# PRIVACY HORIZONS: TERRA INCOGNITA

29th 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

29e 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

# 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

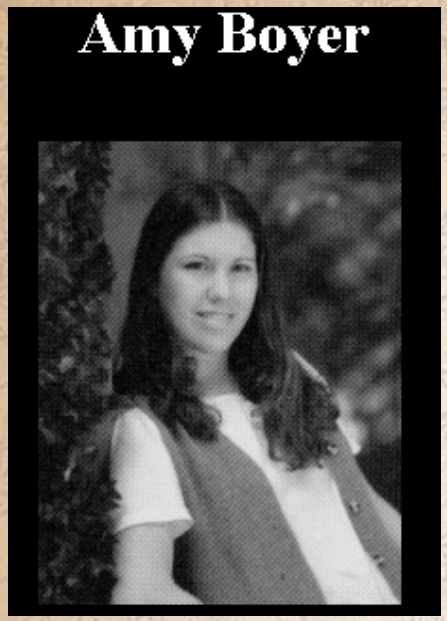
**Greetings Infidels, I am Liam Youens**

# 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 excuess because I was scared. I still feel unconfortable 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 beable 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




# 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.

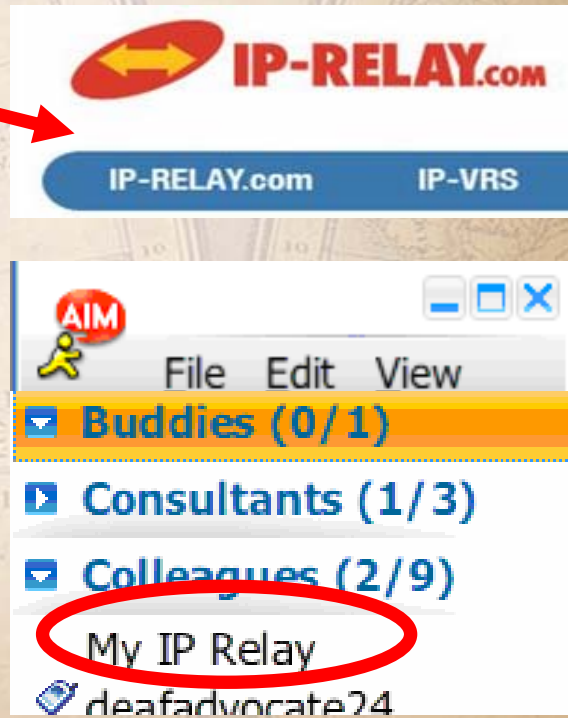
# Les harceleurs et le brouillage téléphonique en ligne


- ❑ 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?

# 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 nº de téléphone sur le site Web d'IP Relay.
- Cliquez sur « AIM ». Ajoutez un ami sous « MyIPRelay ». Envoyez le MI avec le nº 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

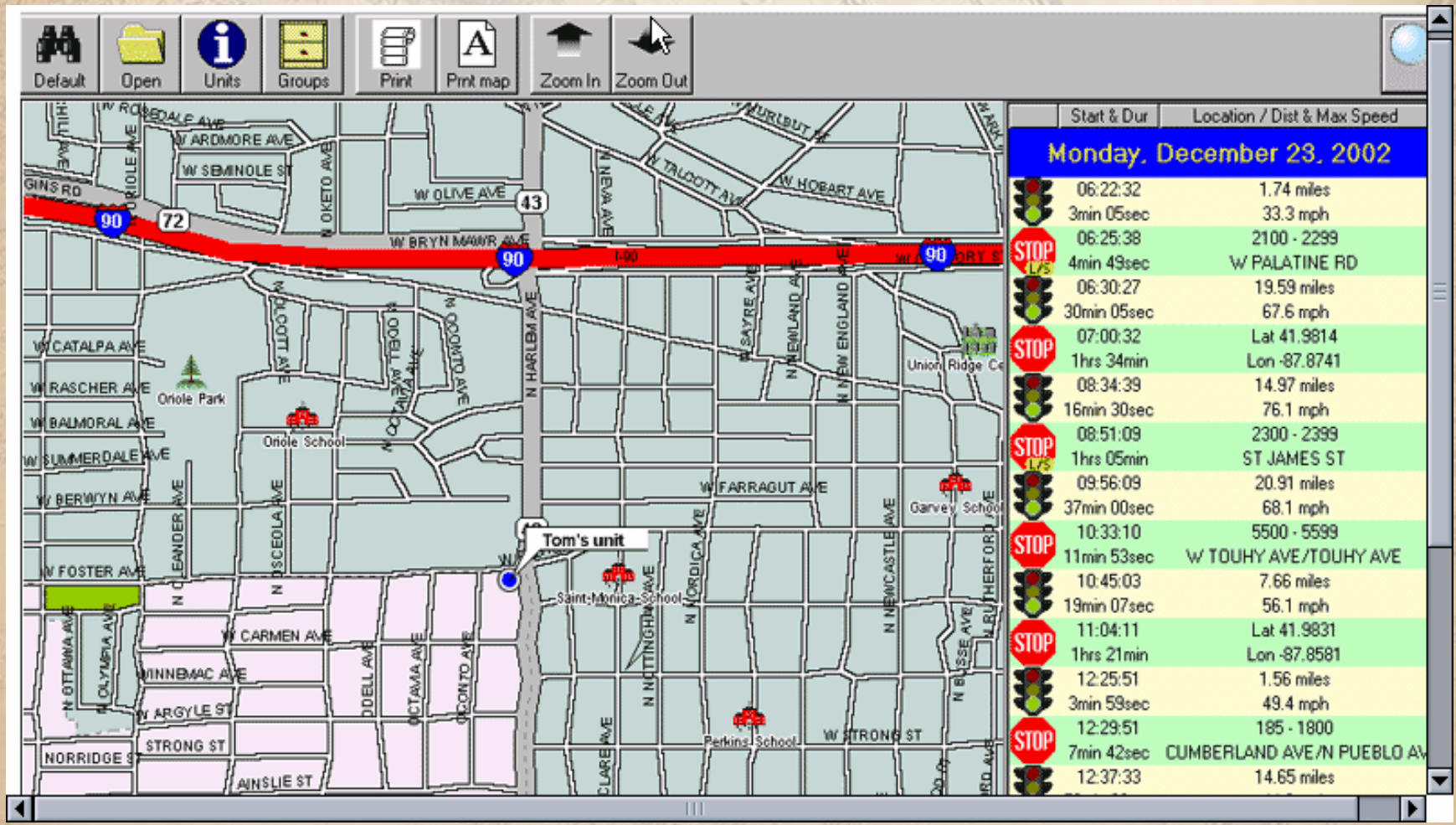
## Connexion à la MI

❑ Connexion aux MI

❑ Connexion aux sites de clavardage

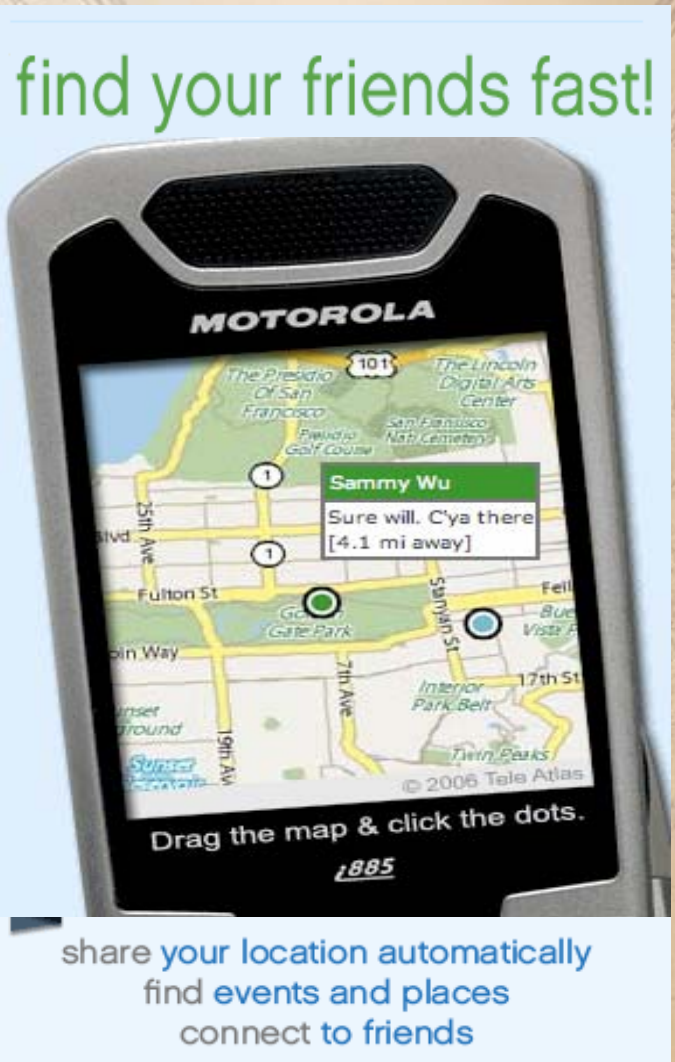
Connexion au disque dur (C:\Document)

# GPS et localisation en ligne



# 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.



# 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

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.


**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.

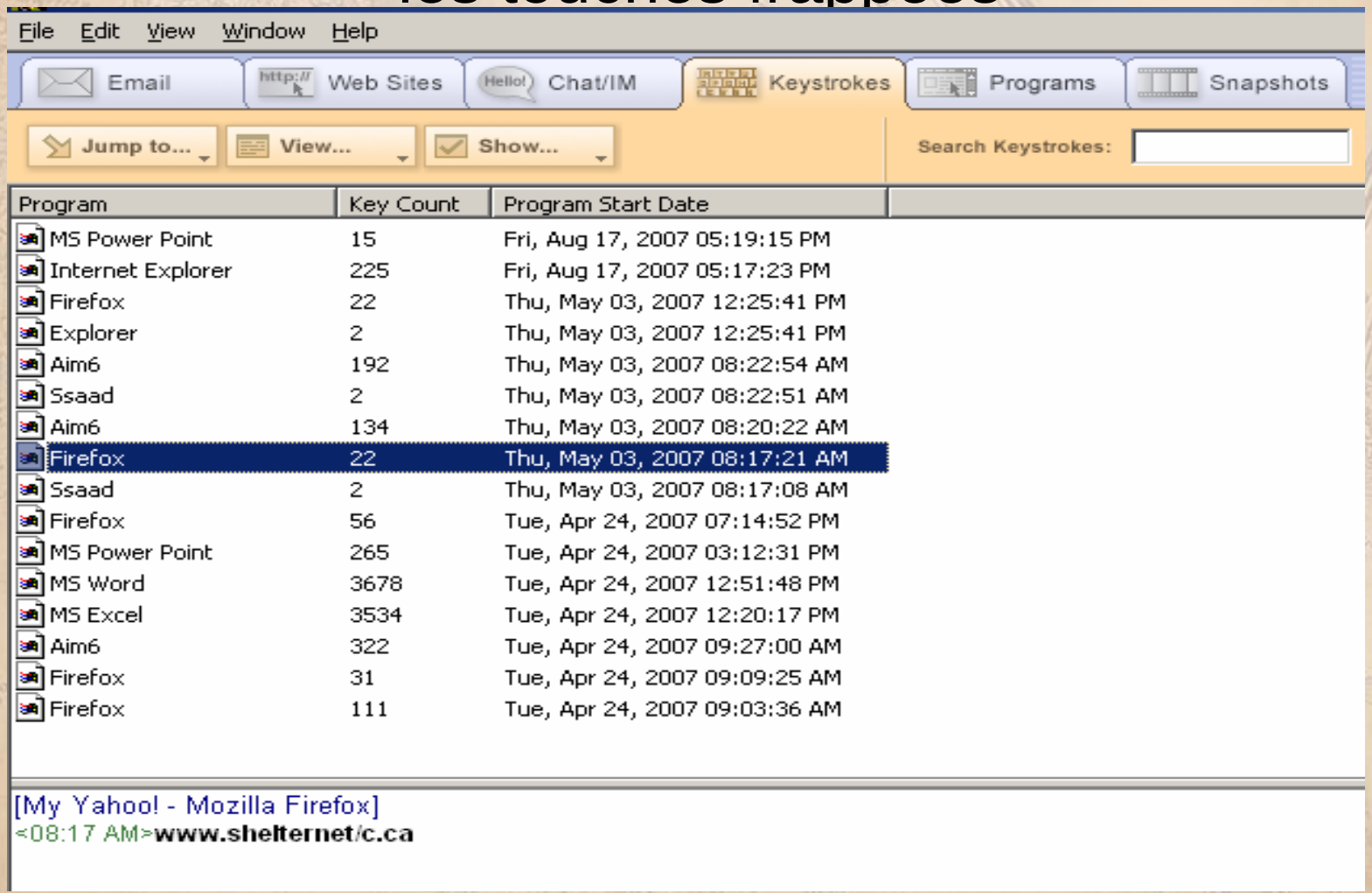
La loi de l'État du Michigan (É.-U.) condamne l'écoute électronique, l'installation de dispositifs d'écoute électronique, l'accès non autorisé et l'utilisation d'un ordinateur à des fins criminelles.

SNOOPSTICK™ From CYBERsitter®

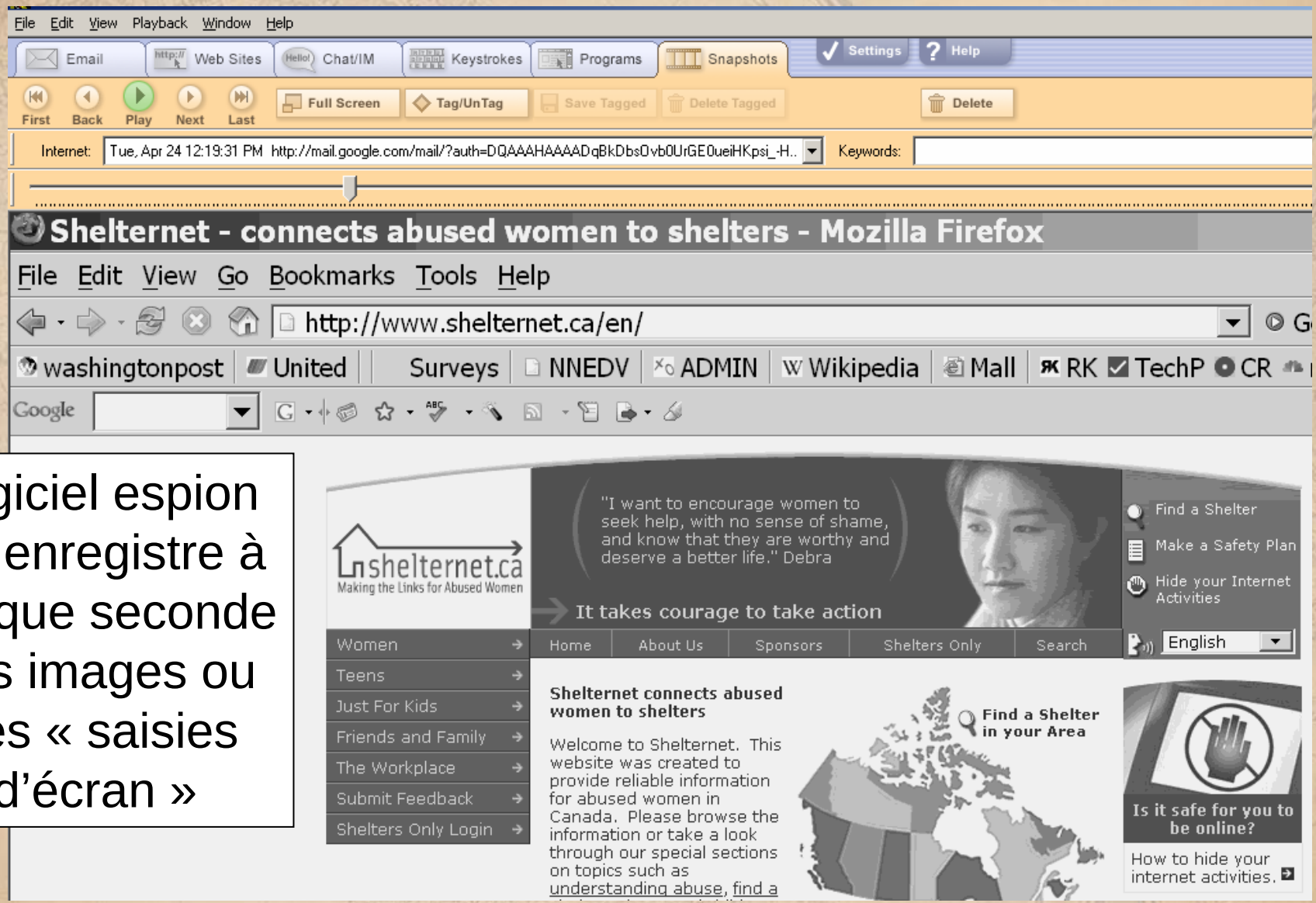
Brèches faciles dans la protection des données – La BBC demande à un enfant d'installer un enregistreur de frappe dans l'ordinateur d'une députée (Angleterre, 23 mars 2007)

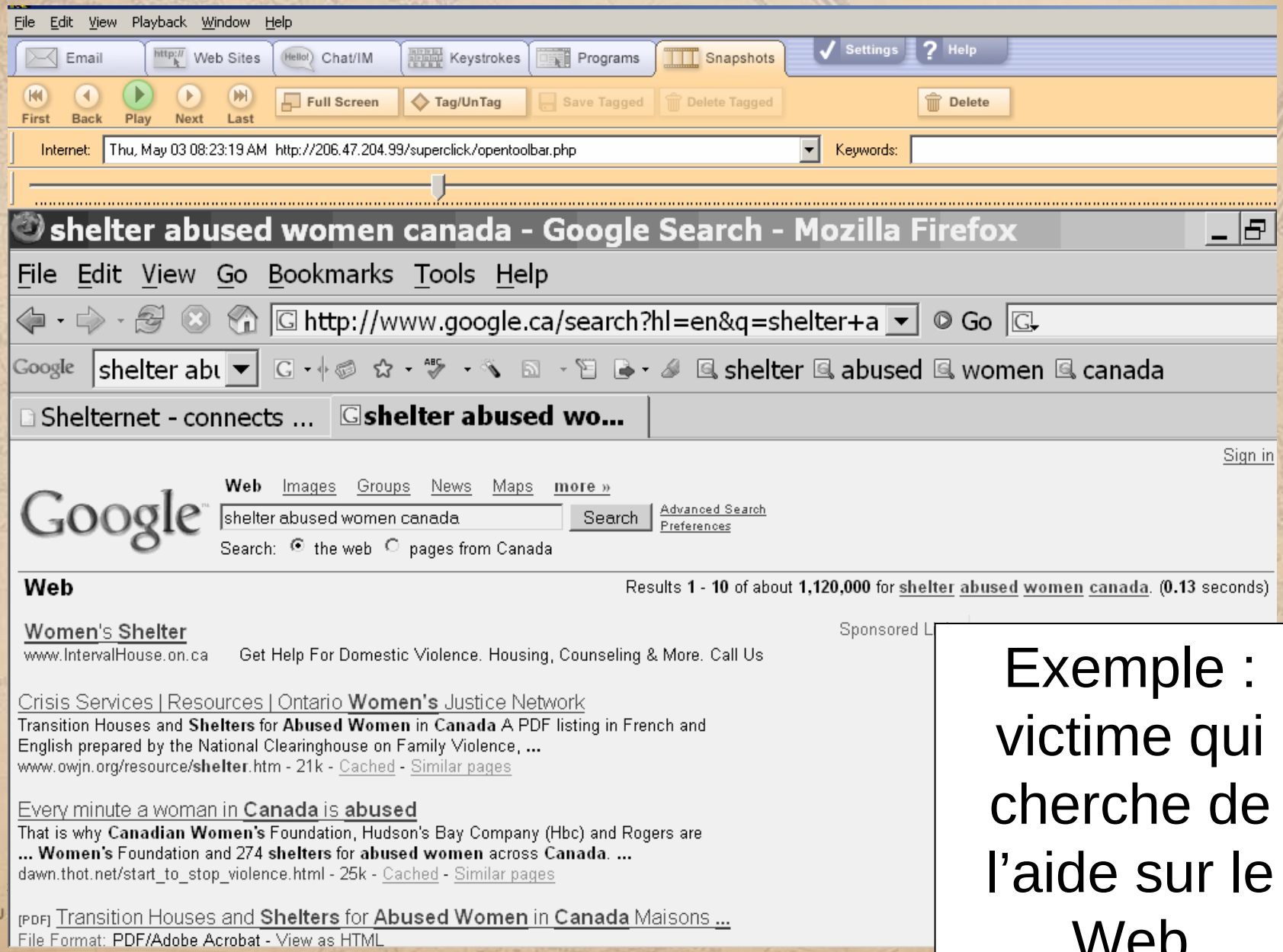
Une fillette âgée de six ans, accompagnée par un journaliste du programme Inside Out de la BBC, a installé un dispositif d'enregistrement de frappe dans l'ordinateur d'une députée. La députée, Anne Milton, a accepté de laisser son ordinateur sans surveillance pendant une minute; l'enfant a installé l'enregistreur 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

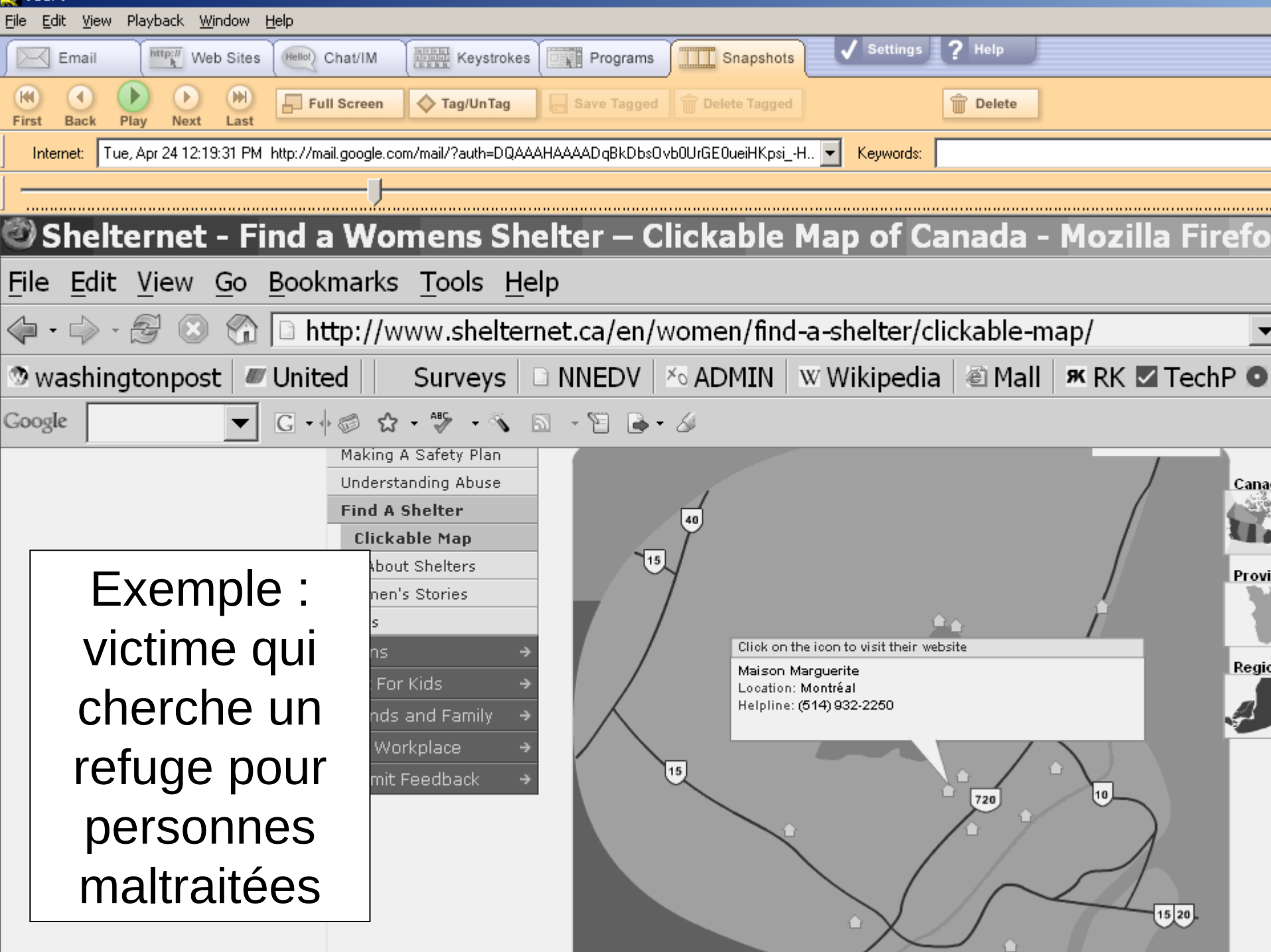


Logiciel espion qui enregistre à chaque seconde des images ou des « saisies d'écran »

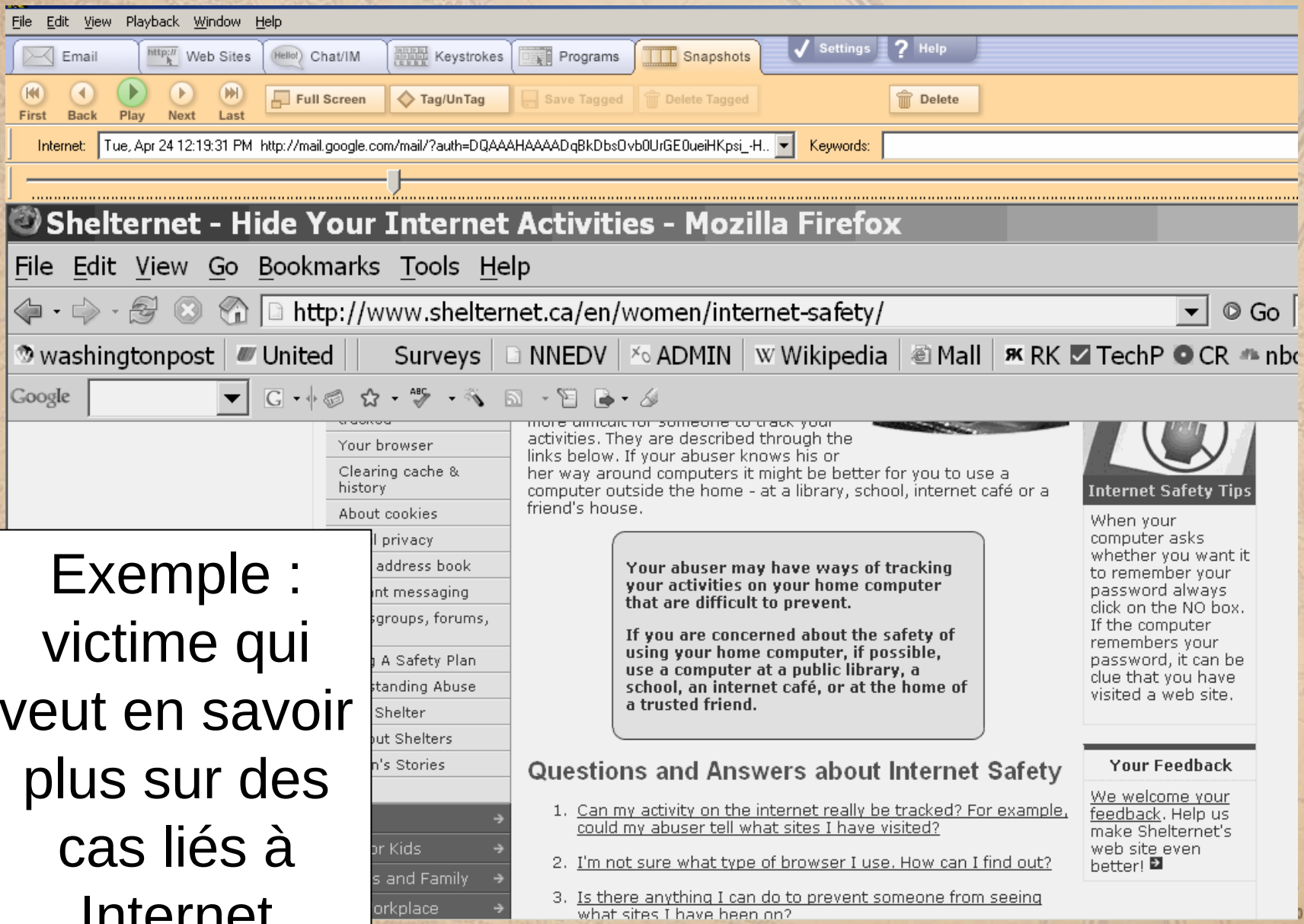




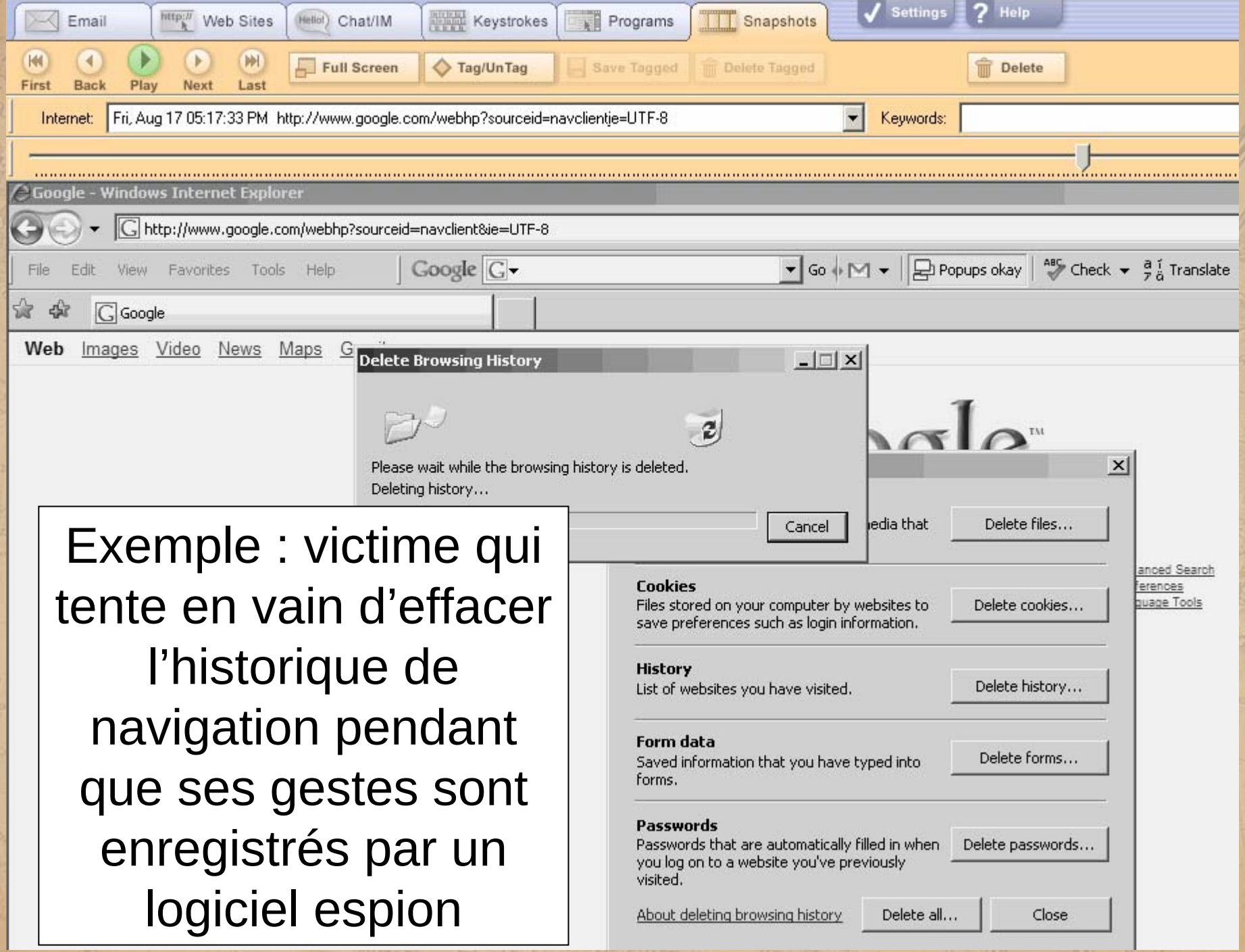

Exemple : victime qui cherche de l'aide sur le Web




Exemple : victime qui cherche un refuge pour personnes maltraitées




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@nnedv.org http://www.nnedv.org

# Situation quant aux menaces liées à Internet Symantec[MC]

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^MC
- Tableau des menaces actuelles – Survol
- Recherche mondiale
- Objectifs
- Méthodes
- Fraude
- Priorités et étapes cruciales

# Réseau d'information mondial de Symantec^MC

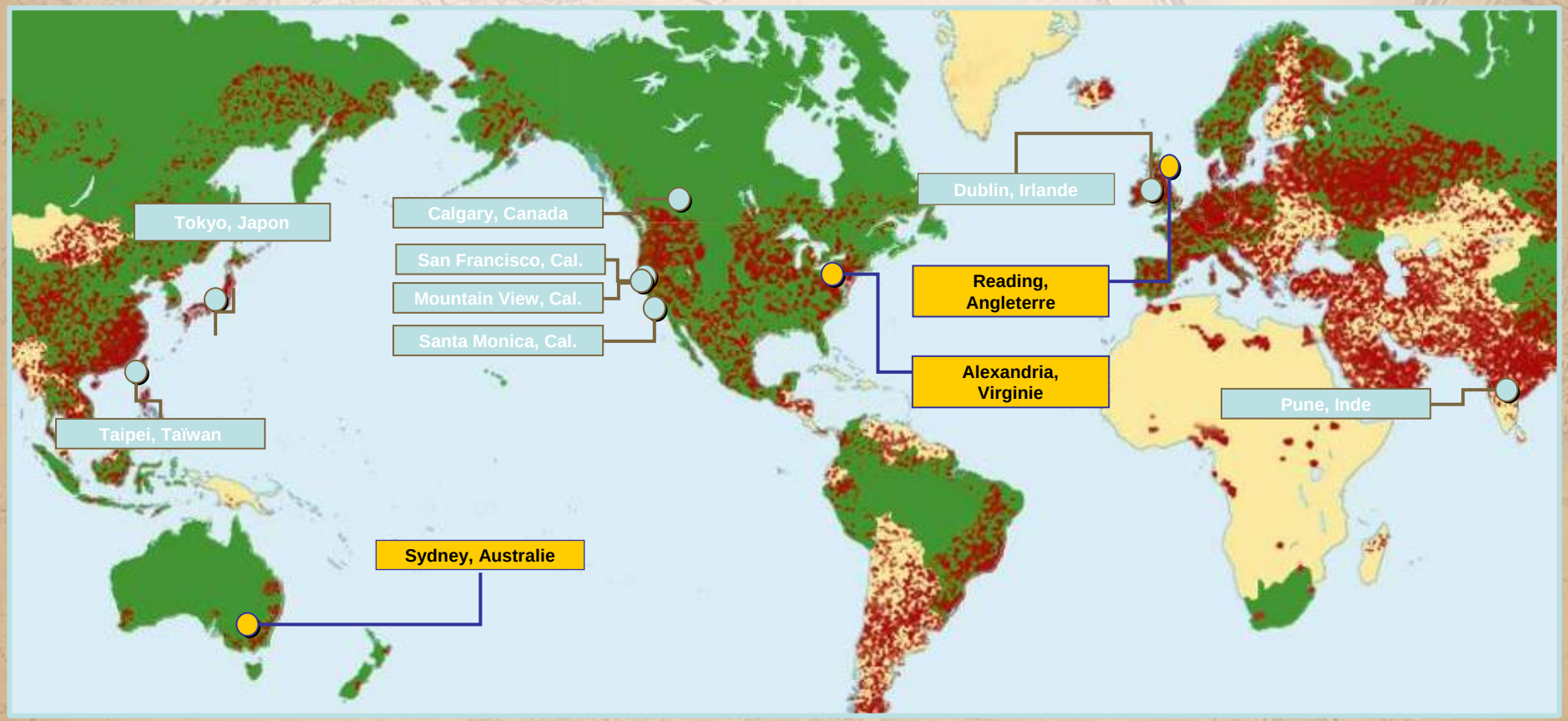
**Trois centres d'exploitation de service**

**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**

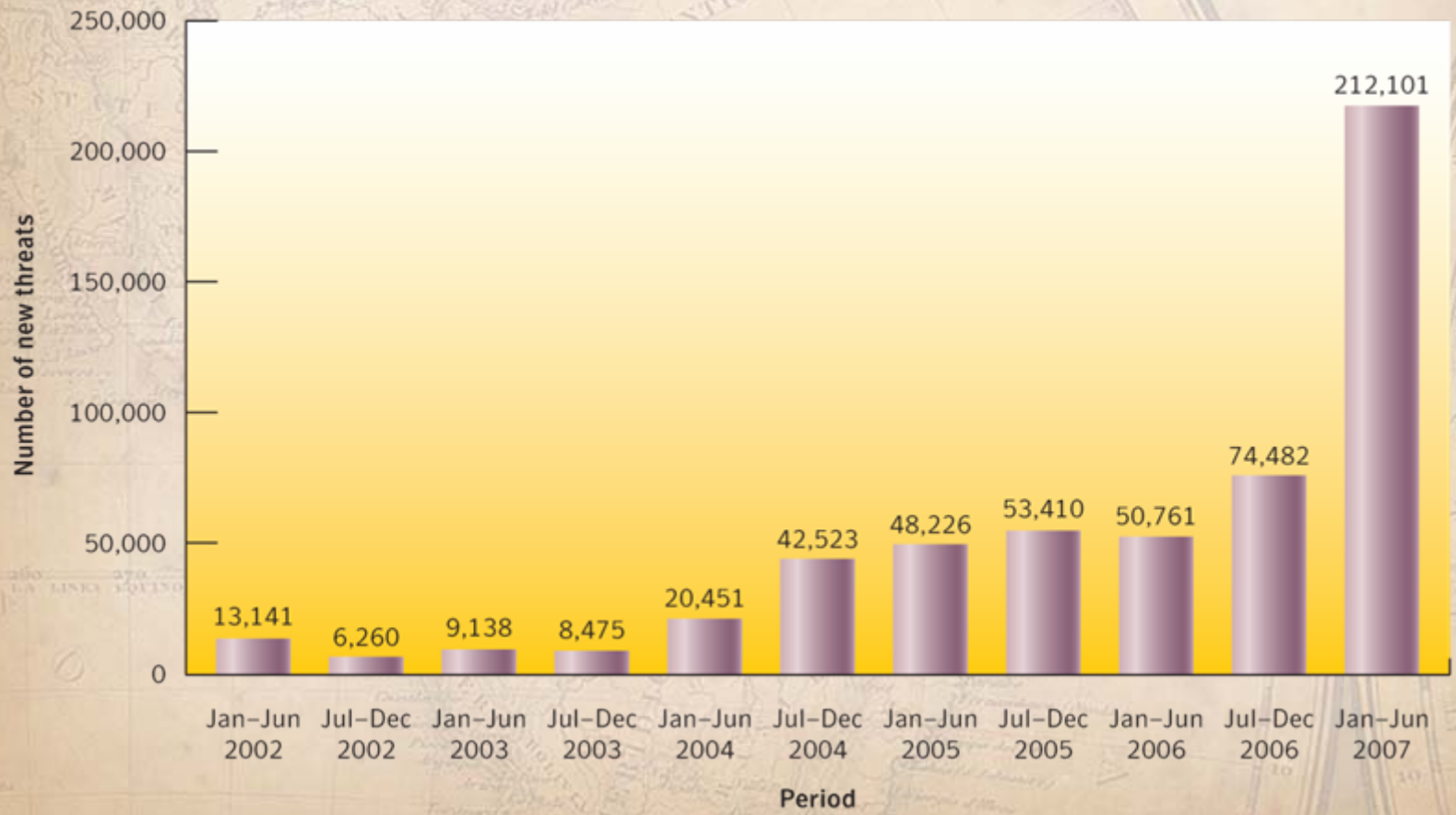


# C'est une économie de marché…


- 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

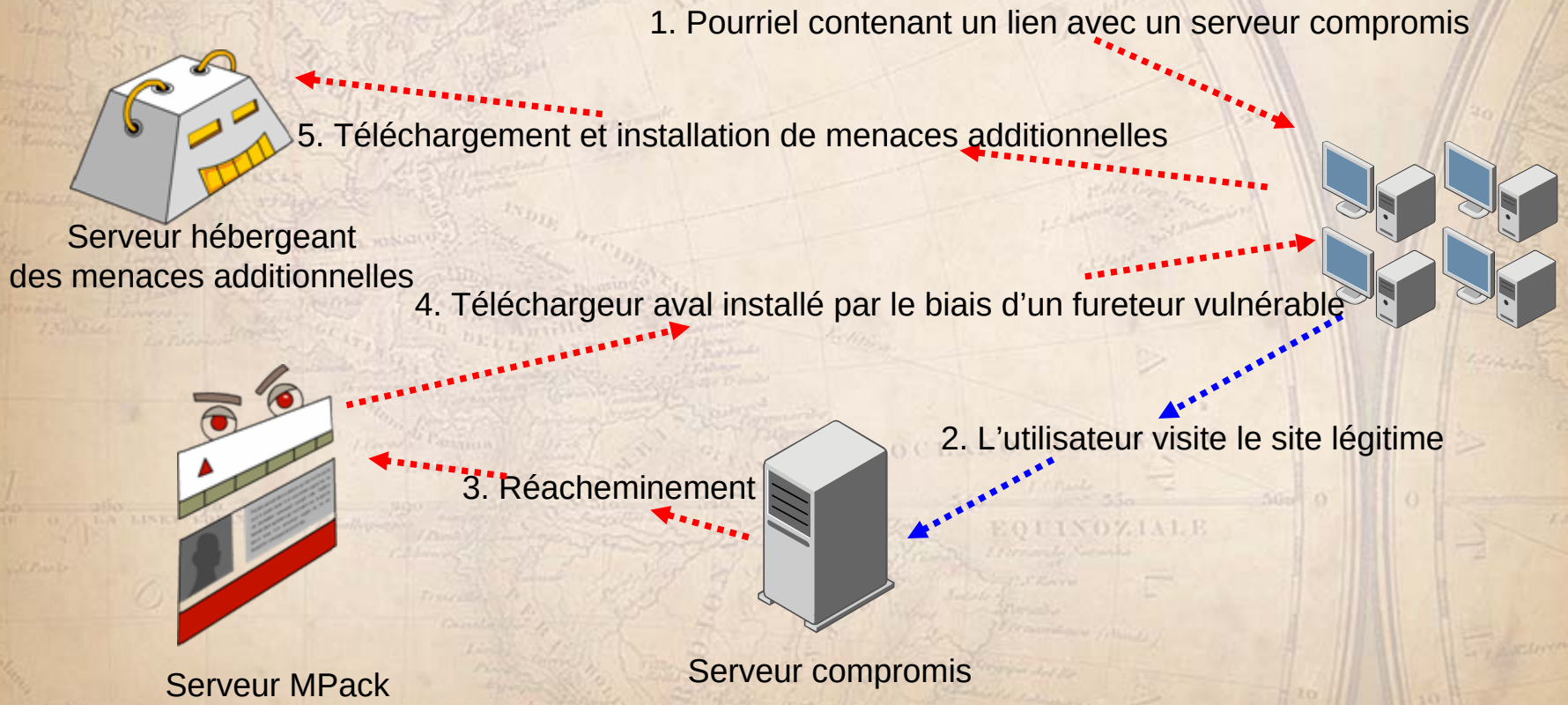
# … et les affaires sont en plein essor!

- 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.

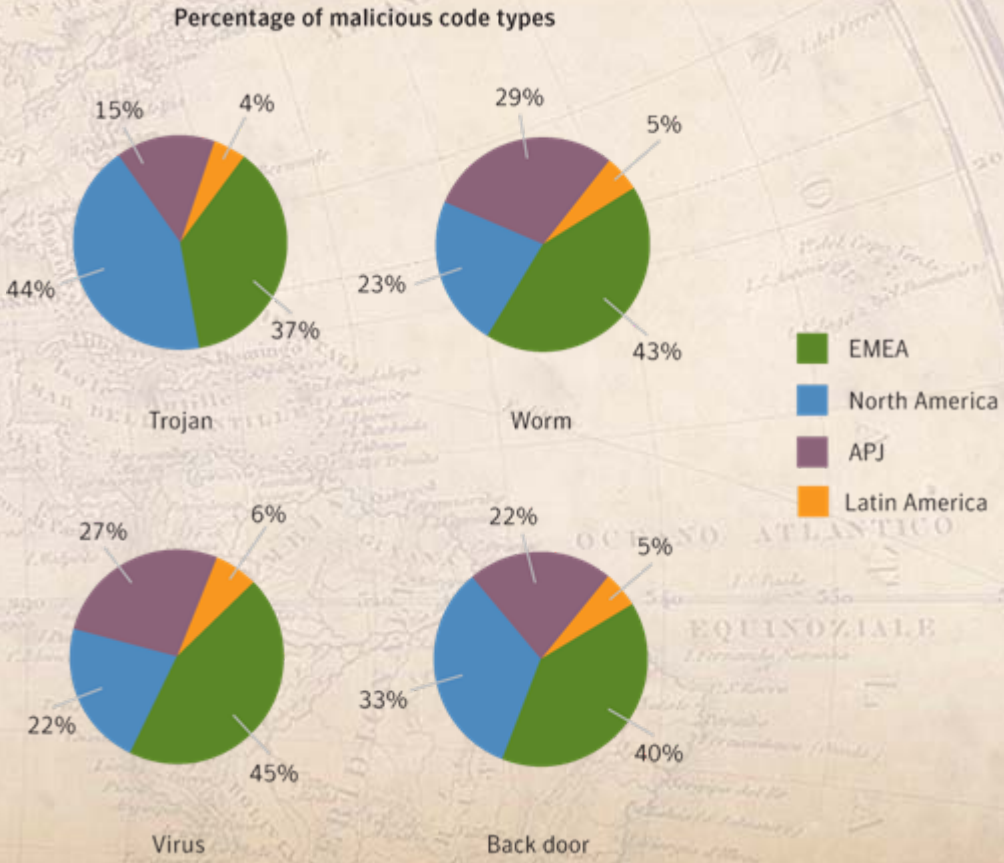


# Changement de tactiques et de cibles


- 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 1er 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 |

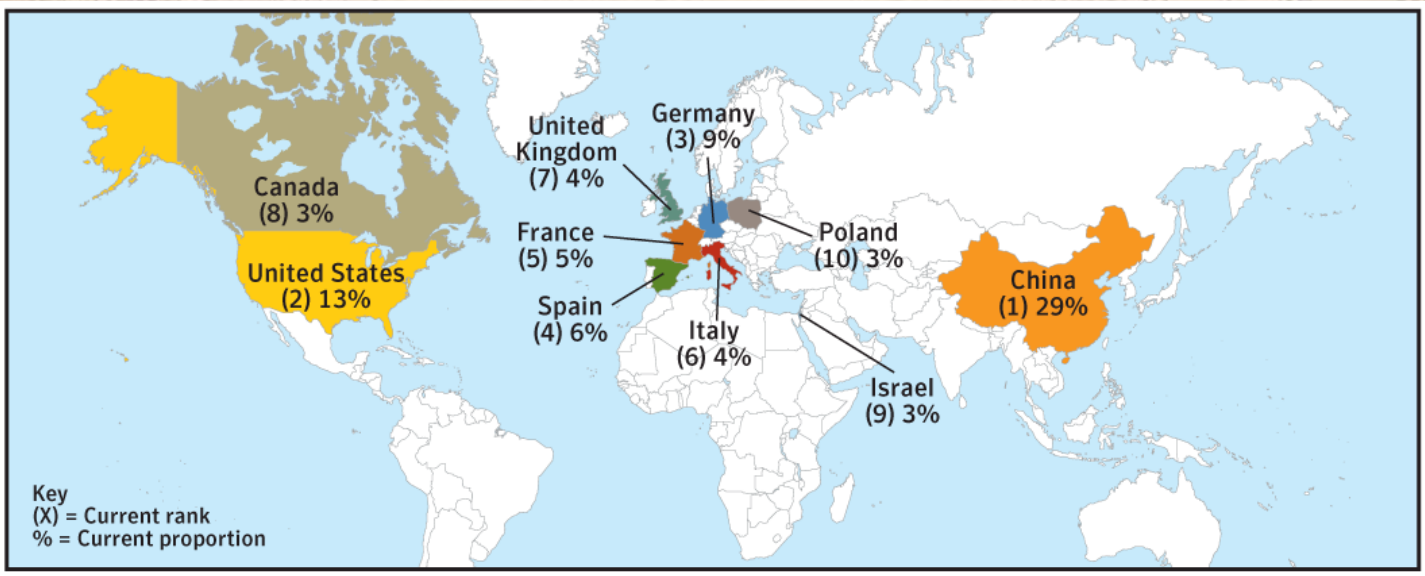
# Emplacements mondiaux des activités frauduleuses

- 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% |

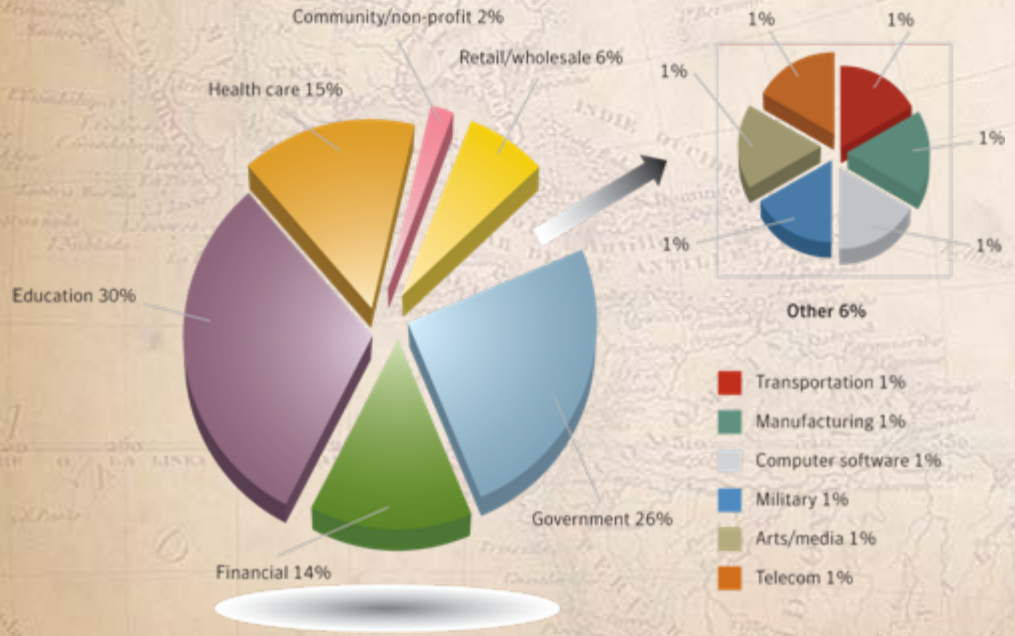
# Infrastructures d'attaques mondiales

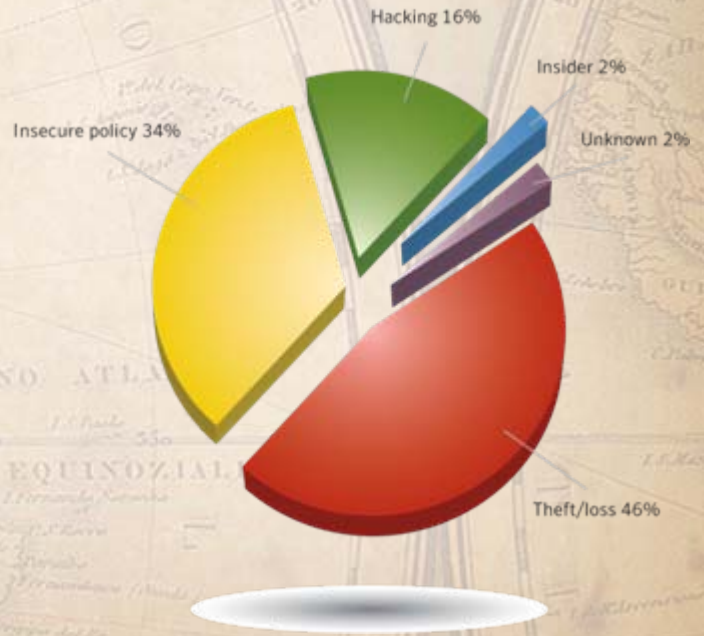
- À l'échelle mondiale, Symantec a observé durant la période de référence actuelle un nombre quotidien moyen de 52 771 ordinateurs de réseau actifs avec inforobot, une baisse de 17 % par rapport à la dernière moitié de 2006. Le total mondial d'ordinateurs distincts avec inforobot infecté qu'a recensés 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.



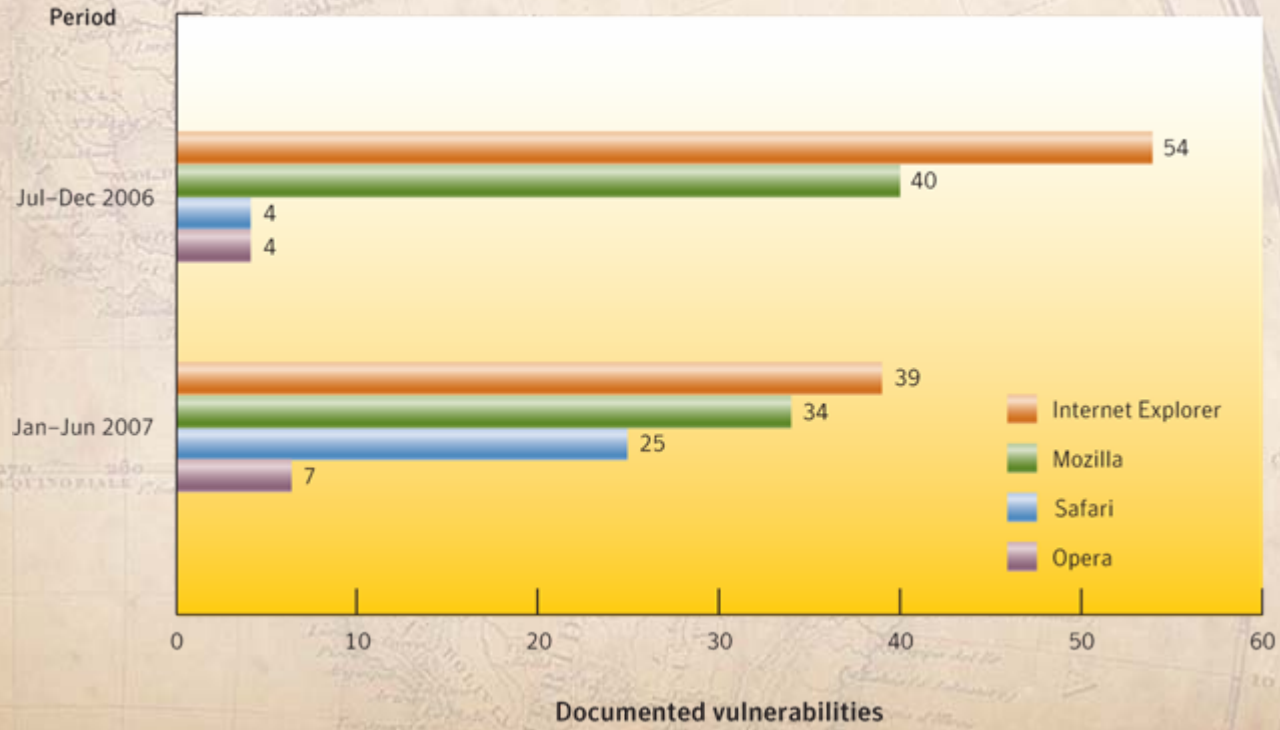
# Économies clandestines mondiales

- 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 |

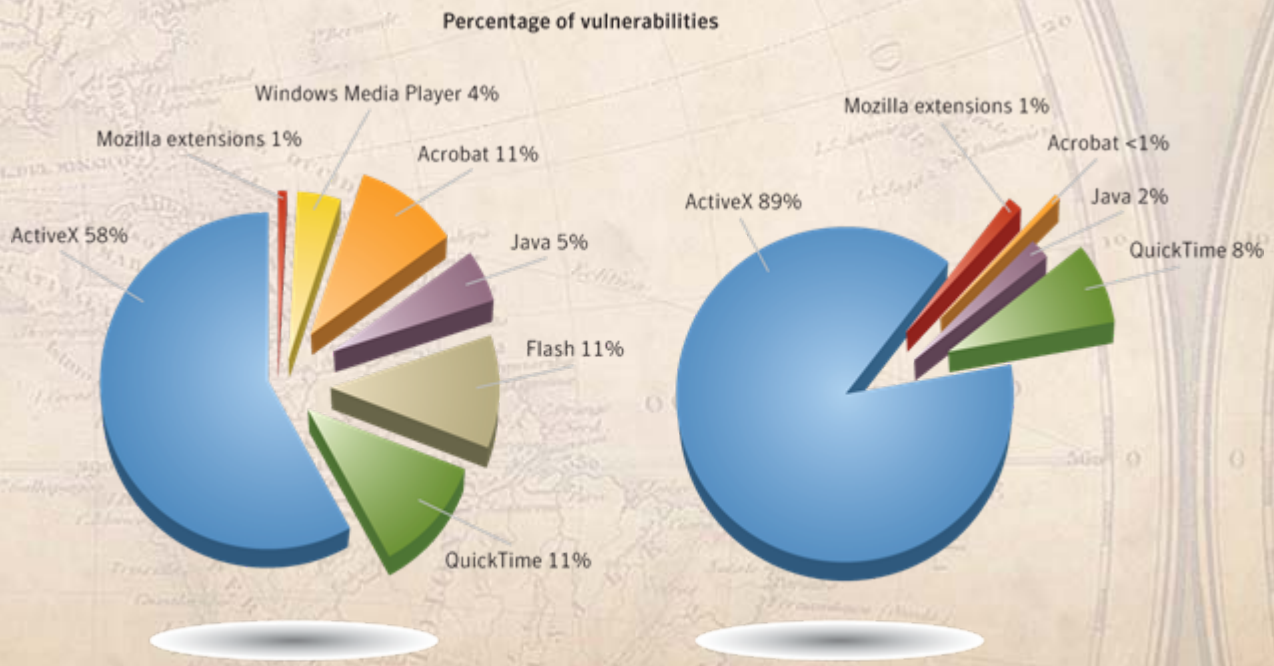
# Technologies cibles – Navigateurs

- 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 composantes ActiveX du navigateur Explorer, ce qui constitue une hausse de 58 % par rapport à la période précédente.

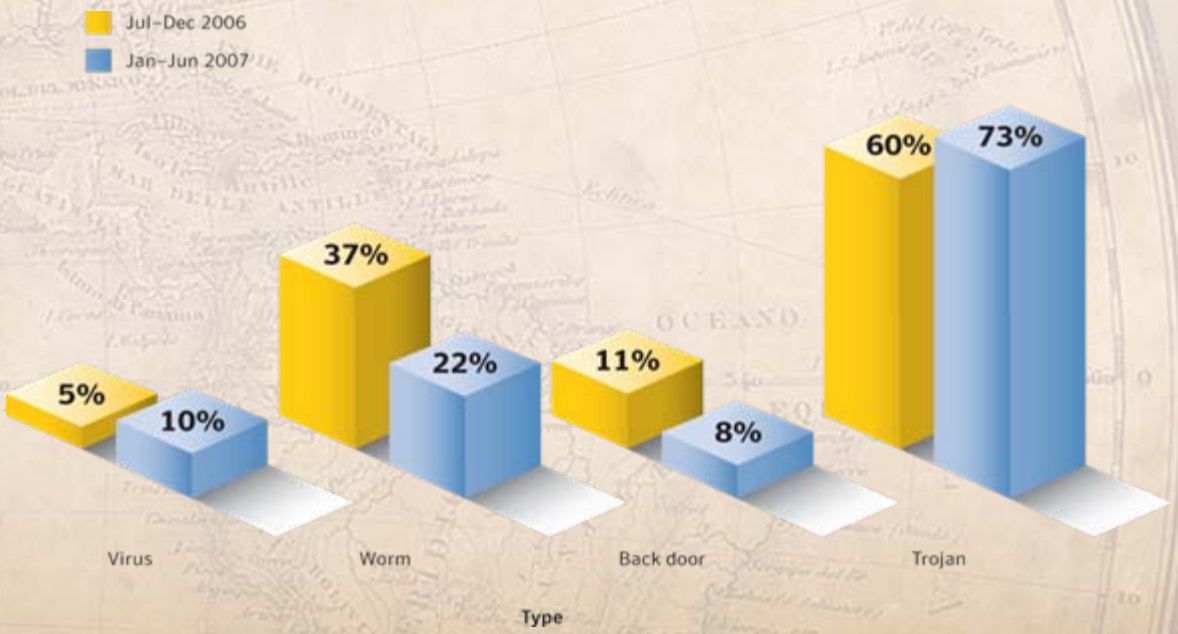


# Technologies cibles – Statistiques clés

- 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.

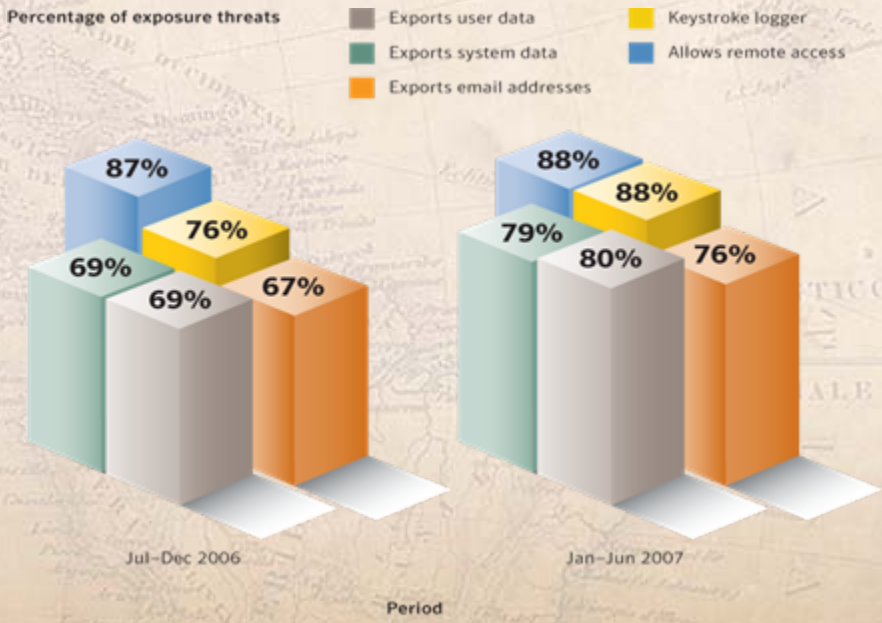
# Méthodes – Logique malveillante

- 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.



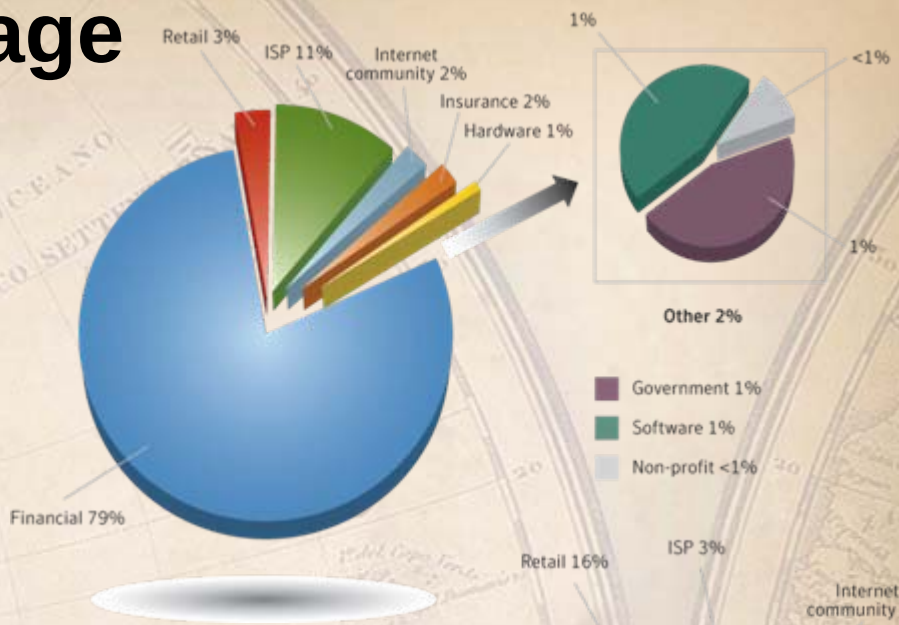
# Méthodes - Propagation

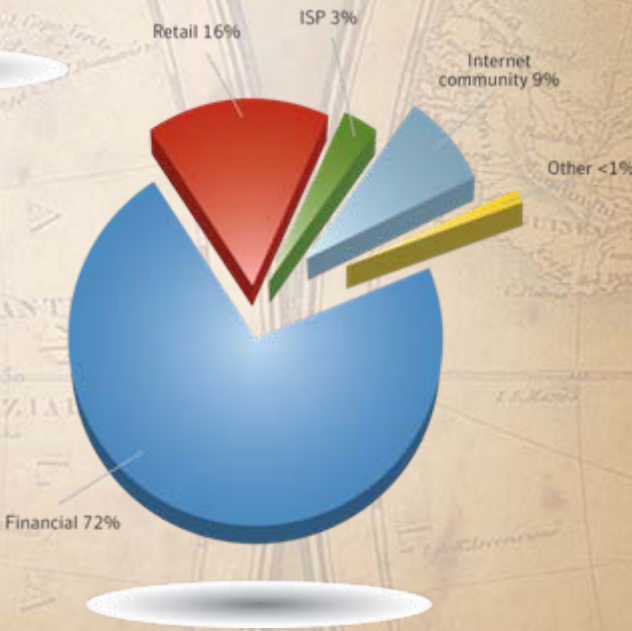
- La propagation par pièce jointe à un courriel constitue le mécanisme numéro un de propagation, avec une proportion de 46 %.
- Au Canada, la propagation par courriel était inférieure à la moyenne mondiale alors que les menaces posées aux systèmes de réseau poste à poste ont dépassé le pourcentage global.

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

# 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

www.idtheft.gov/reports/VolumeII.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