

# PRIVACY HORIZONS: TERRA INCOGNITA

29<sup>th</sup> International Conference of  
Data Protection and Privacy Commissioners

September 25 to 28, 2007  
Montreal, Canada



## LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29<sup>e</sup> Conférence internationale des commissaires  
à la protection des données et de la vie privée

du 25 au 28 septembre 2007  
Montréal, Canada

# Atelier sur le crime sur Internet

Wayne Watson

Directeur général

Direction des enquêtes et des  
demandes de renseignements

Commissariat à la protection de la vie  
privée du Canada

[www.privcom.gc.ca](http://www.privcom.gc.ca)

# **La cybercriminalité**

## **Harcèlement, violence familiale et violence sexuelle**

Présentatrice : Cynthia Fraser

**Safe & Strategic Technology Project**  
(projet de technologies stratégiques et sécuritaires)

**National Network to End Domestic Violence**  
(réseau national pour l'élimination de la violence familiale)



## **Cybercriminalité et mauvais usage de la technologie**

|                       |                      |               |
|-----------------------|----------------------|---------------|
| Interception          | Surveillance         | Environnement |
| Usurpation d'identité | Contrôle             | Manipulation  |
| Harcèlement           | Victimisation        | Préméditation |
| Menaces               | Harcèlement criminel | Localisation  |

## **Objectifs clés**

**Sécurité et protection des renseignements personnels des victimes et des survivants**

**Responsabilisation du délinquant      Changements de système**

**Greetings Infidels, I am Liam Youens**



## Site Web d'un agresseur

« Je n'allais pas la tuer  
cette journée-là; je  
voulais seulement  
savoir le moment exact  
où elle sortirait... »

Update: On Thursday October 7, I was making excuses because I was scared. I still feel uncomfortable about sitting in the parking lot. I pray to God that she parks on the street like last Friday, but I doubt it. My mother is going on vacation so I would be able to use her car. That may make me bold enough to park in the lot at 4:30. Since I wasn't going to kill her today I wanted to get the exact time she leaves, so I can minimize the time I would have to park there. I went around and around doing my best not to get noticed.

I saw her, I saw her, I saw her. At 4:47pm Thursday she was at a red light near the office and I came in from the side. She didn't notice me I don't think. She looked wonderful, like seeing God herself. I think I might have seen her before on a bike and

**Amy Boyer**



## Le meurtre d'Amy Boyer

Courtier en ligne DocuSearch : L'agresseur a fait des appels et a invoqué des prétextes pour obtenir le NAS et l'adresse du lieu de travail d'Amy Boyer. Le courtier a vendu à l'agresseur ces renseignements, qui ont permis à ce dernier de trouver et de tuer Amy.

La famille d'Amy a poursuivi DocuSearch. Cas du New Hampshire (É.-U.) :

- Obtenir des renseignements personnels par faux semblant constitue une violation des lois de protection des consommateurs.
- Les enquêteurs et les courtiers doivent faire preuve d'une diligence raisonnable au moment de divulguer à un client les renseignements personnels d'une tierce partie.

# Les harceleurs et le brouillage téléphonique en ligne

- Identification de l'appelant et modificateur de voix
- Enregistrement des appels et contrôles en ligne
- Achat de cartes d'appel en argent comptant
- Menaces et harcèlement
- Preuves?



SpooferCard calling cards offers you the ability to change what someone sees on their caller ID display when they receive a phone call.

Key Benefits: Make calls truly private, Ability to record calls, Change your voice, Fun and inexpensive, Easy to use and fast to set up!

**Instant Access!**

[→ MORE INFO](#)

#### SPOOFERCARD FEATURES:

- Caller ID Spoofing
- Voice Changer
- Call Recording
- Web Control Panel

No computer needed! Simply dial the toll free number from the calling card you purchase.

1. Enter your pin number.
3. Enter Destination number.
2. Enter Any Caller ID Number you wish to display.
4. Choose the voice you would like to use.
5. Your call is connected using the specified Caller ID Number.

As an added bonus, we offer you the option to record your conversation for **FREE** which you can later retrieve by logging in to your control panel or



#### Control Panel Login

Calling Card Pin:



ENTER

[Lost/Forgot PIN](#)

[BUY INSTANT CALLING MINUTES](#)

[MESSAGE BOARD NEW](#)

[FREQUENTLY ASKED QUESTIONS](#)

[CONTACT US](#)

[CUSTOMER SERVICE](#)

[PRIVACY POLICY](#)

#### Buy \$10 Instant Calling Card

- 60 Minutes talk time
- Caller ID Spoofing
- Voice Changer
- Call Recording
- Customer Service



[Buy Now](#)

#### Buy \$20 Instant Calling Card

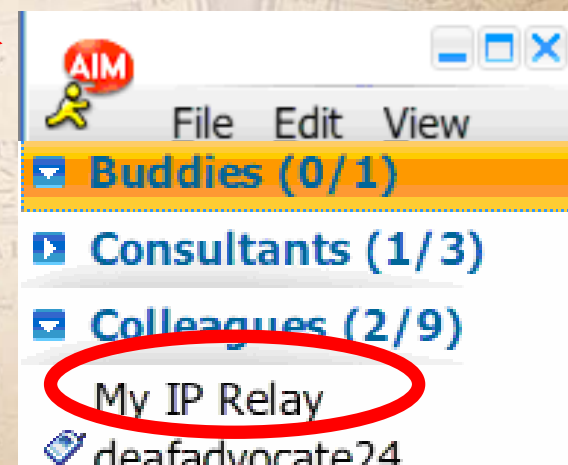
- 120 Minutes talk time
- Caller ID Spoofing
- Voice Changer



# IP Relay, harcèlement et déguisement

« Ici l'opérateur d'IP Relay 5243; nous avons un message. T'es un sans cœur, maudit @\$#%. Crève. Va te faire foutre. Fin du message. Merci. IP Relay... »

- Entrez le n° de téléphone sur le site Web d'IP Relay.
- Cliquez sur « AIM ». Ajoutez un ami sous « MyIPRelay ». Envoyez le MI avec le n° de téléphone.
- L'opérateur d'IP Relay (tiers) redirige la conversation écrite et parlée.
- Est-ce confidentiel sur le plan légal? On peut cependant intercepter le message!





# Le crime – MI et courriel : Nouvelles caractéristiques et nouveaux risques

- Usurpation d'identité, interception, menaces, contrôle, collecte d'éléments de preuve et harcèlement, protection des renseignements personnels et cryptage
- Courriel : reniflage, anonymiseurs, services de courriel anonymes
- MI : connexion, piratage, transfert à un dispositif mobile

## Connexion à la MI

- Connexion aux MI
- Connexion aux sites de clavardage

Connexion au disque dur  
(C:\Document)

VICTIM  SERVICES

*Welcome to Victim Services  
Domestic Violence Shelter Tour  
and Information Site*

Envoyez un courriel  
pour obtenir de l'aide



# GPS et localisation en ligne

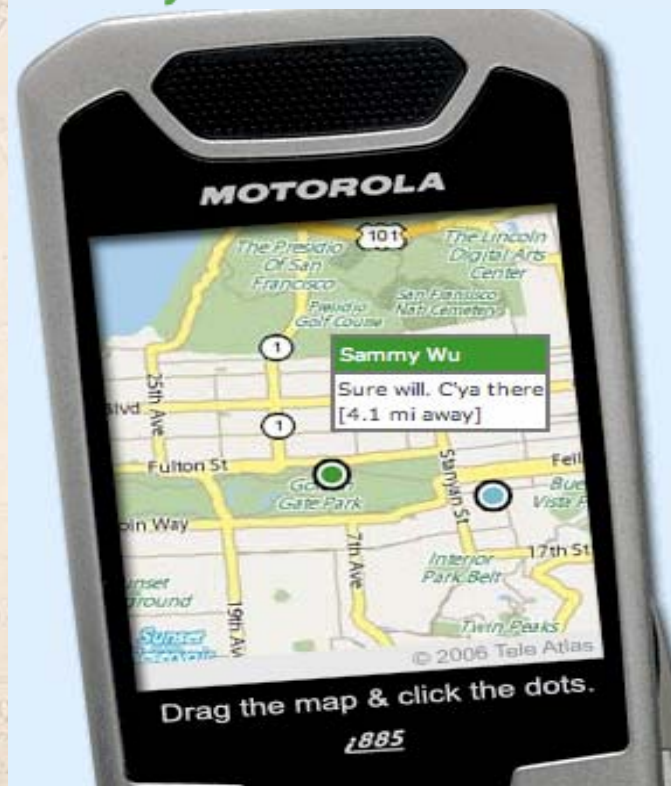
The screenshot shows a GPS navigation application. At the top is a toolbar with icons for Default, Open, Units, Groups, Print, Print map, Zoom In, and Zoom Out. The main map area displays a street grid with a red route highlighted. A blue dot on the map is labeled 'Tom's unit'. To the right of the map is a data table with two columns: 'Start & Dur' and 'Location / Dist & Max Speed'. The table is titled 'Monday, December 23, 2002'. The table contains 14 rows of data, each with a traffic light icon (green, yellow, or red with 'STOP' and 'L/S') to its left. The data includes start times, durations, distances, and locations.

|          | Start & Dur | Location / Dist & Max Speed |
|----------|-------------|-----------------------------|
|          | 06:22:32    | 1.74 miles                  |
|          | 3min 05sec  | 33.3 mph                    |
| STOP L/S | 06:25:38    | 2100 - 2299                 |
|          | 4min 49sec  | W PALATINE RD               |
|          | 06:30:27    | 19.59 miles                 |
|          | 30min 05sec | 67.6 mph                    |
| STOP     | 07:00:32    | Lat 41.9814                 |
|          | 1hrs 34min  | Lon -87.8741                |
|          | 08:34:39    | 14.97 miles                 |
|          | 16min 30sec | 76.1 mph                    |
| STOP L/S | 08:51:09    | 2300 - 2399                 |
|          | 1hrs 05min  | ST JAMES ST                 |
|          | 09:56:09    | 20.91 miles                 |
|          | 37min 00sec | 68.1 mph                    |
| STOP     | 10:33:10    | 5500 - 5599                 |
|          | 11min 53sec | W TOUHY AVE/TOUHY AVE       |
|          | 10:45:03    | 7.66 miles                  |
|          | 19min 07sec | 56.1 mph                    |
| STOP     | 11:04:11    | Lat 41.9831                 |
|          | 1hrs 21min  | Lon -87.8581                |
|          | 12:25:51    | 1.56 miles                  |
|          | 3min 59sec  | 49.4 mph                    |
| STOP     | 12:29:51    | 185 - 1800                  |
|          | 7min 42sec  | CUMBERLAND AVE/N PUEBLO AV  |
|          | 12:37:33    | 14.65 miles                 |

## Dispositif de localisation sans fil : consentir, avertir, se cacher

- Double adhésion : voir l'emplacement sans faire connaître le vôtre.
- Avertissement : messages textuels aléatoires pour être au courant des caractéristiques de localisation activées.
- Fonction marche/arrêt : vous permet de vous cacher de tout le monde ou d'une personne en particulier.
- Emplacement fictif : indiquez, par exemple, que vous êtes à la bibliothèque et rendez-vous à un refuge.

find your friends fast!



share your location automatically  
find events and places  
connect to friends

# GPS et cas de harcèlement aux É.-U.

**CNN.com./TECHNOLOGY**

**Police: GPS device used to stalk woman**

Tuesday, December 31, 2002 Posted: 10:51 AM

**KENOSHA, Wisconsin (AP) – A man was charged Monday with stalking his former live-in girlfriend with help from a high-tech homing device placed under the hood of her car.**

- ❑ Colorado (2000) : Un homme installe un GPS dans la voiture de son ex-conjointe. Il est condamné pour l'avoir traquée à l'aide d'un dispositif de surveillance électronique.
- ❑ Wisconsin (2002) : GPS utilisé pour traquer une ex-petite amie. Il est condamné pour harcèlement et vol.
- ❑ Missouri (décembre 2005) : Un policier met un GPS dans la voiture de son ex-petite amie. Il est congédié.

# Caméras, Internet, voies de fait et agressions

- Voyeurisme et surveillance
- Diffusion de viols filmés
- Relations consensuelles filmées et diffusées sans consentement
- Pornographie juvénile et films dans lesquels transparaissent la contrainte et la préméditation
- Piratage de sites Web et d'ordinateurs, vol d'identité en vue de solliciter, menaces



# Logiciels espions, agresseurs et surveillance informatique



**Attorney General  
Jennifer M. Granholm**

**FOR IMMEDIATE RELEASE**

September 5, 2001



## eBlaster 5.0

The ONLY software that captures their incoming and outgoing emails, chat and instant messages - then IMMEDIATELY forwards them any email address you choose.

eBlaster also creates an hourly Activity Report detailing all emails sent and received, chats, IM's, keystrokes typed, web sites visited, programs launched and peer-to-peer (P2P) files downloaded - then sends it directly to YOUR email address.

In the first case, Steven Paul Brown, age 41 of Belleville, is charged with four felonies for allegedly installing spy software on the computer of Patricia Brown, his estranged wife. He installed a commercially available hacking program on the computer at Ms. Brown's separate residence in Warren. This program caused all of the keystroking activity of her computer, including all e-mails sent and received, all web surfing, and any Internet communications, to be e-mailed to Steven Brown's e-mail account.

La loi de l'État du Michigan (É.-U.) condamne l'écoute électronique, l'installation de dispositifs d'écoute électronique, l'accès non autorisé et l'utilisation d'un ordinateur à des fins criminelles.



Brèches faciles dans la protection des données – La BBC demande à un enfant d'installer un enregistreur de frappe dans l'ordinateur d'une députée (Angleterre, 23 mars 2007)

Une fillette âgée de six ans, accompagnée par un journaliste du programme Inside Out de la BBC, a installé un dispositif d'enregistrement de frappe dans l'ordinateur d'une députée. La députée, Anne Milton, a accepté de laisser son ordinateur sans surveillance pendant une minute; l'enfant a installé l'enregistreur en 15 secondes. Elle a apporté le dispositif à l'insu des membres de la Chambre des communes.

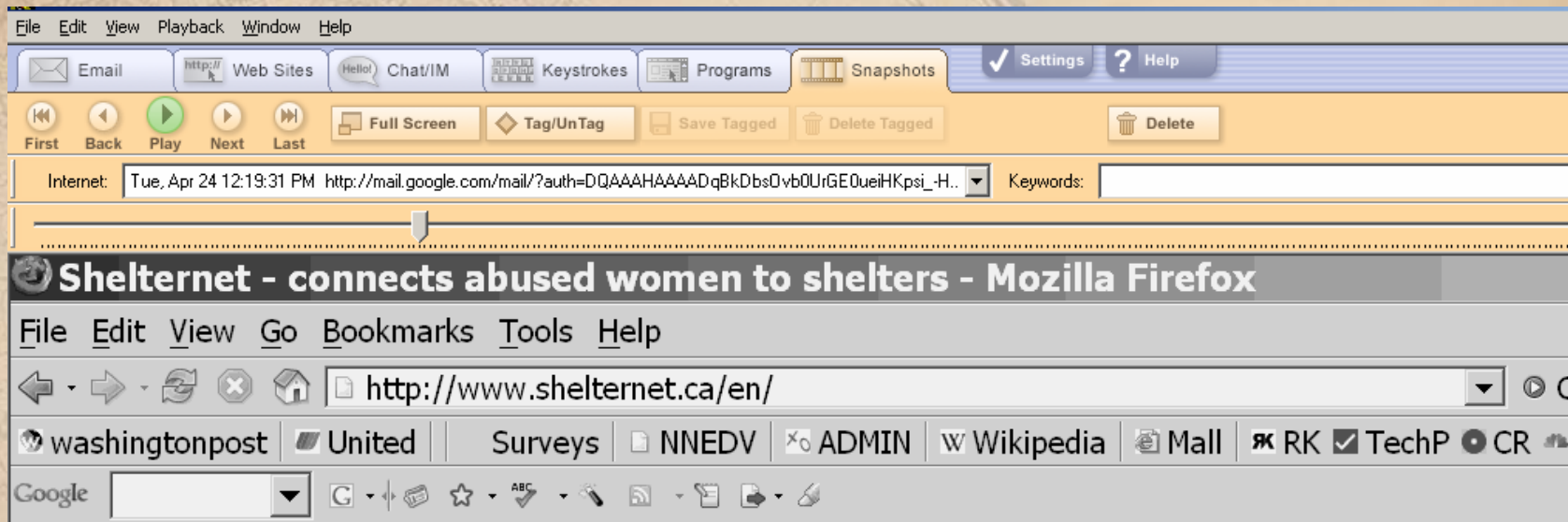
# Logiciel espion qui enregistre toutes les touches frappées

The screenshot shows a software interface with a menu bar (File, Edit, View, Window, Help) and several toolbars. The main toolbar includes buttons for Email, Web Sites, Chat/IM, Keystrokes, Programs, and Snapshots. Below this is a navigation area with 'Jump to...', 'View...', and 'Show...' dropdowns, and a 'Search Keystrokes:' search box. The central part of the interface is a table with three columns: Program, Key Count, and Program Start Date. The table lists various applications and their corresponding key counts and start times. The row for 'Firefox' with a key count of 22 is highlighted. At the bottom, there is a text area containing '[My Yahoo! - Mozilla Firefox]' and '<08:17 AM>www.shelternet/c.ca'.

| Program           | Key Count | Program Start Date            |
|-------------------|-----------|-------------------------------|
| MS Power Point    | 15        | Fri, Aug 17, 2007 05:19:15 PM |
| Internet Explorer | 225       | Fri, Aug 17, 2007 05:17:23 PM |
| Firefox           | 22        | Thu, May 03, 2007 12:25:41 PM |
| Explorer          | 2         | Thu, May 03, 2007 12:25:41 PM |
| Aim6              | 192       | Thu, May 03, 2007 08:22:54 AM |
| Ssaad             | 2         | Thu, May 03, 2007 08:22:51 AM |
| Aim6              | 134       | Thu, May 03, 2007 08:20:22 AM |
| Firefox           | 22        | Thu, May 03, 2007 08:17:21 AM |
| Ssaad             | 2         | Thu, May 03, 2007 08:17:08 AM |
| Firefox           | 56        | Tue, Apr 24, 2007 07:14:52 PM |
| MS Power Point    | 265       | Tue, Apr 24, 2007 03:12:31 PM |
| MS Word           | 3678      | Tue, Apr 24, 2007 12:51:48 PM |
| MS Excel          | 3534      | Tue, Apr 24, 2007 12:20:17 PM |
| Aim6              | 322       | Tue, Apr 24, 2007 09:27:00 AM |
| Firefox           | 31        | Tue, Apr 24, 2007 09:09:25 AM |
| Firefox           | 111       | Tue, Apr 24, 2007 09:03:36 AM |

[My Yahoo! - Mozilla Firefox]  
<08:17 AM>www.shelternet/c.ca





Logiciel espion  
qui enregistre à  
chaque seconde  
des images ou  
des « saisies  
d'écran »

The screenshot shows a Mozilla Firefox browser window. The address bar contains the URL `http://206.47.204.99/superclick/opentoolbar.php`. The search bar contains the text "shelter abused women canada". The search results page shows the following content:

**Web** Images Groups News Maps more »

shelter abused women canada Search Advanced Search Preferences

Search:  the web  pages from Canada

**Web** Results 1 - 10 of about 1,120,000 for shelter abused women canada. (0.13 seconds)

**Women's Shelter** Sponsored Link  
www.IntervalHouse.on.ca Get Help For Domestic Violence. Housing, Counseling & More. Call Us

Crisis Services | Resources | Ontario **Women's Justice Network**  
Transition Houses and **Shelters for Abused Women in Canada** A PDF listing in French and English prepared by the National Clearinghouse on Family Violence, ...  
www.owjn.org/resource/**shelter**.htm - 21k - [Cached](#) - [Similar pages](#)

Every minute a woman in **Canada** is **abused**  
That is why **Canadian Women's Foundation**, Hudson's Bay Company (Hbc) and Rogers are ... **Women's Foundation** and 274 **shelters for abused women** across **Canada**. ...  
dawn.thot.net/start\_to\_stop\_violence.html - 25k - [Cached](#) - [Similar pages](#)

[PDF] Transition Houses and **Shelters for Abused Women in Canada** Maisons ...  
File Format: PDF/Adobe Acrobat - View as HTML

Exemple :  
victime qui  
cherche de  
l'aide sur le  
Web

File Edit View Playback Window Help

Email Web Sites Chat/IM Keystrokes Programs Snapshots Settings Help

First Back Play Next Last Full Screen Tag/UnTag Save Tagged Delete Tagged Delete

Internet: Tue, Apr 24 12:19:31 PM http://mail.google.com/mail/?auth=DQAAAHAAAADqBkDbsDvbOUrGE0ueiHKpsi\_H.. Keywords:

# Shelternet - Find a Womens Shelter – Clickable Map of Canada - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

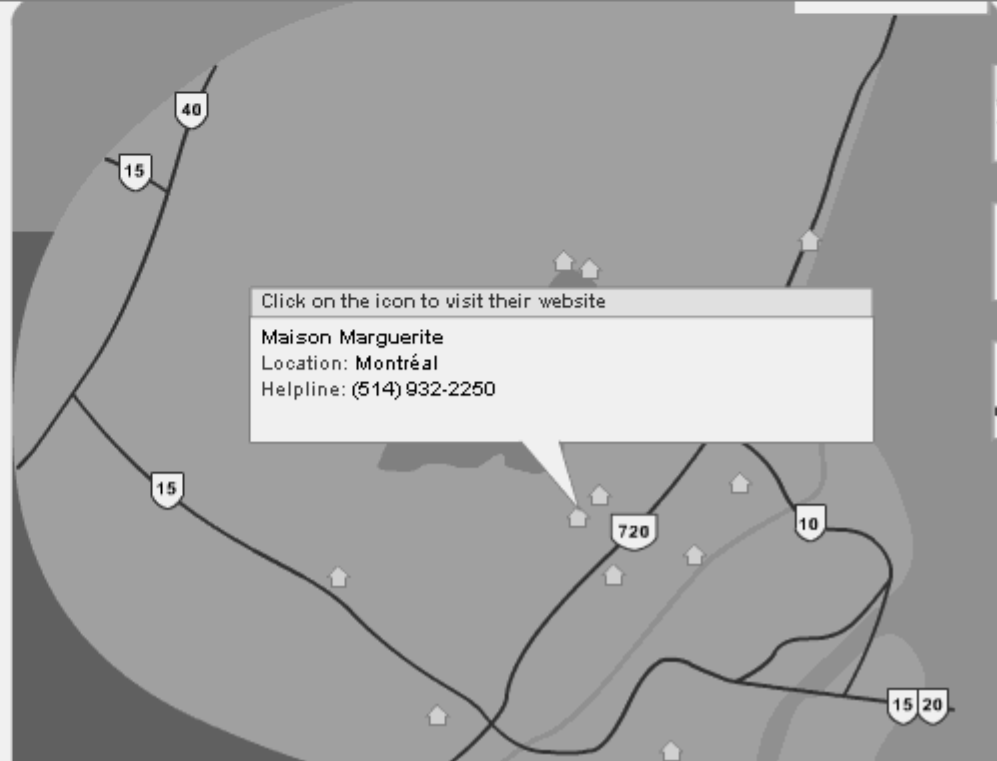
http://www.shelternet.ca/en/women/find-a-shelter/clickable-map/

washingtonpost United Surveys NNEDV ADMIN Wikipedia Mail RK TechP

Google

- Making A Safety Plan
- Understanding Abuse
- Find A Shelter**
- Clickable Map**
- About Shelters
- Women's Stories
- ns →
- For Kids →
- nds and Family →
- Workplace →
- mit Feedback →

Exemple :  
victime qui  
cherche un  
refuge pour  
personnes  
maltraitées



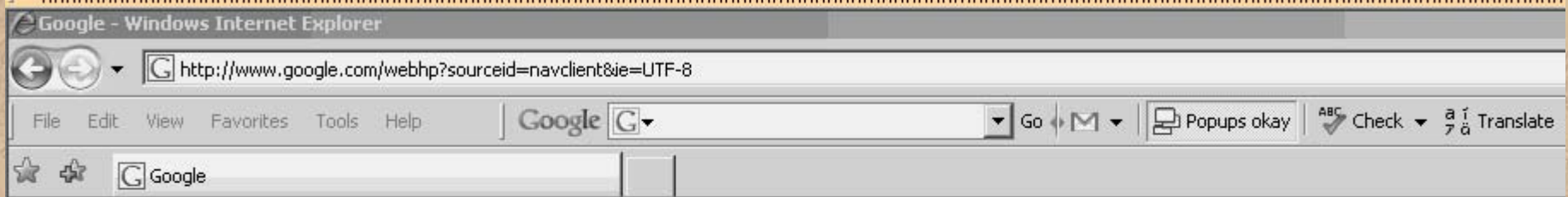
Canada

Provi

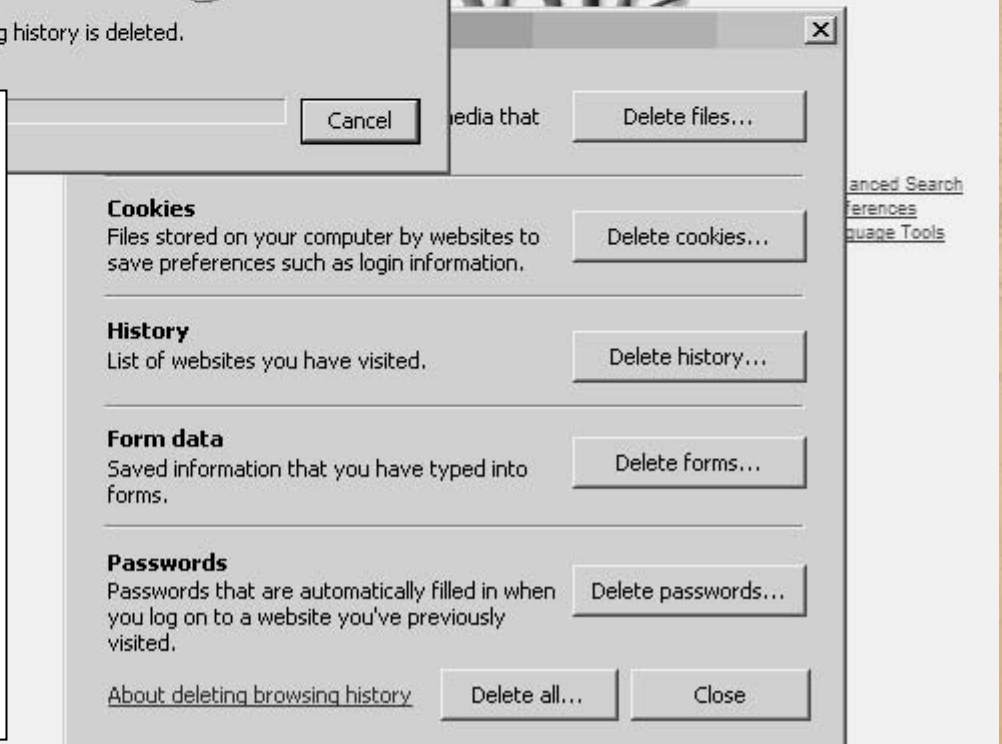
Regio

The screenshot shows a Mozilla Firefox browser window. The address bar contains the URL <http://www.shelternet.ca/en/women/internet-safety/>. The page title is "Shelternet - Hide Your Internet Activities - Mozilla Firefox". The browser's menu bar includes File, Edit, View, Go, Bookmarks, Tools, and Help. The page content features a sidebar with links such as "Your browser", "Clearing cache & history", and "About cookies". The main content area has a heading "Internet Safety Tips" and a text box stating: "Your abuser may have ways of tracking your activities on your home computer that are difficult to prevent. If you are concerned about the safety of using your home computer, if possible, use a computer at a public library, a school, an internet café, or at the home of a trusted friend." Below this is a "Questions and Answers about Internet Safety" section with three numbered questions.

Exemple :  
victime qui  
veut en savoir  
plus sur des  
cas liés à  
Internet



Exemple : victime qui tente en vain d'effacer l'historique de navigation pendant que ses gestes sont enregistrés par un logiciel espion



## Lois et règlements

- Loi fédérale sur le harcèlement et loi semblable dans chaque État (É.-U.), etc.
- Servez-vous des lois de votre pays pour aider les victimes : protection des données, écoute électronique, injonctions restrictives, cybercrimes, etc.
- Donnez une formation sur l'application des lois sur la criminalité.

## Recommandations

- Assurez la protection de toutes les données sur les victimes, particulièrement dans les cas de changements d'identité et de lieu.
- Intégrez le concept de « mauvais usage de la technologie par les agresseurs » à TOUTES les vérifications, formations et campagnes de sensibilisation relatives à la protection des renseignements personnels.
- Informez les défenseurs des victimes.

**Pour de plus amples renseignements,  
veuillez communiquer avec :**

**Cynthia Fraser**

**ou tout autre membre de l'équipe Safety Net Project**

**U.S. National Network to End Domestic Violence**



**2001 S Street NW, Suite 400**

**Washington, DC 20009 USA**

**Téléphone : 202-543-5566**

**SafetyNet@nnev.org**

**<http://www.nnev.org>**

# Situation quant aux menaces liées à Internet Symantec<sup>MC</sup>

Dean Turner

Directeur

Réseau d'information mondial

Interventions de Symantec en matière de  
sécurité

28 septembre 2007



# Discussion d'aujourd'hui

- Réseau d'information mondial de Symantec<sup>MC</sup>
- Tableau des menaces actuelles – Survol
- Recherche mondiale
- Objectifs
- Méthodes
- Fraude
- Priorités et étapes cruciales

# Réseau d'information mondial de Symantec<sup>MC</sup>

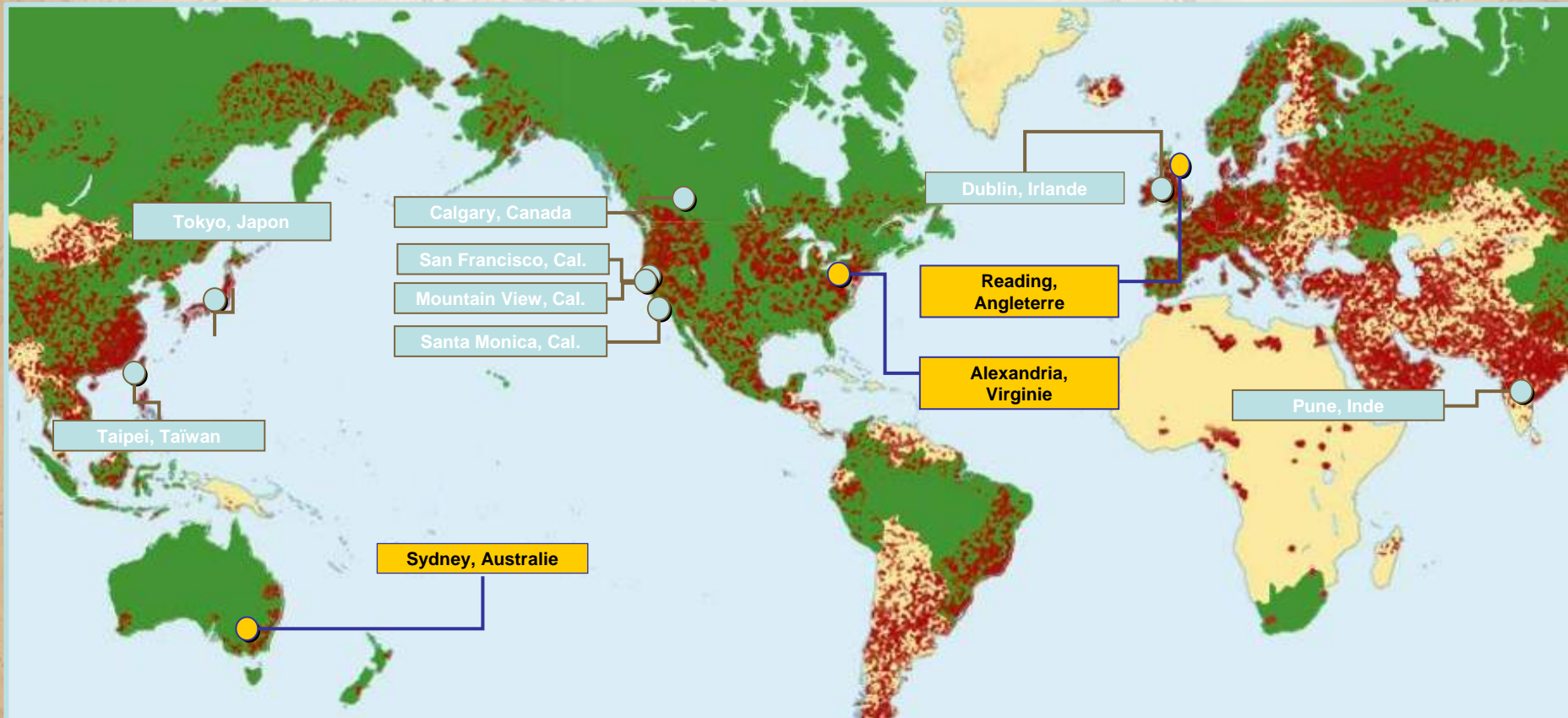
Trois centres  
d'exploitation de service

80 pays sous la  
surveillance de  
Symantec

40 000+ capteurs  
enregistrés dans plus de  
180 pays

Huit centres d'intervention  
de Symantec en matière de  
sécurité

> 6 000 dispositifs de sécurité + 120 millions de systèmes dans le monde + 30 % du trafic mondial des courriels + réseau évolué de pièges à pirates



# C'est une économie de marché...

**NETWORKWORLD** Search / Docfinder Advanced search

**Security** Whitepapers Guides and Reports Webcasts Videos Buyer's Guide

NetworkWorld.com > Security >

## MPack crimeware hits 500,000 victims

By John E. Dunn, TechWorld, 08/01/07

[Start a discussion](#) [Print article](#)

Poor detection of the MPack data-theft toolkit by antivirus software has allowed it to run riot on the Internet, a new analysis from Finjan has claimed.

The company says that the malware system has been used to successfully infect 500,000 consumer and corporate users since it appeared some months ago, achieving unusually high infection rates of 16% from an attack profile of 3.1 million web-borne attempts.

[New! Watch this Network World Webcast - Security Information Management Solutions: Beyond Threat Management](#)

To make matters worse, as of July 29, many of the best-known security programs still couldn't detect software downloaded by it, despite its workings having been known about since as far back as October 2006. Names on the list tested by Finjan that failed to find malware called by the program included Sophos, AVG, Microsoft, Kaspersky, and McAfee. Of the top security brands, only Symantec noticed MPack infection, identifying

**DATA BREACHES**  
**TJX BREACH** Largest breach ever  
 Total credit card numbers stolen: 45.7 million.  
 Banks sue TJX  
 FTC wants answers  
 Case study in what to do wrong  
 TJX apology: We give it a 5

**WHO'S RESPONSIBLE?**  
 Sloppy companies, not hackers  
 Bill puts onus on retailers  
 Boards need to wake up

**MORE DATA BREACH NEWS**  
 Cost of data breaches varies  
 Reporting data breaches won't kill your company  
 So sorry we lost your data

**IT TOOLS & HOW TO'S, JUST POSTED**  
 The Security Treadmill  
 Video: iPods in the workplace - a true security threat?  
 Why Antivirus Solutions Do Not Protect From SpyWare  
 State of Internet Security Report on Protecting Enterprise Systems  
 Planning Considerations for Data Center Facilities Systems

**NETWORK WORLD NEWSLETTER**  
 Sign up for some of our Network Security newsletters.

Security in Practice  
 Virus and Bug Patch Alert

- La criminalité professionnelle nécessite des outils professionnels

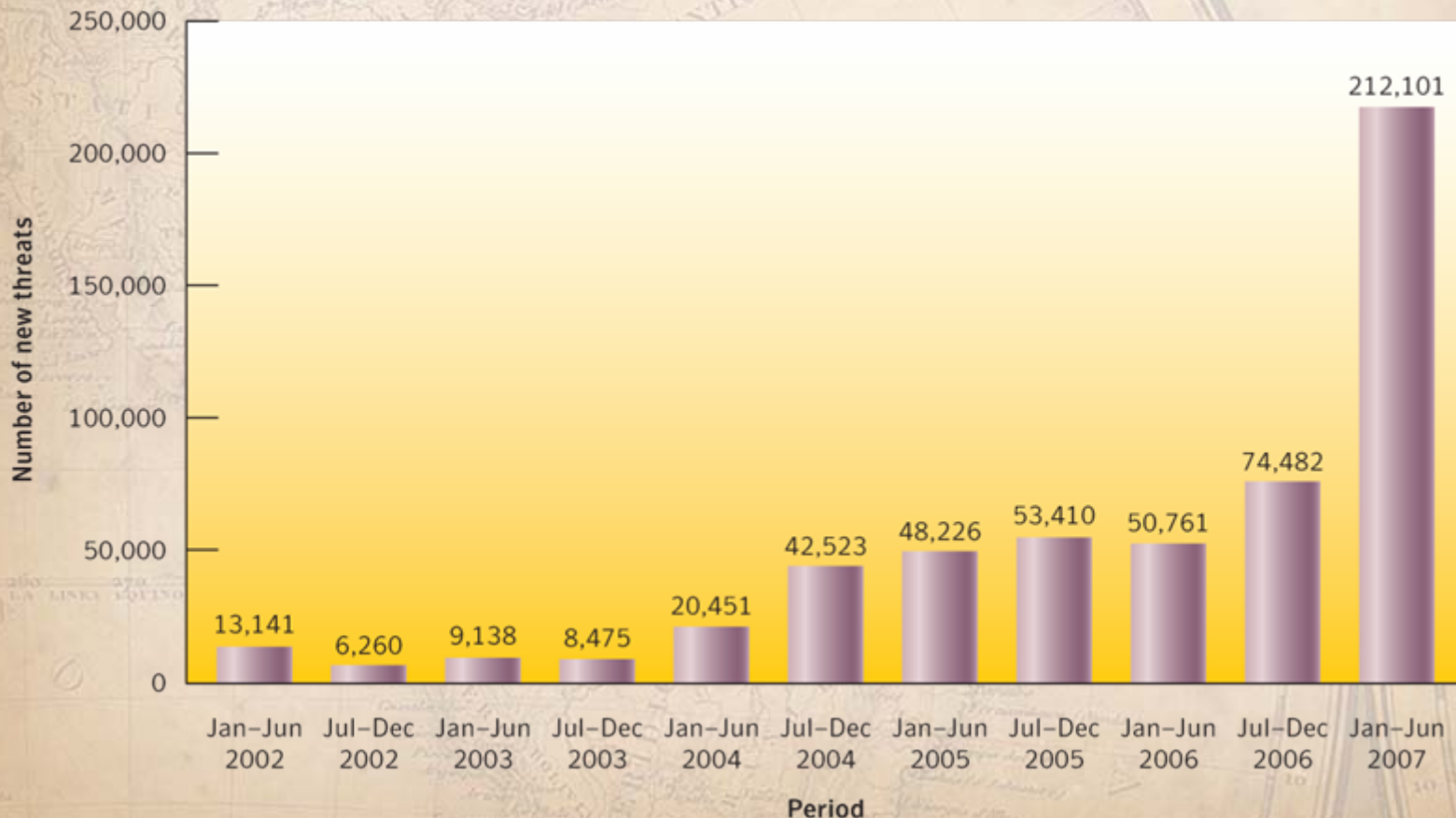
- De plus en plus commercialisé

- Reprise sur rupture de courant, spécifications de développement, AQ, matrice de traçabilité des exigences utilisateurs

- GTM - Prix, distribution, soutien

# ... et les affaires sont en plein essor!

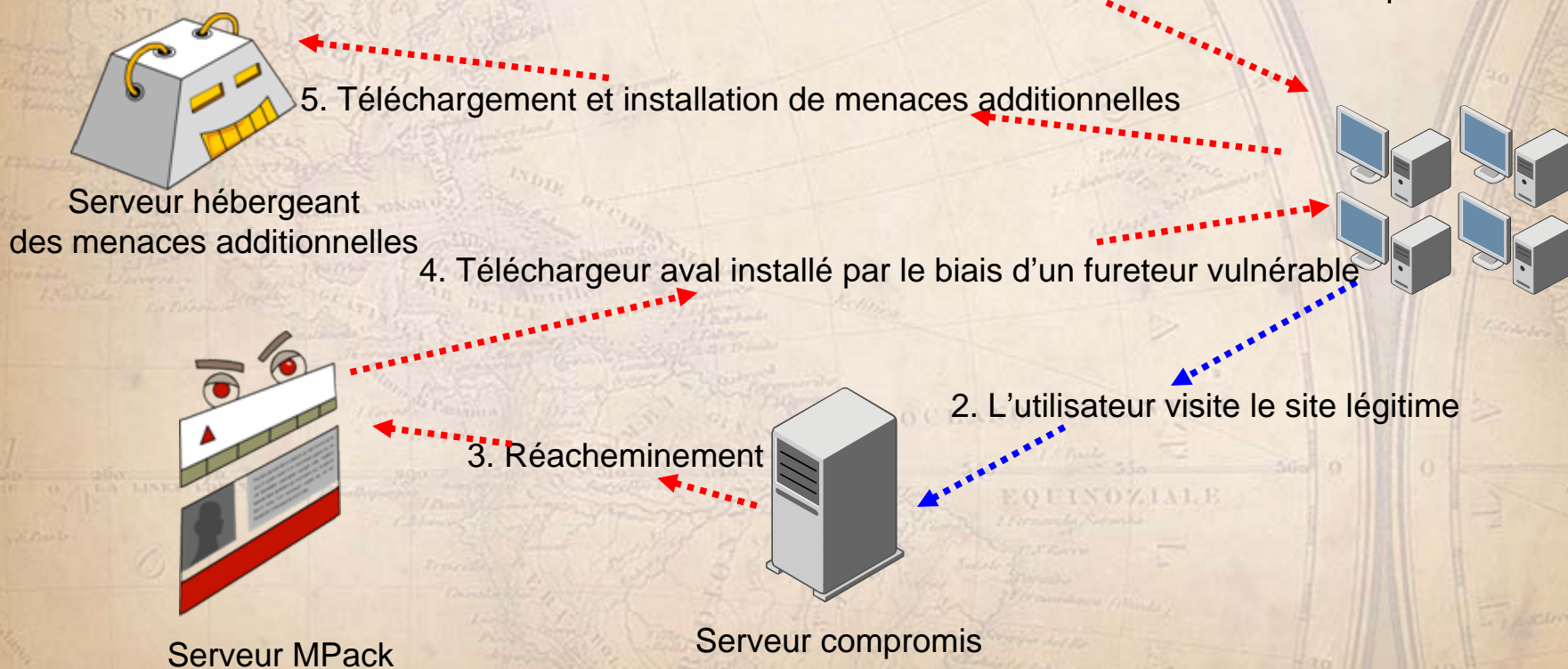
- Dans la première moitié de 2007, on a déclaré à Symantec 212 101 nouvelles menaces de logique malveillante, ce qui représente une augmentation de 185 % par rapport à la deuxième moitié de 2006.



# Attaques par étapes

- Des attaques en plusieurs étapes fonctionnent à partir d'une compromission initiale et de faible envergure visant à établir une tête de pont, à partir de laquelle seront lancées des attaques ultérieures.
- L'assaillant pourra modifier ensuite les étapes de son attaque selon les besoins.

1. Pourriel contenant un lien avec un serveur compromis



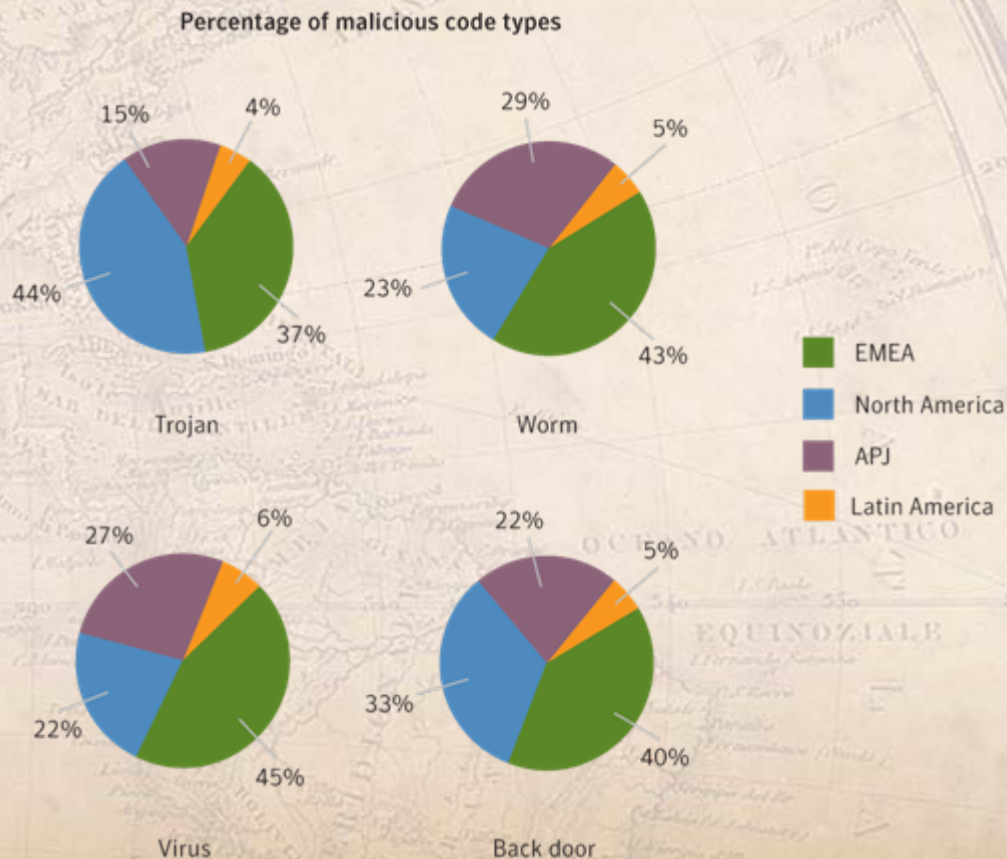
# Changement de tactiques et de cibles



- Pourquoi aller vers vous quand c'est vous qui allez vers eux?
- Terreau fertile
- Difficile d'y exercer un contrôle

# Accent de plus en plus grand sur les régions

- Les menaces sont adaptées à des régions et pays particuliers
- Certains types de menaces de logique malveillante sont plus courants dans certaines régions que d'autres



# Rapport sur les menaces en matière de sécurité Volume XII Principaux faits et chiffres



# Niveaux mondiaux d'activité malveillante

- ▶ Entre le 1<sup>er</sup> janvier et le 30 juin, les États-Unis venaient au premier rang des pays touchés par des activités malicieuses (données brutes), soit 30 % de la proportion globale. La Chine occupait le second rang avec une proportion de 10 %.
- ▶ En fonction des populations d'internautes, Israël occupait le premier rang, avec un taux de 11 %, suivi du Canada avec 6 %. Sept des dix premiers pays dans cette catégorie se trouvaient en Europe-Moyen-Orient-Asie.

| Overall Rank | Previous Rank | Country        | Overall Proportion | Previous Overall Proportion | Malicious Code Rank | Spam Zombies Rank | Command-and-Control Server Rank | Phishing Web sites | Bot Rank | Attack Rank |
|--------------|---------------|----------------|--------------------|-----------------------------|---------------------|-------------------|---------------------------------|--------------------|----------|-------------|
| 1            | 1             | United States  | 30%                | 31%                         | 1                   | 1                 | 1                               | 1                  | 2        | 1           |
| 2            | 2             | China          | 10%                | 10%                         | 2                   | 3                 | 5                               | 18                 | 1        | 2           |
| 3            | 3             | Germany        | 7%                 | 7%                          | 7                   | 2                 | 2                               | 2                  | 3        | 3           |
| 4            | 5             | United Kingdom | 4%                 | 4%                          | 3                   | 15                | 6                               | 3                  | 7        | 5           |
| 5            | 4             | France         | 4%                 | 4%                          | 9                   | 7                 | 12                              | 6                  | 5        | 4           |
| 6            | 7             | Canada         | 4%                 | 3%                          | 6                   | 31                | 3                               | 7                  | 8        | 7           |
| 7            | 8             | Spain          | 3%                 | 3%                          | 10                  | 10                | 22                              | 13                 | 4        | 6           |
| 8            | 10            | Italy          | 3%                 | 3%                          | 5                   | 6                 | 8                               | 12                 | 6        | 8           |
| 9            | 6             | South Korea    | 3%                 | 4%                          | 26                  | 8                 | 4                               | 10                 | 13       | 12          |
| 10           | 11            | Japan          | 2%                 | 2%                          | 4                   | 20                | 13                              | 8                  | 16       | 10          |

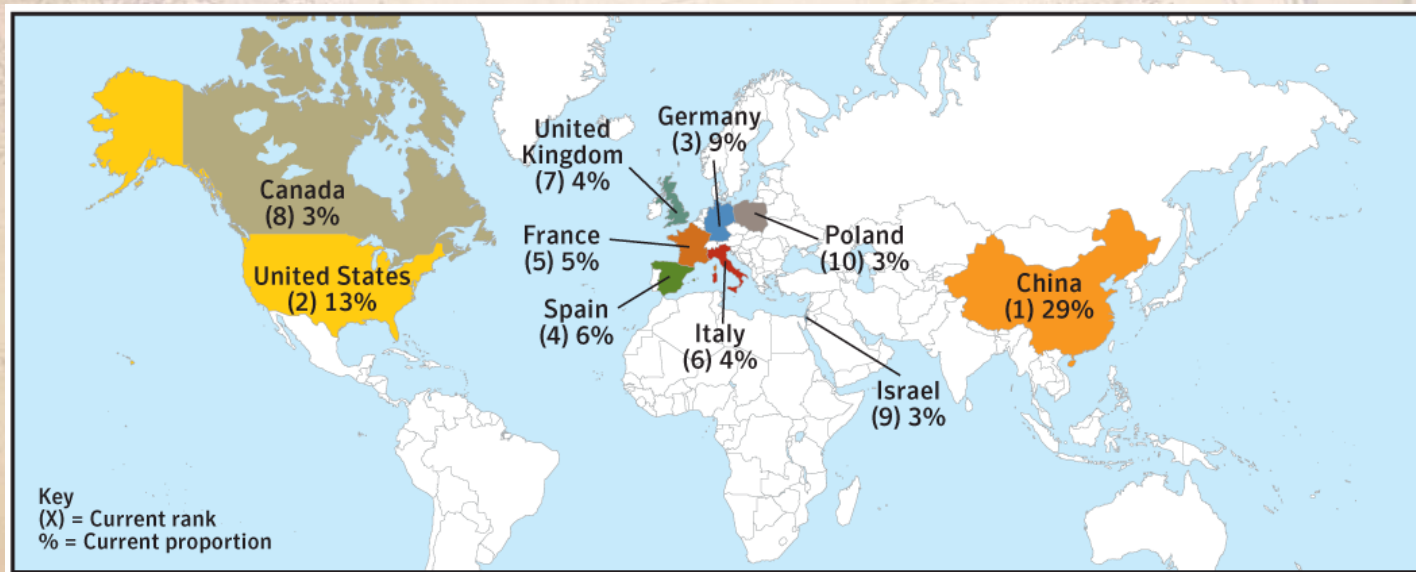
# Emplacements mondiaux des activités frauduleuses

- ▶ 59 % des sites d’hameçonnage connus se trouvaient aux États-Unis, suivis de l’Allemagne avec 6 % et du Royaume-Uni avec 3 %
- ▶ Les É.-U. viennent au premier rang en raison du nombre élevé de fournisseurs de services d’hébergement – particulièrement ceux qui sont gratuits. La hausse de sites d’hameçonnage recensés durant cette période s’explique peut-être en partie par le nombre élevé de chevaux de Troie en Amérique du Nord.

| Rank | Previous Rank | Country        | Current Period | Previous Period |
|------|---------------|----------------|----------------|-----------------|
| 1    | 1             | United States  | 59%            | 46%             |
| 2    | 2             | Germany        | 6%             | 11%             |
| 3    | 3             | United Kingdom | 3%             | 3%              |
| 4    | 10            | Netherlands    | 2%             | 2%              |
| 5    | 11            | Russia         | 2%             | 2%              |
| 6    | 4             | France         | 2%             | 3%              |
| 7    | 7             | Canada         | 2%             | 2%              |
| 8    | 5             | Japan          | 2%             | 3%              |
| 9    | 8             | China          | 1%             | 2%              |
| 10   | 6             | Taiwan         | 1%             | 3%              |

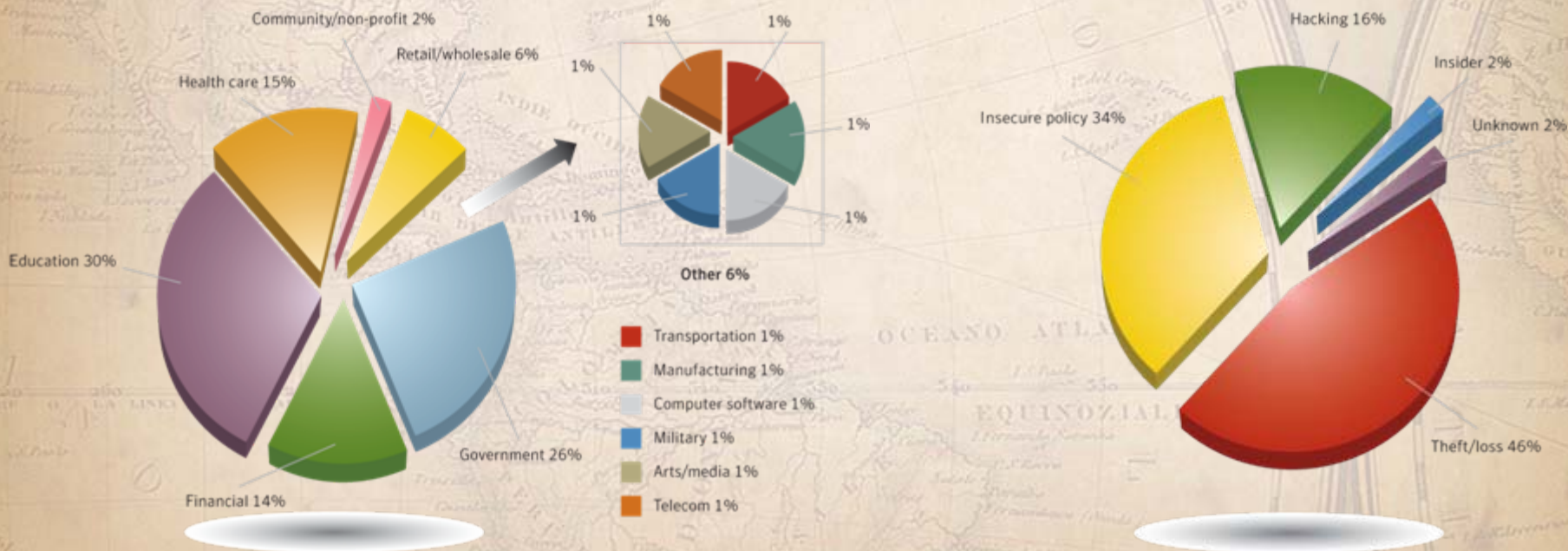
# Infrastructures d'attaques mondiales

- ▶ À l'échelle mondiale, Symantec a observé durant la période de référence actuelle un nombre quotidien moyen de 52 771 ordinateurs de réseau actifs avec inforobot, une baisse de 17 % par rapport à la dernière moitié de 2006. Le total mondial d'ordinateurs distincts avec inforobot infecté qu'a recensés Symantec a chuté pour atteindre 5 029 309, soit une baisse de 17 %. En moyenne annuelle, cela représente néanmoins une hausse de 7 %.
- ▶ Le nombre de serveurs de commande et de contrôle a diminué durant cette période pour atteindre 4 622, une baisse de 3 %. Les É.-U. demeurent le pays où la proportion de serveurs de commande et de contrôle est la plus élevée au monde, à savoir 43 %, ce qui représente une hausse de 3 % par rapport au total précédent.



## Brèches dans la protection des données à l'échelle mondiale

- ▶ C'est dans le secteur de l'éducation que se sont produites la majorité des brèches avec 30 %, suivi du gouvernement avec 26 %, et le secteur des soins de santé avec 15 % - près de la moitié des brèches (46 %) étaient attribuables à des vols ou des pertes, tandis que le piratage représentait 16 %.
- ▶ Le secteur du détail était responsable de 85 % des identités exposées. Le gouvernement vient au deuxième rang. Dans 73 % des cas, le piratage expliquait l'exposition des identités.



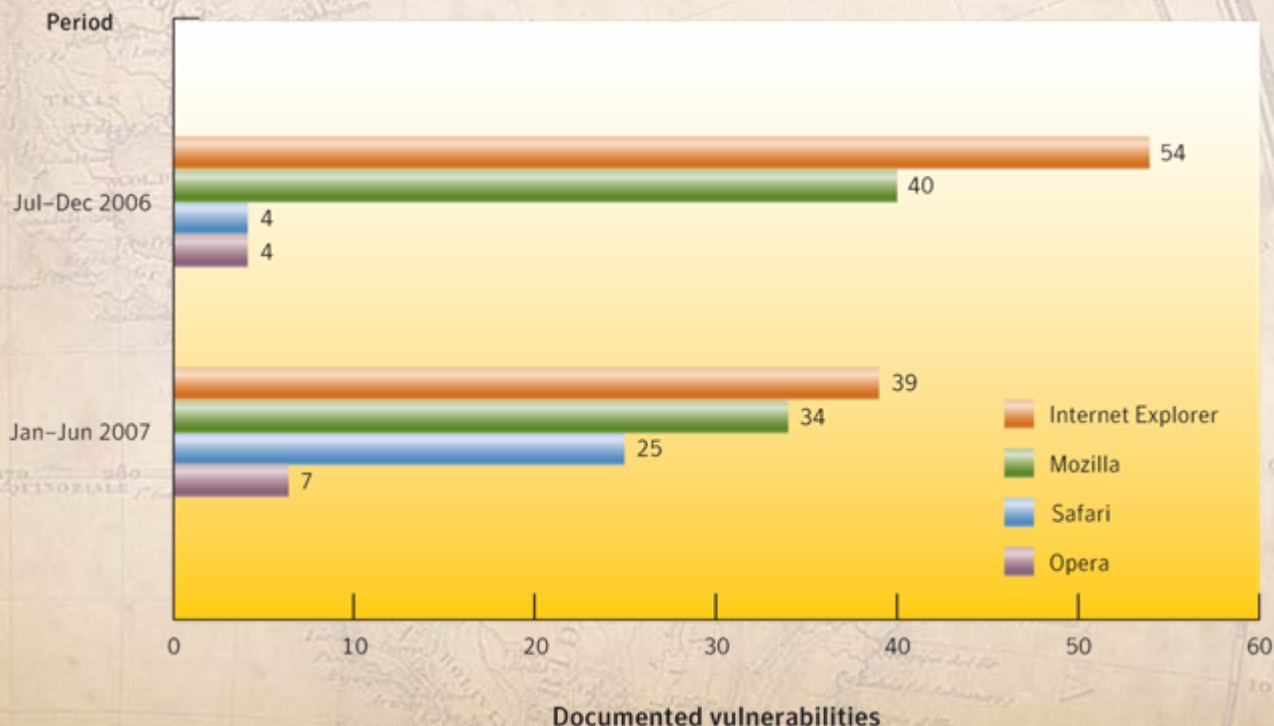
# Économies clandestines mondiales

- ▶ Les cartes de crédit, les identités, les services de paiement en ligne, les comptes bancaires, les inforobots, les outils servant à frauder, etc., sont classés par ordre de marchandises le plus souvent offertes sur les serveurs fonctionnant dans l'économie clandestine.
- ▶ Les cartes de crédit représentaient l'article le plus souvent annoncé (22 %), suivies des comptes bancaires (21 %).
- ▶ Les mots de passe de courriel se vendent presque au même prix qu'un compte bancaire.

| Rank | Item                    | Percentage | Range of Prices |
|------|-------------------------|------------|-----------------|
| 1    | Credit Cards            | 22%        | \$0.50-\$5      |
| 2    | Bank Accounts           | 21%        | \$30-\$400      |
| 3    | Email Passwords         | 8%         | \$1-\$350       |
| 4    | Mailers                 | 8%         | \$8-\$10        |
| 5    | Email Addresses         | 6%         | \$2/MB-\$4/MB   |
| 6    | Proxies                 | 6%         | \$0.50-\$3      |
| 7    | Full Identity           | 6%         | \$10-\$150      |
| 8    | Scams                   | 6%         | \$10/week       |
| 9    | Social Security Numbers | 3%         | \$5-\$7         |
| 10   | Compromised Unix Shells | 2%         | \$2-\$10        |

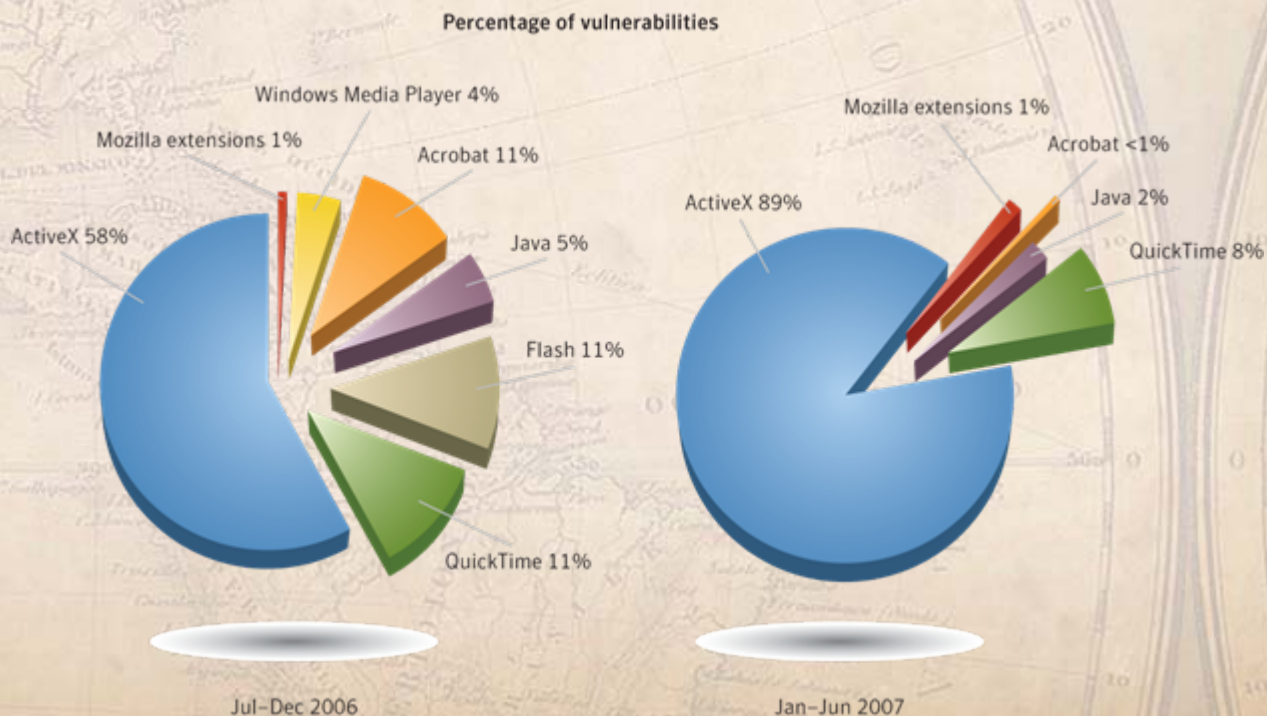
# Technologies cibles – Navigateurs

- ▶ Microsoft présentait le nombre le plus élevé de vulnérabilités, soit 39, suivi de Mozilla avec 34. Ces deux fournisseurs avaient également la fenêtre d'exposition la plus élevée, à savoir cinq jours chacun.
- ▶ On a recensé 25 vulnérabilités dans Safari durant cette période, soit une hausse marquée par rapport aux quatre vulnérabilités de la deuxième moitié de 2006. Toutefois, Safari présente la plus courte fenêtre d'exposition, qui est de seulement trois jours.



# Technologies cibles – Modules externes

- ▶ Les vulnérabilités dans les modules externes de navigation sont fréquemment exploitées pour y installer des logiciels malveillants.
- ▶ Dans la première moitié de 2007, on a recensé 237 vulnérabilités ayant touché les modules externes de navigation comparativement à 108 durant toute l'année 2006.
- ▶ En tout, 89 % des vulnérabilités des modules externes de navigation ont touché les composants ActiveX du navigateur Explorer, ce qui constitue une hausse de 58 % par rapport à la période précédente.



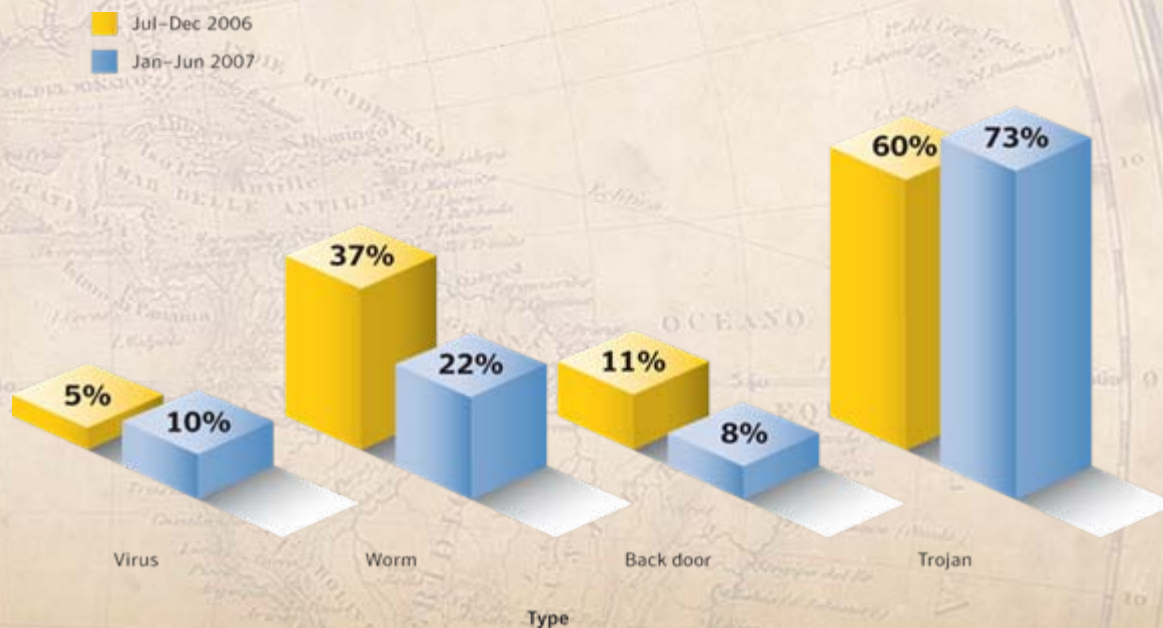
# Technologies cibles – Statistiques clés

- ▶ Symantec a recensé 2 461 vulnérabilités durant la période de référence actuelle, soit 3 % de moins que lors de la période de référence précédente.
- ▶ Classement par gravité : élevée 9 %, moyenne 51 % et faible 40 %.
- ▶ Les applications Web constituaient 61 % de toutes les vulnérabilités documentées.
- ▶ En tout, 72 % des vulnérabilités documentées durant la période de référence étaient facilement exploitables comparativement à 79 % lors de la période précédente.
- ▶ La fenêtre d'exposition pour les fournisseurs de produits d'entreprise était de 55 jours, ce qui représente une hausse par rapport à la moyenne de 47 jours enregistrée dans la deuxième moitié de 2006.



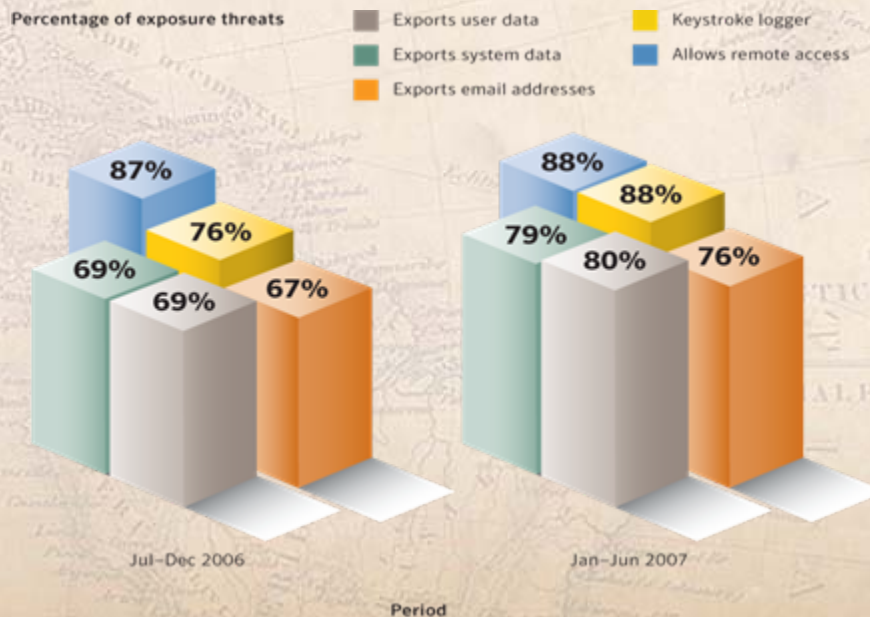
# Méthodes – Logique malveillante

- ▶ Le nombre de chevaux de Troie continue d'augmenter et pourrait constituer une plus grande menace étant donné qu'ils ont tendance à exploiter les navigateurs et que le nombre de journées de vulnérabilité est nul. La proportion de chevaux de Troie qui représentent une source d'infection possible ou une tentative d'infection s'est élevée pour passer de 60 % à 73 % durant cette période.
- ▶ Le nombre de vers a continué de chuter durant cette période, alors qu'ils n'ont représenté que 22 % des infections possibles comparativement à 37 % pour la deuxième moitié de 2006.
- ▶ Le pourcentage de virus s'est accru, passant de 5 % à 10 % durant cette période.



# Méthodes – Vol et fuite de données

- ▶ Durant la période de référence actuelle, les menaces posées à l'information confidentielle composaient 65 % du volume des 50 principales logiques malveillantes causant des infections possibles, comparativement à 53 % lors de la période de référence précédente.
- ▶ Bien que le volume de menaces qui permettent un accès à distance soit demeuré stable par rapport à la même période de référence l'année dernière, les menaces qui enregistrent des touches de frappe et exportent des données de l'utilisateur et du système ont toutes augmenté – les enregistreurs chronologiques de touches de frappe représentent 88 % des menaces à l'information confidentielle.



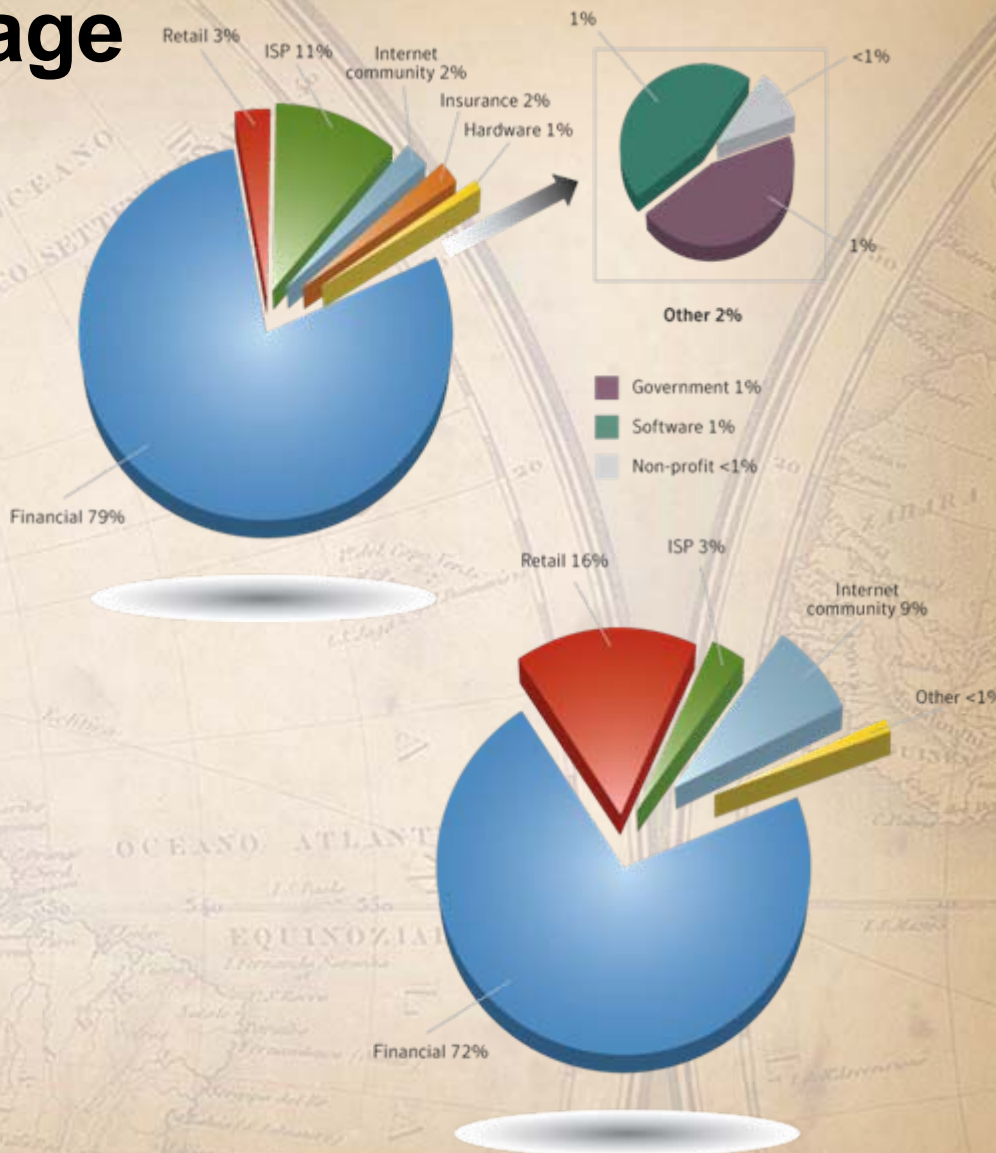
# Méthodes - Propagation

- ▶ La propagation par pièce jointe à un courriel constitue le mécanisme numéro un de propagation, avec une proportion de 46 %.
- ▶ Au Canada, la propagation par courriel était inférieure à la moyenne mondiale alors que les menaces posées aux systèmes de réseau poste à poste ont dépassé le pourcentage global.

| Rank | Propagation Mechanism              | Percentage of Threats |
|------|------------------------------------|-----------------------|
| 1    | File Transfer/Email Attachment     | 46%                   |
| 2    | File Transfer/CIFS                 | 24%                   |
| 3    | File Sharing/Peer-to-Peer          | 22%                   |
| 4    | File Sharing/Executables           | 22%                   |
| 5    | File Sharing/Peer-to-Peer/Kazaa    | 18%                   |
| 6    | Remotely Exploitable Vulnerability | 18%                   |
| 7    | File Sharing/Peer-to-Peer/Morpheus | 15%                   |
| 8    | File Sharing/Peer-to-Peer/eDonkey  | 15%                   |
| 9    | File Sharing/Peer-to-Peer/Winny    | 5%                    |
| 10   | Backdoor/Kuang2                    | 3%                    |

# Fraude - Hameçonnage

- ▶ Le réseau Symantec Probe a détecté un total de 196 860 messages d'hameçonnage uniques, soit une augmentation de 18 % par rapport à la période précédente. Cela se traduit par une moyenne de 1 088 messages d'hameçonnage uniques par jour.
- ▶ Symantec a bloqué plus de 2,3 milliards de messages – une hausse de 53 % par rapport à la dernière moitié de 2006. Une moyenne de 12,5 millions de message d'hameçonnage par jour.
- ▶ Les services financiers représentaient 79 % des marques uniques qui ont été hameçonnées, et composaient 72 % du total des sites Web d'hameçonnage. Le secteur des FSI représentait 11 % des marques uniques hameçonnées et 3 % du nombre total de sites Web d'hameçonnage.
- ▶ Durant les six premiers mois de 2007, Symantec a classifié 78 de 359 marques hameçonnées comme étant des marques de base, c'est-à-dire celles qui sont arnaquées au moins une fois par mois par une attaque d'hameçonnage.



# Priorités et étapes cruciales

| Priorité | Recommandation  |
|----------|---|
| 1        | <b>Recensement et classification des données</b><br><i>Trouvez où se situe la date importante. Commencez là.</i>  |
| 2        | <b>Chiffrement</b><br><i>Prenez ce qui fonctionne le mieux pour votre entreprise, en commençant par les données critiques.</i>  |
| 3        | <b>Sensibilisation et formation</b><br><i>Pour les voyageurs/travailleurs à distance, les manipulateurs de données critiques et tous les autres.</i>                                |
| 4        | <b>Traitement, traitement, traitement</b><br><i>Authentification du service de dépannage, processus d'arrêt, cycle de vie des entrepreneurs, etc.</i>                               |
| 5        | <b>Segmentation et répartition des tâches</b><br><i>Réseaux et employés – ne laissez pas le renard (ou les poules!) garder le poulailler</i>  |
| 6        | <b>Connaissance du périmètre</b><br><i>Les vérifications des réseaux sans fil et la gestion globale des vulnérabilités empêchent le piratage facile</i>                             |
| 7        | <b>Développement d'applications sécuritaires</b><br><i>La façon la moins coûteuse et la plus efficace de protéger les applications est de les développer de manière sécuritaire</i> |
| 8        | <b>Nouvelles solutions techniques</b><br><i>Appliquez les rudiments, mais prenez toujours en considération des solutions telles que des système antifuite des données et Lojack</i> |

# Atelier sur le crime sur Internet

Deborah Platt Majoras

Présidente

Commission fédérale du commerce  
(États-Unis)

# Atelier sur le crime sur Internet

## Rapport du groupe de travail “US Task Force On Identity Theft”

[www.idtheft.gov/reports/StrategicPlan.pdf](http://www.idtheft.gov/reports/StrategicPlan.pdf)

[www.idtheft.gov/reports/Volumell.pdf](http://www.idtheft.gov/reports/Volumell.pdf)

# Atelier sur le crime sur Internet

Contactez-nous

Commission fédérale du commerce

600, avenue Pennsylvania, N-O

Washington (DC) 20580

(États-Unis)

[www.ftc.gov](http://www.ftc.gov)