High Tech Crime Threats: Perspective of Europol

Strasbourg, 11th June 2007

EUROPOL

Overview of The Presentation

- Internet Community
- High Tech Crime Threats
- A quick look to the future
- Desirable initiatives to be taken

EUROPOL

The Usage of Internet

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	933,448,292	14.2 %	33,334,800	3.6 %	3.0 %	638.4 %
Asia	3,712,527,624	56.5 %	398,709,065	10.7 %	35.8 %	248.8 %
Europe	809,624,686	12.3 %	314,792,225	38.9 %	28.3%	199.5 %
Middle East	193,452,727	2.9 %	19,424,700	10.0 %	1.7 %	491.4 %
North America	334,538,018	5.1 %	233,188,086	69.7 %	20.9%	115.7 %
Latin America/Caribbean	556,606,627	8.5 %	96,386,009	17.3 %	8.7 %	433.4 %
Oceania / Australia	34,468,443	0.5 %	18,439,541	53.5 %	1.7 %	142.0 %
WORLD TOTAL	6,574,666,417	100.0 %	1,114,274,426	16.9 %	100.0 %	208.7 %

NOTES: (1) Internet Usage and World Population Statistics were updated on Mar. 10, 2007. (2) CLICK on each world region for detailed regional information. (3) Demographic (Population) numbers are based on data contained in the world-gazetteer website. (4) Internet usage information comes from data published by Nielsen//NetRatings, by the International Telecommunications Union, by local NICs, and other other reliable sources. (5) For definitions, disclaimer, and navigation help, see the Site Surfing Guide. (6) Information from this site may be cited, giving due credit and establishing an active link back to www.internetworldstats.com.

http://www.internetworldstats.com/stats.htm

EUROPEAN UNION	Population (2007 Est.)	Internet Users Latest Data	Penetration (% Population)	Usage % in EU	User Growth (2000-2007)
Austria	8,213,947	**4,650,000**	56.6 %	1.8 %	121.4 %
Belgium	10,516,112	**5,100,000**	48.5 %	2.0 %	155.0 %
Bulgaria	7,673,215	**2,200,000**	28.7 %	12.3 %	411.6 %
Cyprus	971,391	**326,000**	33.6 %	0.1 %	171.7 %
Czech Republic	10,209,643	**5,100,000**	50.0 %	2.0 %	410.0 %
Denmark	5,438,698	**3,762,500**	69.2 %	1.5 %	92.9 %
Estonia	1,332,987	**690,000**	51.8 %	0.3 %	88.2 %
Finland	5,275,491	**3,286,000**	62.3 %	1.3 %	70.5 %
France	61,350,009	**30,837,595**	50.3 %	12.2 %	262.8 %
Germany	82,509,367	**50,471,212**	61.2 %	20.0 %	110.3 %
Greece	11,338,624	**3,800,000**	33.5 %	1.5 %	280.0 %
Hungary	10,037,768	**3,050,000**	30.4 %	1.2 %	326.6 %
Ireland	4,104,354	**2,060,000**	50.2 %	0.8 %	162.8 %
Italy	59,546,696	**30,763,940**	51.7 %	12.2 %	133.1 %
Latvia	2,279,366	**1,030,000**	45.2 %	0.4 %	586.7 %
Lithuania	3,403,871	**1,221,700**	35.9 %	0.5 %	443.0 %
Luxembourg	463,273	**315,000**	68.0 %	0.1 %	215.0 %
Malta	386,007	**127,200**	33.0 %	0.1 %	218.0 %
Netherlands	16,447,682	**12,060,000**	73.3 %	4.8 %	209.2 %
Poland	38,109,499	**11,400,000**	29.9 %	4.5 %	307.1 %
Portugal	10,539,564	**7,782,760**	73.8 %	3.1 %	211.3 %
Romania	21,154,226	**4,940,000**	23.4 %	27.7 %	517.5 %
Slovakia	5,379,455	**2,500,000**	46.5 %	1.0 %	284.6 %
Slovenia	1,962,856	**1,090,000**	55.5 %	0.4 %	263.3 %
Spain	45,003,663	**19,765,032**	43.9 %	7.8 %	266.8 %
Sweden	9,107,795	**6,890,000**	75.6 %	2.7 %	70.2 %
United Kingdom	60,363,602	**37,600,000**	62.3 %	14.9 %	144.2 %
European Union	**493,119,161**	**252,818,939**	**51.3 %**	**100.0 %**	**167.8 %**

High Tech Crimes:
Cyber crimes & computer related crimes

CYBER CRIME: **computer as <u>TARGET</u>**

- **Hacking (D-DOS, Botnets, Zombies…)**
- **Crimewares (Virus, Worms, Trojans…)**
- **Spamming (blackmail, cyber-stalking…)**

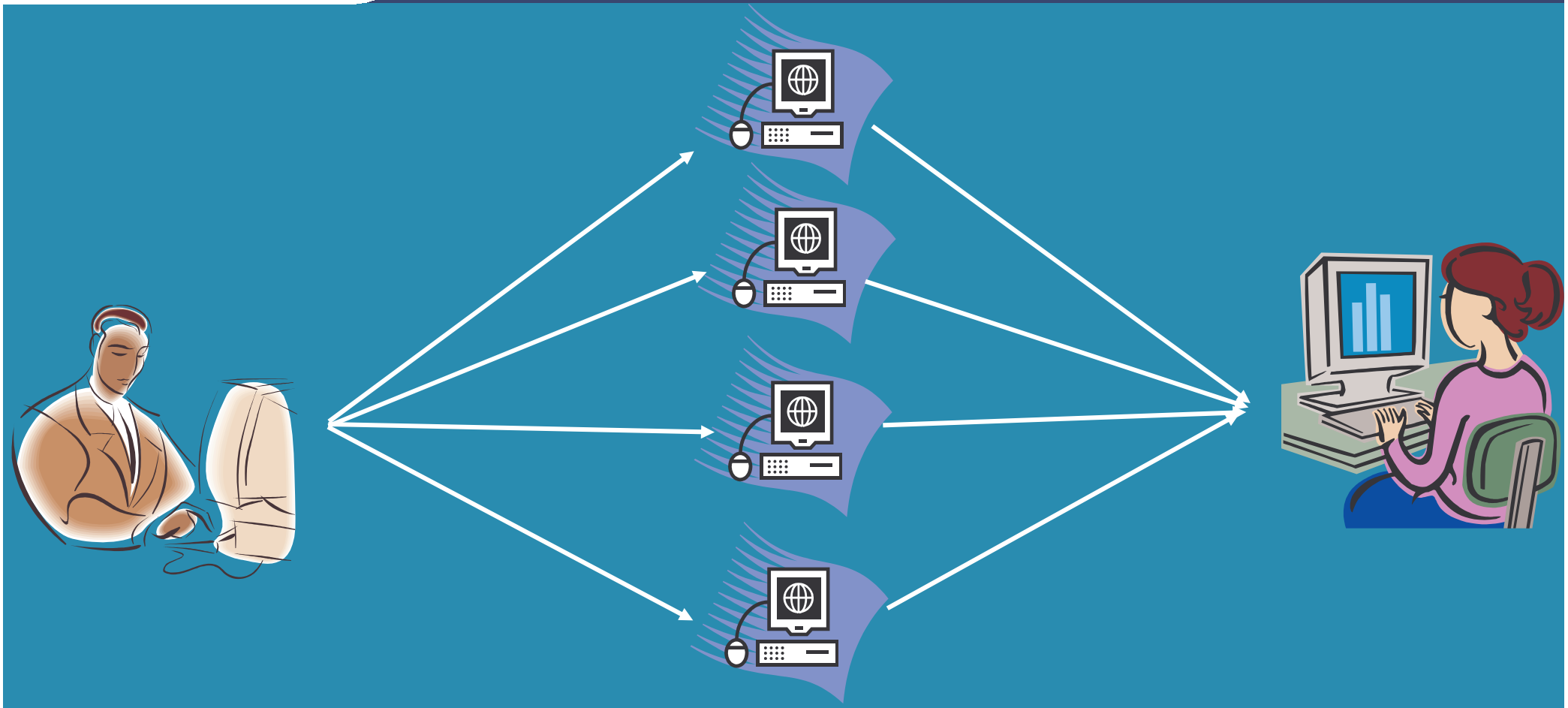
COMPUTER RELATED CRIME: **computer as <u>TOOL</u>**

E-Frauds, E-Laundering, Child Pornography, E-Terrorism, Phishing, ID-Theft, Drugs, Extortions….

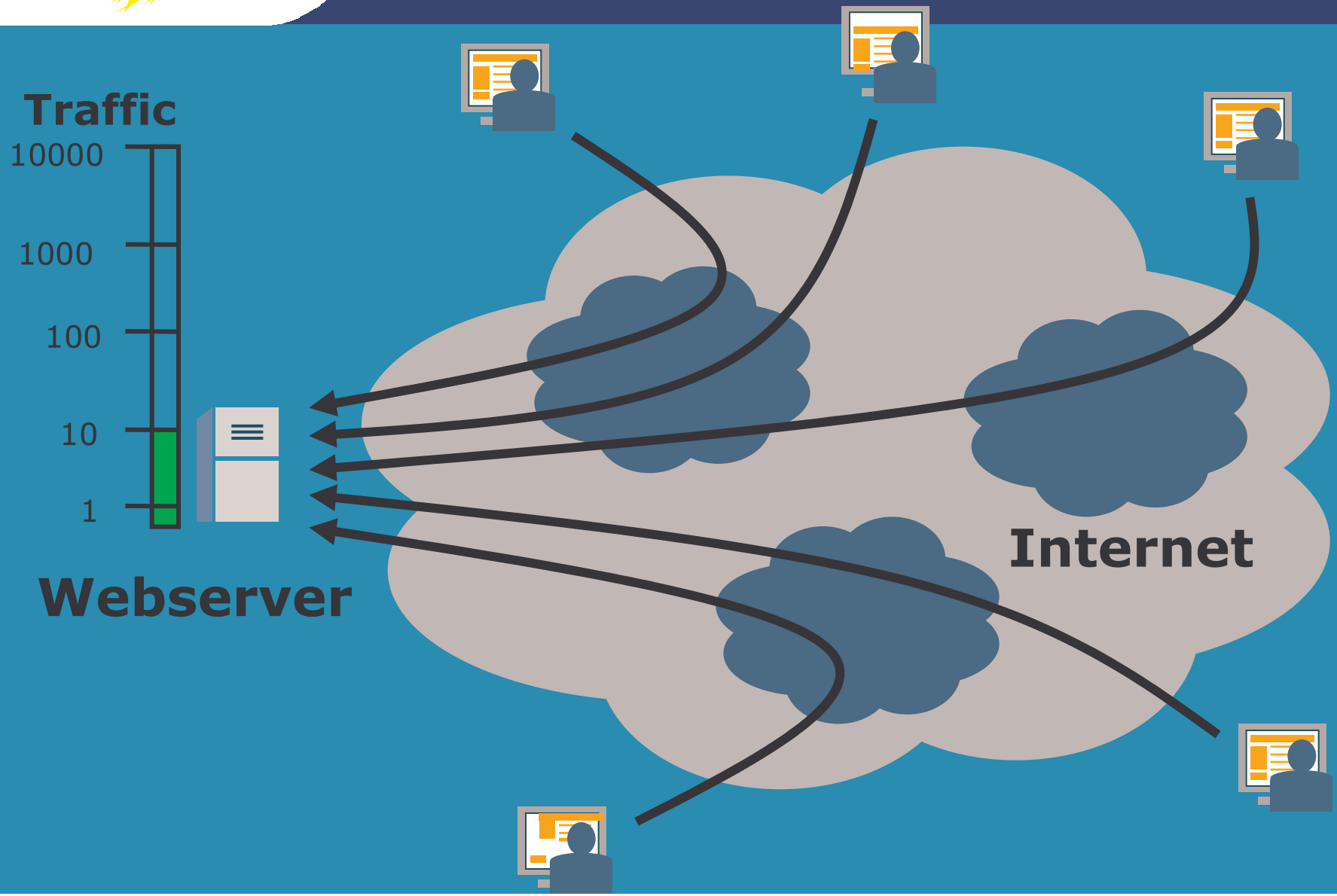
BOTNETS
and Crimewares (Malicious Codes)

- Hackers remotely manipulate millions of compromised machines
- BOTNETS come in many varieties, providing an avenue to spread new crimewares and earn money (extortions)
- New generation of crimewares points at extracting data
- Hackers are well organised and split their activities between compromising machines.
- It is very difficult to work on prevention.
- There are several initiatives at an international level

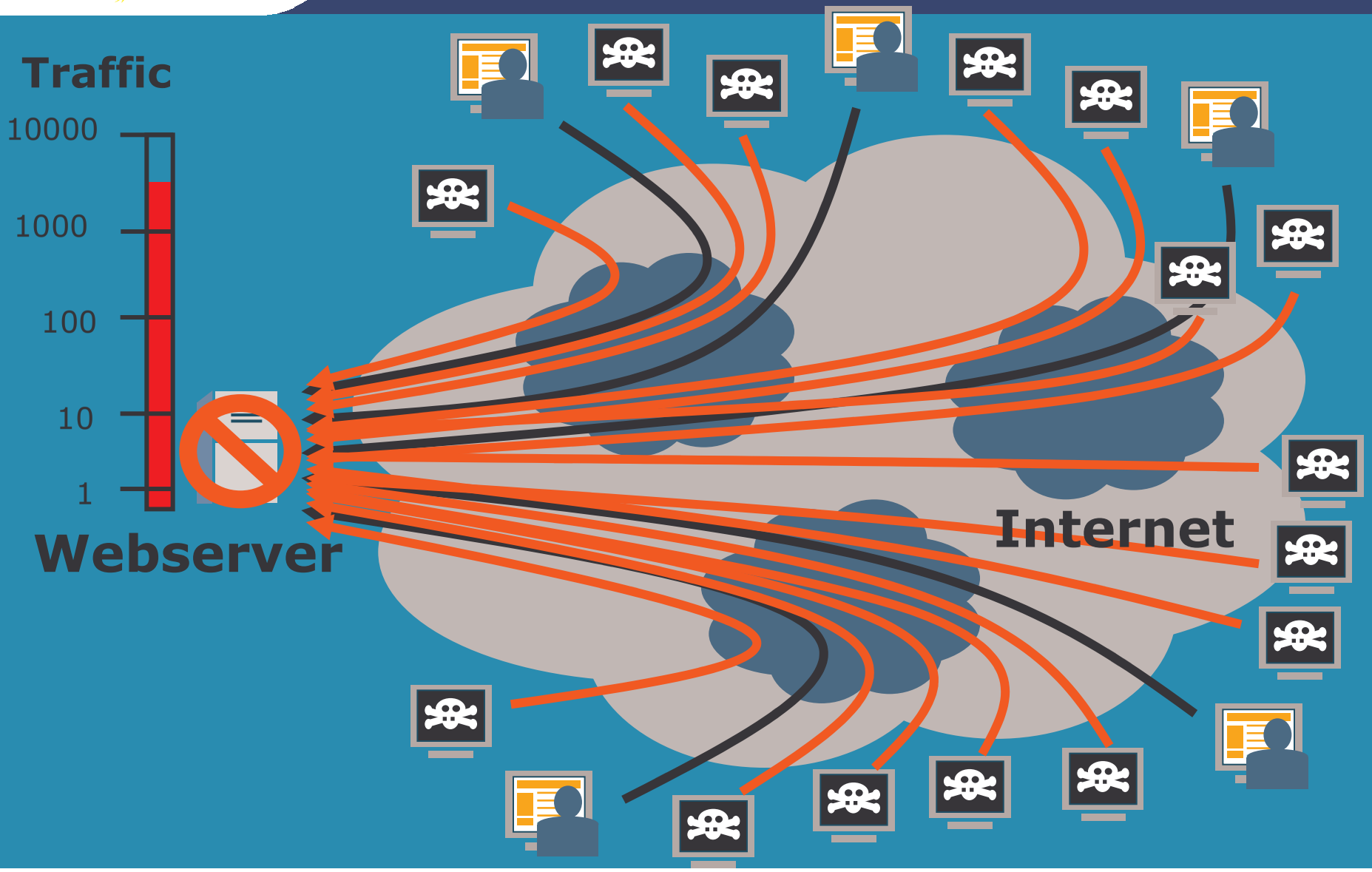
Botnets – The Attack



EUROPOL



EUROPOL



Social Engineering over Internet: Phishing and Its Varieties

- **Phishing**: a combination of E-Fraud and Identity Theft
  - It causes enormous financial losses in terms of lack of revenue and customers' lack of trust in legitimate products
  - There are several initiatives worldwide to combat phishing
  - Organised Crime uses these new e-crime facilities
  - The money obtained by phishing is laundered through other e-facilities
- **Pharming:** Manipulation of Domain Name Server
- **Vishing:** A new trend for criminals to phish over IP
- **SMiShing:** A new trend for criminals to phish over Mobile Phones SMS

Critical Information Infrastructures (CII)

- Convergence is the main issue to manage
- CII become targets of attacks
- Critical information needs to be protected
- Systems are interconnected but lack of interoperability
- Several initiatives at EU level and overseas
- Still little coordination and common strategy at EU level
- Difficulties in incident response
- Difficulties in making a risk assessment

Cyber Terrorism

- Terrorist organisations have understood how to use technology for their purposes
- There are real cyber terrorists and black hats hired to serve terrorist organisations
- Terrorist organisations exploit technology for propaganda, spread of fear, enhance communication amongst inners, and perpetrate attack against enemies' targets
- Internet is also used to e-train members of criminal organisations
- Critical Information Infrastructures networks are also targets

Trafficking of Child Pornography Images on the Internet

- Lack of global overview about the phenomenon of child pornography
- The phenomenon of child pornography is continuously growing
- New technology such as WI-FI, VoIP and Pay-per-View very much used
- Peer to Peer most used for exchange of pictures
- CP generates huge revenues
- More control needed by families, social entities and governments

Drugs trafficking over Internet

- There is widespread use of internet pharmacies without proper control
- Web sites and forums on the internet where people discuss and exchange best practice for the consumption and production of drugs, especially for the heavy trade in precursors to produce synthetic drugs.
- There is an increase in clandestine laboratories that sell drugs using the internet.
- There is a need for more consistent cooperation between law enforcement and private industry in order to better detect the illicit traffic of drugs over the internet.

Organized Crime

- Organised Crime is difficult to map out because Internet has not boundaries; information is too spread and the collection of data is difficult
- Organised crime use horizontally High Technology to pursue criminal goals
- Many individuals have links with criminal organisations
- There is still a huge lack of data about organised crime on the internet
- High Tech make the structure of criminal groups very flexible

Organized Crime

- Criminal groups easily re-shape their frameworks just after the crack down by law enforcements
- Organised crime on the internet has often an international dimension having links within and outside EU
- Organised crime uses e-commerce to launder money
- The criminal activities are a concern for the public

Cyber Criminals' Communities

- It is very difficult to understand the interaction within the cyber criminals' communities

- Depicting the structure of these groups and their interactions is very difficult for many reasons, some of them can be:
  - the communities have still young life
  - there is little background about them
  - little information is still written.

- Cyber criminals' may be driven by several motives (ideology, status, self–esteem, money)
- Groups of criminals operating on the internet are usually heterogeneous

The future??

- New approach on use of internet
- A lot of services online
- Large storage of data to remote servers offered
- Less data stored in computer
- Managing services from remote
- All is going on VOIP
- More encrypted applications (Instant Messaging)
- Growth of online groups

Conclusions

- Lack of consistent data about organised crime due to the volatility of the internet, no common reporting system & lack of reporting by the victims.
- There is little information about internet communities because they are closed groups and it is difficult to penetrate them.
- The horizontal use of hi-tech is more and more beneficial for organised crime
- The main driving factor for criminals is usually money.
- There is a rapid growth of underground economy through attacking computer systems. Hackers sell their skills online to the best bidder; the example of renting 'Exploits' or BOTNETS is very significant.
- The new generation of crimewares is more vicious, aiming at not only destroying the computer system but also to extract data.

Conclusions

- Consistent growth of social engineering on the internet: the Identity Theft is strongly involved as well as the theft of financial data
- E-commerce, and in particular the traffic of stolen credit cards on the internet, is one of the chief ways to launder money and to finance criminal as well as terrorist organizations
- Increase of child abusive content distributed and exchanged over the internet
- The Internet enables organised crime to have a very flexible structure; criminal organisations easily change tactics after a crackdown, have several links at international level with other members, and exploit the internet as a networking tool.
- HTC is beginning to be of public concern to the public: threat to critical information infrastructure networks
- The main critical issues are still users' authentication, anonymity and encryption

A Desirable Action

- Creation of common reporting system
- Improving the common understanding with private industry
- Education of users of internet in how to utilize technologies
- Large ratification of the Cyber Crime Convention for a common legal platform amongst countries
- Regulation of the public internet accesses (cyber cafés, libraries, university..)
- ISP and Telecoms cannot be deemed the only ones responsible for data retention and preservation; some businesses should be considered accountable as well
- Solve the problem of VOIP that is largely used by criminals
- Common strategy in protecting Critical Information Infrastructures
- Strength the effectiveness of communication channels

Thank You
for Your Attention

Nicola DILEONE

High Tech Crime Centre

Raamweg 47

PO-Box 90850

2596HN The Hague

The Netherlands

Tel: +31 (0)70 302 51 32

Mob: +31 (0)6 24 82 31 76

Fax: +31 (0)70 318 08 39

Nicola.Dileone@europol.europa.eu

HTCC@europol.europa.eu