

Council
of Europe

Cybercrime training for
prosecutors and judges in
South-eastern Europe
Ohrid, 17-18 November 2008

Why should judges and prosecutors worry about cybercrime?

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

www.coe.int/cybercrime

1

Preliminary remarks

Suchergebnisse

Auf Ihrem Computer wurde(n) 13 Bedrohung(en) und 186

Threats

- Registry-Wert
- Registry-Schlüssel
- Hoch **Trojan.ISTbar (7 Infizierungen)**
ISTbar is a Trojan downloader which will download a...
- Registry-Wert
- Registry-Schlüssel
- Erhöht **Adware.SideFind (34 Infizierungen)**
SideFind is an Internet Explorer Browser Helper Obj...
- Registry-Wert
- Registry-Schlüssel
- Hoch **Adware.InternetOptimizer (8 Infizierungen)**
InternetOptimizer is adware which will hijack the Inter...
- Registry-Wert
- Registry-Schlüssel
- Hoch **Backdoor.Wootbot.Gen (7 Infizierungen)**
This backdoor allows attackers access to the machin...
- Registry-Wert
- Info **Adware.Component.180Solutions (35 Infizierungen)**
Since threats created by 180 Solutions have similar fil...
- Registry-Wert
- Registry-Schlüssel
- Hoch **Worm.Spybot (1 Infizierungen)**
Worm.Spybot refers to a family of worms which initial...
- Registry-Wert
- Hoch **Adware.Component.IST (10 Infizierungen)**
Since threats created by IST have similar files and ke...
- Registry-Wert
- Registry-Schlüssel

Markierte reparieren ▶ Abbrechen Erstellen Sie vor der Entfernung einen "Restore Point".

Cybercrime affects all of us!

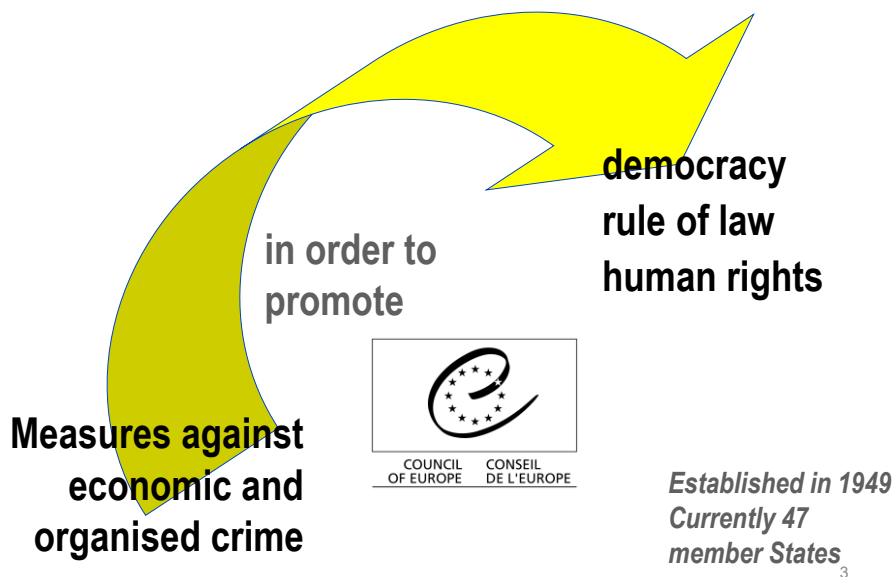
Worm.Spybot
Threat Level: Hoch
Beschreibung: Worm.Spybot refers to a family of worms which initially spread over mIRC and the Kazaa file sharing network, but have now evolved to spreading via other methods. Once infected, the worm contacts a server and performs a range of actions including, system logging including passwords and bank details, performing Denial Of Service Attacks and disabling security software.

[Mehr über diese Bedrohung erfahren](#)

oftware
tools for your PC

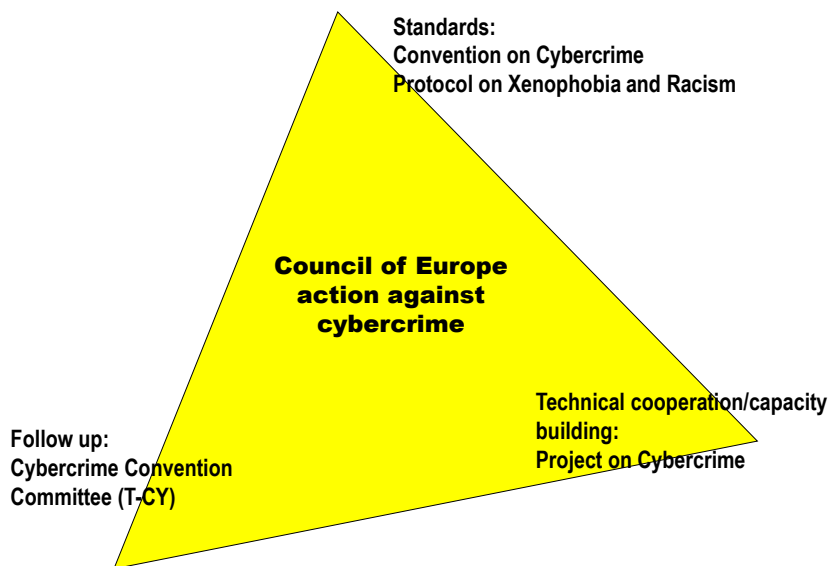
2

About the Council of Europe ... www.coe.int



3

The approach against cybercrime



4

4

1 Why worry about cybercrime?

- Opportunities provided by information and communication technologies
- Information society: where is your private life taking place?
- Confidentiality, integrity, and availability of your computer data
- Reliance of public infrastructure on ICT
- Reliance of business on ICT
- Dependency of societies on ICT = vulnerability to cybercrime
- Need for secure and accessible ICT

But:

- Vast majority of people use ICT for legitimate purposes
- Safeguards and guarantees to ensure security and protect fundamental rights

5

5

2 What is cybercrime?

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Computer-related forgery and fraud
3. Content-related offences (child pornography, xenophobia, racism)
4. Offences related to intellectual property rights and similar rights

6

6

What is cybercrime?

1. Offences against the confidentiality, integrity and availability of computer data and systems (CIA offences)

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices

7

7

What is cybercrime?

2. Computer-related forgery and fraud

Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes

- Security breaches and financial losses in companies
- Credit card fraud and other financial crime
- Advance fee fraud
- Extortion
- Internet marketing and retail fraud
- Auction fraud and stock market manipulation
- Phishing and other forms of identity theft
- Etc.

8

8

What is cybercrime?

3. Content-related offences

- Child pornography
- Xenophobia, racism, hate speech

Issue:

- Security and protection versus freedom of expression

9

9

What is cybercrime?

4. Offences related to intellectual property rights and similar rights

- IPR protected by national and international regulations
- Counterfeit products
- Health and safety risks
- Economic loss to companies and unfair competition
- Feeds organised crime

10

10

What is cybercrime?

Malware

- Software inserted into an information system that causes harm to this or other systems
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

Cross-cutting issues

11

11

What is cybercrime?

SPAM

- Accounts for a large amount of internet traffic (70%+)
- Vector for malware

Cross-cutting issues

12

12

What is cybercrime?

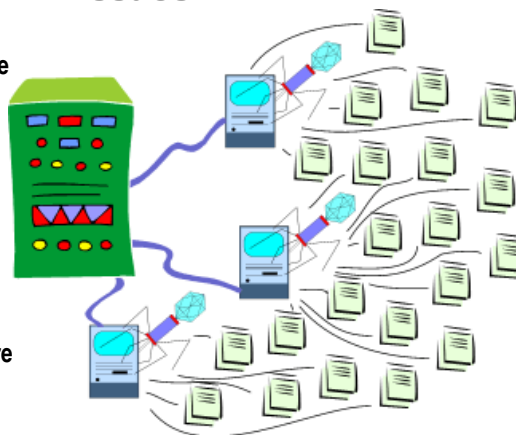
Bots and botnets

Covertly installed programmes on a computer to allow unauthorised remote control

Can be used:

- for distributed denial of service (DDOS) attacks
- to harvest confidential information (identity theft)
- to distribute spam, spyware, adware
- for phishing attacks

Cross-cutting issues



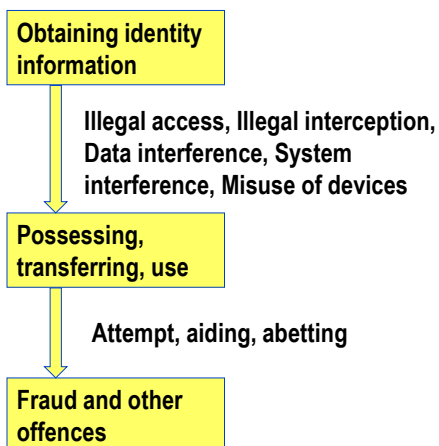
13

13

What is cybercrime?

Cross-cutting issues

Phishing and other forms of identity theft



14

14

What is cybercrime?

Cross-cutting issues

Cybercrime and organised crime

- Offenders increasingly organising for cybercrime
- Botnets an important tool
- ICT facilitate offences by OC groups and networks, in particular economic crime
- ICT creates vulnerabilities -> exploited by OC
- ICT facilitate logistics, anonymity and reduce risks of OC
- ICT facilitate global outreach of OC
- ICT shape OC -> networks

15

15

What is cybercrime?

Cross-cutting issues

Terrorist use of the internet/ICT

- Possible attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life
- Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training
- Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

16

16

3

Investigating, prosecuting, adjudicating cybercrime: challenges for judges & prosecutors

Evidence



17

17

Challenges for judges & prosecutors

Electronic evidence

Sniffer - Local Ethernet (Line speed at 100 Mbps) - [tcp-syn-attack.cap - 2/12 Ethernet frames]

No.	Src	Source Address	Dest Address	Summary
1	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=34 S=2368 SYN SEQ=277351 LEN=0 WIN=0152
2	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=38 S=2368 SYN SEQ=277353 LEN=0 WIN=0152
3	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=42 S=2376 SYN SEQ=277418 LEN=0 WIN=0152
4	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=38 S=2368 SYN SEQ=277366 LEN=0 WIN=0152
5	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=38 S=2368 SYN SEQ=277359 LEN=0 WIN=0152
6	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=42 S=2376 SYN SEQ=277426 LEN=0 WIN=0152
7	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=36 S=2364 SYN SEQ=277372 LEN=0 WIN=0152
8	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=40 S=2372 SYN SEQ=277405 LEN=0 WIN=0152
9	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=44 S=2380 SYN SEQ=277432 LEN=0 WIN=0152
10	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=37 S=2364 SYN SEQ=277379 LEN=0 WIN=0152
11	[x]	[10.1.0.2]	[10.1.0.1]	TCP: D=41 S=2374 SYN SEQ=277411 LEN=0 WIN=0152

TCP: --- TCP header ---

- TCP:
- TCP: Source port = 2368
- TCP: Destination port = 38
- TCP: Initial sequence number = 277353
- TCP: Next expected Seq number = 277394
- TCP: Data offset = 44 bytes
- TCP: Flags = U
- TCP: ...0... (No urgent pointer)
- TCP: ...0... (No acknowledgment)
- TCP: ...0... (No push)
- TCP: ...1... (No reset)

00000030: 00 01 09 40 00 26 00 04 9b 91 00 00 00 00 00 02 ...8.6.11.....*

00000030: 00 00 04 01 00 00 04 04 05 04 01 03 03 00 01 01 ...4.....*****

00000040: 08 06 00 00 00 00 00 00 00 00 00 01 01 04 02

18

Challenges for judges & prosecutors

Many different kind of devices



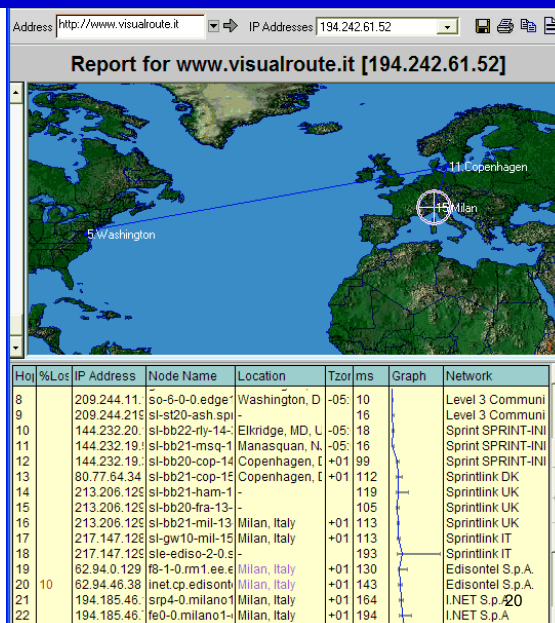
19

19

Challenges for judges & prosecutors

Electronic evidence is volatile evidence

- need for efficient, urgent measures

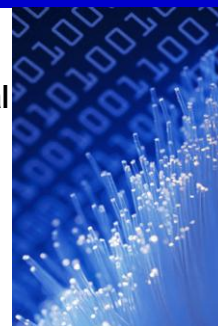


20

Challenges for judges & prosecutors

Electronic evidence

- Any data obtained from an electronic device or digital mean that serves to establish the existence of a matter of fact (01000110)
- Many different types of devices
- Large amounts of data on small storage devices
- Intangible evidence
- Integrity and preservation of evidence
- Specialised knowledge needed for analysis and interpretation
- Volatile evidence



➤ "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service

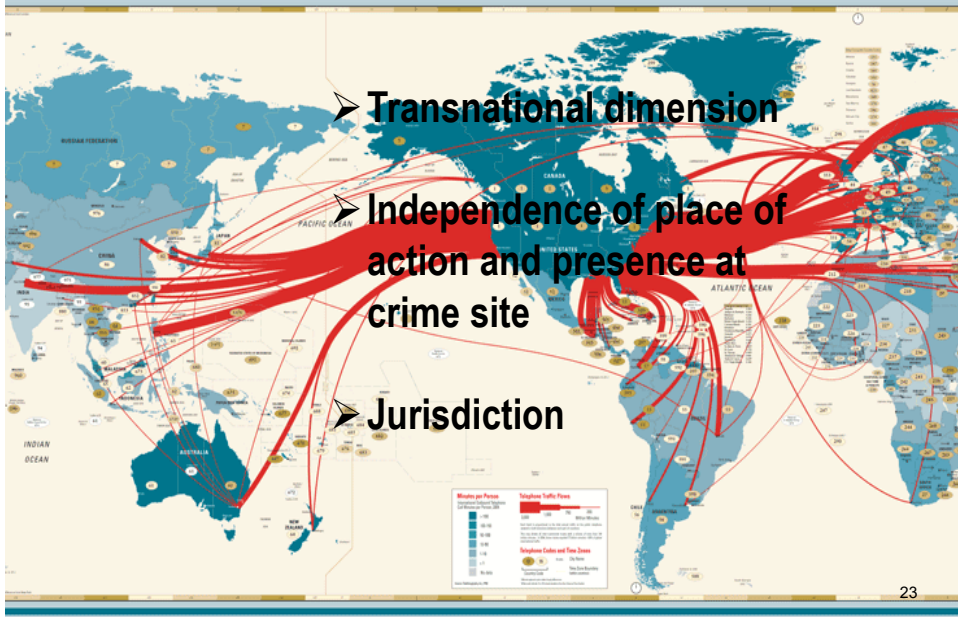
21

Challenges for judges & prosecutors



22

Challenges for judges & prosecutors



23

Follow the money



24

24

Challenges for judges & prosecutors

Law enforcement – private sector cooperation

Why law enforcement authorities (LEA) / Internet service provider (ISP) cooperation is necessary:

- Information society dependend on ICT - vulnerable to cybercrime -
Need to enhance security of ICT
- LEA and ISP play crucial role in a secure Internet
- LEA investigations often not possible without ISP cooperation
- Ensure efficient work of LEA
- Protect ability of ISP to provide services
- Ensure due process
- Protect rights of users
- How to enhance, how to structure cooperation?
- Guidelines for cooperation (Strasbourg, April 2008)

25

25

Challenges for judges & prosecutors

Security concerns and freedom rights:

- a question of balance?

**German Constitutional Court February 2008:
Confidentiality and integrity of computer data
and systems a basic right**

26

26

Challenges for judges & prosecutors

Resources, skills, training, specialisation

27

27

Challenges for judges & prosecutors

**How will judges and prosecutors deal
with these challenges?**

28

28

Global Octopus Conference

Strasbourg, 10-11 March 2009

**Legislation:
Criminalising child
pornography**

**Effectiveness of
international
cooperation against
cybercrime**

**Training resources
for law enforcement,
prosecutors, judges
and industry**

**Follow the money on
the internet**

29

29

Thank you

Alexander.seger@coe.int

30

30