

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

29^e 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



NNEDV

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 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



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?



SpoofCard 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](#)

SPOOFCARD 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

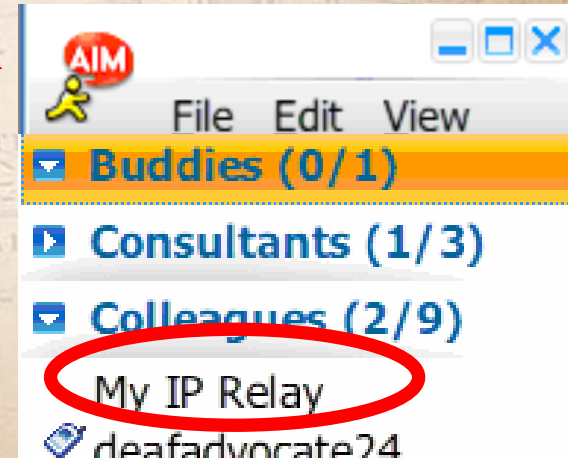
- 120 Minutes talk time
- Caller ID Spoofing
- Voice Changer



IP Relay, 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

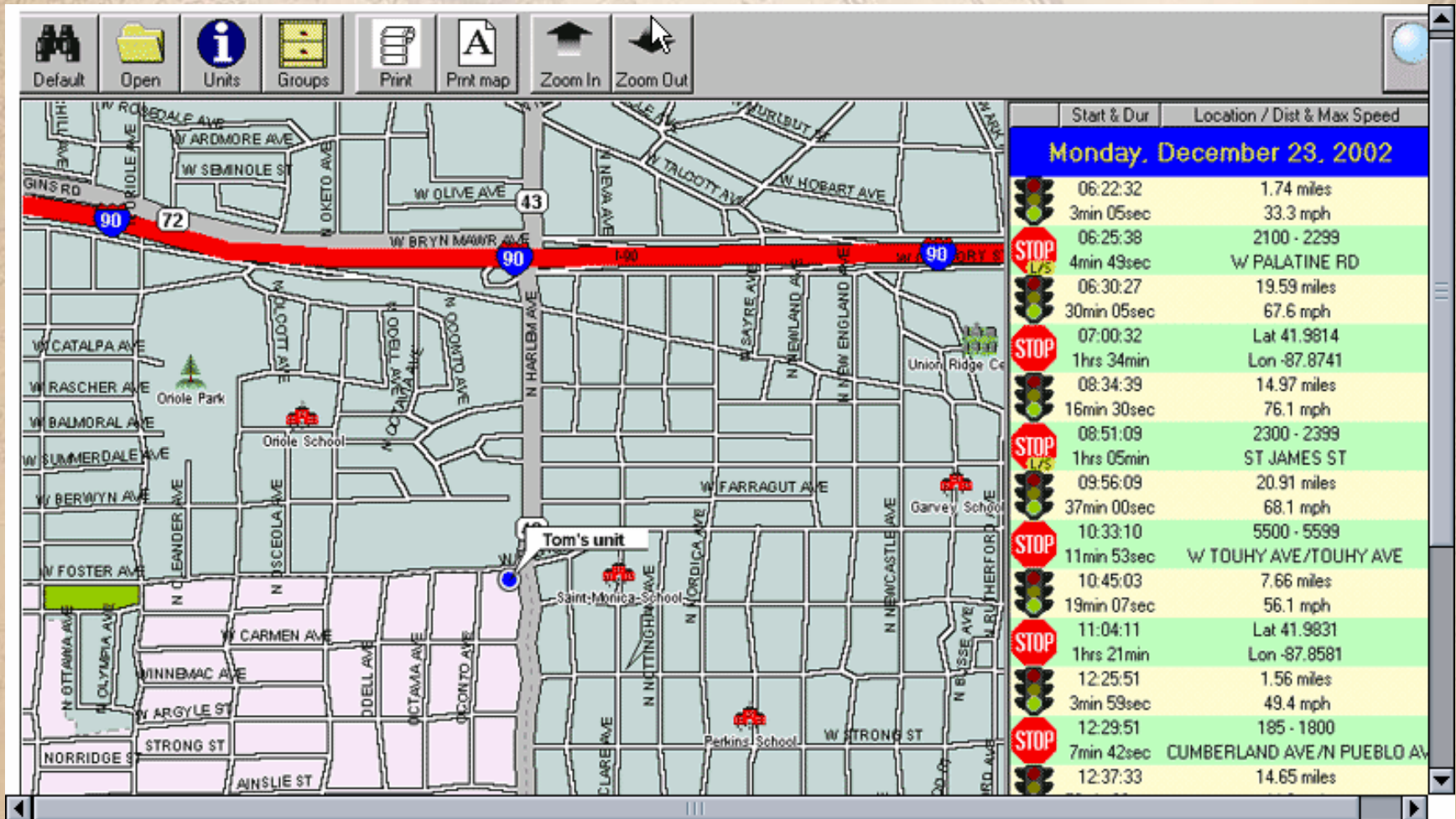
VICTIM  SERVICES

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

Email for help



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.

find your friends fast!



share your location automatically
find events and places
connect to friends

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



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.

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



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

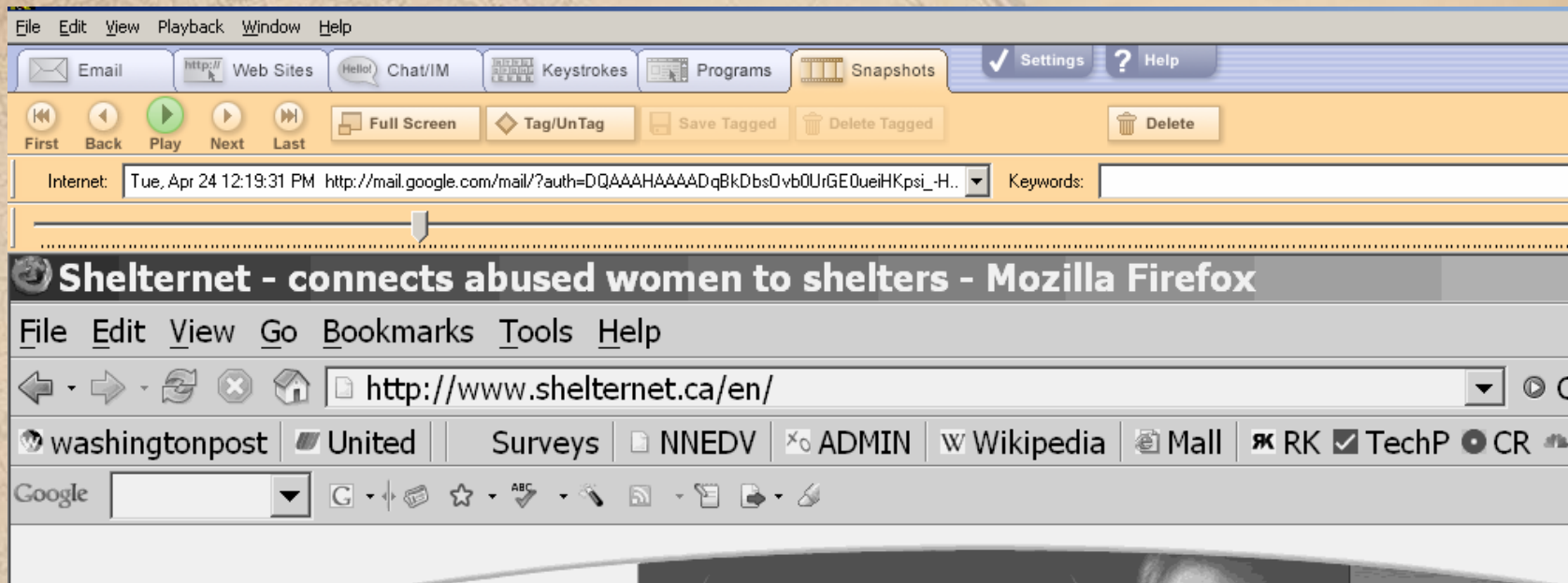
A 6-year-old girl, accompanied by BBC's Inside Out television program reporter, attached a keystroke logging device to an MP's computer. MP Anne Milton agreed to leave her computer unattended for one minute; the child attached a keystroke logger within 15 seconds. The girl brought the device undetected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

SpyWare Records Every Keystroke Typed

The screenshot shows a spyware application window 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 window is a table with three columns: Program, Key Count, and Program Start Date. The table lists various programs and their corresponding key counts and start dates. The row for 'Firefox' with a key count of 22 is highlighted. At the bottom of the window, 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



Spyware
Records
Images or
“screenshots”
every second

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

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

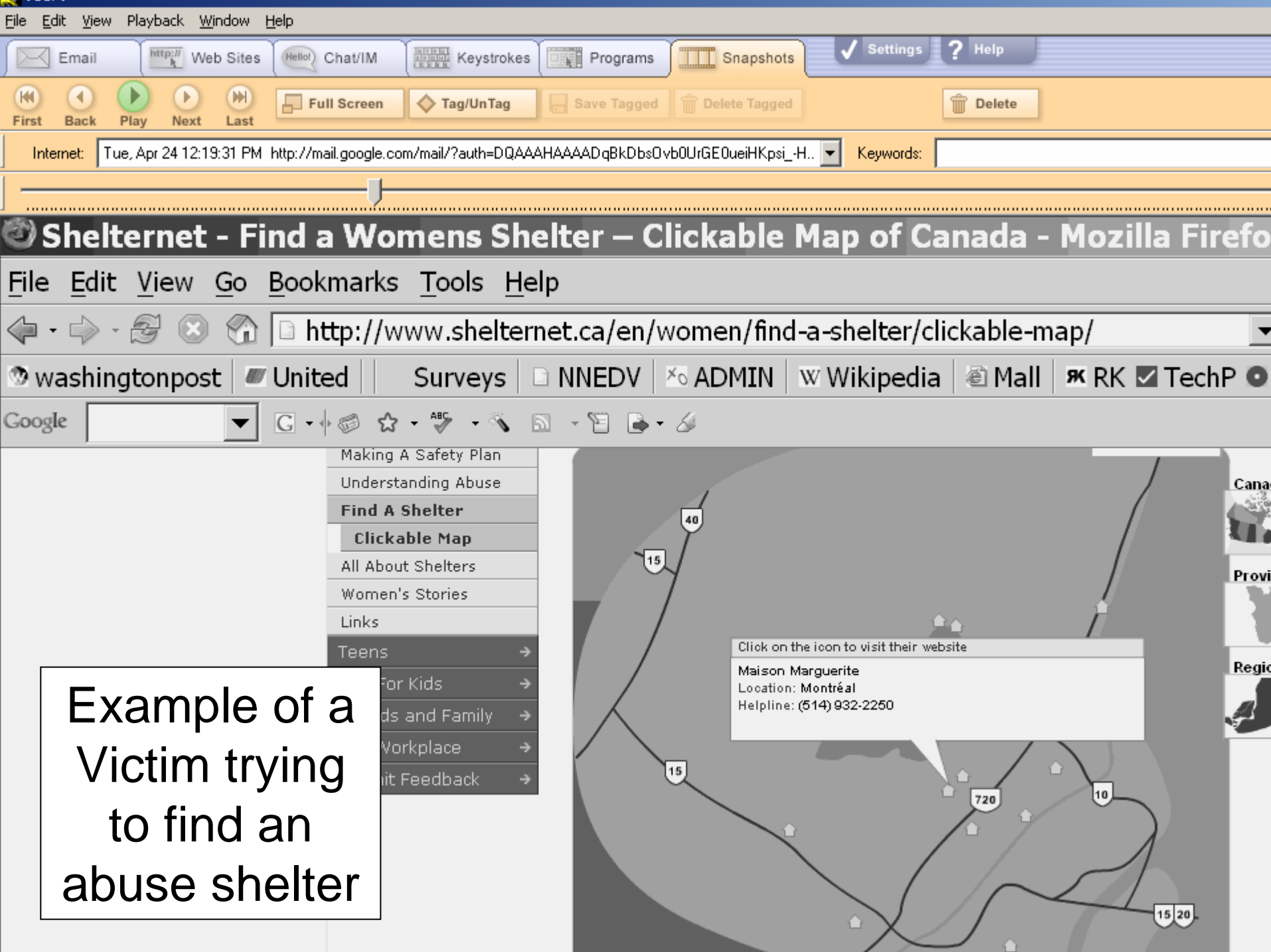
Women's Shelter Sponsored Link
www.IntervalHouse.on.ca Get Help For Domestic Violence. Housing, Counseling & More. Call Us

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

Example of a victim searching for help on the Web



Internet: Tue, Apr 24 12:19:31 PM http://mail.google.com/mail/?auth=DQAAAHAAAADqBkDbsDvb0UrGE0ueiHKpsi_H..

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**
- All About Shelters
- Women's Stories
- Links
- Teens →
- For Kids →
- ds and Family →
- Workplace →
- it Feedback →



Example of a Victim trying to find an abuse shelter

Example of a Victim trying to learn about Internet Histories

Shelternet - Hide Your Internet Activities - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.shelternet.ca/en/women/internet-safety/

washingtonpost United Surveys NNEDV ADMIN Wikipedia Mail RK TechP CR nbc

Google

Your browser
Clearing cache & history
About cookies
Internet privacy
Address book
Instant messaging
Groups, forums,
A Safety Plan
Standing Abuse
Shelter
Out Shelters
n's Stories
or Kids
s and Family
The Workplace

more difficult for someone to track your activities. They are described through the links below. If your abuser knows his or her way around computers it might be better for you to use a computer outside the home - at a library, school, internet café or a friend's house.

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.

Internet Safety Tips

When your computer asks whether you want it to remember your password always click on the NO box. If the computer remembers your password, it can be clue that you have visited a web site.

Your Feedback

We welcome your feedback. Help us make Shelternet's web site even better! ▶

Questions and Answers about Internet Safety

1. Can my activity on the internet really be tracked? For example, could my abuser tell what sites I have visited?
2. I'm not sure what type of browser I use. How can I find out?
3. Is there anything I can do to prevent someone from seeing what sites I have been on?

Internet: Fri, Aug 17 05:17:33 PM http://www.google.com/webhp?sourceid=navclient&ie=UTF-8

Keywords:

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

Google - Windows Internet Explorer

http://www.google.com/webhp?sourceid=navclient&ie=UTF-8

File Edit View Favorites Tools Help Google G Go Popups okay Check Translate

Google

Web Images Video News Maps G

Delete Browsing History

Please wait while the browsing history is deleted.
Deleting history...

Cancel

Cookies
Files stored on your computer by websites to save preferences such as login information.
Delete cookies...

History
List of websites you have visited.
Delete history...

Form data
Saved information that you have typed into forms.
Delete forms...

Passwords
Passwords that are automatically filled in when you log on to a website you've previously visited.
Delete passwords...

About deleting browsing history Delete all... Close

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@nnev.org

<http://www.nnev.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

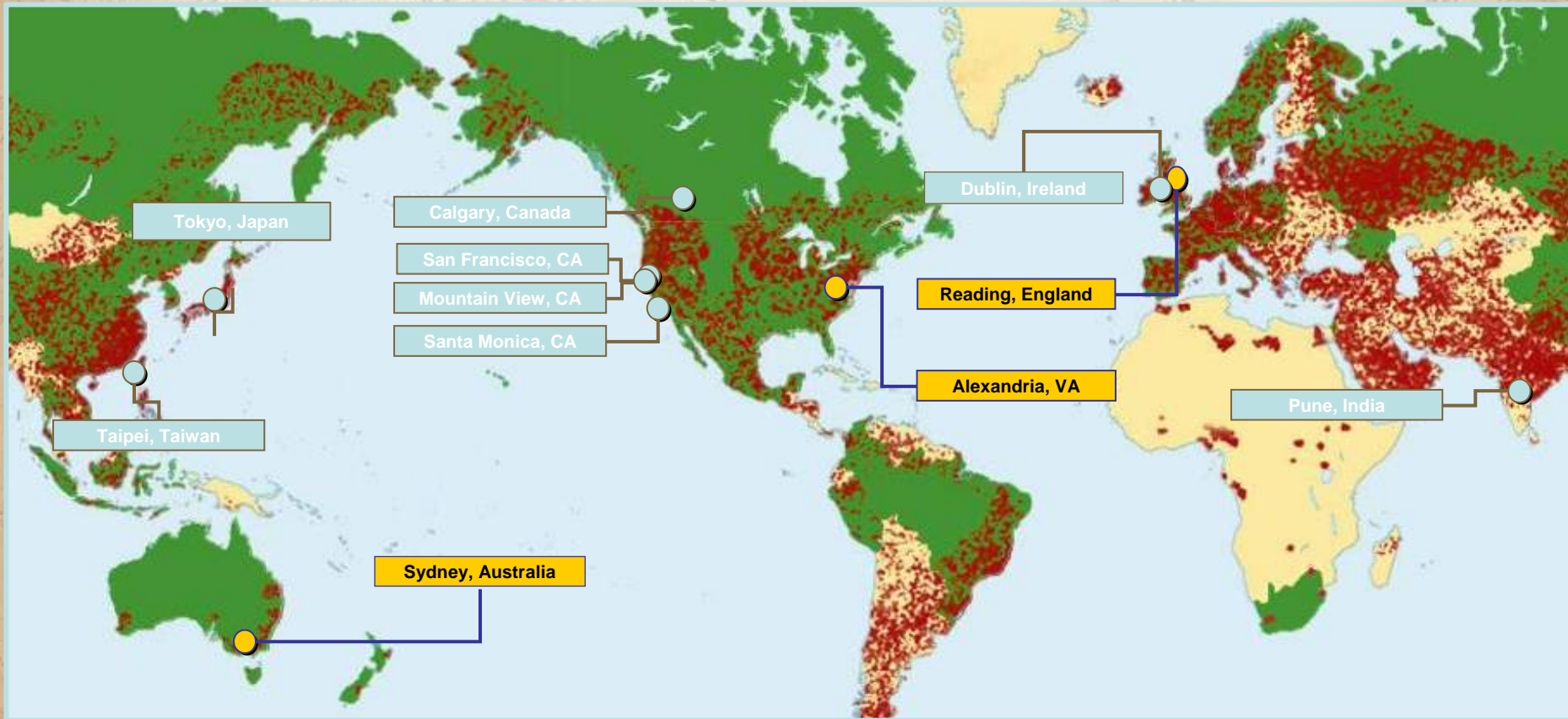
3 Symantec SOCs

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...

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

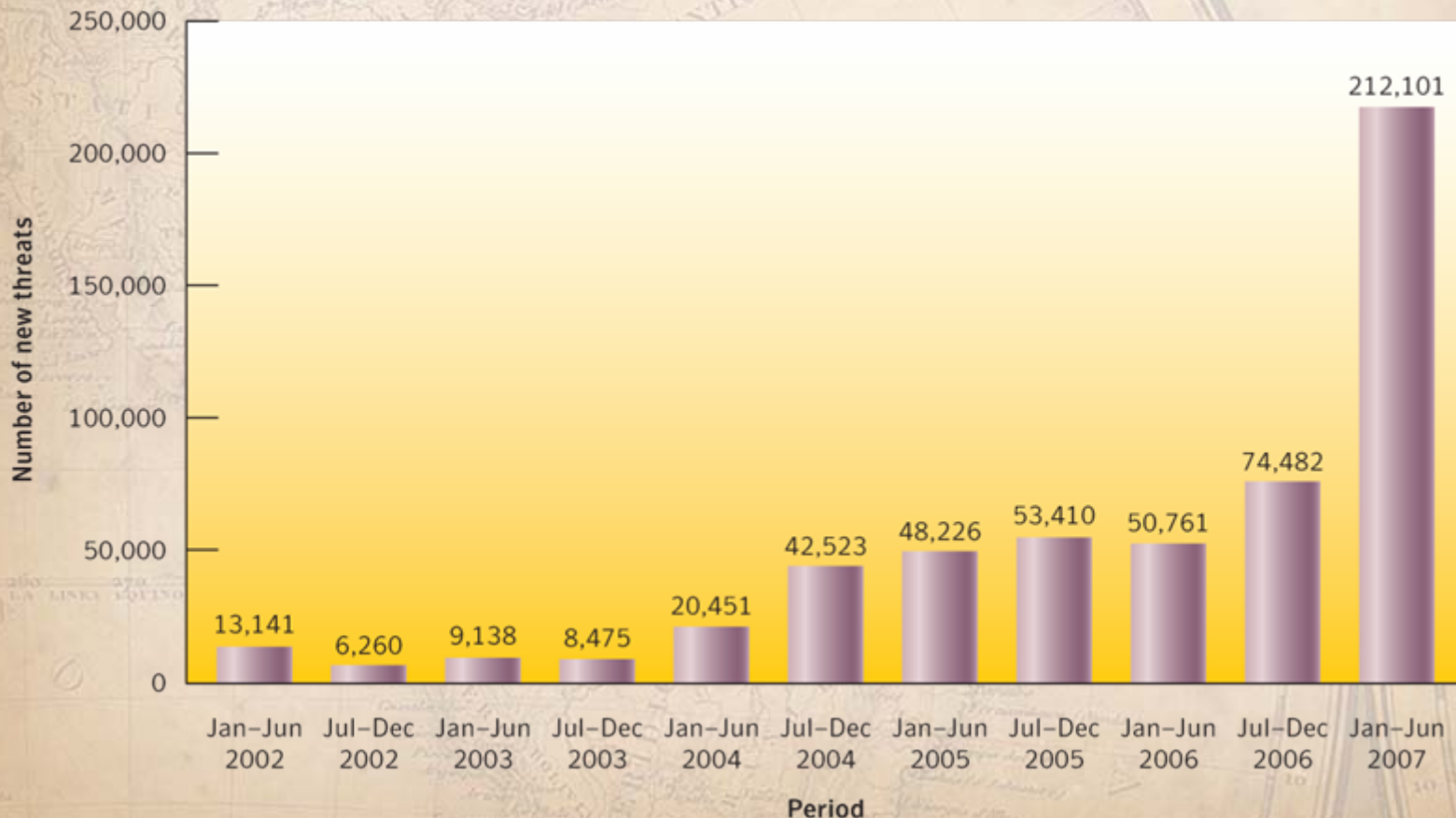
NETWORK WORLD NEWSLETTER
 Sign up for some of our Network Security newsletters.

Security in Practice
 Virus and Bug Patch Alert

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

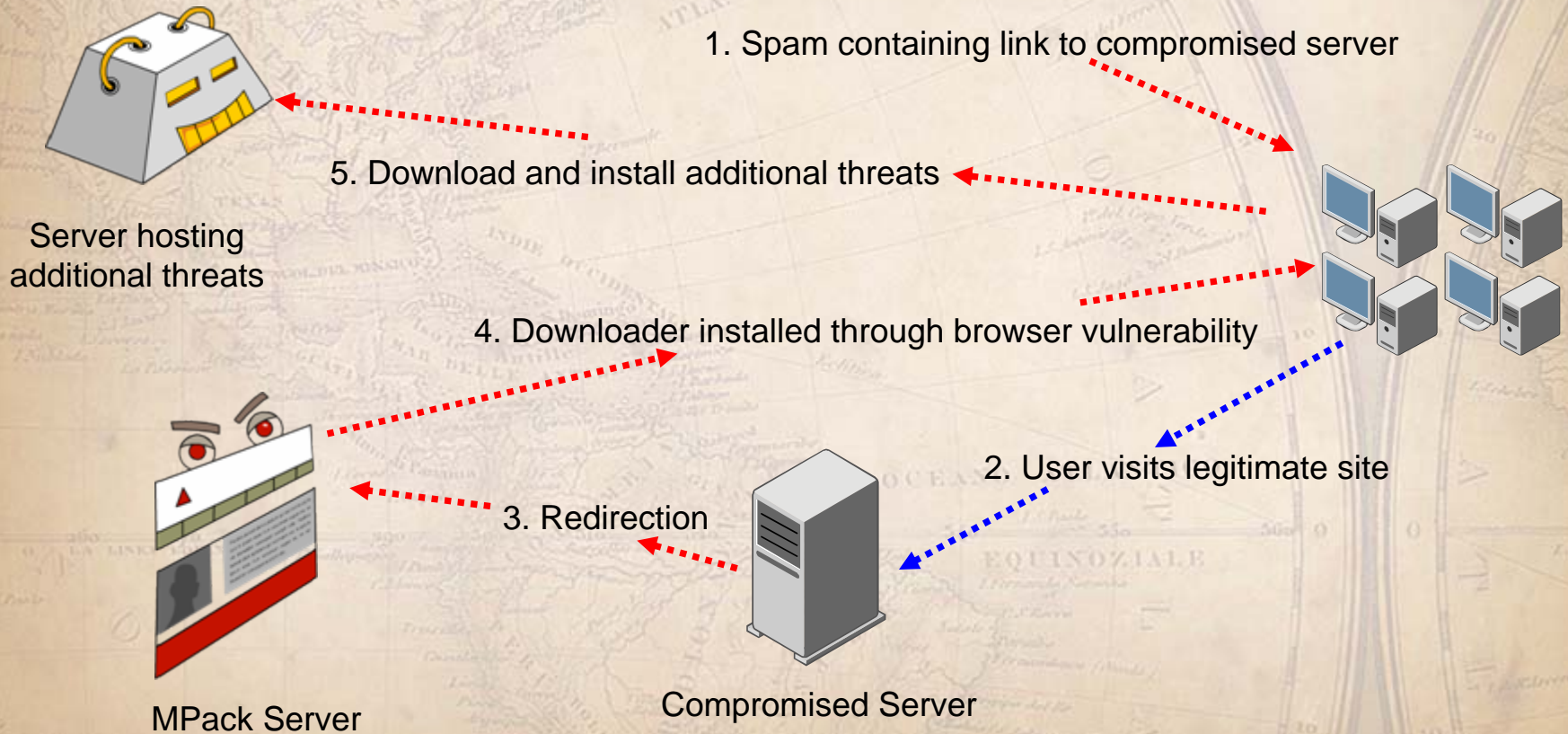
...and business is booming!

- 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



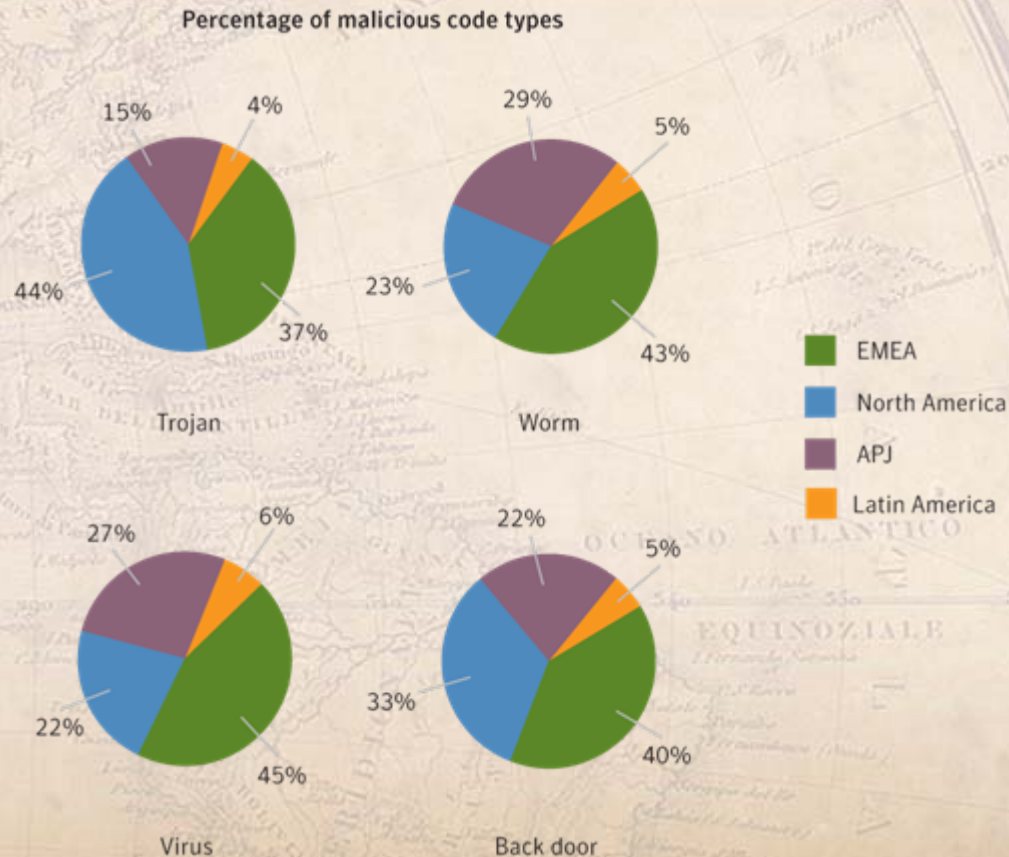
Change in Tactics and Targets



- 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

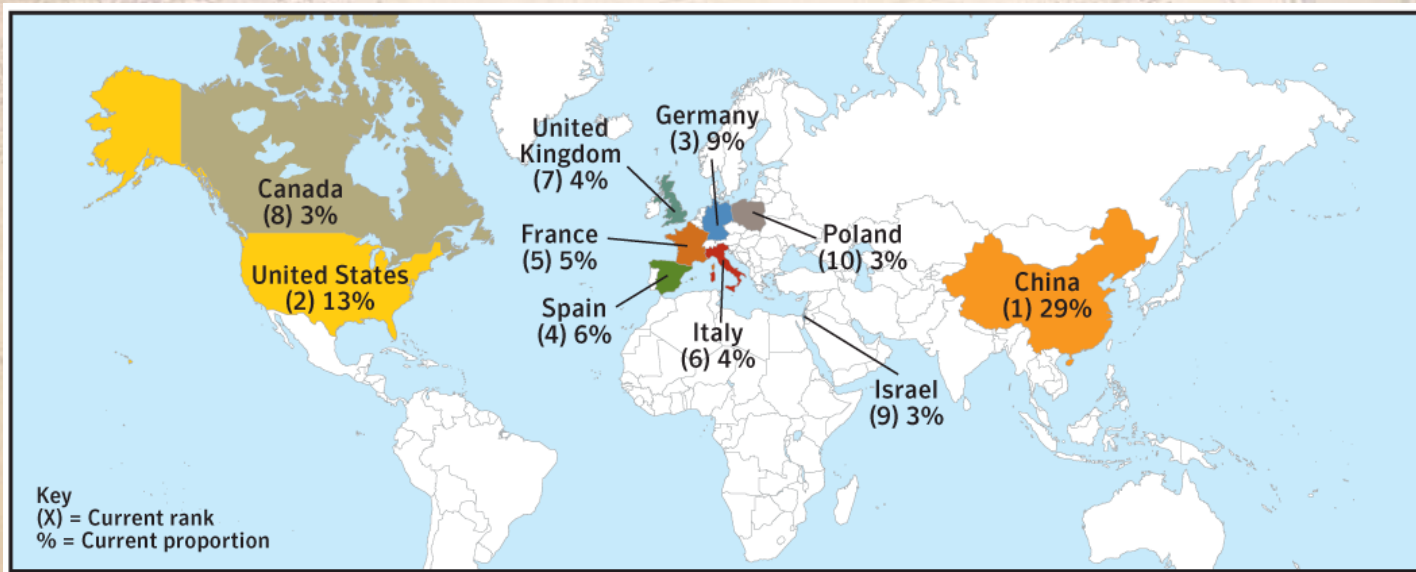
Global locations of fraud

- ▶ 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%

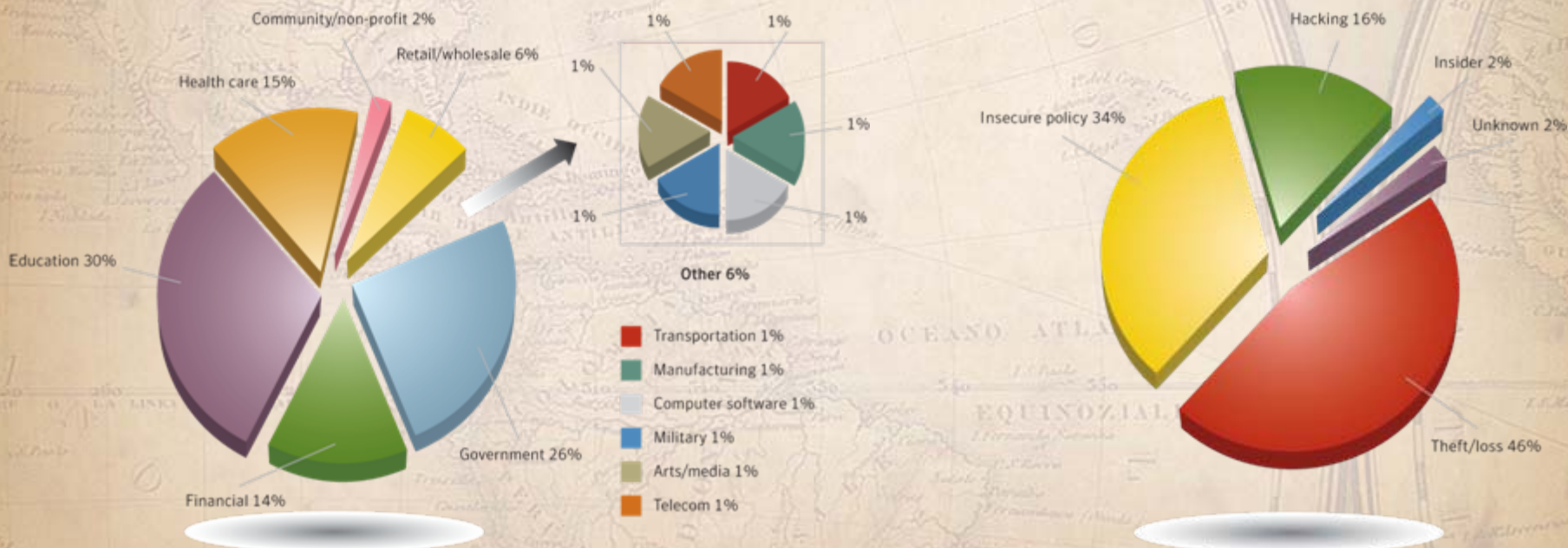
Global attack infrastructures

- ▶ 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.



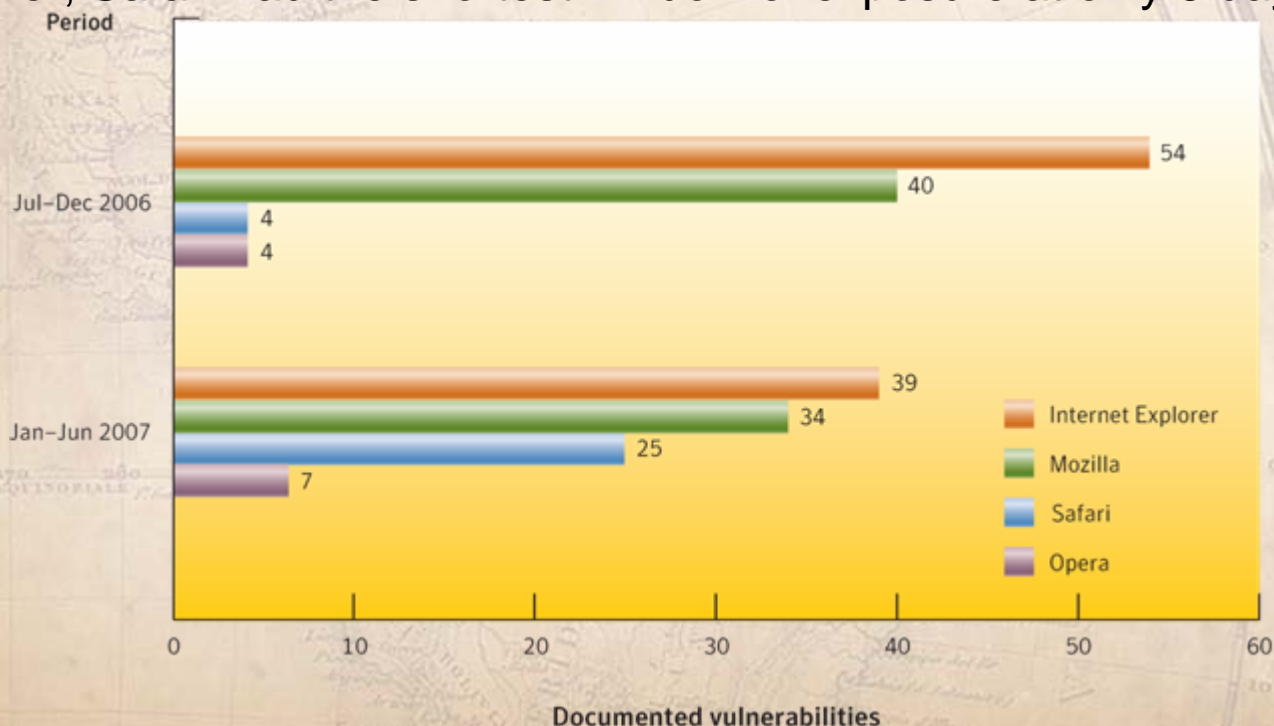
Global underground economies

- ▶ 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

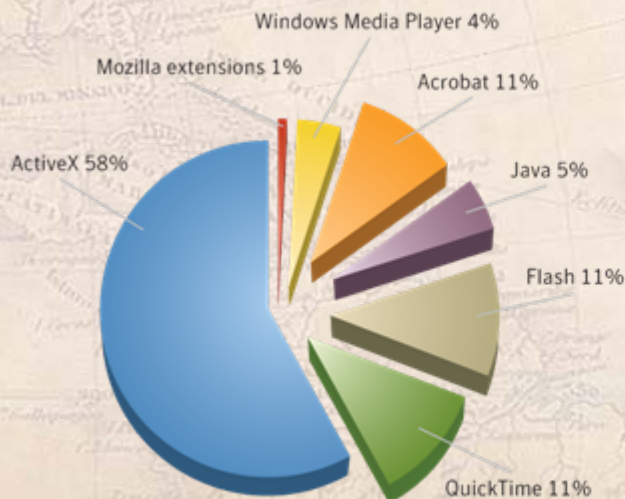
- ▶ Microsoft had the highest number of documented vulnerabilities with 39 followed by Mozilla with 34. Both these vendors also had the highest window of exposure at 5 days each.
- ▶ There were 25 vulnerabilities documented in Safari this period, a significant increase from the 4 documented in the last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



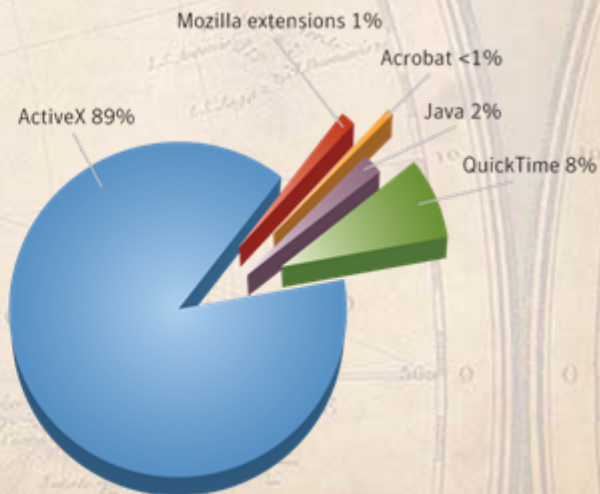
Target technologies - Plug-ins

- ▶ 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.

Percentage of vulnerabilities



Jul-Dec 2006



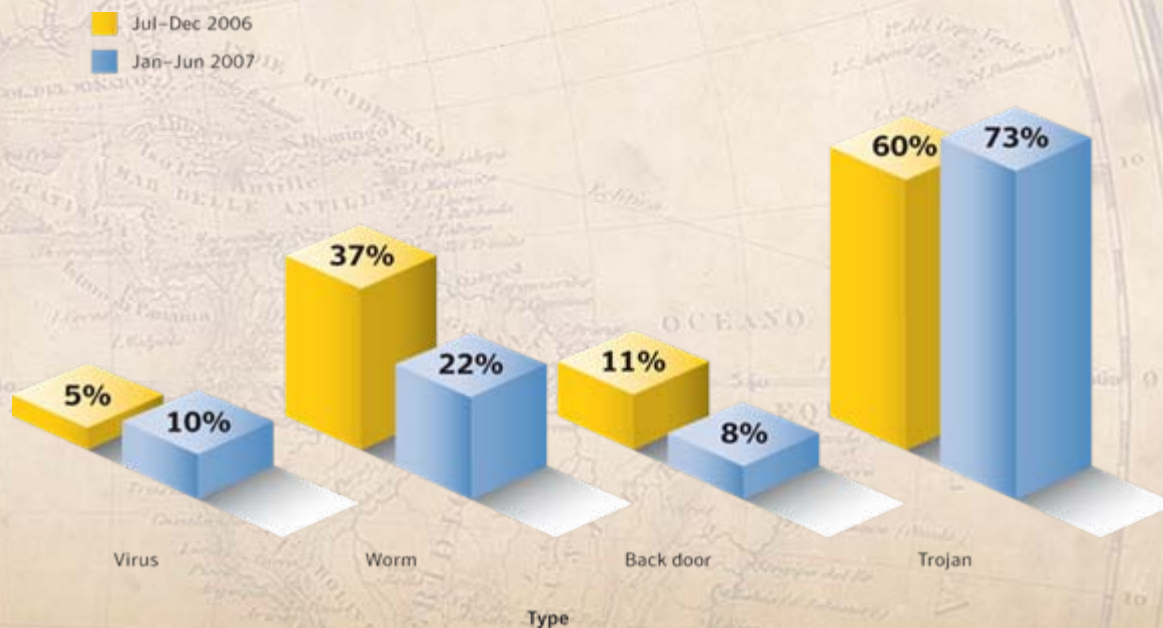
Jan-Jun 2007

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.

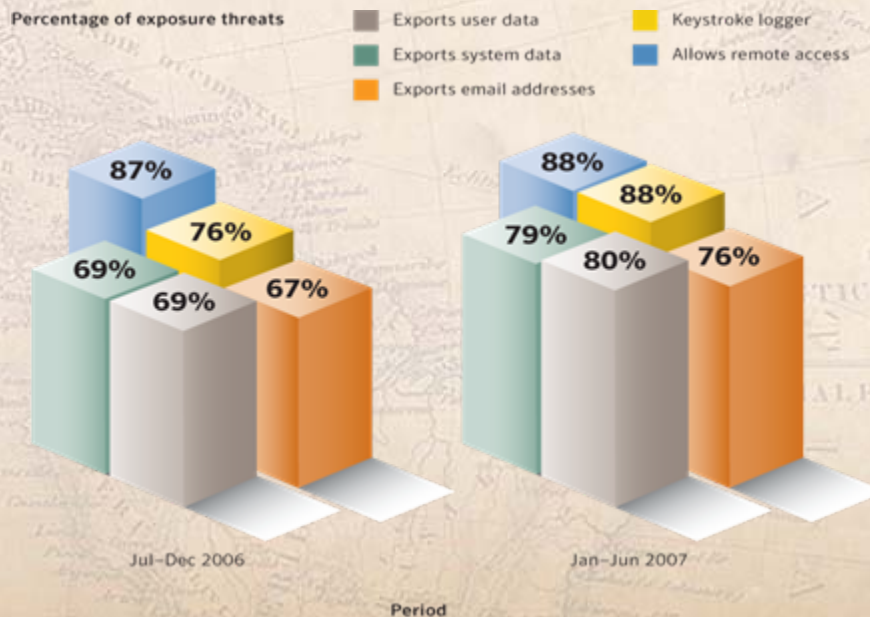
Methods - Malicious code

- ▶ 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.



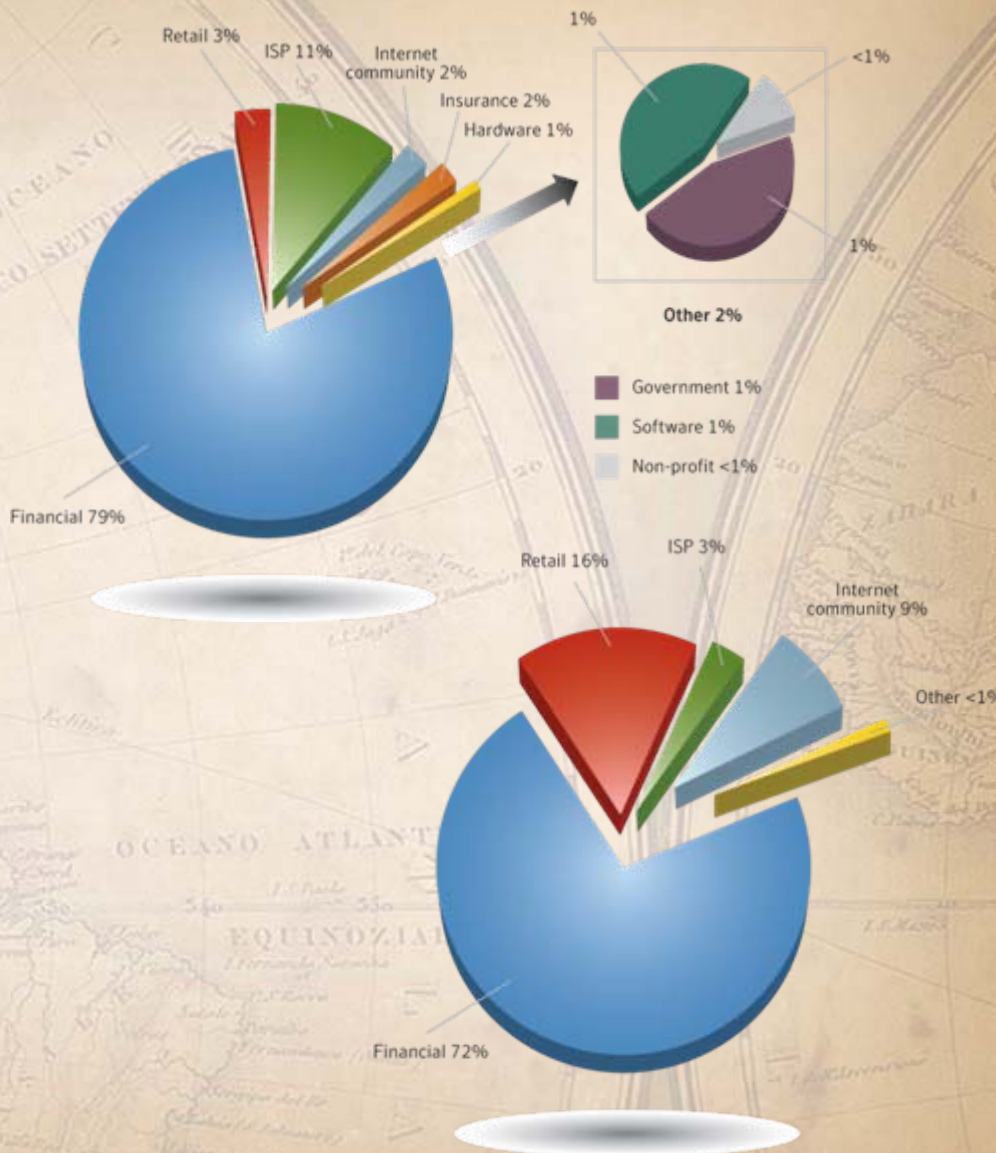
Methods - Propagation

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

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/Volumell.pdf

Internet Crime Workshop

Contact us

Federal Trade Commission

600 Pennsylvania Avenue, N.W.

Washington D.C. 20580

United States

www.ftc.gov