

HACKER
Cracked on 12/25/85
by Mr. Clean

The Bank 303-771-7531



One more Virus Alert
or Hacker and
MySpace Is Gone!



Sicurezza e Internet 01



Alcune statistiche recenti

- For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations.
- 522 security professionals responded.



<http://www.gocsi.com/>

2008

CSI Computer Crime & Security Survey

The latest results from the longest-running project of its kind

By Robert Richardson, CSI Director

For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations. Over 500 security professionals responded. Their answers are inside...

Alcune statistiche recenti

The most expensive computer security incidents were those involving financial fraud...

...with an average reported cost of close to \$500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with “bot” computers within the organization’s network, reported to cost an average of nearly \$350,000 per respondent. The overall average annual loss reported was just under \$300,000.

Virus incidents occurred most frequently...

...occurring at almost half (49 percent) of the respondents’ organizations. Insider abuse of networks was second-most frequently occurring, at 44 percent, followed by theft of laptops and other mobile devices (42 percent).

Almost one in ten organizations reported they’d had a Domain Name System incident...

...up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.

Alcune statistiche recenti

Twenty-seven percent of those responding to a question regarding “targeted attacks”...

...said they had detected at least one such attack, where “targeted attack” was defined as a malware attack aimed exclusively at the respondent’s organization or at organizations within a small subset of the general business population.

The vast majority of respondents said their organizations either had (68 percent)...

...or were developing (18 percent) a formal information security policy. Only 1 percent said they had no security policy.

Alcune statistiche recenti

Cyber Crime Statistics from the Annual Computer Crime and Security Survey*

- **Between 2006 and 2007 there was a net increase in IT budget spent on security.**
- **Significantly, however, the percentage of IT budget spent on security awareness training was very low, with 71% of respondents saying less than 5% of the security budget was spent on awareness training, 22% saying less than 1% was spent on such training.**
- **71% of respondents said their company has no external insurance to cover computer security incident losses.**
- **90% of respondents said their company experienced a computer security incident in the past 12 months.**
- **64% of losses were due to the actions of insiders at the company.**

The top 3 types of attack, ranked by dollar losses, were:

- **financial fraud (\$21.1 million)**
- **viruses/worms/trojans (\$8.4 million)**
- **system penetration by outsiders (\$6.8 million)**

http://www.computer-forensics-recruiter.com/home/cyber_crime_statistics.html

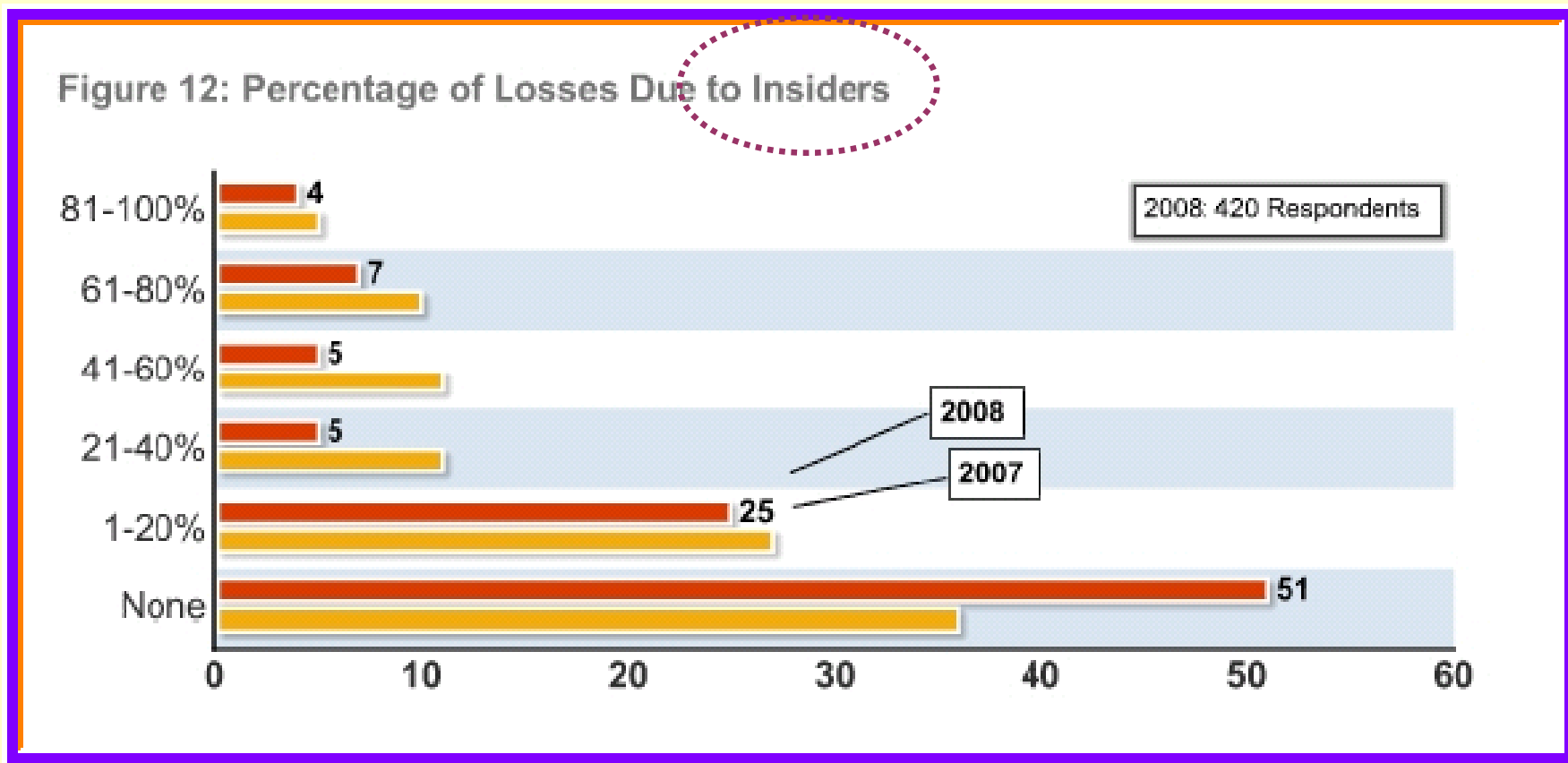
Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches



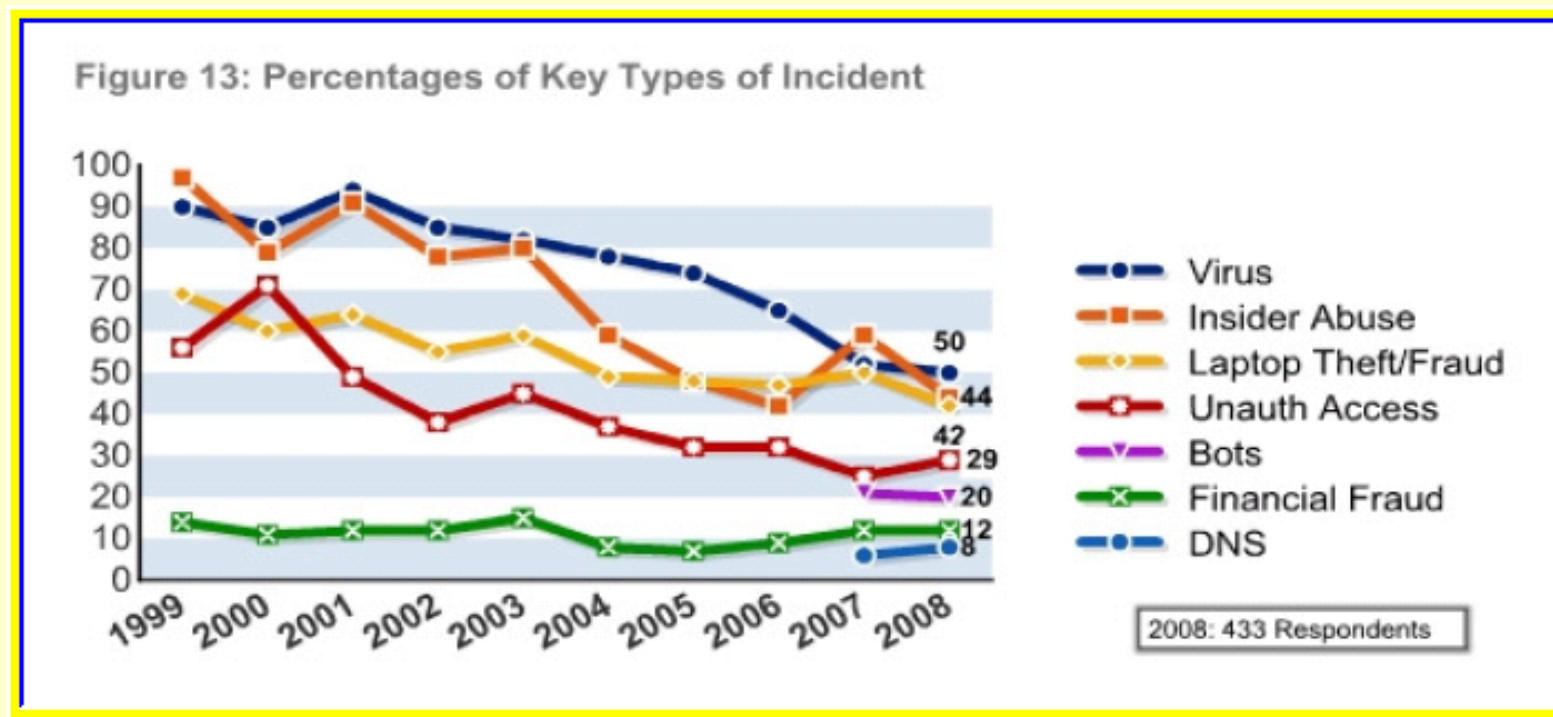
Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches



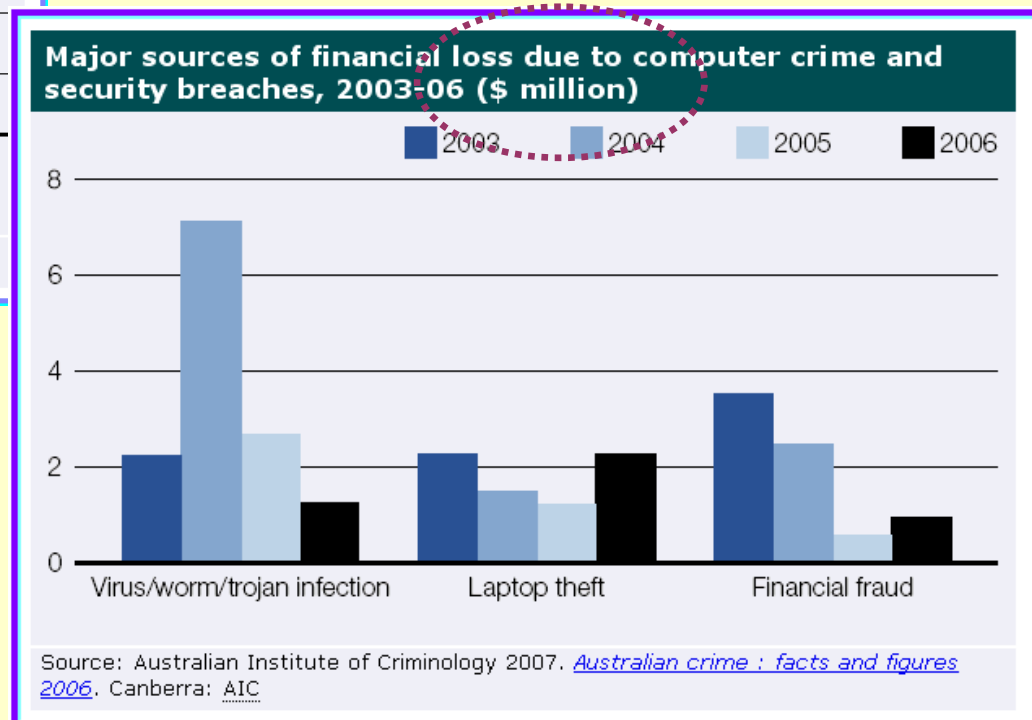
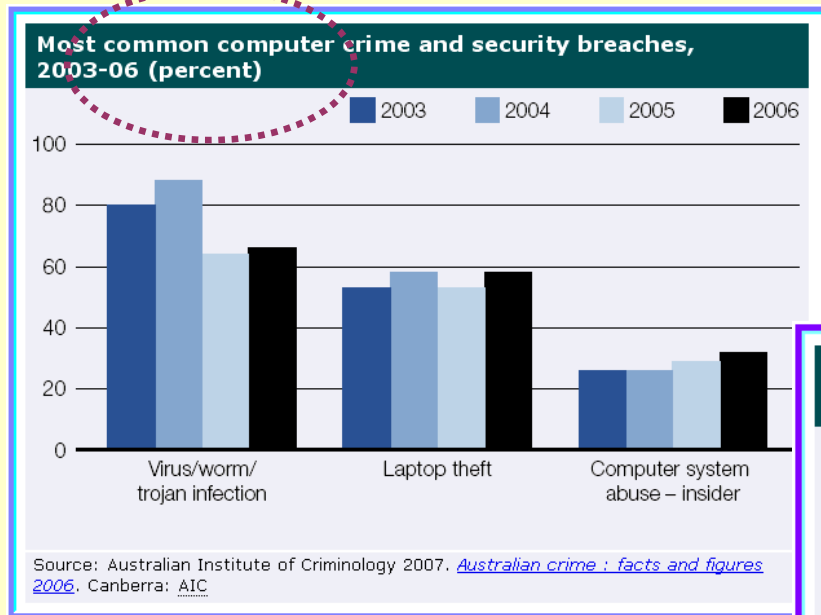
Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches



Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches

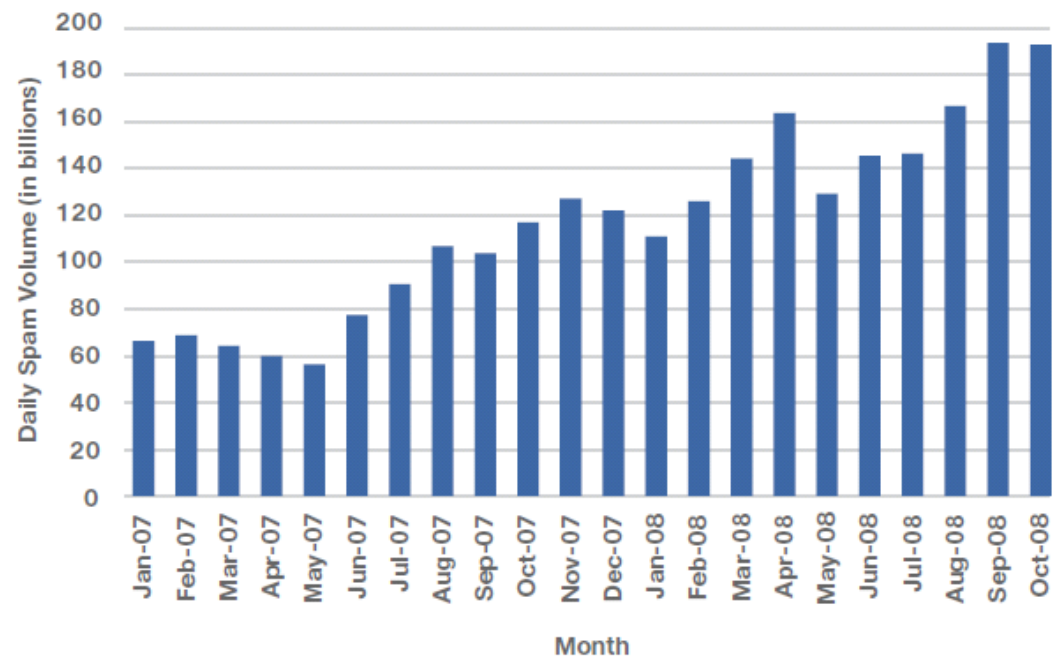


Lo SPAM

Spam by Originating Country for 2008

| Originating Country | Percentage of Global Spam |
|---------------------|---------------------------|
| USA | 17.2% |
| Turkey | 9.2% |
| Russia | 8.0% |
| Canada | 4.7% |
| Brazil | 4.1% |
| India | 3.5% |
| Poland | 3.4% |
| Korea | 3.3% |
| Germany | 2.9% |
| United Kingdom | 2.9% |
| Thailand | 2.8% |
| Spain | 2.8% |
| Italy | 2.4% |
| Argentina | 2.1% |
| Columbia | 2.1% |
| France | 2.0% |
| Other | 26.7% |

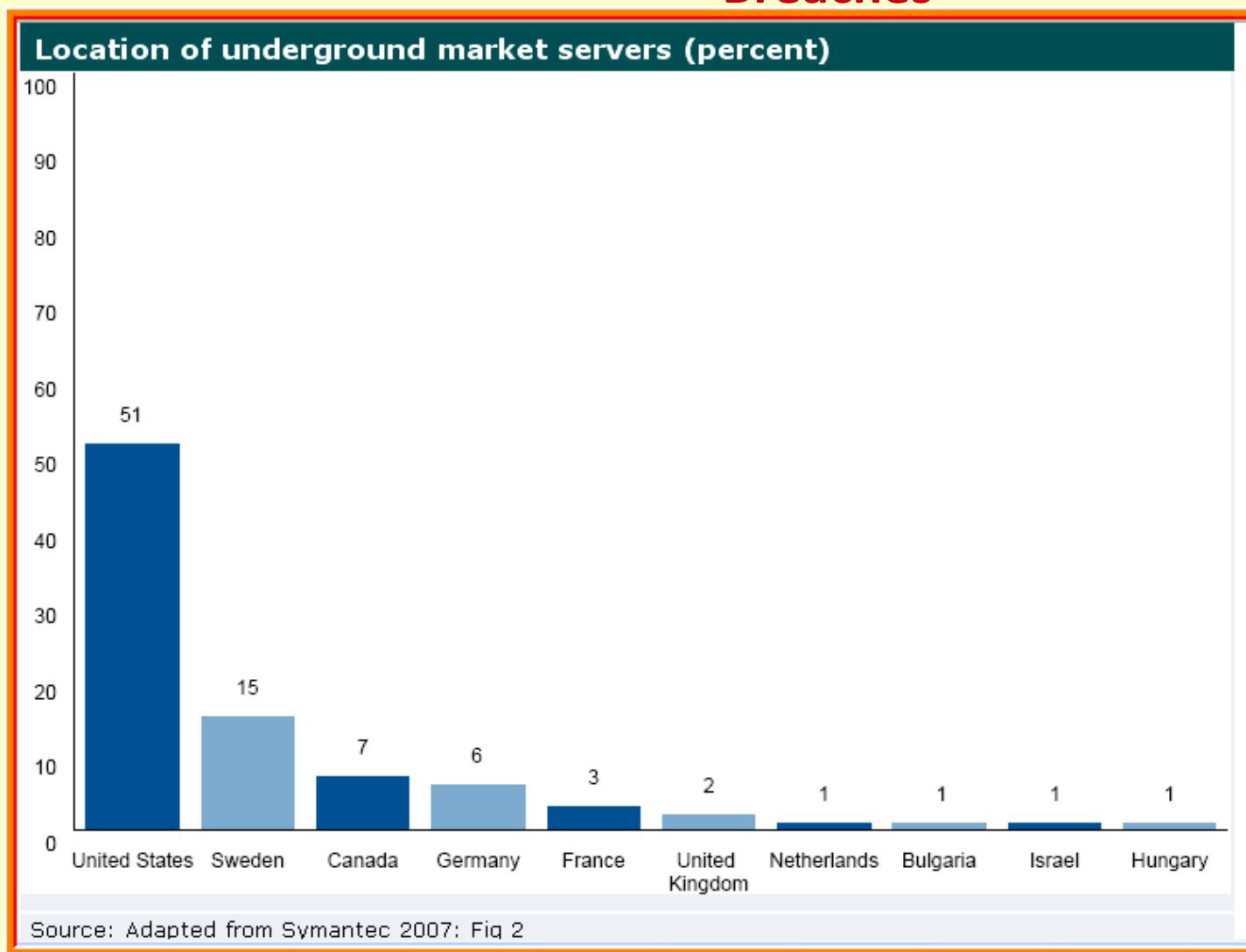
Average Daily Spam Volume



Daily spam volumes have nearly doubled in 2008 relative to 2007.

Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches



Alcune statistiche recenti

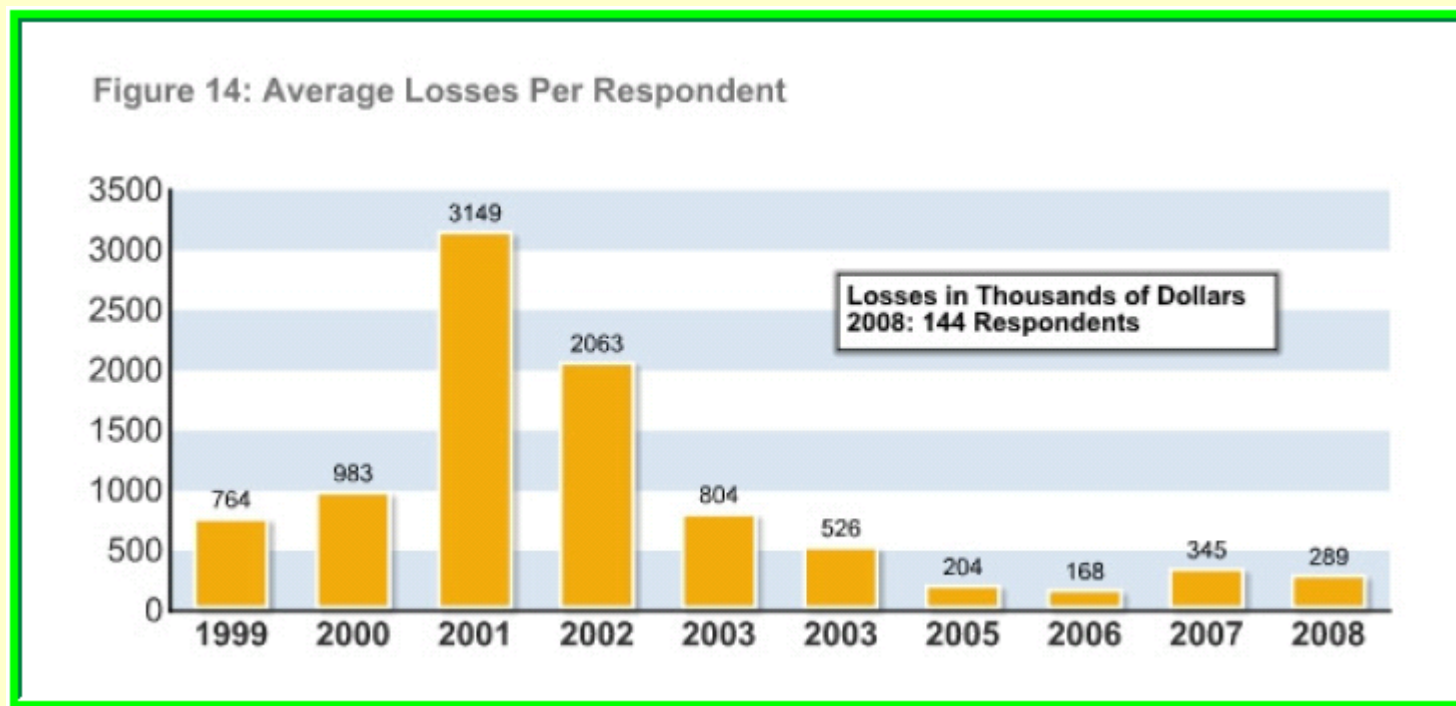
Frequency, Nature and Cost of Cybersecurity Breaches

| Table 1 | 2004 | 2005 | 2006 | 2007 | 2008 |
|--------------------------------|------|------|------|------|------|
| Denial of service | 39% | 32% | 25% | 25% | 21% |
| Laptop theft | 49% | 48% | 47% | 50% | 42% |
| Telecom fraud | 10% | 10% | 8% | 5% | 5% |
| Unauthorized access | 37% | 32% | 32% | 25% | 29% |
| Virus | 78% | 74% | 65% | 52% | 50% |
| Financial fraud | 8% | 7% | 9% | 12% | 12% |
| Insider abuse | 59% | 48% | 42% | 59% | 44% |
| System penetration | 17% | 14% | 15% | 13% | 13% |
| Sabotage | 5% | 2% | 3% | 4% | 2% |
| Theft/loss of proprietary info | 10% | 9% | 9% | 8% | 9% |
| from mobile devices | | | | | 4% |
| from all other sources | | | | | 5% |
| Abuse of wireless network | 15% | 16% | 14% | 17% | 14% |
| Web site defacement | 7% | 5% | 6% | 10% | 6% |
| Misuse of Web application | 10% | 5% | 6% | 9% | 11% |
| Bots | | | | 21% | 20% |
| DNS attacks | | | | 6% | 8% |
| Instant messaging abuse | | | | 25% | 21% |
| Password sniffing | | | | 10% | 9% |
| Theft/loss of customer data | | | | 17% | 17% |
| from mobile devices | | | | | 8% |
| from all other sources | | | | | 8% |

2008 CSI Computer Crime & Security Survey

Alcune statistiche recenti

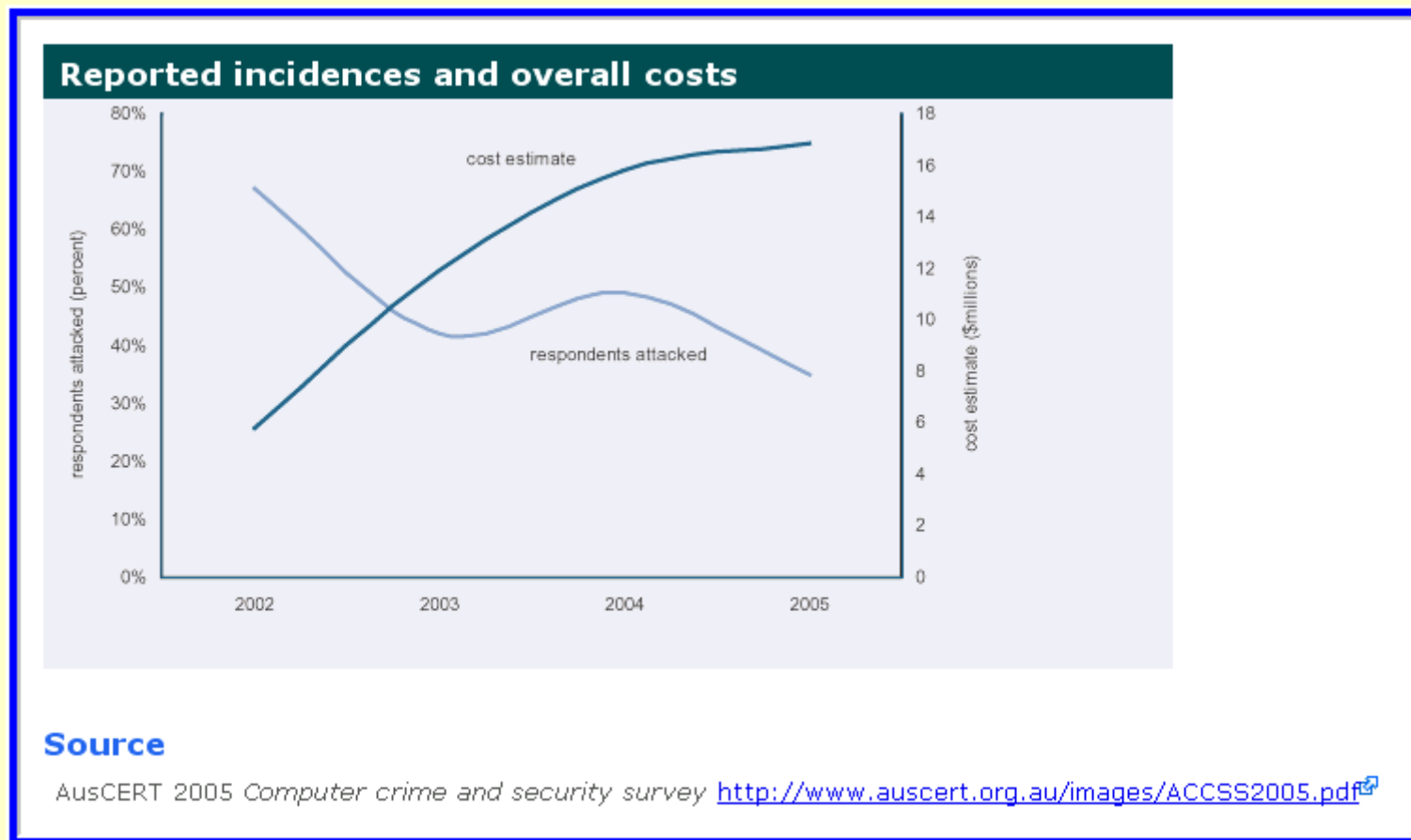
Frequency, Nature and Cost of Cybersecurity Breaches



- This year, the average loss per respondent was \$288,618, down from \$345,005 last year, but up from the low of \$167,713 two years ago.

Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches



Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches

| Table 2: Technologies Used | 2008 |
|---|------|
| Anti-virus software | 97 % |
| Anti-spyware software | 80 % |
| Application-level firewalls | 53 % |
| Biometrics | 23 % |
| Data loss prevention / content monitoring | 38 % |
| Encryption of data in transit | 71 % |
| Encryption of data at rest (in storage) | 53 % |
| Endpoint security client software / NAC | 34 % |
| Firewalls | 94 % |
| Forensics tools | 41 % |
| Intrusion detection systems | 69 % |
| Intrusion prevention systems | 54 % |
| Log management software | 51 % |
| Public Key Infrastructure systems | 36 % |
| Server-based access control lists | 50 % |
| Smart cards and other one-time tokens | 36 % |
| Specialized wireless security systems | 27 % |
| Static account / login passwords | 46 % |
| Virtualization-specific tools | 29 % |
| Virtual Private Network (VPN) | 85 % |
| Vulnerability / patch management tools | 65 % |
| Web / URL filtering | 61 % |
| Other | 3 % |

2008 CSI Computer Crime & Security Survey

Alcune statistiche recenti

Frequency, Nature and Cost of Cybersecurity Breaches

Figure 20: Actions Taken After an Incident

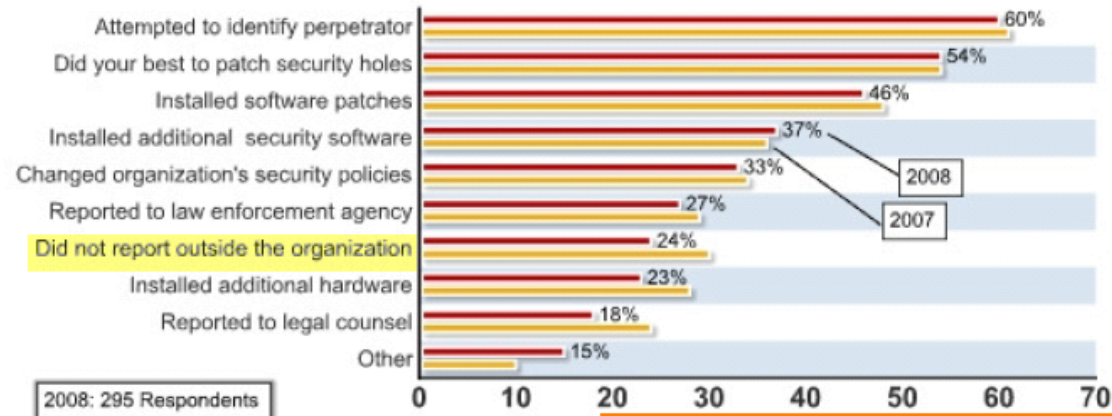
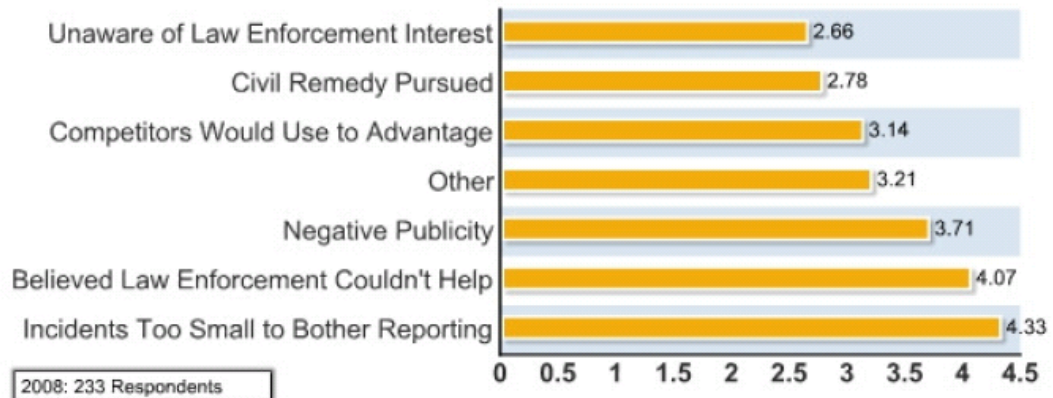


Figure 21: Reasons for Not Reporting

Average response on a 1 to 7 scale, with 1 "of no importance" and 7 "of great importance"



La più grande frode conosciuta



La più grande frode conosciuta



The image is a screenshot of an MSNBC news website. At the top left is the MSNBC logo. To its right is a search bar and navigation links for 'Today Show', 'Nightly News', 'Dateline', and 'Meet the Press'. Below the navigation is a breadcrumb trail: 'Technology & science / Security'. On the left side, there is a vertical menu with categories like 'U.S. news', 'World news', 'Politics', 'Business', 'Sports', 'Entertainment', 'Tech & science', 'Space', 'Science', 'Tech and gadgets', 'Games', and 'Style'. The main article is titled 'T.J. Maxx data theft worse than first reported' in red text, with a subtitle 'Data stolen covers transactions dating as far back as December 2002'. The byline is 'Ap Associated Press' and the update time is 'updated 3:31 p.m. ET March 29, 2007'. The article text states that information from at least 45.7 million credit and debit cards was stolen by hackers who accessed TJX's customer information in a security breach that the discount retailer disclosed more than two months ago. It also mentions that TJX Cos., the owner of about 2,500 stores, said in a regulatory filing late Wednesday that about three-quarters of those cards had either expired at the time of the theft, or data from their magnetic strips had been masked — stored as asterisks rather than numbers. To the right of the article is a 'FREE VIDEO' section with a thumbnail image of a T.J. Maxx store sign.

msnbc featuring [Today Show](#) [Nightly News](#) [Dateline](#) [Meet the Press](#)

Technology & science / Security

T.J. Maxx data theft worse than first reported

Data stolen covers transactions dating as far back as December 2002

Ap Associated Press
updated 3:31 p.m. ET March 29, 2007

BOSTON - Information from at least 45.7 million credit and debit cards was stolen by hackers who accessed TJX's customer information in a security breach that the discount retailer disclosed more than two months ago.

TJX Cos., the owner of about 2,500 stores, said in a regulatory filing late Wednesday that about three-quarters of those cards had either expired at the time of the theft, or data from their magnetic strips had been masked — stored as asterisks rather than numbers.

FREE VIDEO



Corporate Liability – About the Company

TJX is the parent company of a family of discount retailers

United States

Marshalls

TJ-Maxx

HomeGoods

Canada

Winners

HomeSense

UK, Ireland, Germany

TK-Maxx

Corporate Liability – How it Happened

Attack originated at a Marshalls store in St. Paul, Minnesota

Attackers used telescope-shaped antenna to read WiFi



- WiFi enabled price scanners targeted to get network access info
- Once on the network, database was targeted
- Data harvesting started mid 2005 and carried through end of 2006

Corporate Liability – What was affected

Initially thought to be 45.6M

credit card numbers

compromised, later

updated to 94M

Included Track 2 Data

Over 80 GB of network

traffic send to outside

server

94,000,000



Biggest credit card number heist in history

Corporate Liability – Example of use

- Nov. '06 Florida law enforcement claims at least 10 thieves used credit card data in a gift card scheme
- Over \$8M in gift cards purchased
- 6 people tied to gift card scheme were arrested
- Gift card scheme was carried out months before TJX discovered the compromise

Corporate Liability – Aftermath

- Believed to be responsible for between \$68M and \$83M fraud in over 13 countries
- Class-action consumer lawsuit settled
 - \$20 store voucher
 - 3 years credit monitoring
 - \$20,000 ID Theft Coverage
- Banks and financial institutions sued
 - Yet to be determined
- Estimated costs to TJX are over ~~\$150M~~ **\$250M**

Corporate Liability – Conclusions

- Every company needs to be concerned
- Does not have to be credit cards
- Governments creating laws requiring disclosure
- One incident can cost much more than years of a quality security infrastructure



Le Previsioni

I Trend

Alcune previsioni recenti

To get the experts' consensus view of the cybercrime landscape, the authors conducted an online survey of 260 tech-security professionals. The survey was conducted in February and March 2007, and produced two major findings. The first was that there is a consensus expectation among security experts that computer intrusions, data theft, and identity fraud will continue on the upswing for the foreseeable future.

Criminals' use of the following attack vectors will track as follows through 2010:

| | Decline | Stay the same | Rise |
|-----------------------------------|---------|---------------|-------|
| Viral e-mail attachments | 25.2% | 28.3% | 46.5% |
| Botnets | 5.7% | 17.3% | 77.0% |
| Phishing scams | 7.1% | 12.5% | 80.3% |
| Keyloggers | 7.6% | 23.7% | 68.7% |
| Rootkits | 5.0% | 27.5% | 67.6% |
| Browser-based exploits | 12.9% | 17.9% | 69.2% |
| Insider theft of personal data | 2.7% | 23.0% | 74.4% |
| Database hacking of personal data | 3.5% | 18.6% | 77.9% |

Alcune previsioni recenti

Consumers' exposure to the following types of identity theft will track as follows through 2010:

| | Decline | Stay the same | Rise |
|---------------------------------------|---------|---------------|------|
| Personal data gets stolen | 1% | 7% | 91% |
| Credit card gets used in fraud | 3% | 22% | 75% |
| Debit card gets used in fraud | 3% | 24% | 73% |
| Funds hijacked from an online account | 4% | 18% | 77% |
| Data gets used in new account fraud | 2% | 13% | 85% |

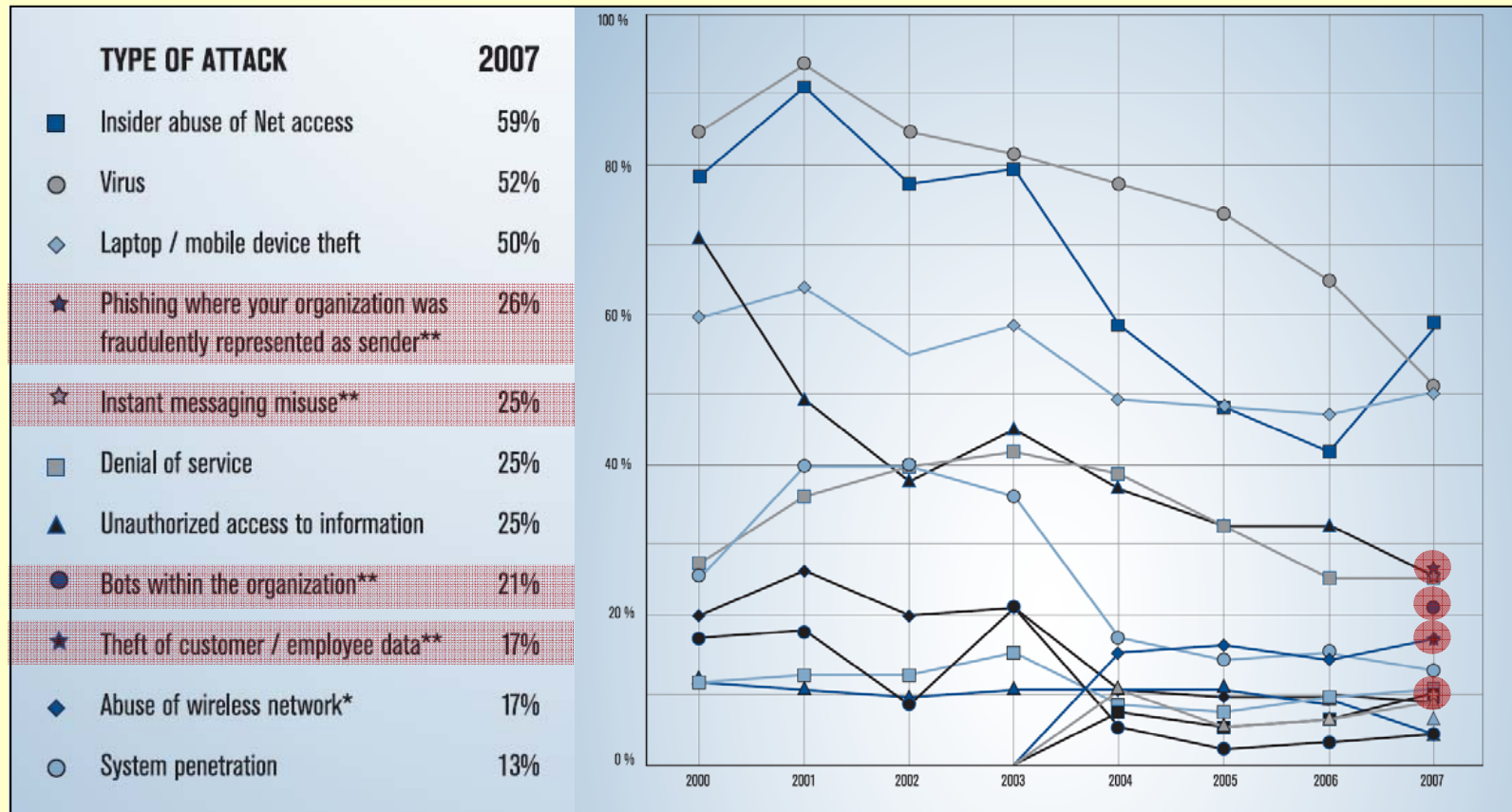
Alcune previsioni recenti

Have you or anyone in your family ever encountered the following:

Security experts responding
in the affirmative

| | |
|---|-------|
| Had computer infected by malware | 81.5% |
| Had credit card used fraudulently | 52.5% |
| Had personal data stolen or lost | 33.2% |
| Had personal data used in new account fraud | 12.7% |
| Had debit card used fraudulently | 10.7% |
| Had funds hijacked from an online account | 4.9% |

New Attack Types



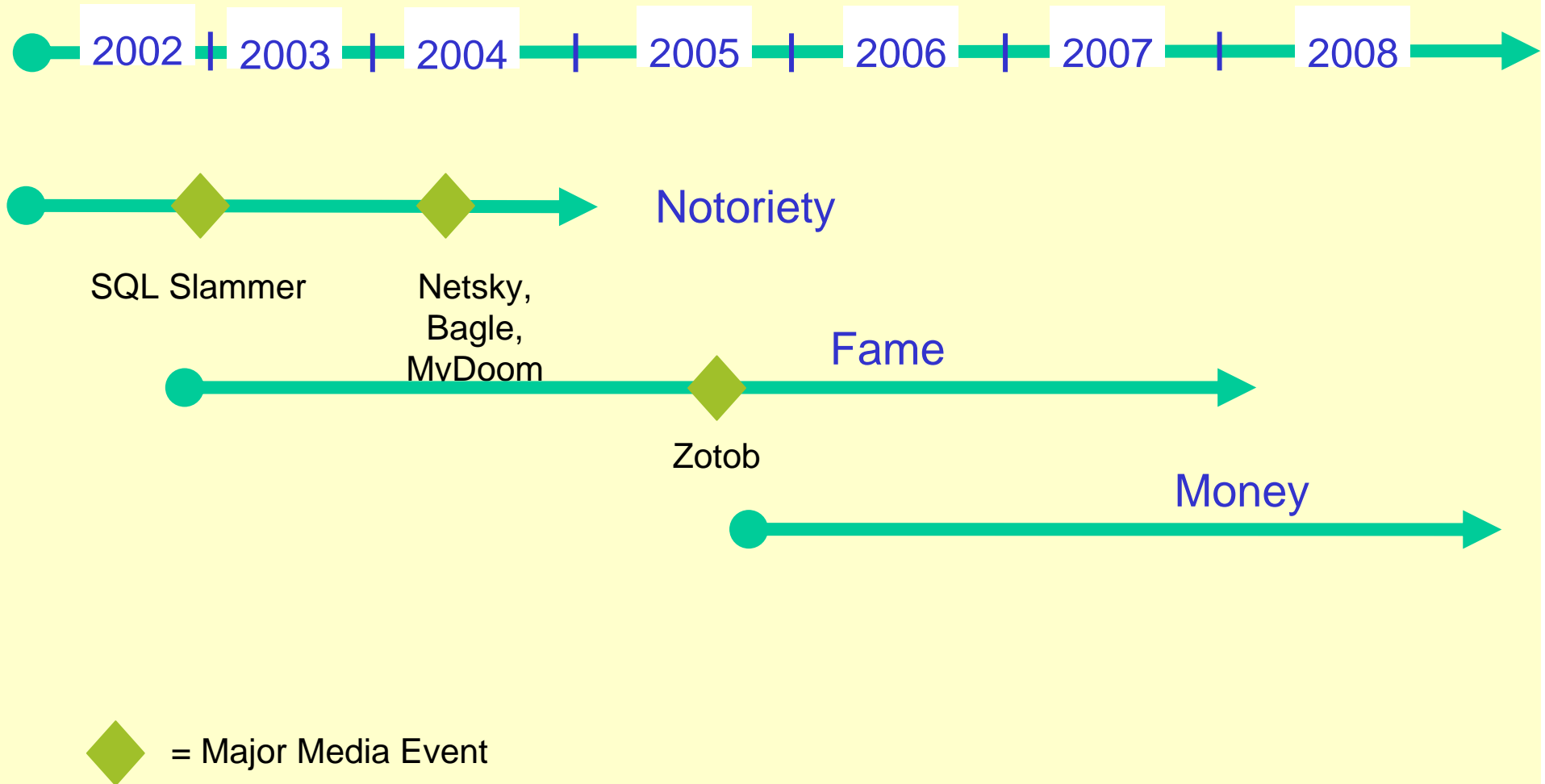
Source: 2007 CSI Survey

Threats on the Horizon

- Voice over IP Threats
- Mobile Devices
- Data Leakage
- Outsourcing
- Distributed Workforce
- Video Files Format Vulnerabilities
- New OSes
- Being Unprepared



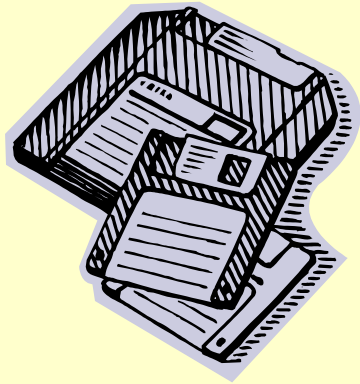
Evolution of Intent



I virus dall'esterno



I virus dall'esterno



Una azione di disturbo ...
divertimento per qualcuno

Il passaggio avviene mediante files
e/o programmi trasportati dai
media come i floppy

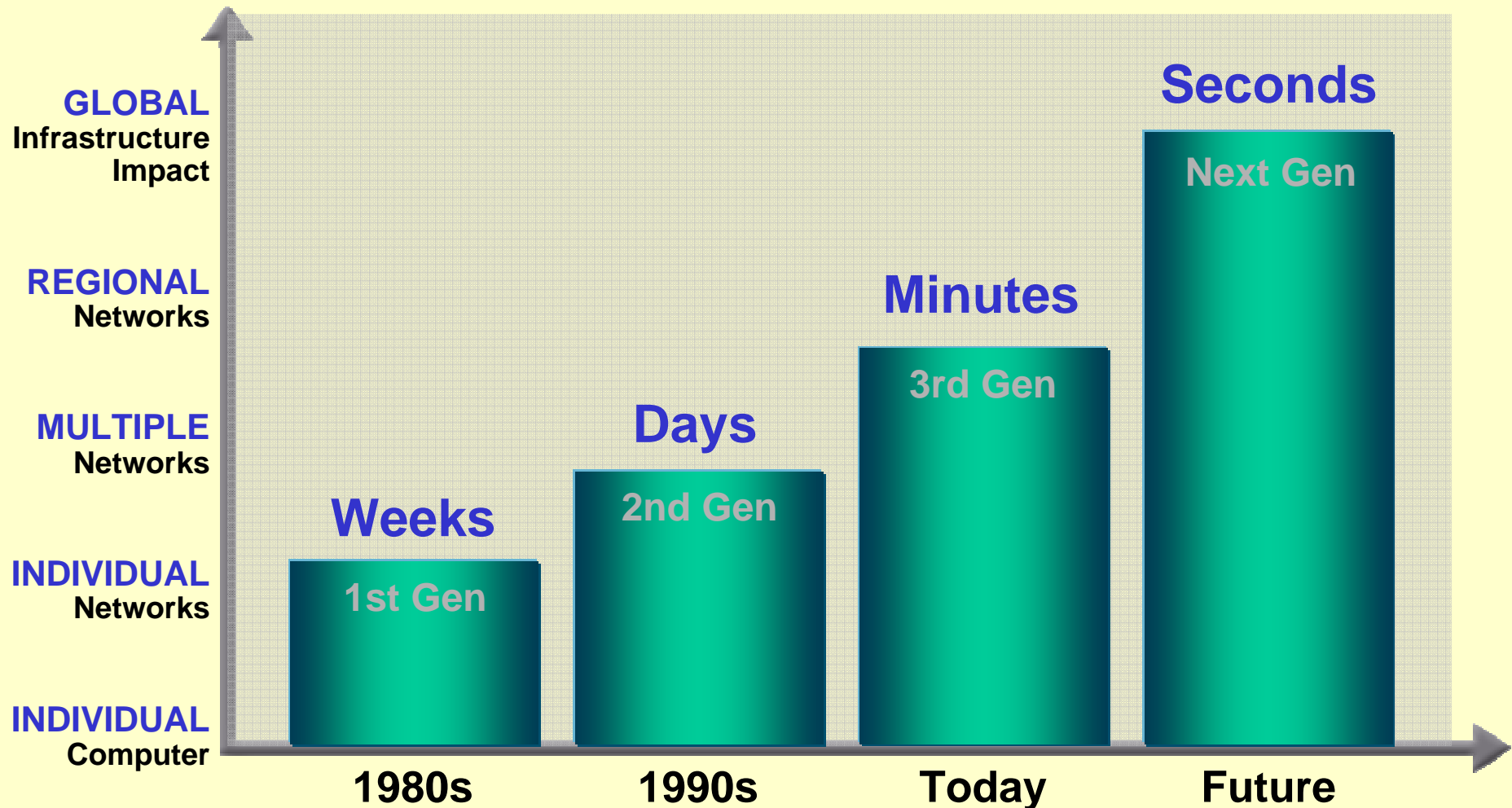
La nascita di Internet e i virus

Il computer connesso ... a pericolo di infezione

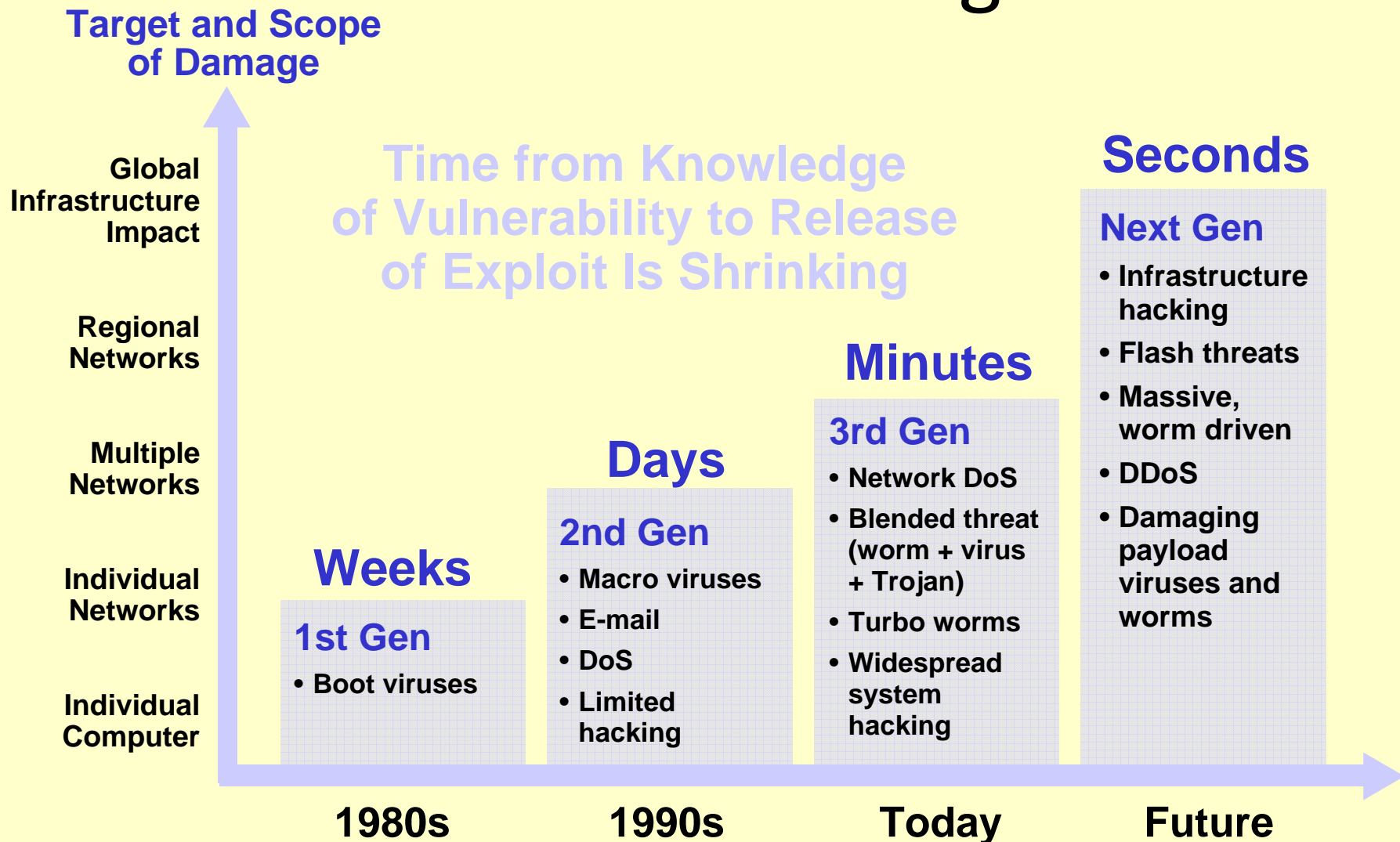
1. I dati e/o programmi sono prelevati dal Web
 - Possibilità di virus in entrata
 - Tramite la posta elettronica c'è lo scambio di dati e/o programmi
2. Il PC diventa accessibile dall'esterno con l'avvento del Peer to Peer (gennaio '99)
3. Seguono altri veicoli (Skype, Facebook,)

Evolution of Security Challenges

Target and Damage



Evolution of Security Challenges

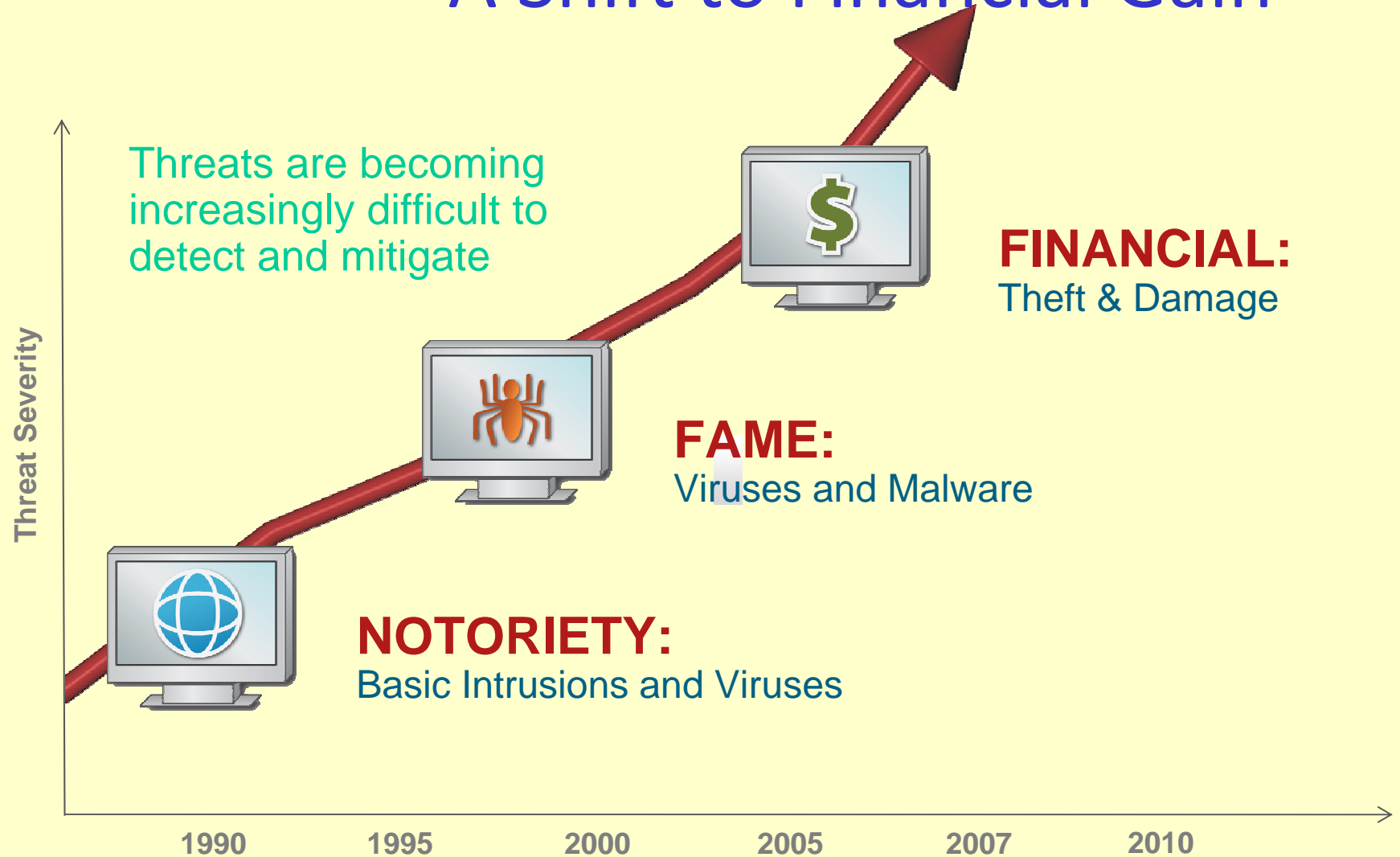


Il tempo di propagazione

- La fine degli anni 90 vede la diffusione di massa di Internet per come è intesa al giorno d'oggi, e molti virus writers videro che non era più necessario aspettare mesi e mesi affinché un floppy disk infetto potesse infettare il mondo intero.
- Internet collegava il mondo intero e il tutto a pochi secondi di distanza.
- Inizia a nascere quindi il periodo dei worm che si diffondono via e-mail, tutt'ora vivo.
- Tra i nomi di maggior spicco prima del 2000 possiamo ricordare **Melissa**, **Happy99** e **BubbleBoy**, il primo worm capace di sfruttare una falla di Internet Explorer e di autoeseguirsi da Outlook Express senza bisogno di aprire l'allegato.
- Il 2000 viene ricordato come l'anno dell'amore, con il famoso **I Love You** che, a catena, dà il via ad un breve periodo di script virus.
- Dal 2001 vediamo un incremento di worm che utilizzano falle di programmi o sistemi operativi per diffondersi senza nessun intervento dell'utente, fino a raggiungere l'apice nel 2003 e nel 2004: **SQL/Slammer**, il più rapido worm della storia e i due worm che tanto hanno fatto parlare di sé: **Blaster** e **Sasser**.

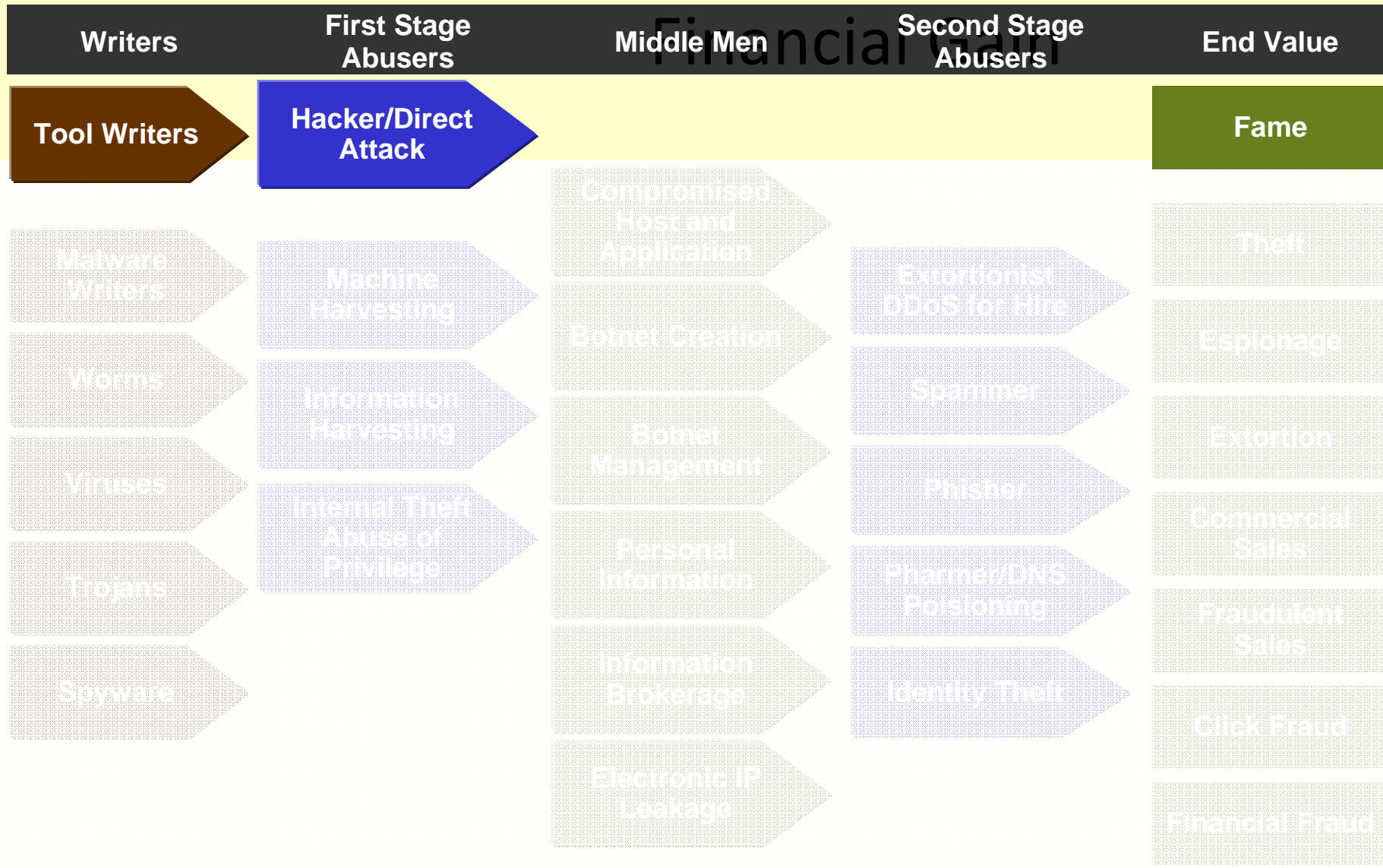
The Evolution of Intent

A Shift to Financial Gain

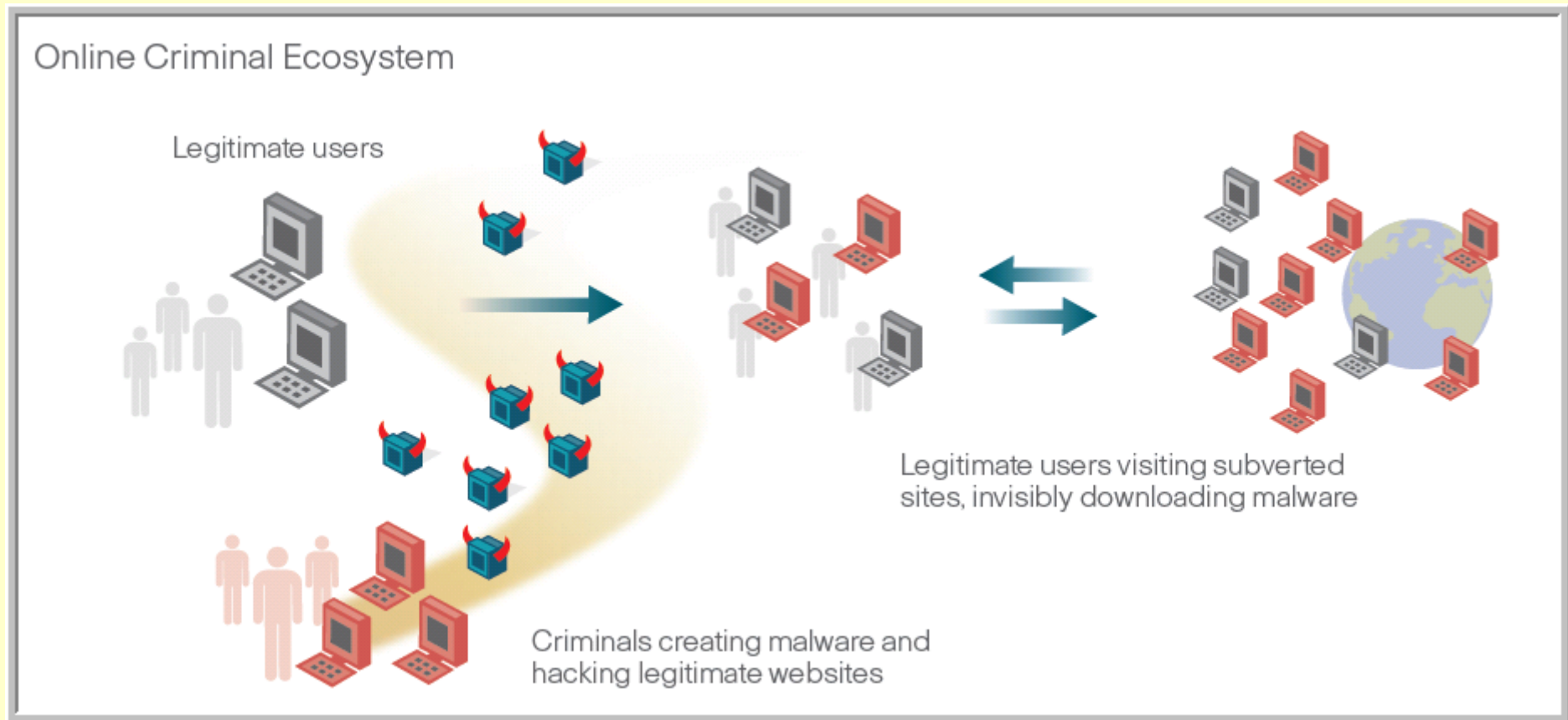


Environment

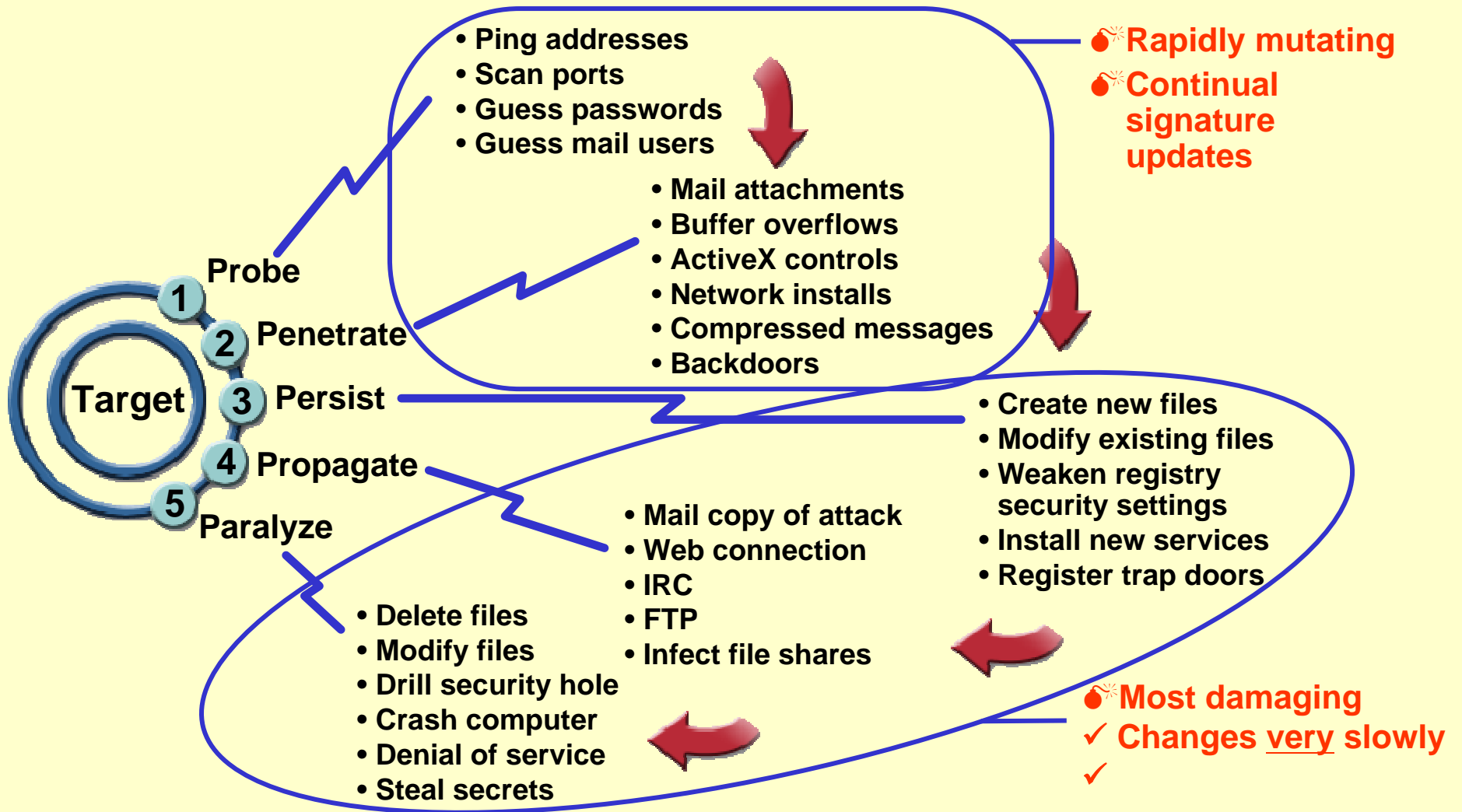
With a Structured Network for



L'ecosistema



Malicious Behavior



L'industria del crimine



“informatico” Cybercrime

- Gruppi sviluppano il “malcode” o “malware”
- Il “malware” viene venduto
- Gli amministratori dei providers sono pagati per ospitare “malware” nei siti che essi controllano
- Il Malware colleziona usernames e passwords come pure numeri di carte di credito
- I numeri di Carte di Credito, gli usernames e le passwords sono messe in vendita

L'organizzazione

- *Ecco alcuni dei diversi **ruoli** necessari per portare a compimento un attacco:*
- ***Spammer:** responsabile dell'invio di e-mail di phishing al maggior numero di indirizzi di e-mail possibile.*
- ***Progettisti Web:** responsabili della creazione di siti Web nocivi che assomigliano il più possibile a quelli legittimi da emulare.*
- ***Exploiter:** in genere aggressori dilettanti noti come "script kiddies", ragazzini degli script, i quali identificano i computer vittima (chiamati "root") che saranno utilizzati per ospitare un sito di phishing o per trasmettere i messaggi di spamming. In alcuni casi, gli exploiter si introducono direttamente nei database di carte di credito per raccogliere i dati, saltando del tutto la fase di phishing.*
- ***Cassieri:** responsabili del ritiro dei fondi da una carta di credito o da un conto bancario compromessi e della trasformazione in denaro per conto del phisher.*
- ***Ricettatori:** questi membri sono in grado di ricevere merci acquistate con i dati di carte di credito rubati presso un punto di raccolta non rintracciabile. I beni acquistati con informazioni su carte di credito e conti correnti bancari rubate sono considerati "carded" e i truffatori di questo tipo "carder".*

Gli Individui

The cyber criminals constitute various groups/ category.

1. ***Children and adolescents between the age group of 6 – 18 years –***
 - The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.
2. ***Organised hackers-***
 - These kinds of hackers are mostly organised together to fulfill certain objective. The reason may be to fulfill their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfill their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.
3. ***Professional hackers / crackers –***
 - Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are ven employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.
4. ***Discontented employees-***
 - This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

Facts on the Ground: Real Threats Affecting Real Networks



**James Ancheta,
small time hacker from California**



Ancheta used a variety of malware to take control of **400,000** computers globally

Ancheta used these machines to make **hundreds of thousands** of dollars

- Renting the machines to spammers
- Installing spyware on the machines

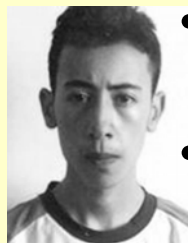


He got caught while infecting computers used in weapons research by the US Gov't

Sentenced to 5 years in jail in May 2006

Zotob Secrets Revealed:

All About the Money



- Zotob created by Diabl0, otherwise known as Farid Essebar
- Essebar was a small-time adware/spyware installer, using Mytob to infect machines and install adware for money
- Diabl0 integrated publicly available Proof of Concept exploit code for the PnP vulnerability into an existing Mytob variant
- FBI has said they hold evidence that Essebar was paid by Atilla Ekici (“Coder”) with stolen credit card numbers to build Mytob variants, as well as Zotob
- On Aug 25, 2005, Essebar was arrested in Morocco, and Ekici in Turkey

Source: <http://www.securityfocus.com/news/11297>

KEY QUESTION: Why Were They Caught?

- **Consensus answer:** Essebar was clumsy
- **Due to lack of experience, Zotob got out of hand and got too much attention – largely because it accidentally infecting some major institutions (CNN, CIBC, others)**
- **In other words: had they been smarter and stealthier, they’d likely never have been caught**

Spyware for Sale

The New Corporate Espionage



- Ruth and Michael Haephrati charged with writing custom spyware for corporate intelligence gathering
- Michael Haephrati began developing the Trojan in 2000
- Wife Ruth Haephrati marketed it to three private investigation companies in 2004
- Leveraged both known and unannounced vulnerabilities on Windows systems
- Captured various data using standard behaviors: keystroke logging, screen capture, file transmissions, etc.

"Organized criminals are hell bent on stealing information and **making a profit**. This case sends out a strong message that the menace of spyware is growing, and that companies need to realize that it's not just home users who are at risk."

Source: TechWeb

<http://www.techweb.com/article/showArticle.jhtml;jsessionid=U45GMNUB4Y4VOQSNDLPSKH0CJUNN2JVN?articleId=181501294&pgno=2>

Can you put a price on stolen data?

| Current Rank | Previous Rank | Goods and Services | Current Percentage | Previous Percentage | Range of Prices |
|--------------|---------------|-------------------------|--------------------|---------------------|--|
| 1 | 2 | Bank accounts | 22% | 21% | \$10-\$1000 |
| 2 | 1 | Credit cards | 13% | 22% | \$0.40-\$20 |
| 3 | 7 | Full identities | 9% | 6% | \$1-\$15 |
| 4 | N/A | eBay accounts | 7% | N/A | \$1-\$8 |
| 5 | 8 | Scams | 7% | 6% | \$2.50/week-\$50/week for hosting, \$25 for design |
| 6 | 4 | Mailers | 6% | 8% | \$1-\$10 |
| 7 | 5 | Email addresses | 5% | 6% | \$0.83/MB-\$10/MB |
| 8 | 3 | Email passwords | 5% | 8% | \$4-\$30 |
| 9 | N/A | Drop (request or offer) | 5% | N/A | 10%-50% of total drop amount |
| 10 | 6 | Proxies | 5% | 6% | \$1.50-\$30 |

Table 4. Breakdown of goods and services available for sale on underground economy servers⁵⁵

Source: Symantec Corporation

Il mercato nero

Marketing e promozioni

- L'esempio seguente, ripreso da un forum di frodi on-line, illustra che questi "fornitori" considerano molto seriamente i propri affari, in alcuni casi offrendo promozioni, svendite e garanzie.
- Nella "promozione" seguente viene offerto uno sconto per acquisti a volume e schede telefoniche gratuite.
- Smile Buy Cheap Cvv2s And Get Gifts
- Hello all carders ! Iam glad to offer my service to serve all you guys.
- Iam selling US cvv2 with NO LIMIT (UK & Canadian and International cvv2s will be available soon) *
- Cvv2s have the following information: -
 - Card Number -
 - Card Expiry -
 - CVV2 -
 - First & Last Names -
 - Address & City -
 - State & Zip/Postal code -
 - Country (US) -
 - Phone #

```
===== Here is the price =====

* For US cvv2 :

1 -> 40 cvv2s : $1.5 per card
100+ cvv2s : $1 per card

* For UK ccs : 1$ per each (come with : Name, Address,
Town, County, Postcode, Ccnumber, exp, from date,
and issue number)

* If you request the following information for Cvv2:

Special Card Type +$0.50
Email, Password +$3
Special Gender +$2
Special bins : +$1
* Special Offers :

If your order > 50$ , u will get a calling card with 5$
If your order > 100$ , u will get a calling card with 10$
```

I metodi



BOTnet (zombie machines)



Il metodo principe

Definizione di BOT

- Il termine **bot** (abbreviazione di robot) si riferisce, in generale, a un programma che accede alla rete attraverso lo stesso tipo di canali utilizzati dagli utenti umani (per esempio che accede alle pagine Web, invia messaggi in una chat, e così via).
- Programmi di questo tipo sono diffusi in relazione a molti diversi servizi in rete, con scopi vari ma in genere legati all'automazione di compiti che sarebbero troppo gravosi o complessi per gli utenti umani.
- Non è in sé un sintomo di attività illegale

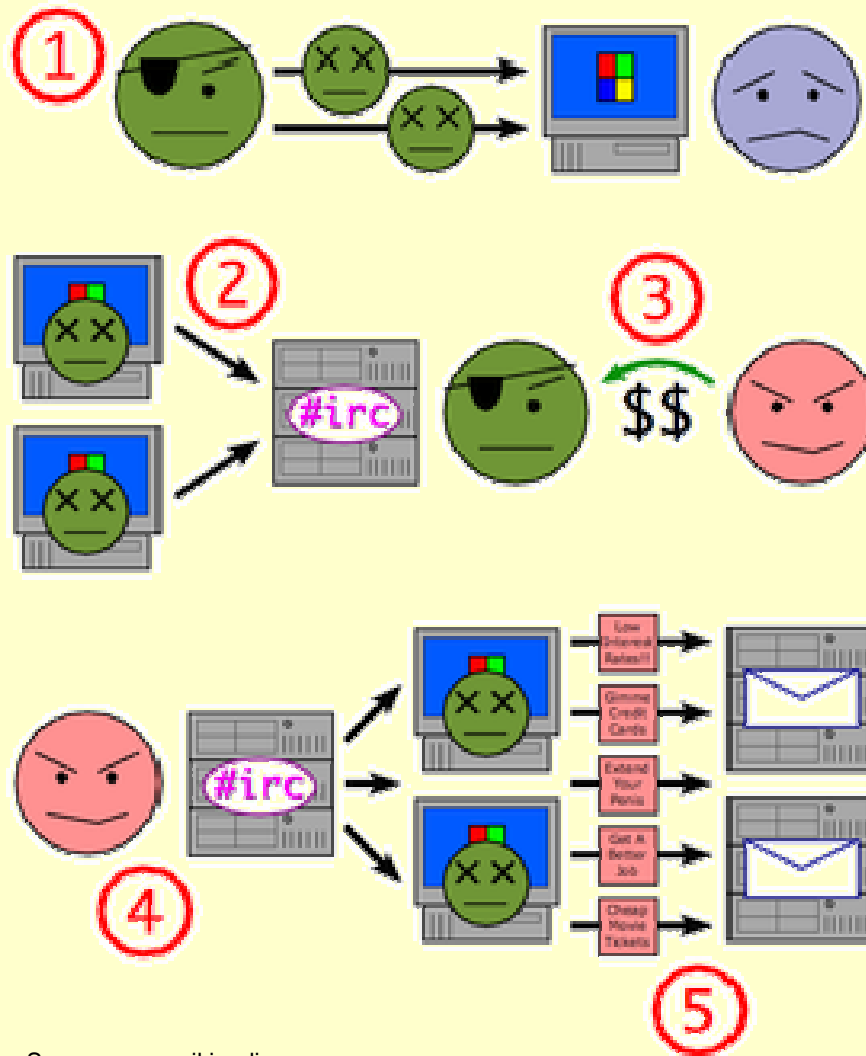
Definizione

- Nelle terminologie legate alla sicurezza in Internet, il termine bot si riferisce, in generale, a un computer infettato da virus che lo rende governabile da utenti remoti.
- Il bot in questo caso viene anche detto “Zombie”
- http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm

Definizione

- Una **botnet** è una rete di computer che, a causa di falle nella sicurezza o mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, sono stati infettati da virus informatici o trojan i quali consentono ai loro creatori di controllare il sistema da remoto.
- Questi ultimi possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi distribuiti del tipo denial-of-service (DDoS) contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite, in taluni casi agendo persino su commissione di organizzazioni criminali.

Spam



- 1. A botnet operator propagates by viruses, worms, spam, and malicious websites
- 1. The PCs log into an IRC server or other communications medium
- 1. A spammer purchases access to the botnet from the operator
- 1. The spammer sends instructions via the IRC server to the infected PCs—
- 1. ... causing them to send out spam messages to mail servers

Uso dei BOT

- Bots perform many jobs for cybercriminals.
- In next example, the bot works as an assistant for identity thieves on the blackmarket.
- The bot has been specifically created for an online forum for cybercriminals to help perform basic identity theft tasks, such as determining whether stolen credit cards are valid, the credit card limits, and additional data such as the CVV2 code and expiration date.

Uso dei BOT

- A chat session between cybercriminals:

<redeyezz> !cclimit 4854xxxxxxxxxxxx

<Forumbot> redeyezz I found limit for your Visa (4854xxxxxxxxxxxx): 7.536 \$

An identity thief named "redeyezz" asks the bot the limit of a presumably stolen credit card using the command "!cclimit" and the credit card number.

<Vietnamhack> !chk 4158xxxxxxxxxxxx xx0x

<Forumbot> Vietnamhack 4158xxxxxxxxxxxx : xx0x (Valid cc)

<jyde> !chk 6011xxxxxxxxxxxx xx0x

<Forumbot> jyde 6011xxxxxxxxxxxx : xx0x (You're Card Is Declined)

Two identity thieves check the validity of 2 different credit cards, one which is still valid and another which is no longer valid and therefore declined.

Creazione dei BOT

- Bot software is created by professional crimeware authors.
- While much of the source code (the "raw" code for the bot's design) is freely available, specially created versions of bot software are available for purchase from crimeware professionals for several hundred dollars if not more.
- Crimeware authors will market their bot programs with claims that they can evade security software and avoid detection.

Uso dei BOT

- Much like the rest of crimeware and cybercrime in general, bots are a global problem.
- The map shows the geographic locations of active bot command and control servers (the heart of a botnet) in late 2005.
- Bots and botnets are the multi-purpose "swiss army knives" of cybercrime.
- Bots play a role in nearly every type of popular cybercrime today.
- The botnet owners rent out their illicit networks for a fee to other criminals or use the bots themselves in order to commit numerous types of crimes.



Top 10 Botnets

| Botnet | # of Bots | Spam capability |
|--------------|-----------|-----------------|
| Srizbi | 315K | 60B/day |
| Bobax | 185K | 9B/day |
| Rustock | 150K | 30B/day |
| Cutwail | 125K | 16B/day |
| Storm | 85K | 3B/day |
| Grum | 50K | 2B/day |
| Onewordsub | 40K | Unknown |
| Ozdok | 35K | 10B/day |
| Nucrypt | 20K | 5B/day |
| Wopla | 20K | 600M/day |

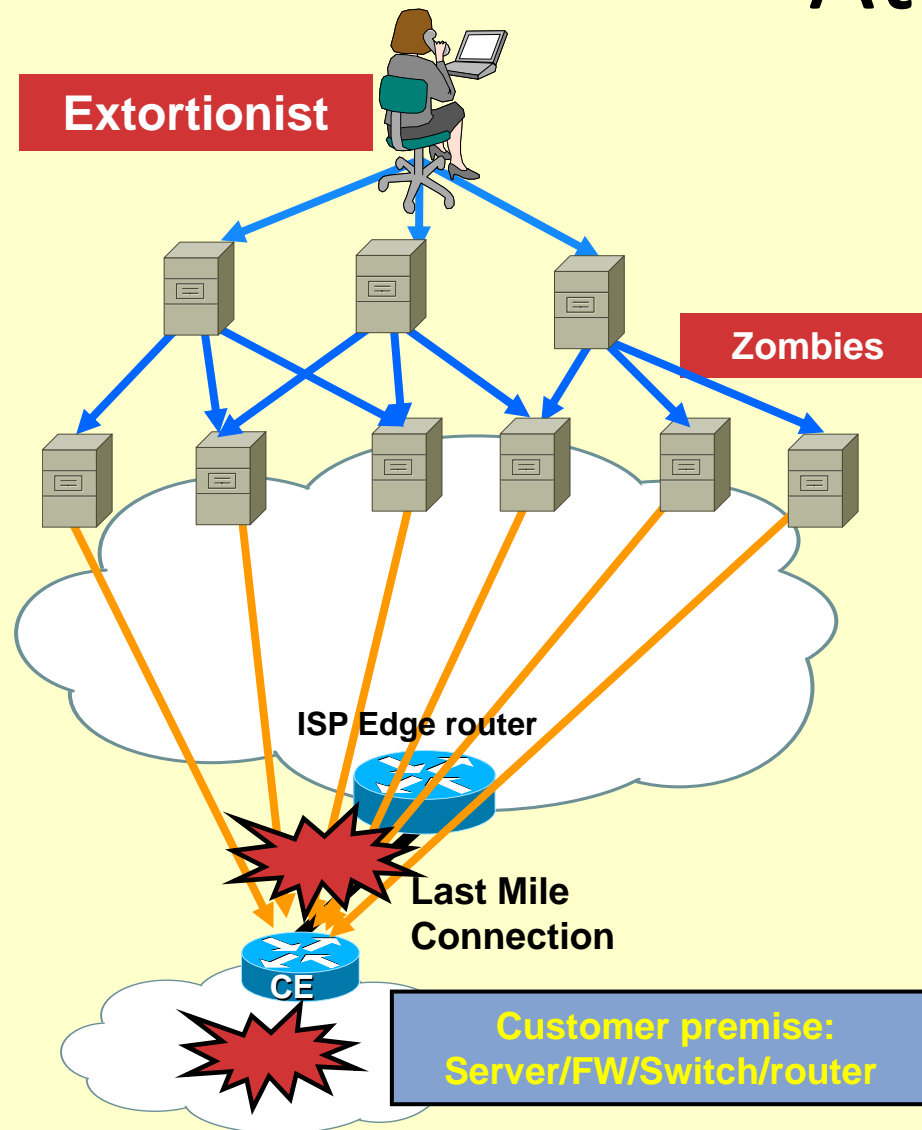
Source: RSA Conference - April 09, 2008 (Computerworld)

<http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9076278>

| Crimine | Usò di BOT e BOTNET |
|-------------------------|---|
| Denial of Service (DoS) | Since the 1990s, networks of zombie machines have been used to try and knock Web sites offline, making them unusable by their customers – often times preventing e-commerce. Sometimes denial-of-service attacks are mere Internet “joyrides” and other times they are orchestrated by competitors. |
| Estorsione | While some denial-of-service attacks are executed by zombie machines against an unsuspecting Web site or other online service, some are warned in advance in what is known as a protection racket or extortion. In such schemes, the criminal threatens to knock the company’s Web site or online service off the Internet for a period of time if they are not paid, usually at a peak hour that would be the most noticeable and do the most damage (i.e. as frustrated customers take their business elsewhere). |
| Furto di Identità | While bots are typically part of an identity theft, sometimes they play the main and supporting role infecting a computer, and also stealing personal information from the victim and sending it to criminal. |
| Spamming | Botnets operate at the heart of today’s spam industry—bots both harvest email addresses for spammers and are also used to spam messages out. Sending spam through botnets is particularly common since it makes spammers more difficult to detect as they can send messages from many machines (all the infected machines in the botnet) rather than through a single machine. This tactic has become so common that in the first half of 2005, 64 percent of the top threats Symantec saw were capable of being used for sending spam. |
| Frode (Phishing) | In nearly every phisher’s toolbox is an army of bots. Much like spammers, phisher’s use bots to identify potential victims and send fraudulent emails, which appear to come from a legitimate organization such as the user’s bank. Bots are also used by phishers to host the phony Web sites, which are used to steal people’s personal information and serve as collection points (“dead drop” or “egg drop” servers) for stolen data. An animated overview of online fraud is available that explains the different components of a phishing operation. |


Fonte “Symantec - <http://www.symantec.com/norton/cybercrime/definition.jsp>

Botnets Make DDoS Attacks Easy



- A “**Botnet**” is a group of compromised computers on which extortionists have installed special programs (zombies) that can be directed to launch DoS attacks against a specific target.
 - **Botnets** are triggered from a “central controller”
 - **Botnets** allow for all the types of DDOS attacks: ICMP Attacks, TCP Attacks, UDP Attacks, HTTP overload
 - Options for deploying **Botnets** are extensive and new tools are created to exploit the latest system vulnerabilities
- A relatively small **Botnet** can cause a great deal of damage.
 - 1000 home PCs with an average upstream bandwidth of 128KBit/s can offer more than 100MBit/s against a target
- The size of the attacks are ever increasing and independent of last mile bandwidth

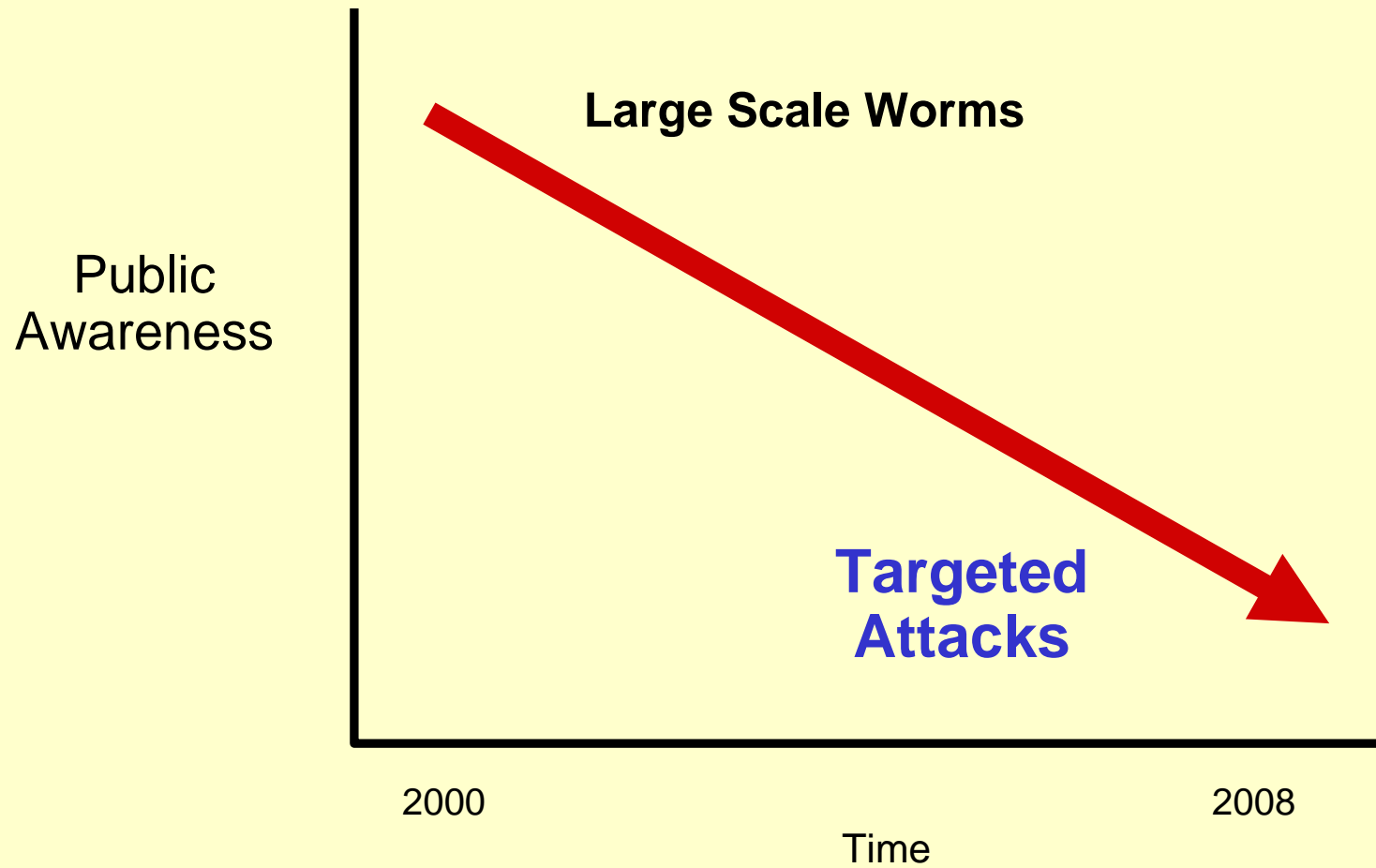
Trend attuale

Maggiore discrezione 

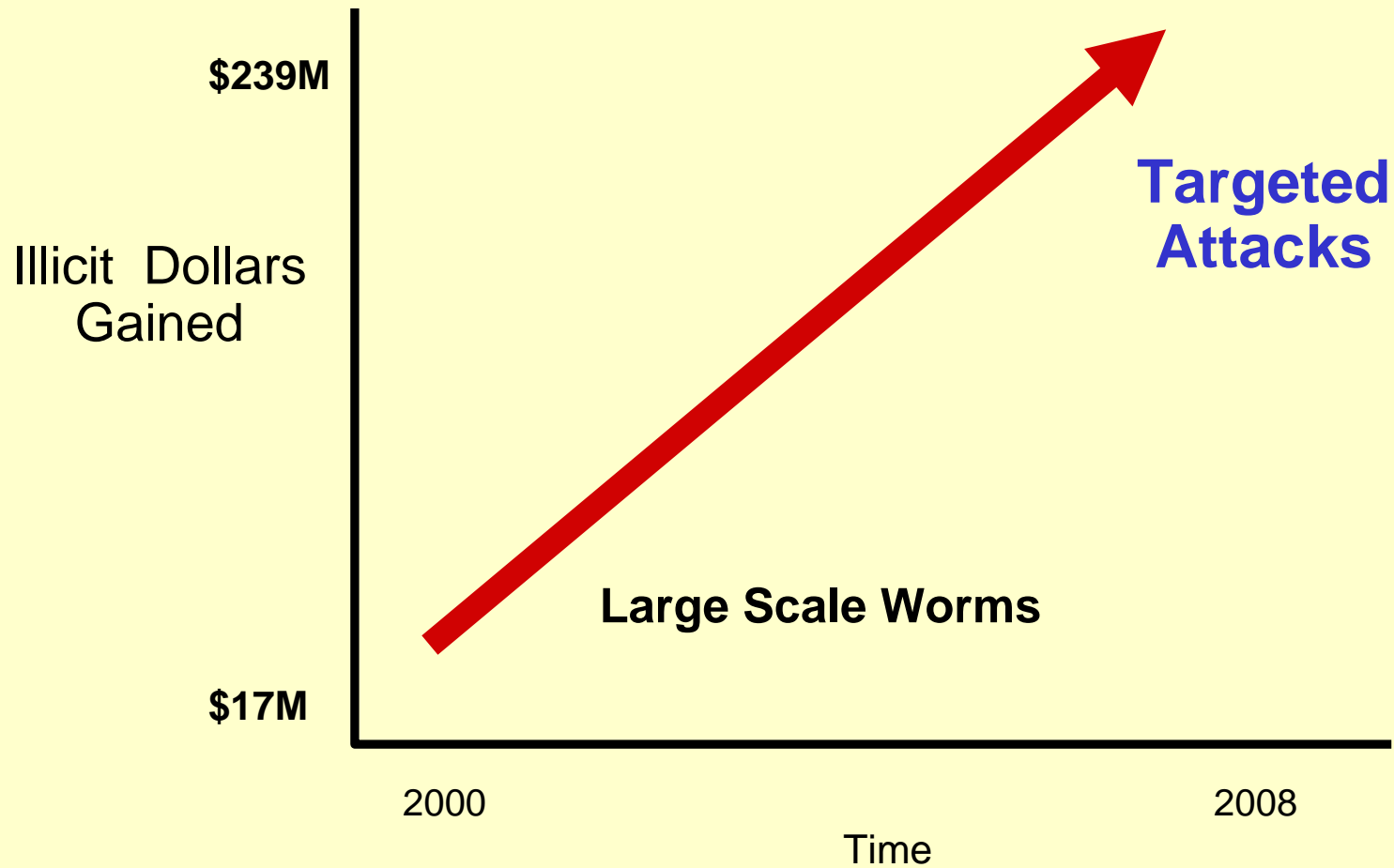
vs.

maggior profitto

“Noise” Level

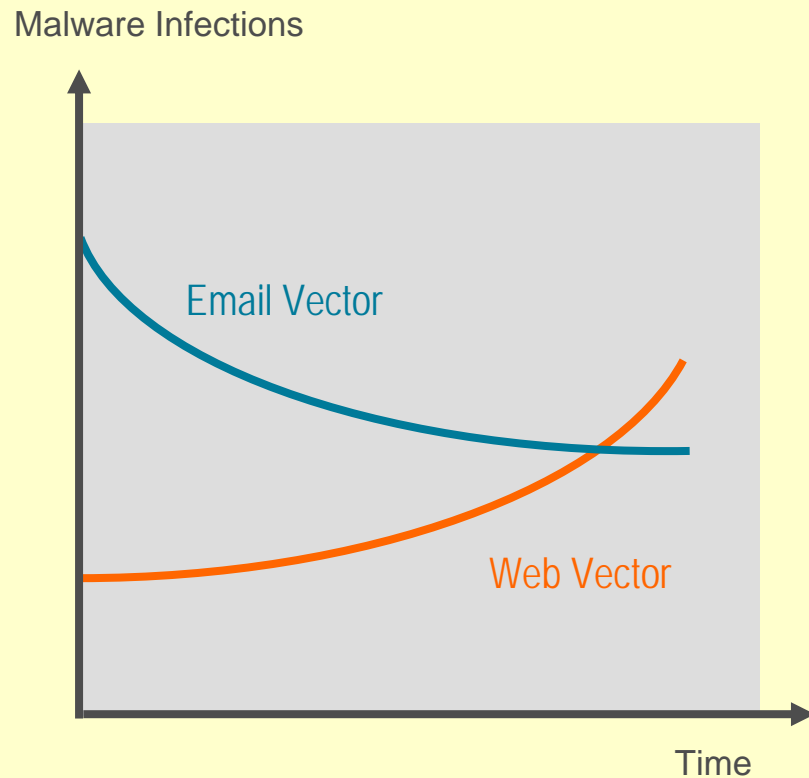


Cyber Crime Profit Level



Source: ICR 2001, 2007

Distribution



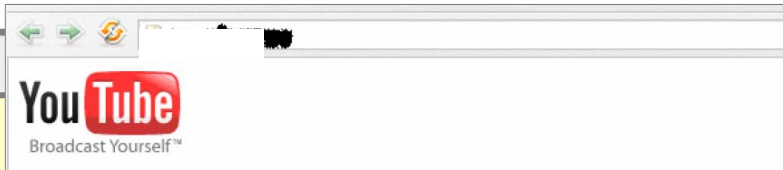
Malware infection vectors are shifting from email to web

TD Ameritrade Breach Affects 6.3M Customers

Brokerage firm uncovers data-sucking malware during system audit

From

Man you have got to tell me where you picked her up. I saw this on the web, it has to be you. check it out yourself <http://www.youtube.com/watch?v=IHZbpJLfppV>



Your **NETWORKWORLD**

you C This story appeared on Network World at <http://www.networkworld.com/news/2007/020207-dolphins-web-sites-hacked-in.html>

Dolphins' Web sites hacked in advance of Super Bowl

IT WEEK About Contacts Subscribe Advertise Jobs S

Home News Analysis Comment

IT Week > News > Hacking

Smart malware steals from SSL streams

Is nothing safe?

Iain Thomson, vnunet.com, 22 May 2007

A new variant of th

Classificazione

- The subject of cyber crime may be broadly classified under the following three groups. They are-
- **1. Against Individuals**
 - a. their person &
 - b. their property of an individual
- **2. Against Organization**
 - a. Government c. Firm, Company, Group of Individuals.
- **3. Against Society at large**

Against Individuals

- i. Harassment via e-mails.
- ii. Cyber-stalking.
- iii. Dissemination of obscene material.
- iv. Defamation
- v. Unauthorized control/access over computer system.
- vi. Indecent exposure
- vii. Email spoofing
- viii. Cheating & Fraud

Against Individual Property

- i. Computer vandalism.
- ii. Transmitting virus.
- iii. Netrespass
- iv. Unauthorized control/access over computer system.
- v. Intellectual Property crimes
- vi. Internet time thefts

Against Organization

- i. Unauthorized control/access over computer system
- ii. Possession of unauthorized information.
- iii. Cyber terrorism against the government organization.
- iv. Distribution of pirated software etc.

Against Society at large

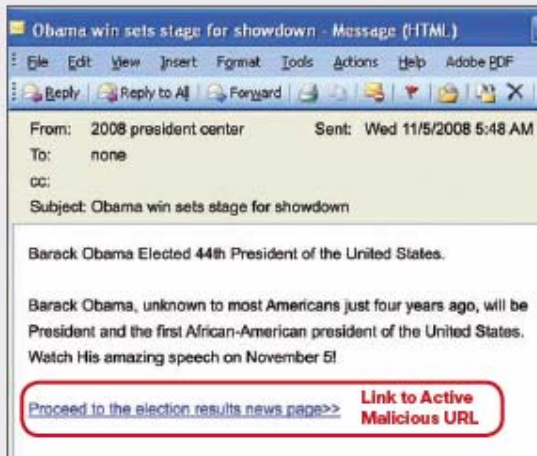
- i. Pornography (basically child pornography).
- ii. Polluting the youth through indecent exposure.
- iii. Trafficking
- iv. Financial crimes
- v. Sale of illegal articles
- vi. Online gambling
- vii. Forgery

ESEMPI



Tutte le occasioni sono

New President, New Malware



Current events-oriented email messages convince recipients to open and act on the email. In a recent example, a spam campaign invited recipients to watch a video of President-elect Barack Obama's victory speech. Subject line examples included:

- Election Results Winner
- The New President's Cabinet?
- Obama Win Sets Stage for Showdown

The email directed recipients to a fake government-themed botsite. Once there, they were prompted to install an Adobe Flash Player update, which was actually data-stealing malware. Once installed, the malware stole screenshots and passwords, sending that information to a Web server located in Kiev, Ukraine.



Government-Themed Botsite



The Real America.gov Site

Tutte le occasioni sono

Beijing Olympics Fake Ticketing Scams

One of the most elaborate social engineering internet scams of 2008 was related to the Beijing Olympics, with criminals making a profit of an estimated US\$40 to \$50 million. People in several countries, from New Zealand to the United States, were taken in by fake ticketing sites that sold illegitimate or nonexistent tickets to Olympic events. Some individuals paid thousands of dollars for particularly hard-to-come-by tickets, such as those for the opening ceremonies.

The biggest offender was Beijingticketing.com, a professional-looking website that featured the official Beijing Games logo. This fraudulent website was superior to the official ticketing site, with a better ticketing purchasing process and integration with social networking sites like Facebook to virally spread the fake site. Even MSNBC initially believed the site was credible: An MSNBC Forbes Traveler article featured a link to the site. This helped it gain a high search engine ranking, which resulted in ticket seekers who used search engines to look for tickets going to the fake site rather than legitimate sites.

Beijingticketing.com asked users to register—and provide confidential information—before they could purchase tickets. After registration, users provided credit card numbers and “bought” tickets, which they never received. Not only did the scammers net millions of dollars, but they also scooped up thousands of valid credit card numbers for later use or resale to other online criminals.



Scam Ticketing Site



Official Ticketing Site

Fraudulent Olympics ticketing websites, such as Beijingticketing.com, took advantage of thousands eager to buy tickets to the 2008 Beijing Summer Olympics.

Spam e malware come un'arma






Mouse Hijacking

Multiple Browsers and Adobe Flash Player Mouse Click Hijacking Vulnerability

SECURITY ACTIVITY BULLETIN

Powered by **IntelliShield**

| | | | | |
|-------------------|--|--------------|---------------------|---|
| Threat Type: | IntelliShield: Security Activity Bulletin | Urgency: | Possible Use |  |
| IntelliShield ID: | 16770 | Credibility: | Confirmed |  |
| Version: | 8 | Severity: | Mild Damage |  |
| First Published: | October 01, 2008 12:41 PM EDT | | | |
| Last Published: | January 07, 2009 03:31 PM EST | | | |
| Port: | Not Available | | | |
| CVE: | CVE-2008-4503 | | | |
| BugTraq ID: | 31625 | | | |

Version Summary: **Sun has released an alert notification and patches to address the mouse click hijacking vulnerability in Adobe Flash Player.**

Phishing and its variants

- Traditional phishing still in use
- Spear-phishing
 - Targeted phishing attempts
- Whaling
 - Phishing attempts specifically targeting a high value target

Il Meccanismo del Phishing

Typical spear-phishing attacks consist of four steps:

- 1 By launching malware, hacking into networks or buying lists from other nefarious online resources, scammers obtain a specialized distribution list of valid email addresses.
- 2 They register a domain and build a fake (but credible-looking) website to which phishing email recipients are directed.
- 3 They send phishing emails to their distribution list.
- 4 Scammers receive login or other account details from victims, and steal data and/or funds.

Spear-phishing attacks require criminals to efficiently build appropriate resources and trick victims into revealing valuable private information.

Subject: Internal Revenue Service Complaint for [REDACTED] (case id: #602f41571ba161cc3dc795df7886f000)

Mr./Mrs. [REDACTED]

We regret to inform you that your company is currently being investigated by our CI department for criminal tax fraud due to a complaint that was filled by a Mr. Keith McCall on 05/06/2007

Complaint Case Number: MT1CF23A
Complaint made by: Mr. Keith McCall
Complaint registered against: [REDACTED]
Date: 05/06/2007

You are being investigated for submitting false income tax returns with the Franchise Tax Board. Instructions on how to resolve this issue aswell as a copy of the original complaint can be found on the link bellow.

Complaint Documents < [REDACTED] >

Blended Attacks

Malicious “anti-spyware” sites.

antispyware911.com

Spoofed NFL (*National Football League*) sites

Game tracker download was actually Storm

Spurious Youtube sites

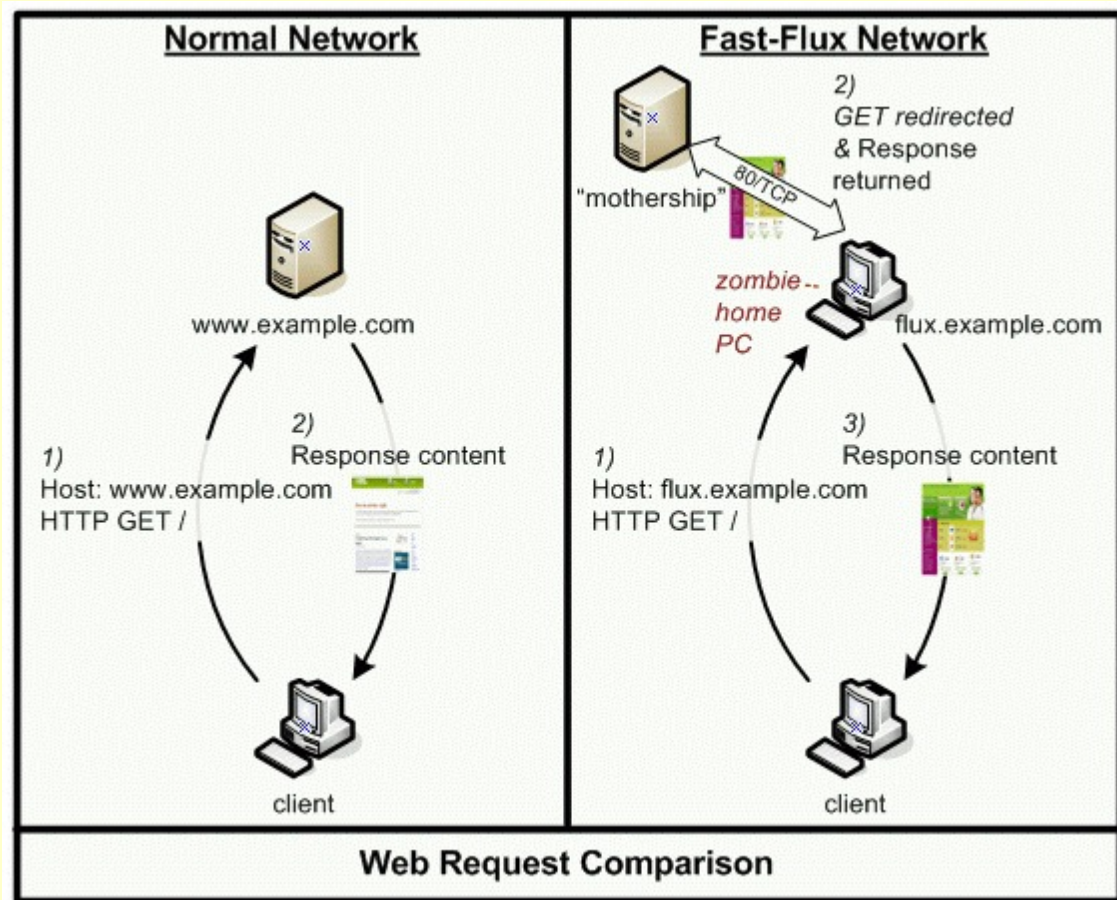
Click play actually downloads malware

Youth-oriented applications and sites

Free Games, Psycho kitty

Fast Flux

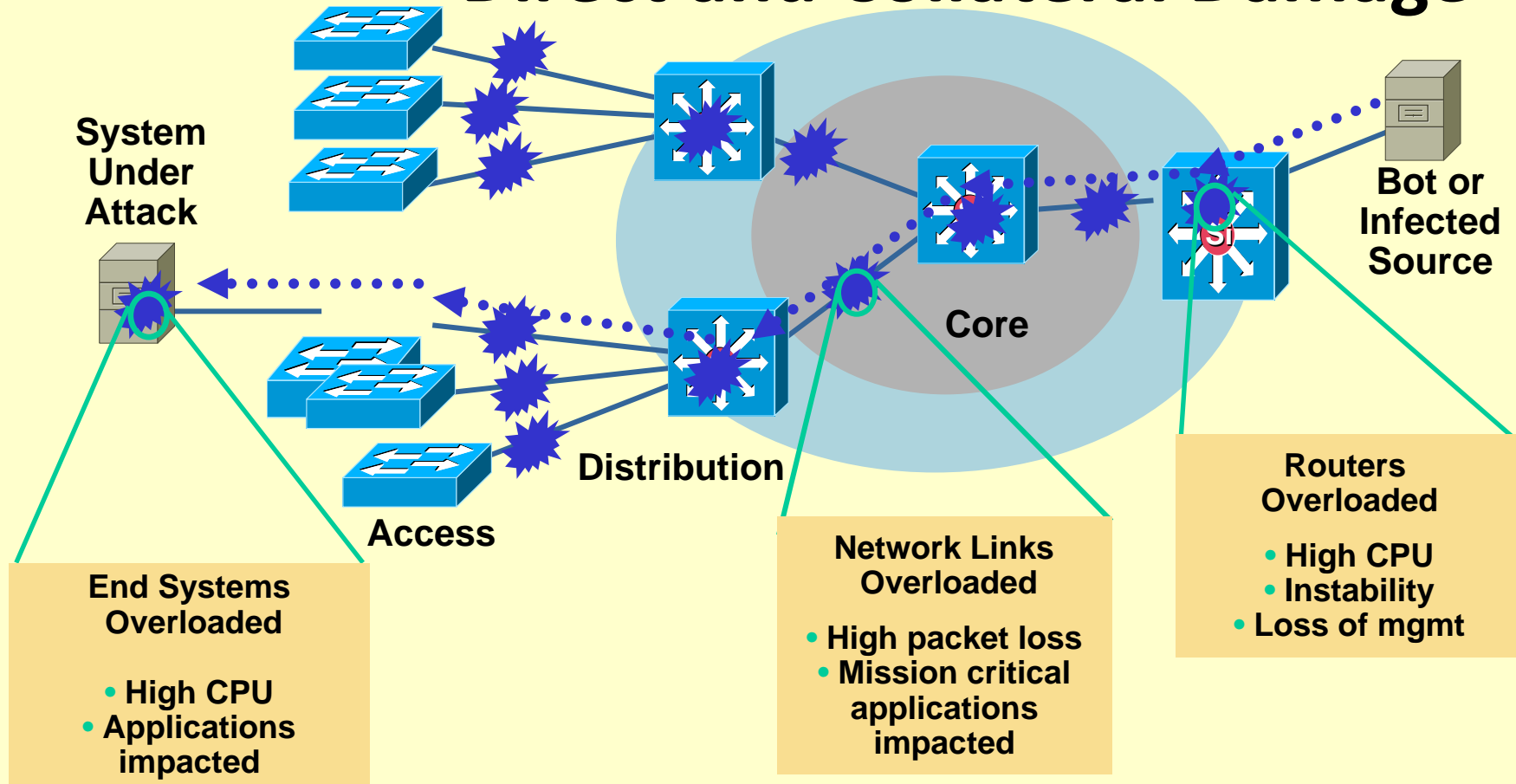
- Control system is hidden
- Very low time to live (TTL) in A Record
- Botnets are the new DNS servers



Source: honeynet.org

Impact of DoS and Worms

Direct and Collateral Damage



Availability of Networking Resources Impacted by the Propagation of the Attack

I Metodi

1. *Unauthorized access to computer systems or networks / Hacking-*

- This kind of offence is normally referred as hacking in the generic sense. However the framers of the *Information and Communication Technology Act, 2006* have nowhere used this term so to avoid any confusion we would not interchangeably use the word hacking for ‘unauthorized access’ as the latter has wide connotation.

2. *Theft of information contained in electronic form-*

- This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

3. *Email bombing-*

- This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

4. *Data diddling-*

- This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerised.

5. *Salami attacks-*

- This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank’s system, which deducted 10 cents from every account and deposited it in a particular account.

6. *Denial of Service attack-*

- The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

I Metodi

7. *Virus / worm attacks-*

- Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be \$ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. Almost brought development of Internet to a complete halt.

8. *Logic bombs-*

- These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

9. *Trojan attacks-*

- This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorized programme. The most common form of installing a Trojan is through e-mail. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

10. *Internet time thefts-*

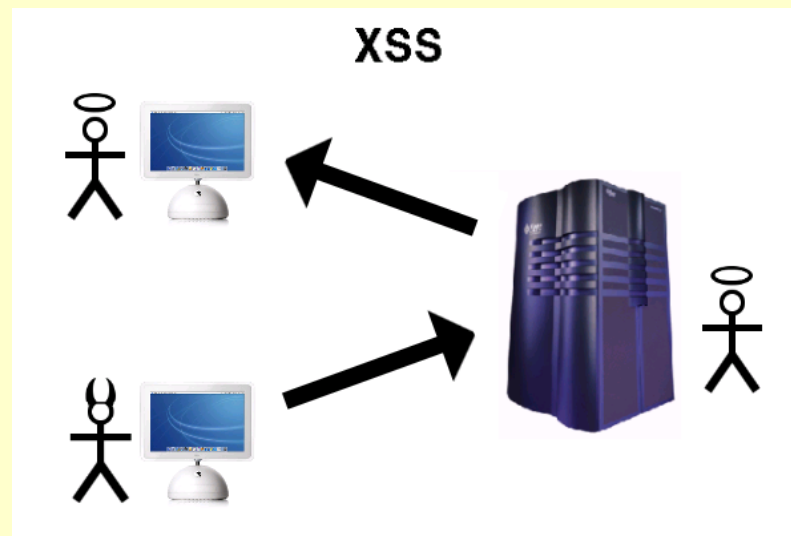
- Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password. E.g. Colonel Bajwa's case- the Internet hours were used up by any other person. This was perhaps one of the first reported cases related to cyber crime in India. However this case made the police infamous as to their lack of understanding of the nature of cyber crime.

11. *Web jacking-*

- This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US \$ 1 million was demanded as ransom. Thus web jacking is a process where by control over the site of another is made backed by some consideration for it.

L'ultima novità

XSS / Cross-site Scripting



Cross-Site Scripting (XSS)

- **What is it?**
 - A malicious script is echoed back into HTML returned from a trusted web site. The scripts executes locally on the client.
- **What are the implications?**
 - Web Site Defacement
 - Session IDs stolen (cookies exported to hacker's site)
 - Browser security compromised – control given to hacker
 - All data sent between client and server potentially hijacked

Clustered search on <script>alert('hi')</script> - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://...query-meta?=<script%3Ealert%28%27hi%27%29%3C%3E

DHNet.be - La Une Slashdot Le Soir en ligne: le fil i... Netcraft ha.ckers.org MercuryNews.com SecuriTeam Blogs Web Application Secu...

Proxy: None Apply Edit Remove Add Status: Using No Proxy Preferences

The Page You Have Requested Is Not ... XSS (Cross Site Scripting) Cheat Sheet UTF-16 Charset Encoder Test Vivisimo - Clustered search

Topic Search

<script>alert('hi')</script> Search Search within results

All

Search Term
route\$
75??
oute*

?q=<script>alert('hi')</script>

Clustered Results

Query

The page at http://topic says:

! hi

OK

“So... what’s the worst thing you can do with XSS?

Steal every piece of sensitive information you’ve ever inputted or will ever input on any website you’re authenticated to.

Yes, it’s potentially that bad..”

RSnake (Founder and CEO, SecTheory.com)

<http://ha.ckers.org>

The XSS attack process

