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

Internet Crime Workshop

Wayne Watson

Director General

Investigations and Inquiries Branch

Office of the Privacy Commissioner of Canada

www.privcom.gc.ca

Internet Crimes

As Part of Stalking,

Domestic & Sexual Violence

Presenter: Cynthia Fraser

Safe & Strategic Technology Project

National Network to End Domestic Violence

Internet Crimes & Technology Misuse:

Interception	Surveillance	Environmental
Impersonation	Monitoring	Manipulation
Harass	Victimize	Grooming
Threaten	Stalk	Tracking

Key Goals:

Victim/survivor safety & privacy

Offender accountability

Systems change

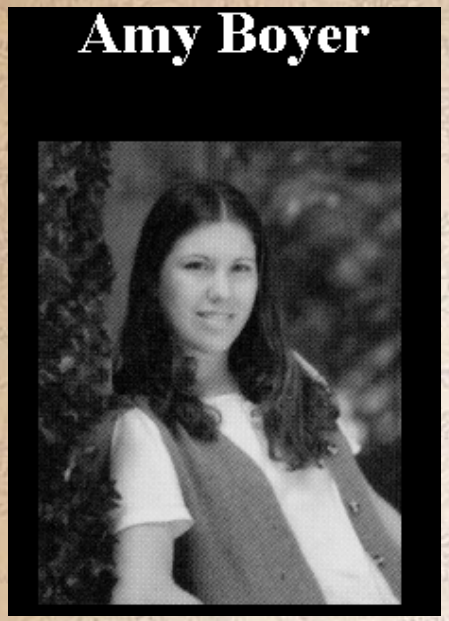
Greetings Infidels, I am Liam Youens

Stalker's Website

"I wasn't going to kill her today I wanted to get the exact time she leaves…."

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



Amy Boyer's Murder

Online broker DocuSearch: Stalker used pretext calls to get Amy Boyer's US SSN & place of employment. Sold to stalker who then found & killed Amy.

Family sued online broker. U.S. New Hampshire case:

- Gathering personal information by pretext violates consumer protection laws
- Investigators/brokers must exercise reasonable care in disclosing 3rd party personal info to client

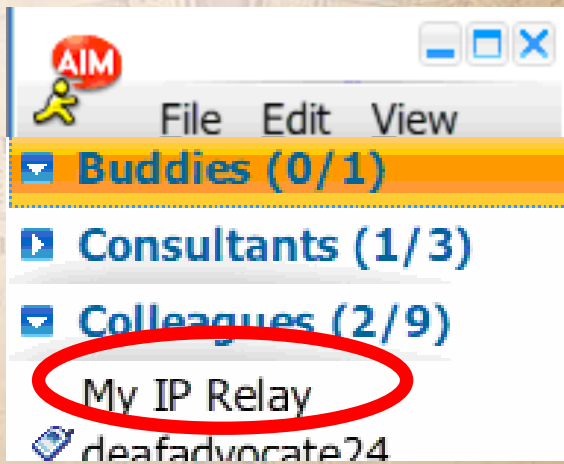
Abusers & Web-based Call Spoofing

- ❑ Caller ID & Voice changer
- ❑ Record calls & web controls
- ❑ Buy calling cards with cash
- ❑ Threaten & stalk
- ❑ evidence?

IP Relay, Stalking, & Impersonation

"This is relay operator 5243 we have a message. You're a heartless, sick, nerdy b@$#%. Die and go to hell. End of message. Thank you IP relay…"

- Enter phone # at relay website
- Open AIM. Create "MyIPRelay" buddy. Send IM with phone #.
- IP relay operator (3rd party) relays typed & spoken conversation
- legally confidential? but can intercept!



IM & Email in Crimes: New Features & Risks

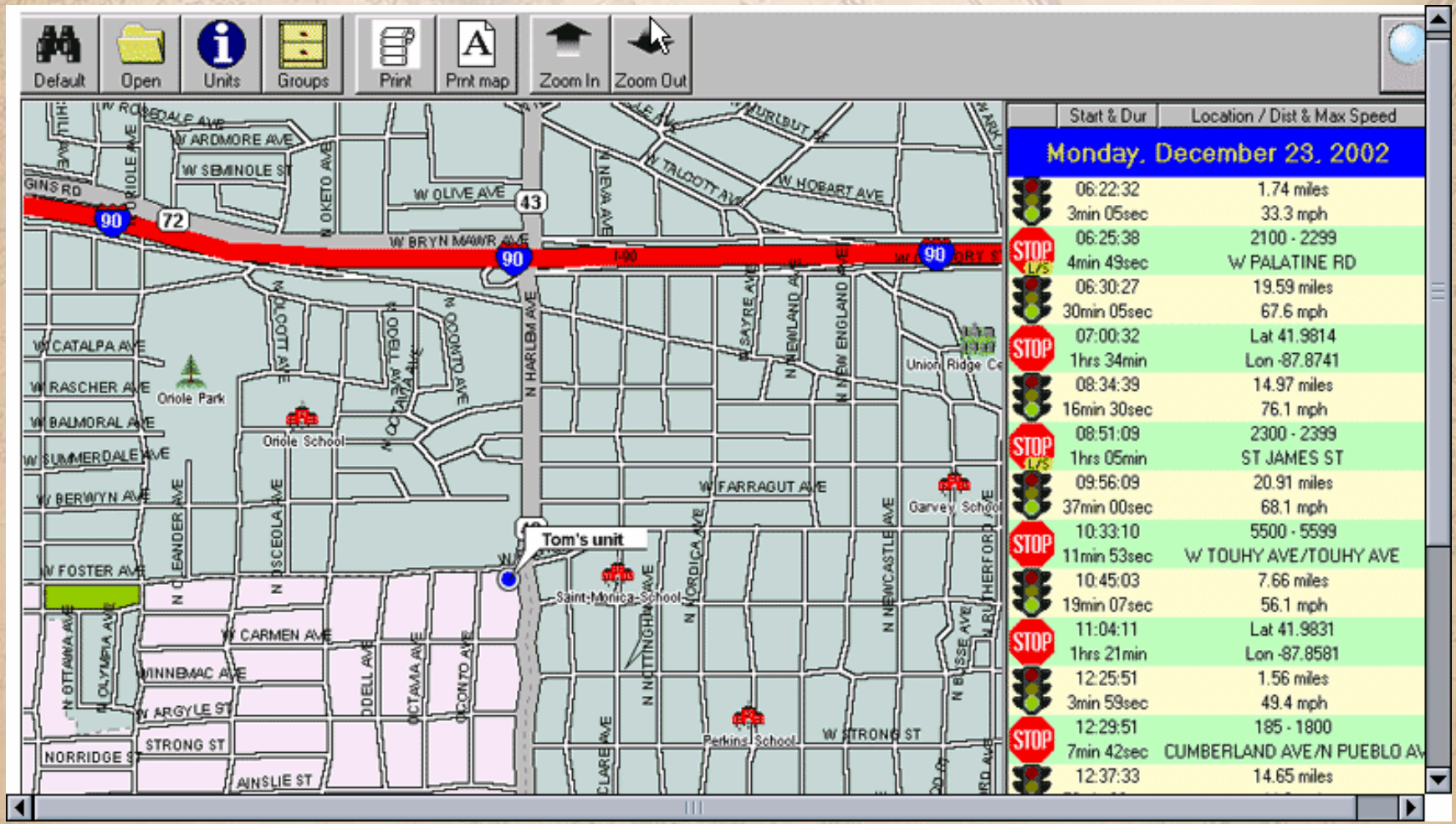
- Impersonation, interception, threats, monitoring, evidence collection & tracing, privacy & encryption
- Email: sniffing, anonymizers, remailers
- IM: logging, hacking, forward to mobile device

IM Logging:

- ❑ Log IMs
- ❑ Log Chats

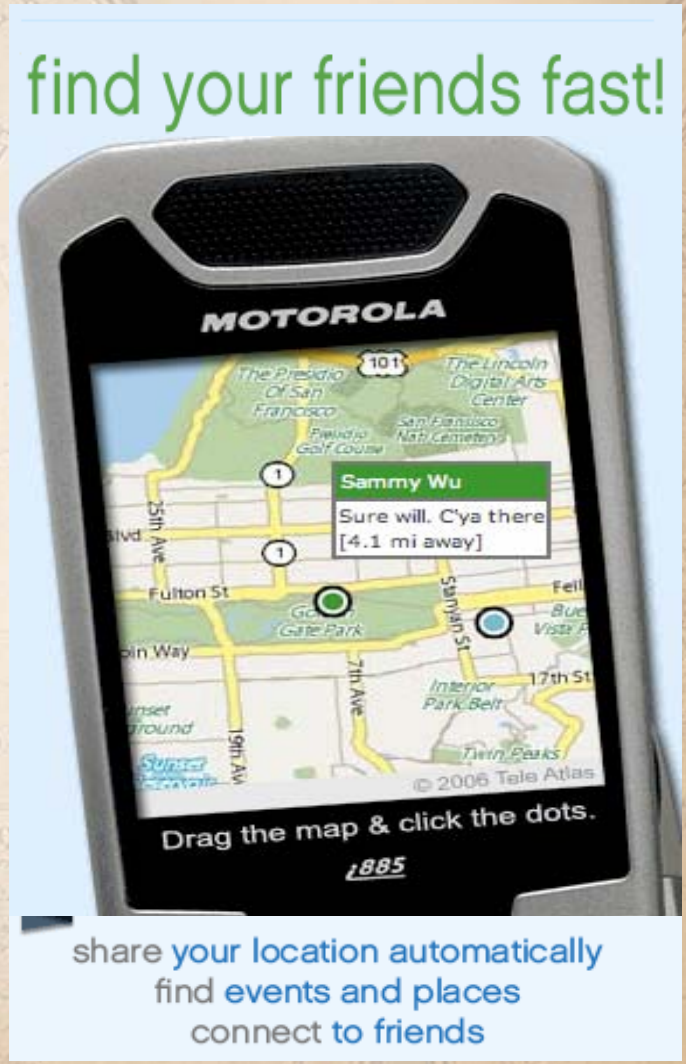
Store Logs: C:\Documen

GPS & Online Location Tracking



Mobile Location Tracking: Consent, Notify, Hide

- Double opt-in: see location without sharing yours.
- Notification: random text messages to notify about activated location features.
- On/off feature: set yourself invisible to all or one person
- Set false location: set location at library & visit shelter.



GPS & U.S. State Stalking Cases


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: Put GPS in ex-wife's car. Convicted: stalking "electronic surveillance."
- Wisconsin 2002: GPS to track former live-in girlfriend. Convicted: stalking, burglary.
- Missouri 12/05: Police officer put GPS in ex-girlfriend's car. Officer fired.

Cameras, Internet, Assault & Abuse

- Voyeurism, Surveillance
- Distribute footage of rape

- consensual interaction taped & distributed without consent
- Child pornography, coerced & groomed filming
- website/computer hacks, impersonate to solicit, threats

Spyware, Abusers & Computer Monitoring

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.

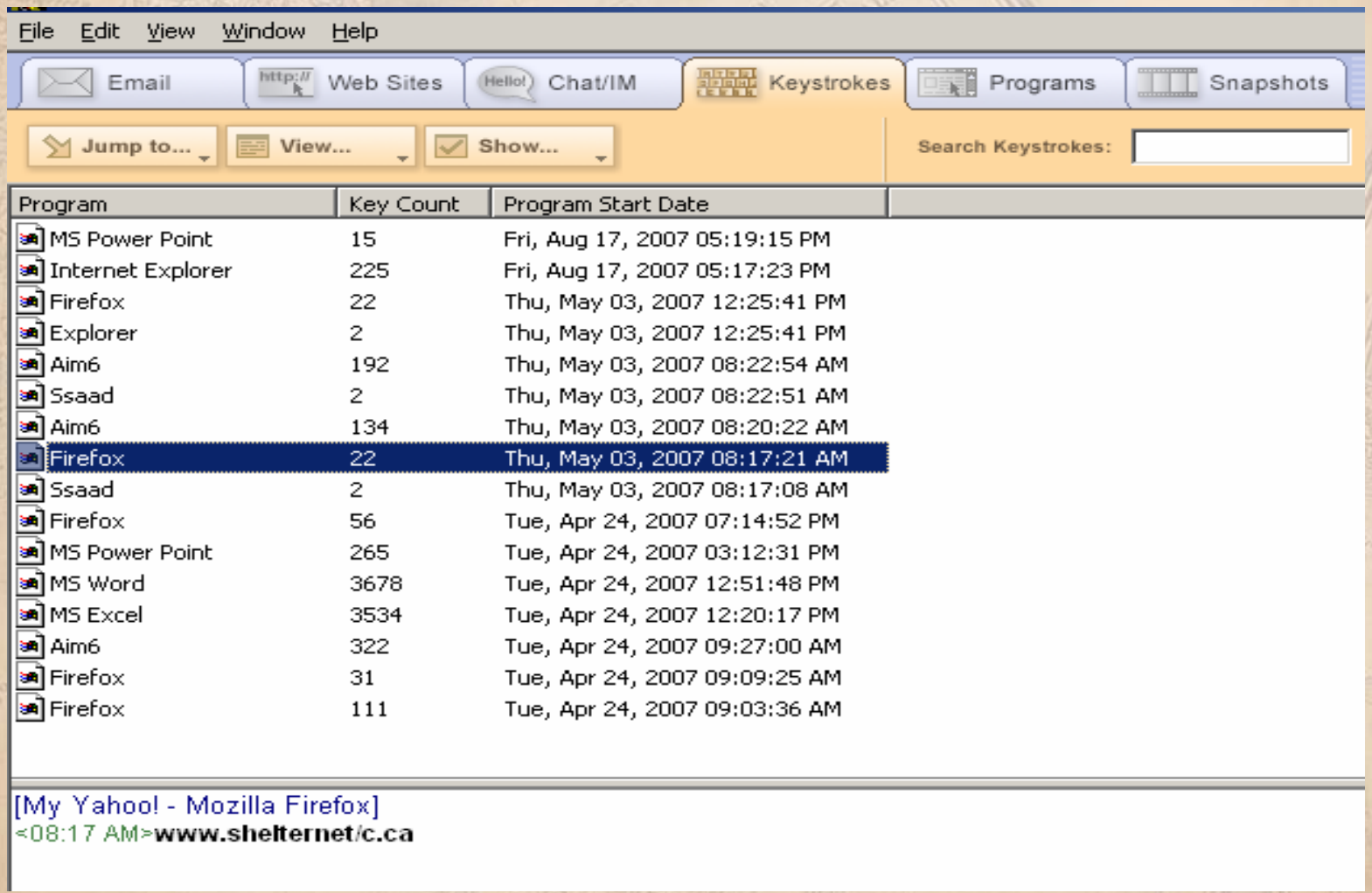
U.S. Michigan State Law charged: Eavesdropping, Installing an Eavesdropping Device, Unauthorized Access, & Using a Computer to Commit a Crime

SNOOPSTICK™ From CYBERsitter®

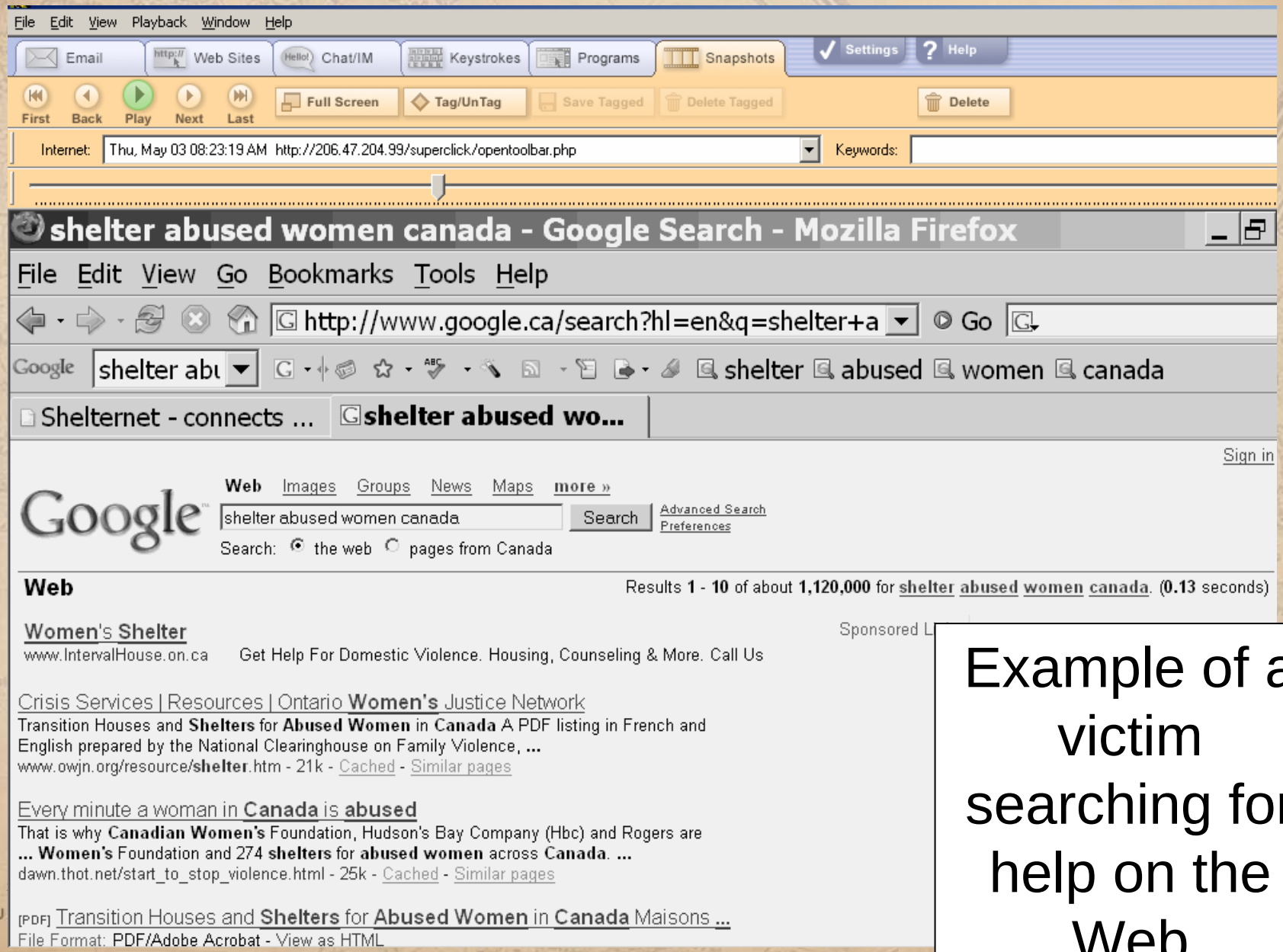
Easy Data Breaches -- BBC Program has Child Put Keylogger on MP's Computer (March 23, 2007, England)

A 6-year-old girl, accompanied by BBC's Inside Out television program reporter, attached a keystroke logging device to an MP's computer. MP Anne Milton agreed to leave her computer unattended for one minute; the child attached a keystroke logger within 15 seconds. The girl brought the device undetected into the House of Commons.

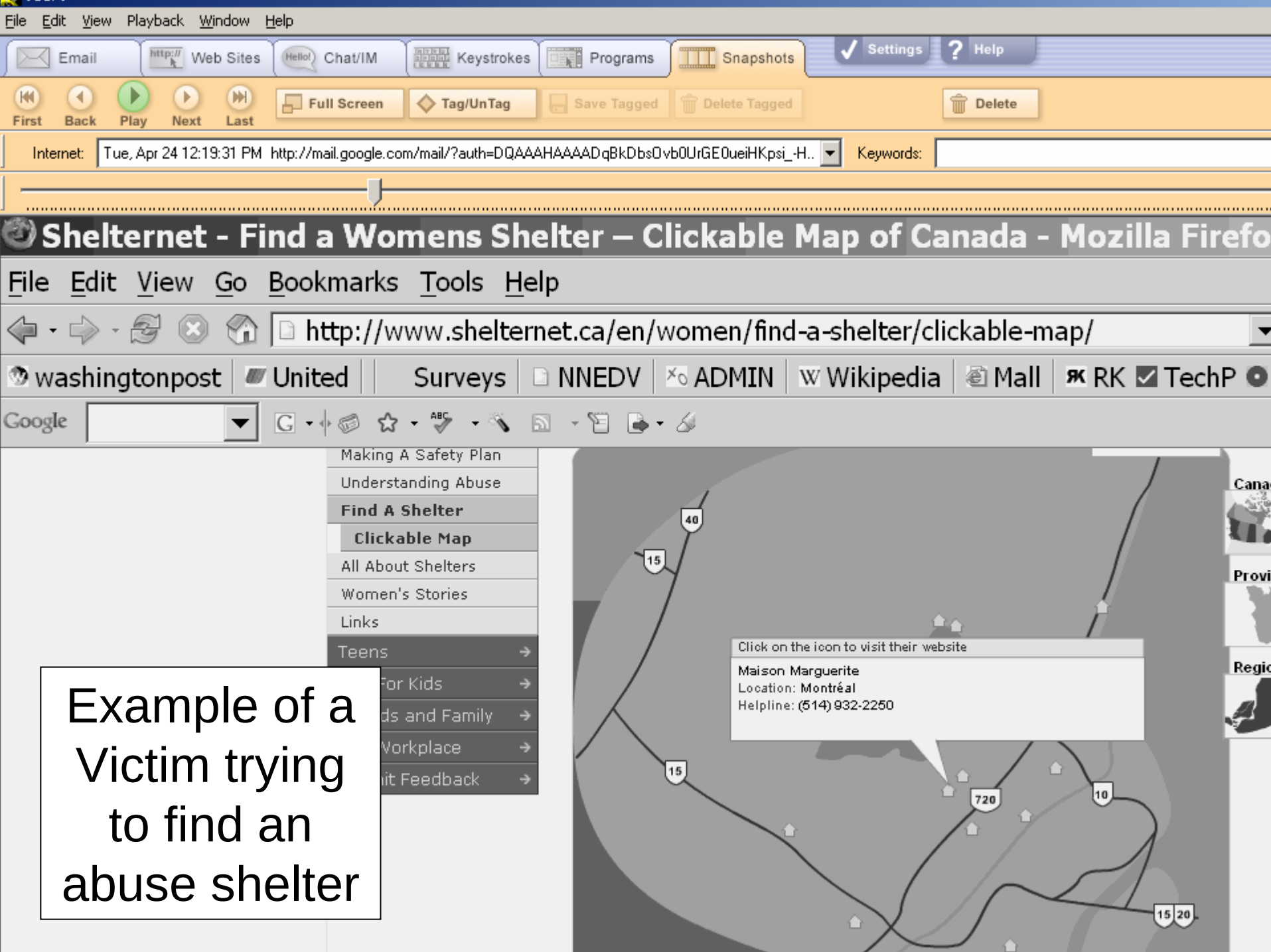
SpyWare Records Every Keystroke Typed

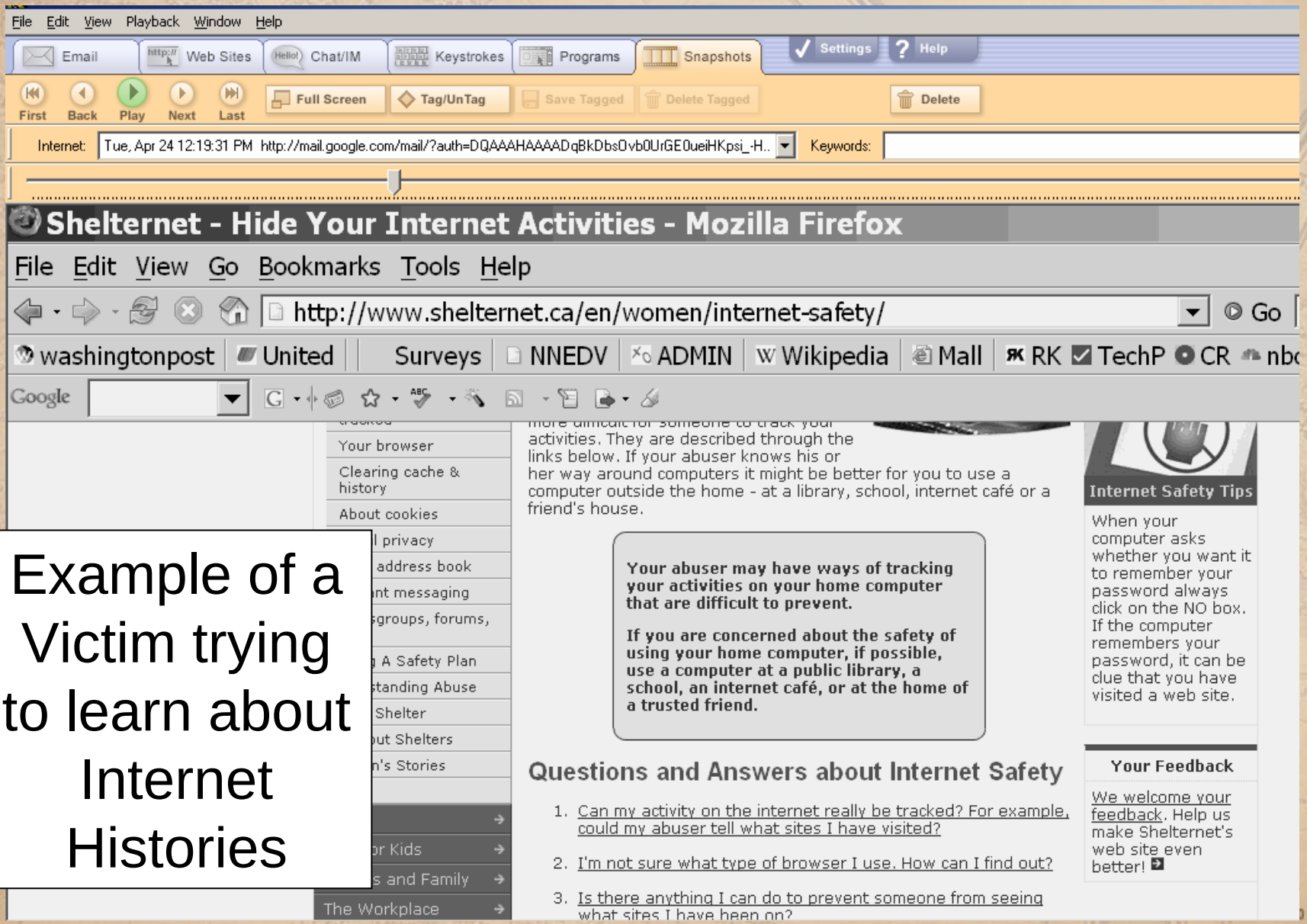


Spyware Records Images or “screenshots” every second

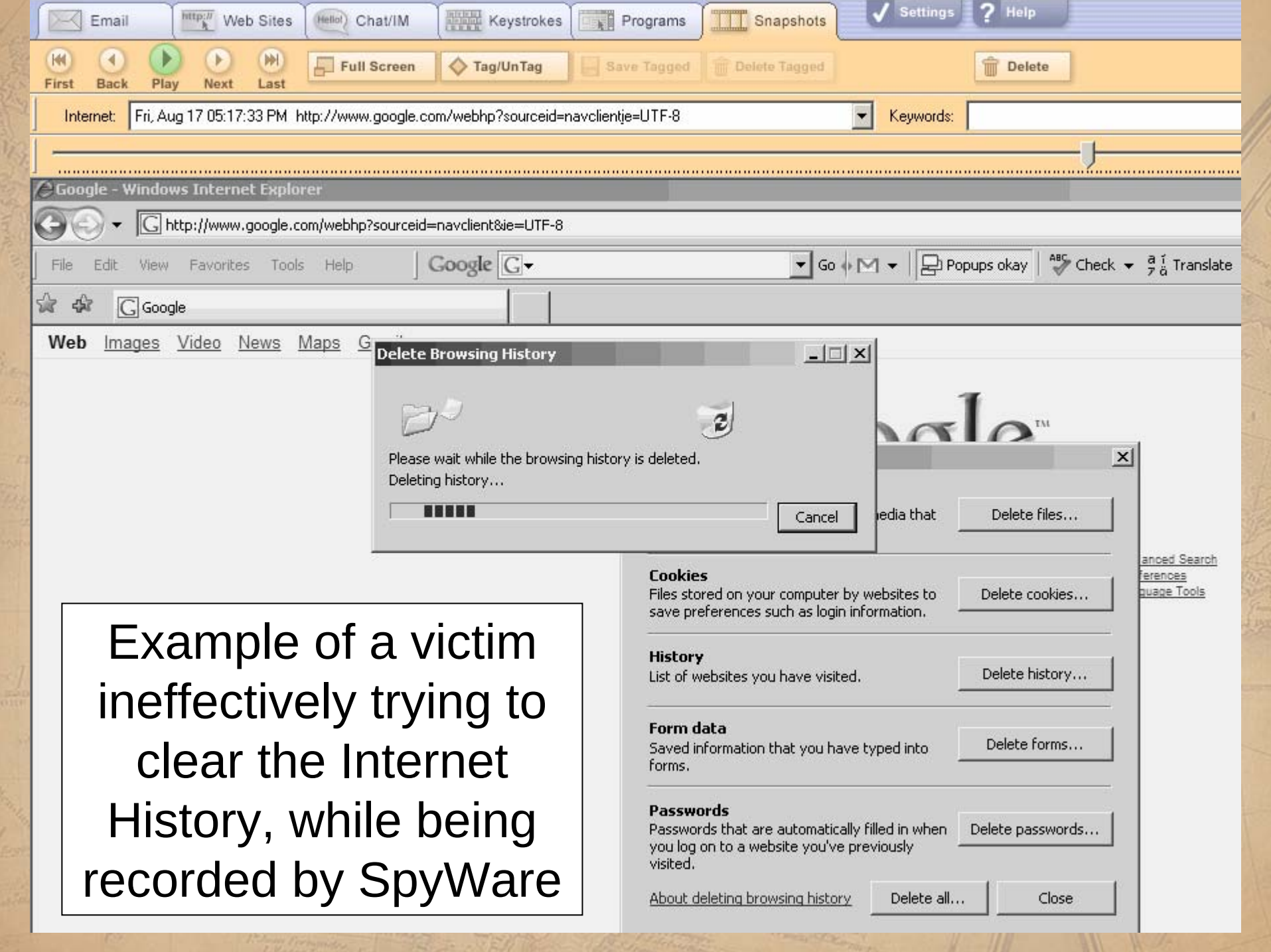


Example of a victim searching for help on the Web


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=DQAAAHAAAADqBkDbsOvb0UrGE0ueiHKpsi_-H..
Keywords:
Shelternet - Find a Womens Shelter – Clickable Map of Canada - Mozilla Firefo
File Edit View Go Bookmarks Tools Help
http://www.shelternet.ca/en/women/find-a-shelter/clickable-map/
washingtonpost
United
Surveys
NNEDV
ADMIN
Wikipedia
Mall
RK
TechP
Google
Making A Safety Plan
Understanding Abuse
Find A Shelter
Clickable Map
All About Shelters
Women's Stories
Links
Teens
For Kids
ds and Family
Workplace
it Feedback
Click on the icon to visit their website
Maison Marguerite
Location: Montréal
Helpline: (514) 932-2250
40
15
15
720
10
15
20
Example of a Victim trying to find an abuse shelter



Example of a Victim trying to learn about Internet Histories



Example of a victim ineffectively trying to clear the Internet History, while being recorded by SpyWare

Laws & Regulations

- U.S. federal stalking law & in every state, etc.
- Use your country's laws to support survivors: data privacy, eavesdrop, restraining orders, internet crimes, etc.
- Train law enforcement on crimes & laws

Recommendations

- Ensure privacy of all victim data, especially in identity changes, borders
- Include "technology misuse by abusers" in ALL data privacy audits, trainings, & awareness campaigns
- Educate victim advocates

For More Information, contact:

Cynthia Fraser

or any member of the Safety Net Project team

U.S. National Network to End Domestic Violence

2001 S Street NW, Suite 400

Washington, DC 20009 USA

Phone: 202-543-5566

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

The Internet Threat Landscape Symantec ™

Dean Turner
Director
Global Intelligence Network
Symantec Security Response

September 28, 2007

Today's Discussion

- Symantec Global Intelligence Network™
- Today's Threat Landscape - Overview
- Global Reach
- Targets
- Methods
- Fraud
- Critical Priorities and Steps

Symantec™ Global Intelligence Network

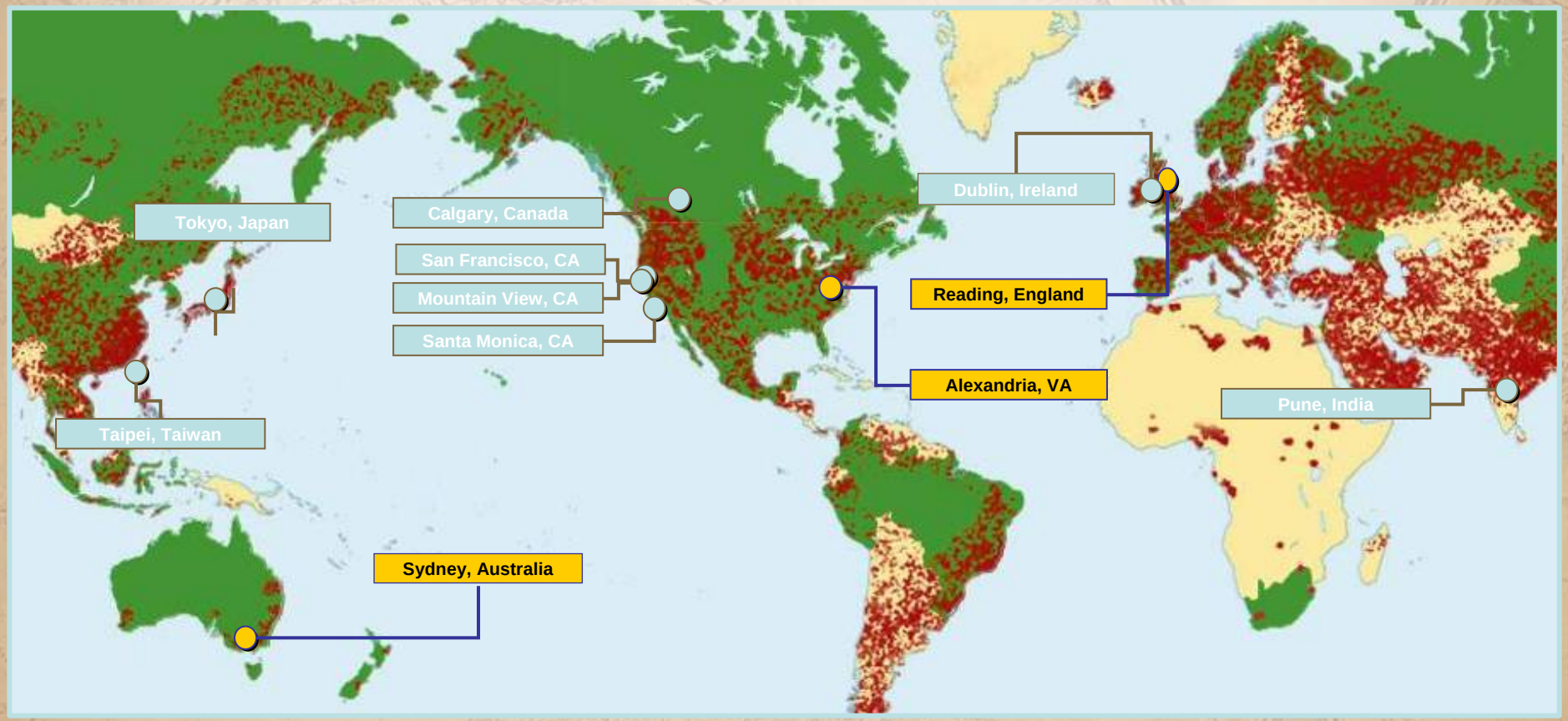
3 Symantec SOCs

80 Symantec Monitored Countries

40,000+ Registered Sensors in 180+ Countries

8 Symantec Security Response Centers

> 6,000 Managed Security Devices + 120 Million Systems Worldwide + 30% of World's email Traffic + Advanced Honeypot Network

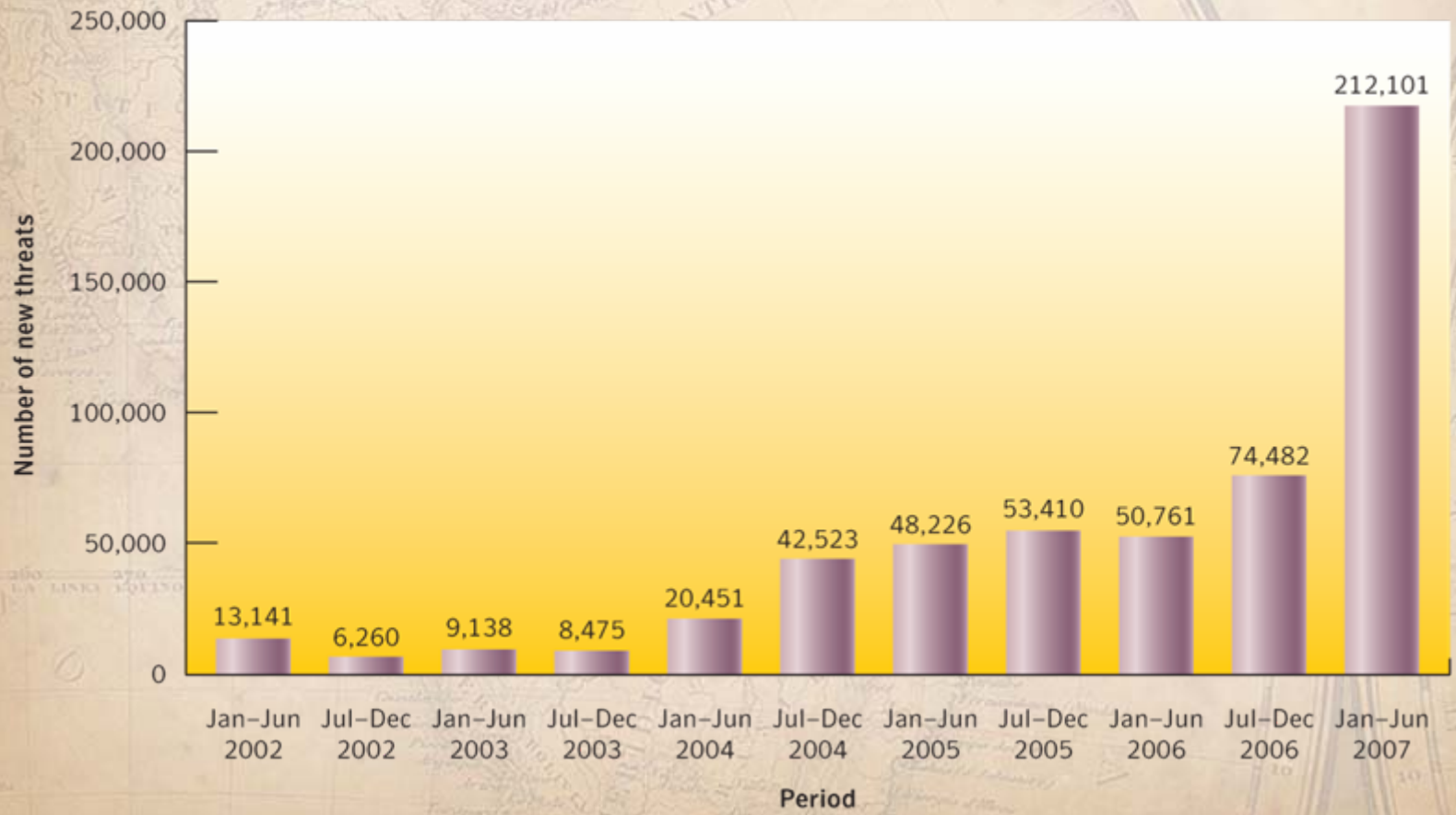


It's a Market Economy…

- Professional crime requires professional tools
- Increasingly commercialized
- PFR, Development spec., QA, RTM
- GTM - Pricing, distribution, support

…and business is booming!

- In the first half of 2007, 212,101 new malicious code threats were reported to Symantec. This is a 185% increase over the second half of 2006.



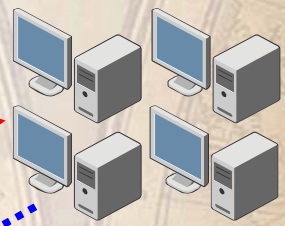
Attacks in Stages

- Multi-staged attacks use a small and quiet initial compromise to establish a beachhead from which subsequent attacks are launched
- Later stages of an attack can be changed to suit the attacker's needs

Server hosting additional threats

1. Spam containing link to compromised server

5. Download and install additional threats

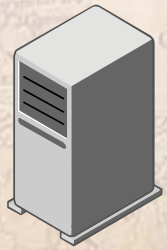


4. Downloader installed through browser vulnerability

MPack Server

2. User visits legitimate site

3. Redirection



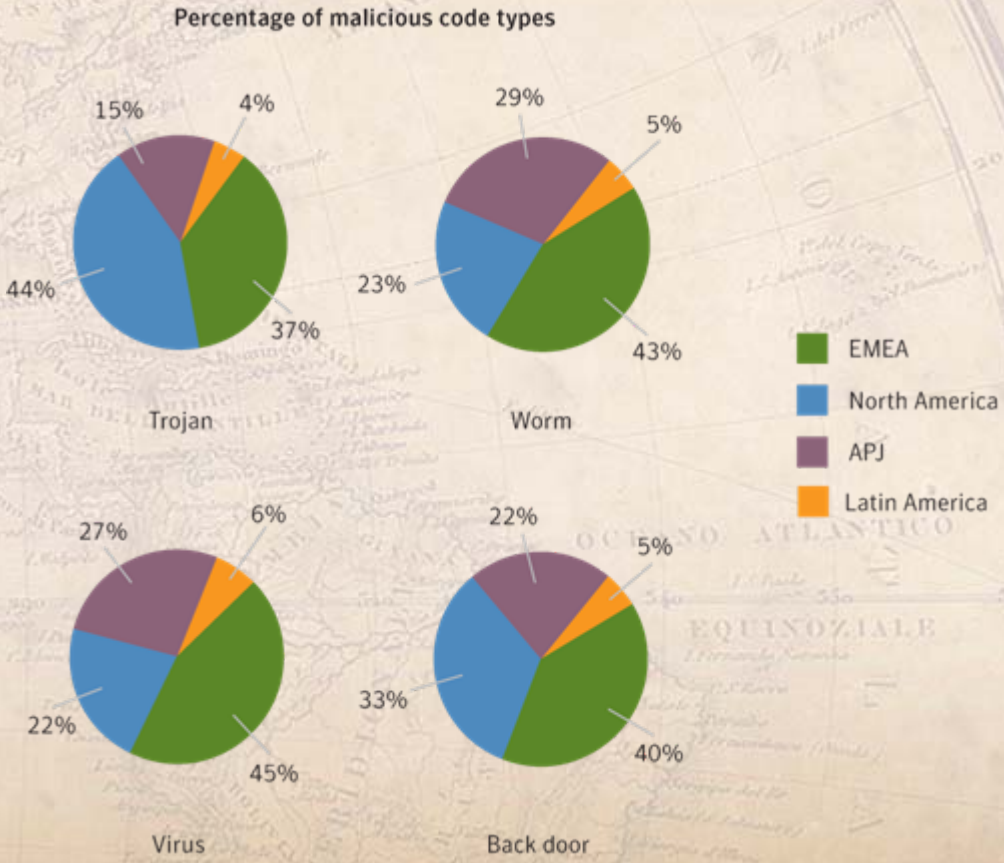
Compromised Server

Change in Tactics and Targets

- Why go to you when you'll come to them?
- Fertile ground
- Difficult to police

Increasing Regional Focus

- Threats are being tailored to specific regions and countries
- Some malicious code types are more prevalent in certain regions than others



Internet Security Threat Report
Volume XII
Key Facts and Figures

Global levels of malicious activity

- Between January 1st and June 30th the United States was the top country for malicious activity (raw numbers) with 30% of the overall proportion. China was ranked second with 10%.
- When accounting for Internet populations, Israel was the top country with 11% followed by Canada with 6%. Seven of the top ten countries in this metric were located in EMEA.

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

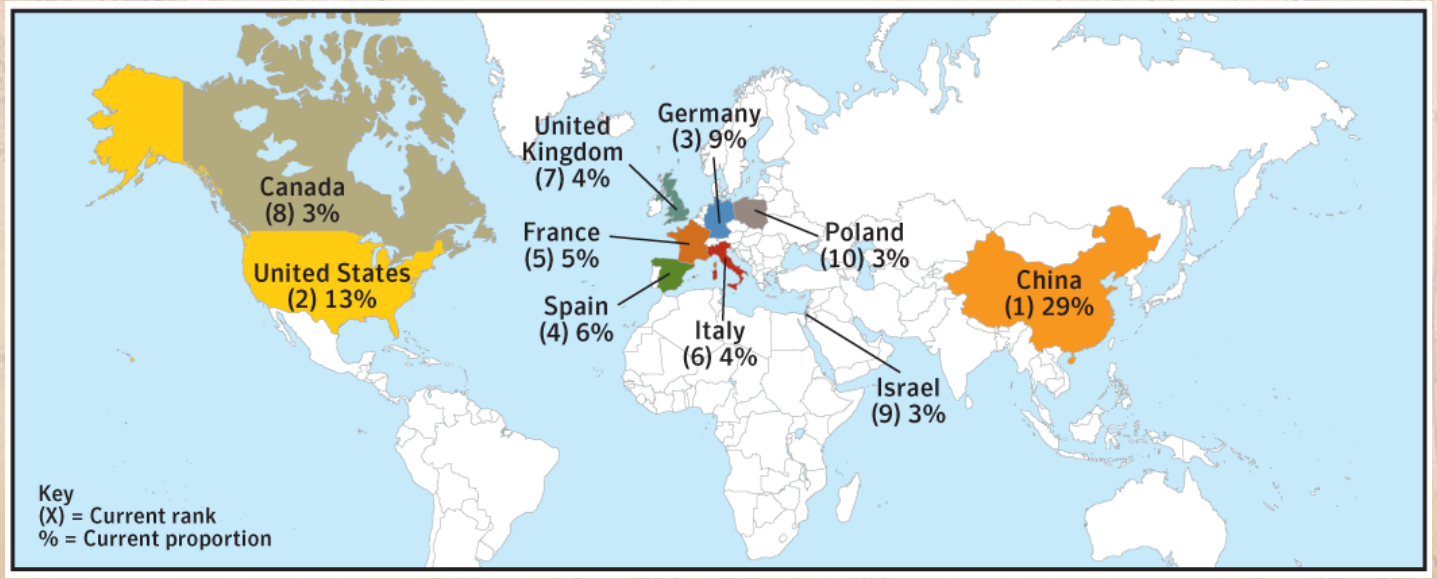
Global locations of fraud

- 59% of known phishing sites were located in the United States followed by Germany with 6% and the United Kingdom with 3%
- The U.S. is number one because a large number of Web-hosting providers—particularly free Web hosts— are located in the United States. The increase in phishing sites there this period may be in part due to the high number of Trojans in North America.

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%

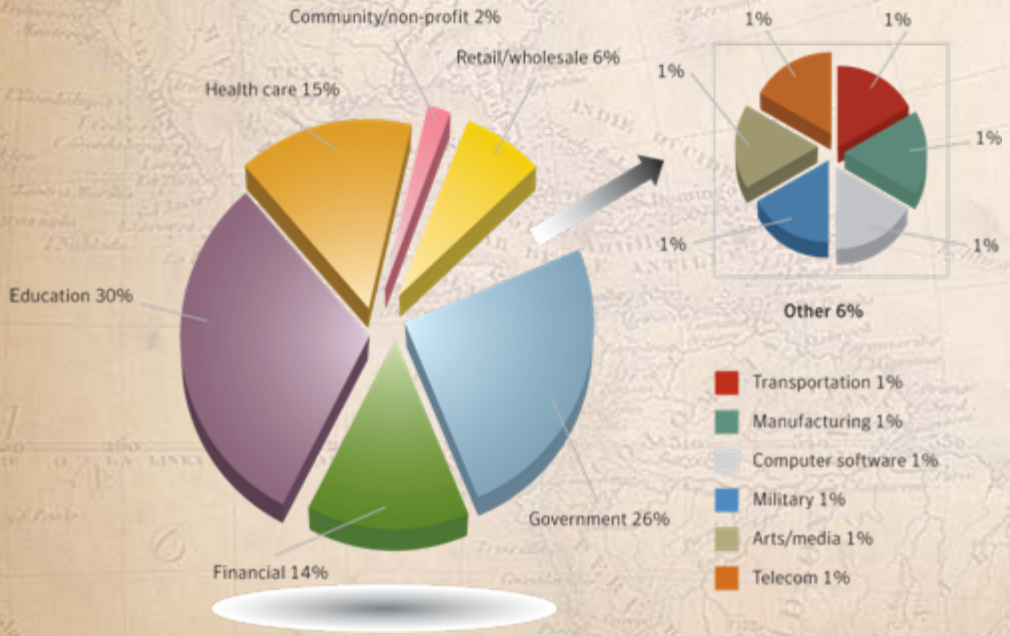
Global attack infrastructures

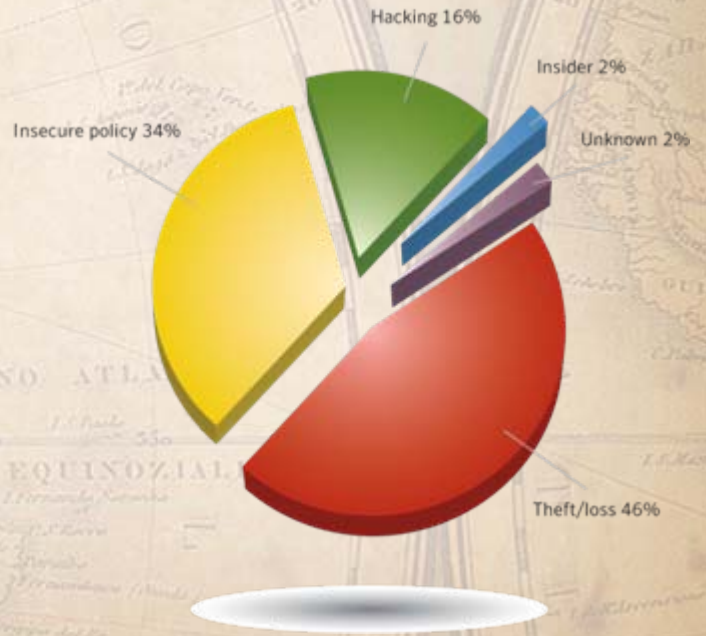
- Globally, during the current reporting period Symantec observed an average of 52,771 active bot network computers per day, a 17% decrease from the last half of 2006. The worldwide total of distinct bot-infected computers that Symantec identified dropped to 5,029,309 - a 17% decrease. Year over year, this still represents a 7% increase.
- Command and control servers decreased during this period to 4,622 - a 3% decrease. The United States continues to have the highest number of command and control servers worldwide with 43% - a 3% increase from its previous total.



Global Data breaches

- The Education sector accounted for the majority of data breaches with 30%, followed by Government (26%) and Healthcare (15%) - almost half of breaches (46%) were due to theft or loss with hacking only accounting for 16%.
- The retail sector was responsible for 85% of exposed identities followed by Government. Where identities were exposed, 73% were due to hacking.





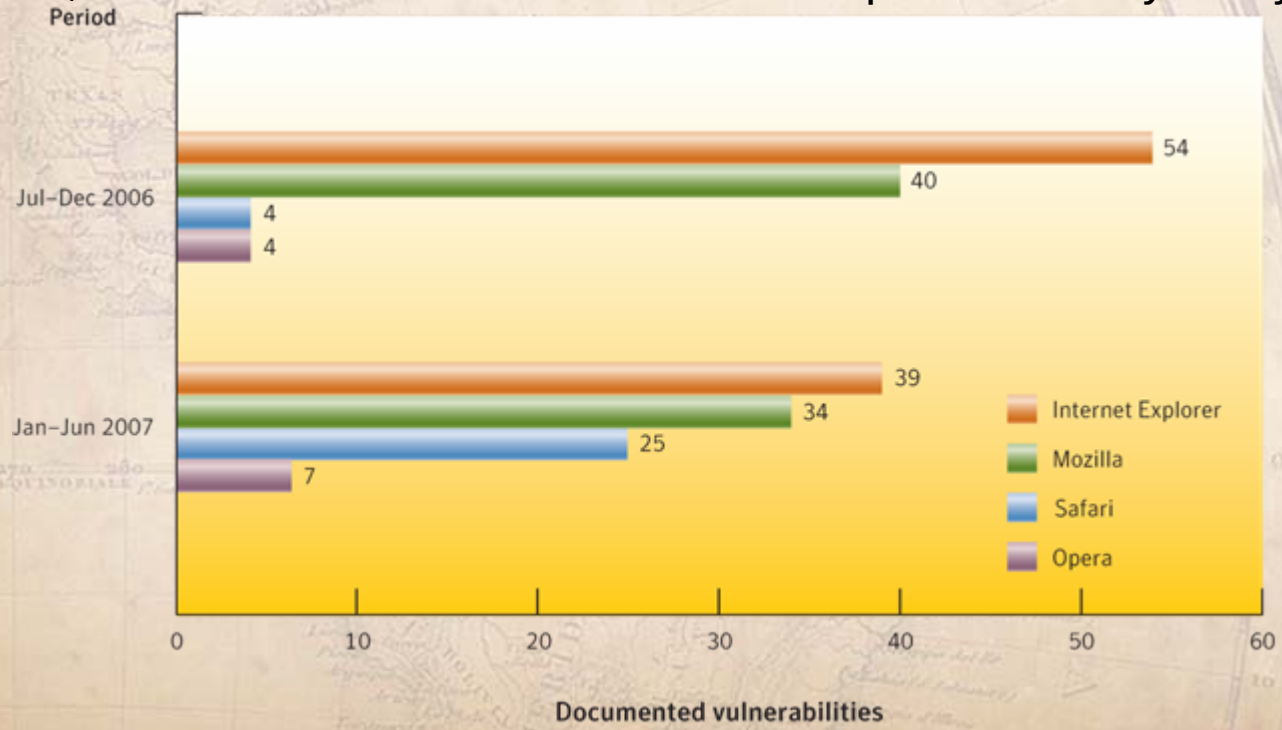
Global underground economies

- Trading in credit cards, identities, online payment services, bank accounts, bots, fraud tools, etc. are ranked according to goods most frequently offered for sale on underground economy servers.
- Credit cards were the most frequently advertised item (22%) followed by bank accounts (21%).
- Email passwords sell for almost as much as a bank account.

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

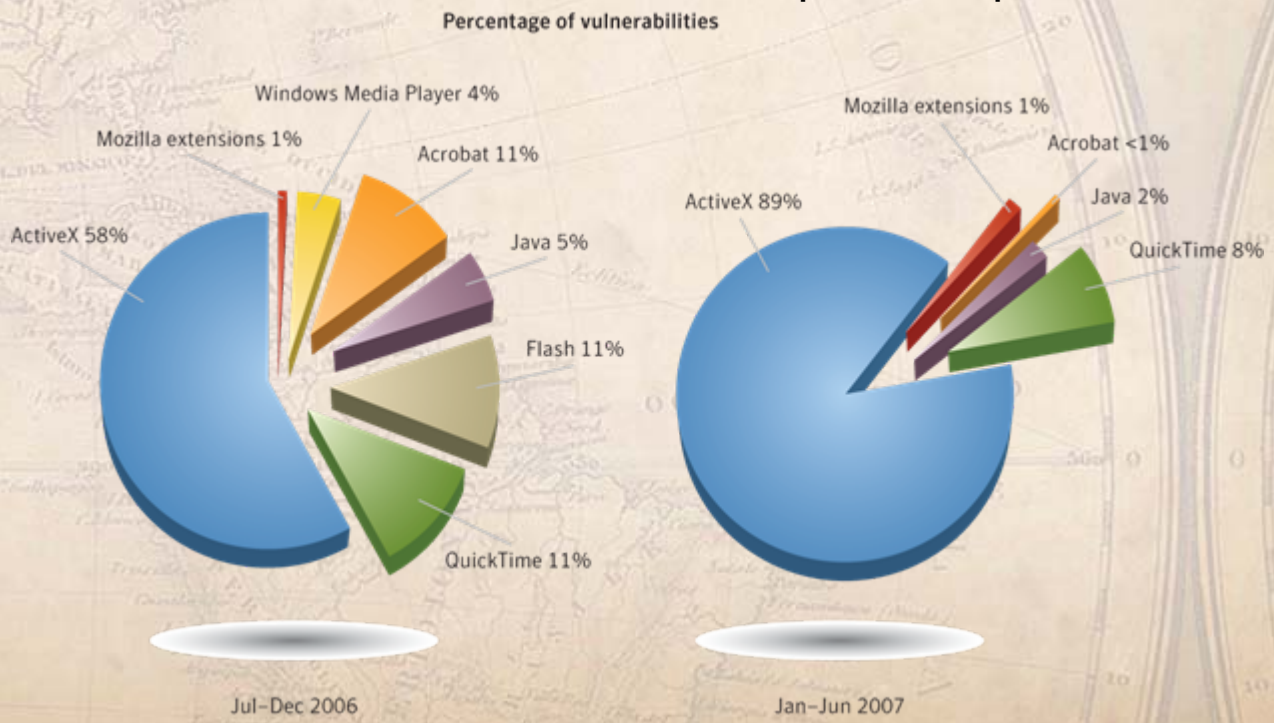
Target technologies - Web browsers

- Microsoft had the highest number of documented vulnerabilities with 39 followed by Mozilla with 34. Both these vendors also had the highest window of exposure at 5 days each.
- There were 25 vulnerabilities documented in Safari this period, a significant increase from the 4 documented in the last half of 2006. However, Safari had the shortest window of exposure at only 3 days.



Target technologies - Plug-ins

- Vulnerabilities in Web browser plug-ins are frequently exploited to install malicious software.
- In the first half of 2007, 237 vulnerabilities affecting browser plug-ins were documented compared to 108 in all of 2006.
- 89% of browser plug-in vulnerabilities affected ActiveX components for Internet Explorer, an increase over the 58% in the previous period.

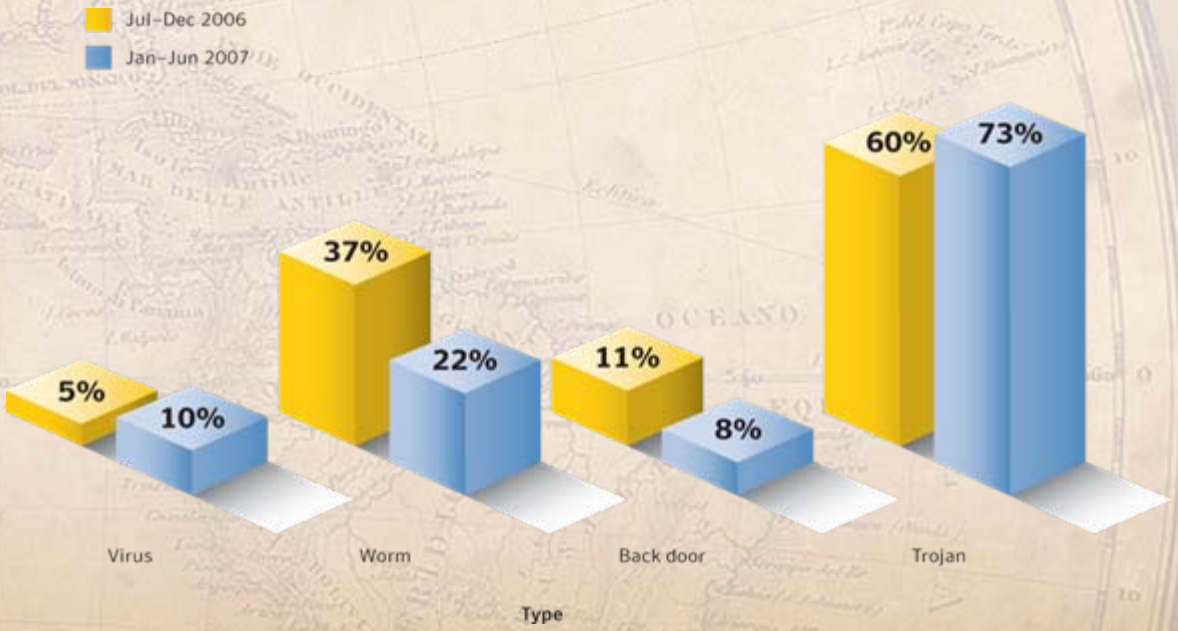


Target technologies - Key statistics

- Symantec documented 2,461 vulnerabilities in the current reporting period, 3% fewer than the previous reporting period.
- Severity classification: High severity 9%, Medium severity 51% and Low severity 40%.
- Web applications constituted 61% of all documented vulnerabilities.
- 72% of vulnerabilities documented this period were easily exploitable compared to 79% in the previous period.
- The W.O.E. for enterprise vendors was 55 days, an increase over the 47 day average in the second half of 2006.

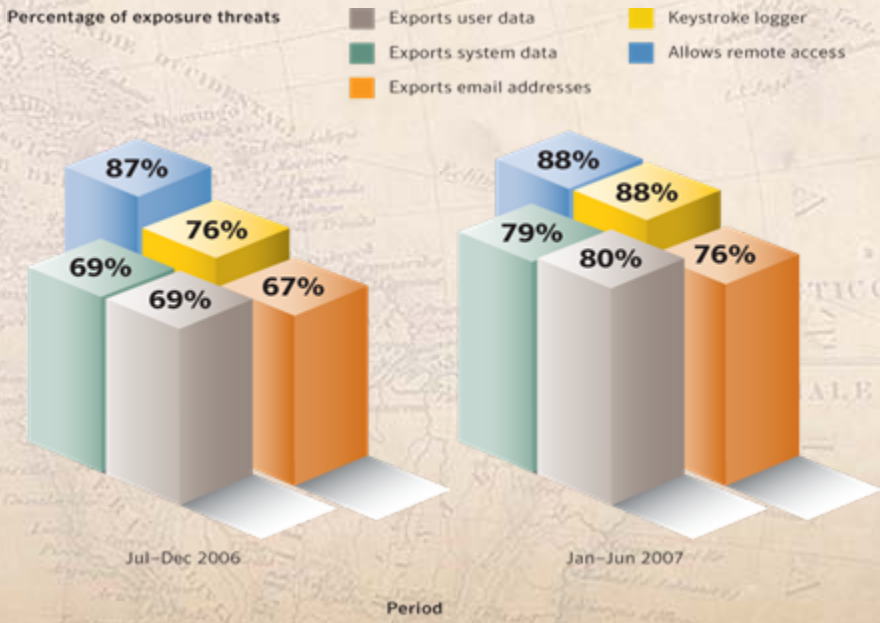
Methods - Malicious code

- Trojans continue to rise and may constitute a greater threat because they tend to exploit web browser and zero-day vulnerabilities. Trojans causing potential/attempted infections increased from 60% to 73% this period.
- Worms continue to drop this period, only accounting for 22% of potential infections. This is a decrease from the 37% in the last half of 2006.
- The percentage of viruses increased from 5% to 10% this period.



Methods - Data theft and data leakage

- During the current reporting period, threats to confidential information made up 65% of the volume of top 50 malicious code causing potential infections, up from 53% in the previous reporting period.
- While the volume of threats that allow remote access remained stable from the same reporting period last year, the volume of threats that log keystrokes and export user and system data have all increased - Keystroke loggers represent 88% of the report threats to confidential information.



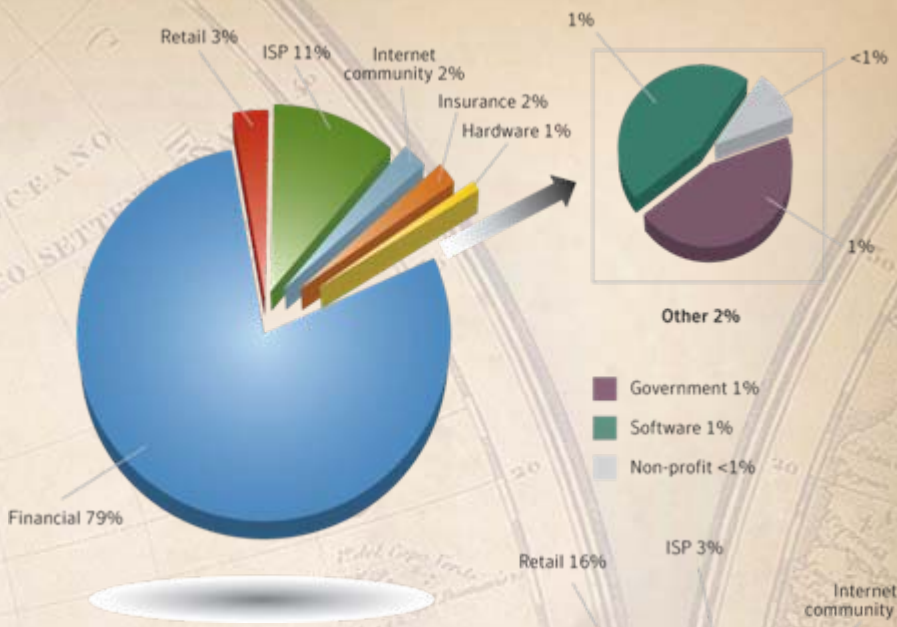
Methods - Propagation

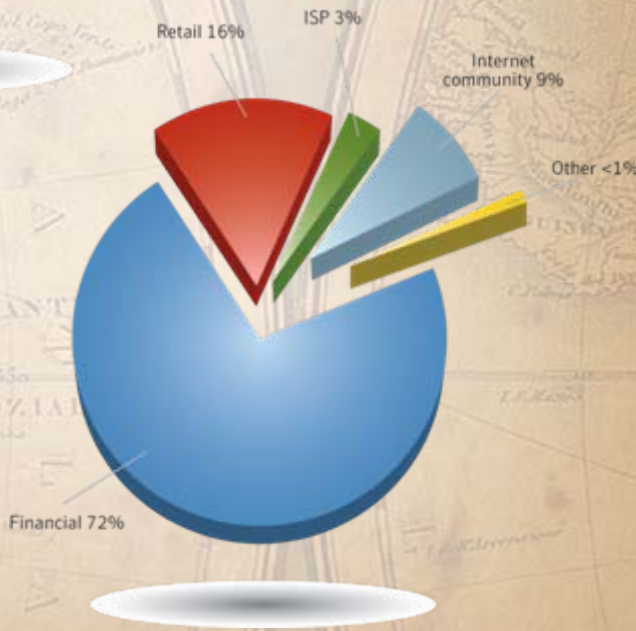
- Email attachment propagation is the number one propagation mechanism at 46%.
- In Canada, email propagation was less than the global average while P2P increased over the global percentage.

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%

Fraud - Phishing

- The Symantec Probe network detected a total of 196,860 unique phishing messages, an 18 percent increase from the previous period. This translates into an average of 1,088 unique phishing messages per day.
- Symantec blocked over 2.3 billion phishing messages - an increase of 53% over the last half of 2006. An average of 12.5 million phishing messages per day.
- Financial services accounted for 79% of the unique brands that were phished while making up 72% of the total phishing websites. The ISP sector accounted for 11% of unique brands phished and 3% of the total number of phishing websites.
- During the first six months of 2007, Symantec classified 78 of the 359 brands being phished as core brands. Core brands are those that are spoofed at least once each month by a phishing attack.





Critical priorities and steps

Priority	Recommendation
1	**Data Inventory & Classification** *Figure out where the important date lives. Start there.*
2	**Encryption** *Pick what works best for your business, critical data first.*
3	**Awareness & Training** *For travelers/remote workers, critical data handlers & everyone else.*
4	**Process, Process, Process** *Helpdesk authentication, termination process, contractor lifecycle, etc.*
5	**Segmentation & Separation of Duties** *Networks & employees– don't let the fox (or the hens!) watch the henhouse*
6	**Know Thy Perimeter** *Wireless audits & overall vulnerability management prevent "easy" hacks*
7	**Develop Secure Applications** *Cheapest and best means of protecting applications is to develop them securely*
8	**New Technical Solutions** *Do the basics but also consider solutions such as data leakage & lojack*

Internet Crime Workshop

Deborah Platt Majoras

Chairman

Federal Trade Commission

(United States)

Internet Crime Workshop

US task force report on identity theft

www.idtheft.gov/reports/StrategicPlan.pdf

www.idtheft.gov/reports/VolumeII.pdf

Internet Crime Workshop

Contact us

Federal Trade Commission

600 Pennsylvania Avenue, N.W.
Washington D.C. 20580

United States

www.ftc.gov