'interno delle macchine degli utenti ed eseguire l'hooking di risorse cruciali del sistema.

### Chi vincerà?

Che cosa fanno i fornitori di sistemi di sicurezza per sconfinare il nemico occulto? I creatori di adware e spyware sono spinti da motivazioni troppo forti per abbassare le armi, anzi, si stanno impegnando con tutte le loro risorse per aggirare i sistemi di rilevamento, in un modo che ricorda la battaglia sferrata contro le strategie anti-spam. Come già accennato in precedenza, uno dei sistemi utilizzati dai creatori di PUP per stare al passo con i sistemi di rilevamento è quello di rendere i criteri di rilevamento sempre meno applicabili. Mediante la progettazione di tecnologie che non vengono prese in considerazione oppure confondendo il confine tra una pratica illecita e comportamenti che potrebbero essere considerati accettabili in particolari contesti, gli autori di PUP tentano di ingannare i sistemi anti-spyware. Le società che si occupano della sicurezza hanno fatto il possibile per rafforzare e rendere più severi criteri, definizioni e analisi. Grazie alla ASC, ciò che un tempo era solo una raccolta confusa di definizioni univoche è stato rimodellato in un compendio di definizioni e linee guida per l'intero settore. (Tali documenti possono essere consultati presso il sito <http://www.antispywarecoalition.org/documents/index.htm>. Si tratta del risultato di un importante lavoro portato avanti da esperti del settore e gruppi a difesa dei consumatori.)

I rootkit sono una sottoclasse dei PUP in rapida diffusione. In virtù della loro natura furtiva, i rootkit sono estremamente complessi e rischiosi da rilevare e risolvere. Secondo i McAfee® Avert® Labs, attualmente sono in circolazione più di 12.000 varianti di rootkit non ancora individuate. In realtà, la sempre più ampia diffusione dei rootkit ha imposto un'evoluzione non solo della tecnologia anti-virus, ma anche delle tecnologie core impiegate da progettisti e installatori di chip e sistemi operativi.<sup>13</sup>

Proprio in virtù della loro capacità di nascondere componenti e attività, i rootkit sono stati utilizzati anche da diversi programmi "leciti". Tra questi, ricordiamo il famigerato XCP (eXtended Copy Protection) di Sony BMG, che, tra le altre cose, scatenò un acceso dibattito sulla protezione delle copie e sulla gestione dei diritti digitali (DRM). Senza chiedere un consenso o informare l'utente, il rootkit si installava in modo invisibile all'interno del sistema e non offriva alcuno strumento di disinstallazione. Alla

fine, Sony fu costretta a ritirare tutti i CD distribuiti che contenevano il pacchetto rootkit.<sup>14</sup>

Recentemente, Sony ha fatto ancora parlare di sé per un altro software simile a un rootkit. Veniva distribuito all'interno di unità USB della Sony, conosciute come Fingerprint Access Software, che utilizzavano driver e software sviluppati da Fineart Technology. In pratica, il file eseguibile può essere inserito in qualsiasi directory; quando viene eseguito, esso nasconde immediatamente tutti i file e le cartelle a esso associate all'interno della propria directory nascosta.<sup>15</sup>

I rootkit possono avere anche finalità lecite, come nel caso di Sony, tuttavia la loro implementazione offre comunque possibilità di sfruttamento, sia malevolo che legittimo, e i programmi in grado di porre rimedio a queste potenti funzionalità sono ancora molto limitati.

### Aspetti sociali dello spyware

Lo spyware non è semplicemente una seccatura da un punto di vista tecnico, ma può anche essere utilizzato per scopi criminali. Sono state promosse iniziative nazionali finalizzate a educare il grande pubblico sulle pericolose insidie che questi programmi contengono e su come combatterle.

L'uso di spyware a scopo di sorveglianza in casi di abusi domestici è una questione molto seria. L'installazione di un software che controlli e tenga traccia di tutte le attività eseguite sul computer di un utente ignaro ha implicazioni sia sociali che legali. In una società in cui il livello di dipendenza da computer e da altre tecnologie, quali i telefoni cellulari, è così elevato, gli spyware diventano uno strumento ideale per i responsabili di abusi, che spesso devono poter controllare ogni aspetto dell'esistenza delle loro vittime. Poter monitorare le telefonate, l'uso di Internet o l'attività informatica generale di una vittima è di importanza fondamentale per chi desidera controllare o fare del male a un individuo.

Il National Network to End Domestic Violence (Rete nazionale per la lotta alla violenza domestica) con sede a Washington si sta attivando per educare le vittime di violenza domestica e l'opinione pubblica in generale sull'uso sicuro degli strumenti informatici. Molte aziende che si occupano di sicurezza hanno fatto consistenti donazioni in denaro a questa organizzazione per sostenere la formazione e per aiutare a proteggere le vittime di violenza domestica. (Per ulteriori informazioni, visitare il sito <http://www.nnedv.org/internet-safety.html>.)

<sup>13</sup> "Intel readies rootkit-rooting hardware" (Intel appronta un hardware per il rilevamento dei rootkit), [http://www.theregister.co.uk/2005/12/09/intel\\_anti-rootkit\\_chip/](http://www.theregister.co.uk/2005/12/09/intel_anti-rootkit_chip/)

<sup>14</sup> Voce di Wikipedia: [http://en.wikipedia.org/wiki/2005\\_Sony\\_BMG\\_CD\\_copy\\_protection\\_scandal](http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal)

<sup>15</sup> <http://www.avertlabs.com/research/blog/index.php/2007/08/28/hide-me-sony-one-more-time>

L'ampia diffusione dell'adware può danneggiare e demoralizzare gli utenti ignari dei sistemi. In un blog dei McAfee Avert Labs, Hiep Dang, responsabile della ricerca sul malware, chiede se si può rischiare la prigione per non avere ripulito il proprio PC infettato da spyware.<sup>16</sup> La risposta è, potenzialmente, sì. Si prenda, ad esempio, il caso di Julie Amero, un'insegnante elementare processata e condannata in Connecticut per avere esposto i suoi alunni a immagini pornografiche. (La sentenza è poi stata respinta da un secondo giudice e ora Amero è in attesa di un nuovo processo.)<sup>17</sup> In questo caso, una semplice applicazione scaricata e installata sul sistema di un utente ha portato a conseguenze tutt'altro che irrilevanti. Gli esperti sostengono che le immagini pornografiche presenti nel PC di Julie Amero erano frutto di annunci pubblicitari pop-up generati da adware. Ciononostante, le conseguenze sono state tremende: le immagini hanno spaventato i bambini e la Amero sta vivendo un vero e proprio incubo per difendere la sua reputazione. Questa è forse la conseguenza più pubblicizzata della diffusione incontrollata dell'adware, ma sicuramente non l'unica.

## Problemi legali

Si è assistito a numerosi tentativi da parte di vari gruppi di imporre restrizioni tangibili allo spyware e ai suoi creatori. In particolare, la Camera dei deputati degli Stati Uniti ha approvato nel 2004 un controverso disegno di legge finalizzato a rendere lo spyware illegale.<sup>18</sup> I risultati dell'Internet Spyware Prevention Act, o I-SPY Act, sono stati fortemente contestati da numerose agenzie pubblicitarie. Recentemente, il senatore Mark Pryor dell'Arkansas ha introdotto il Counter Spy Act del 2007, con l'intento di rendere illegale per "aziende e truffatori" l'installazione di spyware sui computer di altre persone senza il loro consenso. Secondo Pryor e i suoi sostenitori, "lo spyware è un reato molto serio che implica la violazione di livelli fondamentali di riservatezza e sicurezza. Esistono pochissime motivazioni lecite che giustifichino il perpetuarsi di questa pratica, mentre non si contano i motivi validi per interromperla, primo tra tutti il furto di identità o, più

semplicemente, il peggioramento delle prestazioni del computer". In poche parole, il Counter Spy Act prevede che la Federal Trade Commission applichi la legge in modo che la sua violazione costituisca una prassi scorretta o ingannevole, aprendo in tal modo le porte a cause civili, oltre che a sanzioni penali, per violazione della legge.

## Conclusioni

Lo spyware sta lentamente scomparendo dai radar di molti utenti domestici e amministratori IT per lasciare il posto ad altri "pericoli" tecnologici comparsi sulla scena negli ultimi mesi. Tuttavia, la realtà dello spyware non è cambiata, tutt'al più si è trasformata in una minaccia alla sicurezza meno percettibile e più ingegnosa. Dal software di distribuzione di pop-up pubblicitari palesemente indesiderati, si è passati a programmi di tracciamento installati in modo invisibile e dall'attività impercettibile. Aziende creatrici di adware, quali WhenU, hanno cambiato nome più volte, nella speranza di passare inosservate dalla distribuzione palese di annunci pubblicitari al monitoraggio occulto dei sistemi mediante il loro programma MeMedia, MeMe.<sup>19</sup> Inoltre, la distinzione tra ciò che viene considerato trojan e un programma PUP è sempre meno chiara, ora che sempre più PUP vengono distribuiti e installati come se fossero trojan.

Con l'evolversi dei PUP e delle altre minacce in risposta al rapido mutamento delle esigenze di aziende e organizzazioni di altro tipo, tutti noi dobbiamo stare all'erta più che mai perché il nemico è insidioso e invisibile.

## Informazioni sull'autore



Anna Stepanov gestisce il programma Anti-Spyware per i McAfee Avert Labs, è membro dell'ASC e ha pubblicato una serie di articoli per tale organizzazione e per gli Avert Labs. Stepanov ha inoltre partecipato al Anti-Phishing Working Group e ha avuto un ruolo fondamentale nella progettazione del motore anti-spam della versione consumer di McAfee SpamKiller®.

<sup>16</sup> Blog dei McAfee Avert Labs: <http://www.avertlabs.com/research/blog/?p=174>

<sup>17</sup> Voce di Wikipedia: [http://en.wikipedia.org/wiki/Julie\\_Amero](http://en.wikipedia.org/wiki/Julie_Amero)

<sup>18</sup> Definizioni di SearchSecurity.com: [http://searchsecurity.techtarget.com/Definition/0,,sid14\\_gci1093105,00.html](http://searchsecurity.techtarget.com/Definition/0,,sid14_gci1093105,00.html)

<sup>19</sup> Blog dei McAfee Avert Labs: <http://www.avertlabs.com/research/blog/index.php/2007/06/14/when-is-whenu-meme/>

McAfee, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054, USA  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee, Avert Labs, SpamKiller e/o altri prodotti McAfee citati nel presente documento sono marchi o marchi registrati di McAfee, Inc. e/o delle sue società affiliate negli Stati Uniti e/o in altri Paesi. Il rosso McAfee utilizzato con riferimento alla sicurezza è una caratteristica distintiva dei prodotti con marchio McAfee. Tutti gli altri prodotti e marchi commerciali registrati e/o non registrati non appartenenti a McAfee citati nel presente documento sono utilizzati esclusivamente come riferimento e appartengono ai rispettivi proprietari. © 2007 McAfee, Inc. Tutti i diritti riservati. 6-na-cor-spy-wp-001-1107