

Council
of Europe

**READI Workshop on Cybercrime Legislation
in ASEAN Member States,
27-28 November 2008,
Kuala Lumpur, Malaysia**

The threat of cybercrime: what legislative responses?

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!

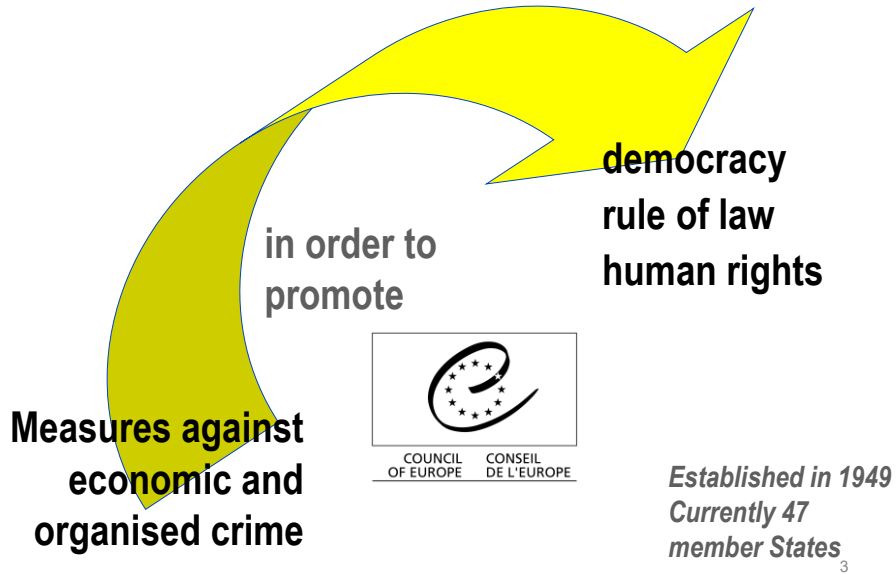
Worm.Spybot
Threat Level: Hoch
Beschreibung: Worm.Spybot refers to a family of worms which initially spread over mIRC and the Kazaa file sharing network, but have now evolved to spreading via other methods. Once infected, the worm contacts a server and performs a range of actions including, system logging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

[Mehr über diese Bedrohung erfahren](#)

oftware
tools for your PC

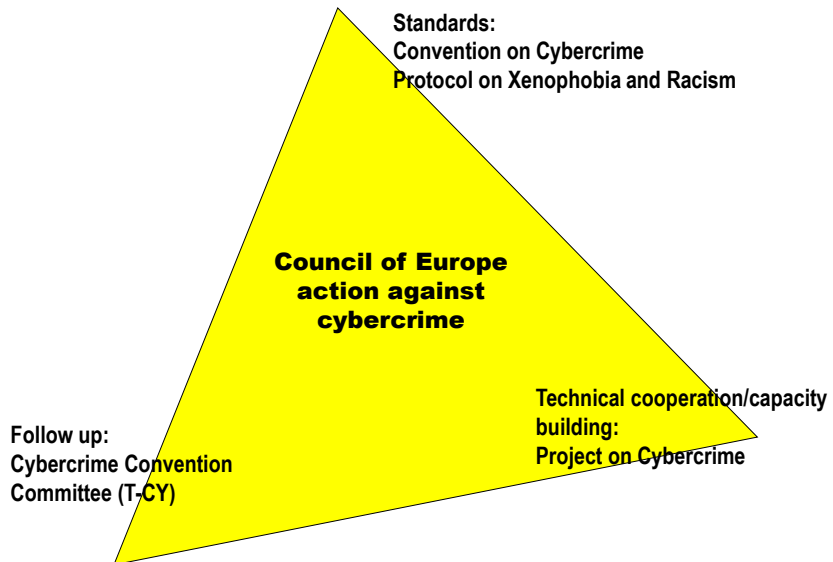
2

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?

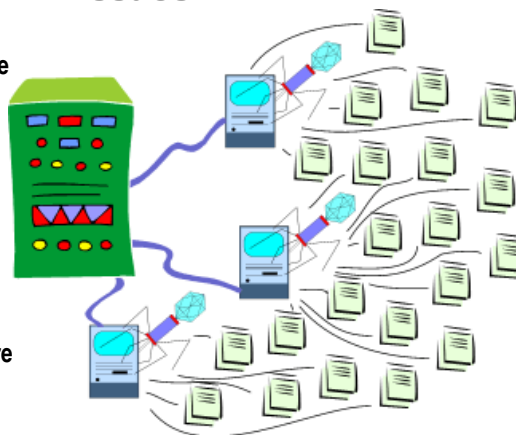
Bots and botnets

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



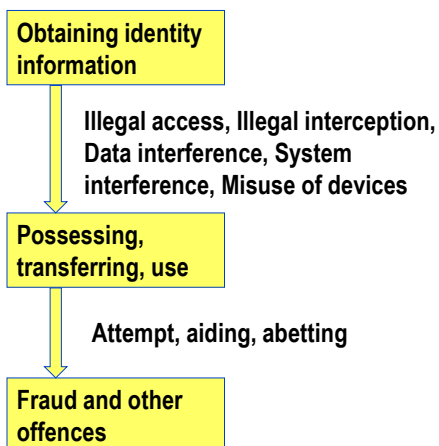
13

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

The legislative response 1: Substantive Criminal Law

Legislation to deal with – as a minimum:

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery and fraud
- Child pornography, xenophobia, racism
- Infringement of copyright and related rights

Criminalising specific techniques/technologies or conduct?

17

17

3

Investigating, prosecuting, adjudicating cybercrime: challenges

Evidence



18

18

Challenges

Electronic evidence

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of 11 packets, all originating from source IP 10.1.0.2 and destined for 10.1.0.1. The bottom pane shows the details of a selected TCP packet, including source and destination ports, sequence number, and flags.

No.	Time	Source Address	Dest Address	Summary
1	0.000000	10.1.0.2	10.1.0.1	TCP: D=34 S=2360 SYN SEQ=277351 LEN=0 WIN=8192
2	0.000000	10.1.0.2	10.1.0.1	TCP: D=38 S=2368 SYN SEQ=277353 LEN=0 WIN=8192
3	0.000000	10.1.0.2	10.1.0.1	TCP: D=42 S=2376 SYN SEQ=277418 LEN=0 WIN=8192
4	0.000000	10.1.0.2	10.1.0.1	TCP: D=36 S=2362 SYN SEQ=277366 LEN=0 WIN=8192
5	0.000000	10.1.0.2	10.1.0.1	TCP: D=39 S=2370 SYN SEQ=277399 LEN=0 WIN=8192
6	0.000000	10.1.0.2	10.1.0.1	TCP: D=43 S=2378 SYN SEQ=277426 LEN=0 WIN=8192
7	0.000000	10.1.0.2	10.1.0.1	TCP: D=36 S=2364 SYN SEQ=277372 LEN=0 WIN=8192
8	0.000000	10.1.0.2	10.1.0.1	TCP: D=40 S=2372 SYN SEQ=277405 LEN=0 WIN=8192
9	0.000000	10.1.0.2	10.1.0.1	TCP: D=44 S=2380 SYN SEQ=277432 LEN=0 WIN=8192
10	0.000000	10.1.0.2	10.1.0.1	TCP: D=37 S=2366 SYN SEQ=277378 LEN=0 WIN=8192
11	0.000000	10.1.0.2	10.1.0.1	TCP: D=41 S=2374 SYN SEQ=277411 LEN=0 WIN=8192

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 = 02
 - TCP: ...B... (No urgent pointer)
 - TCP: ...B... (No acknowledgment)
 - TCP: ...0... (No push)
 - TCP: ...1... (No reset)

00000030: 00 01 09 40 00 36 00 04 3b 91 00 00 00 00 b0 02 ...B... ..
 00000030: 20 00 b4 01 00 00 02 04 05 b4 01 03 00 01 01 ..B... ..
 00000040: 08 0a 00 00 00 00 00 00 00 01 01 04 02

19

Challenges

Many different kind
of devices



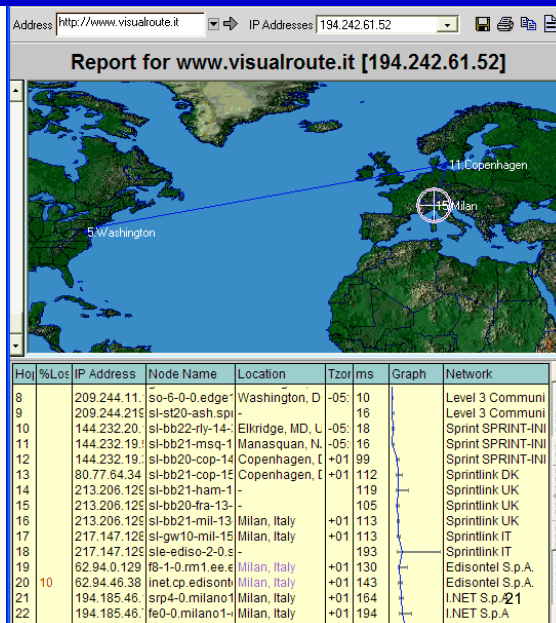
20

20

Challenges

Electronic evidence is volatile evidence

- need for efficient, urgent measures



21

The legislative response 2: Procedural Law

Legislation to provide for – as a minimum:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards

22

22

The legislative response 3: International cooperation

- Harmonise legislation with other countries
- Join international agreements
- Provide for mutual legal assistance and other provisions for international cooperation
- Introduce specific provisions for:
 - Expedited preservation of stored computer data
 - Expedited disclosure of preserved computer data
 - Mutual assistance regarding accessing stored computer data
 - Trans-border access to stored computer data (public/with consent)
 - Mutual assistance in real-time collection of traffic data
 - Mutual assistance regarding interception of content data
 - 24/7 network

25

= The Convention on Cybercrime

The Budapest Convention on Cybercrime as a response:

- A guideline for consistent substantive and procedural legislation
- A framework for efficient international cooperation

26

26



Thank you

Alexander.seger@coe.int

