CHALLENGE OF DRAFTING CYBERCRIME LEGISLATION

ITU, ICB4PAC

03.03.2011, Vanuatu

Prof. Dr. Marco Gercke, Director Cybercrime Research Institute

2. OPPORTUNITIES

OPPORTUNITIES

- Availability of computer technology improved the ability of law enforcement to carry out investigations
- DNA sequence analysis and finger print databases are examples for an emerging use of information technology in traditional criminal investigation

Picture removed in print version
Bild zur Druckoptimierung entfernt

FINGERPRINT DATABASE

OPPORTUNITIES

- New forensic technology can be very useful in computer crime and Cybercrime investigation as well
- Software tools that automatically search for key-words in text documents on the suspects computer or check the hash-values of pictures to identity child pornography are examples for highly effective forensic tools
- Internet can in addition be used to inform public about the search for suspects

Picture removed in print version
Bild zur Druckoptimierung entfernt

INTERPOL INVESTIGATION

TRACES

- “Nobody knows you are a dog” ?
- Internet users leave traces
- Access-Provider for example often for a certain period of time keep records to whom a dynamic IP-address was assigned
- Data retention obligations even increase the volume of data stored (but go along with questions related to the legality of this investigation instrument)

Picture removed in print version
Bild zur Druckoptimierung entfernt

INFORMATION STORED

E-MAIL FORENSICS

- Uses of Internet-services such as e-mail leave various traces
- Information contained in an e-mail go way beyond sender, recipient, subject and content
- Header information can help law enforcement to identify the sender of threatening mails

Picture removed in print version
Bild zur Druckoptimierung entfernt

E-MAIL FORENSICS

3. CHALLENGES INVESTIGATION

AUTOMATE

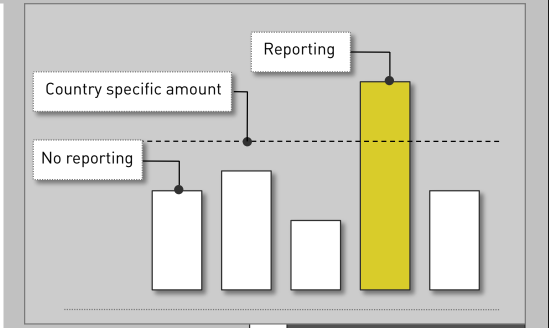
- Computer and Networks enable offenders to automate attacks
- Within minutes millions of spam mails can be send out without generating high costs - sending out one million regular letters would be very expensive and take days
- The fact that millions of approaches to illegally enter a computer system are detected every day is not a result of the high number of offenders but the ability to automate attacks

Picture removed in print version
Bild zur Druckoptimierung entfernt

WWW.HACKERWATCH.COM

AUTOMATE

- Automation enables offenders to generate high profit by committing various offences with rather small amounts each
- Background: Victims that have just lost rather small amounts tend not to report the crime



Reporting

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent of crime
- This is especially relevant with regard to the involvement of organized crime
- Available information from the crime statistics therefore not necessary reflect the real extent of crime

The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office.

HEISE NEWS 27.10.2007

AVAILABILITY OF DEVICES

- In the early days of computer and computer networks offenders committing computer crimes tend to be experts
- Today a significant number of offences are carried out by using easy-to-use tools that do not require technical knowledge

Picture removed in print version
Bild zur Druckoptimierung entfernt

RPC EXPLOIT

AVAILABILITY OF ACCESS

- Numerous possibilities to get access to the network
- Regular Internet Connection
- Mobile Data Services
- Public Terminals
- Wireless Access Points

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE INTERNET CAFE

Cybercrime
Research Institute

AVAILABILITY OF ACCESS

- Wireless networks are increasingly used to connect people
- Use of wireless networks are especially popular as they do not require the installation of wires
- But use of wireless networks increases vulnerability if the networks are not well protected
- Comfort vs. Security

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: DEMAND IN A CAFE

Cybercrime
Research Institute

AVAILABILITY OF INFORMATION

- Information that previously were available only to secret service (e.g. satellite pictures) or from very selected sources (e.g. instructions how to build bombs) are today available via the Internet
- Possibilities to restrict access to such information are limited

Picture removed in print version
Bild zur Druckoptimierung entfernt

SAT. PICTURE (WWW.MAP24.DE)

AVAILABILITY OF INFORMATION

- Industry can play a role in limiting the negative impact of the availability of information about high level targets
- Example is the restriction of resolution in satellite pictures
- Such measures can only have an impact if they are coordinated

Picture removed in print version
Bild zur Druckoptimierung entfernt

GOOGLE EARTH

AVAILABILITY OF INFORMATION

- Robots used by Search-engines can lead the disclosure of secret information
- Handbooks on how to build explosives and construct chemical and even nuclear devices are available
- Internet sources have been used by the offenders in a number of recent attacks

Picture removed in print version
Bild zur Druckoptimierung entfernt

TERRORIST HANDBOOK

AVAILABILITY OF INFORMATION

- Information regarding the construction of weapons were available long time before the Internet was developed
- Ragnar‘s Action Encyclopaedia of Practical Knowledge and Proven Techniques
- Approaches to criminalise the publication of information that can be used to

Picture removed in print version
Bild zur Druckoptimierung entfernt

RAGNAR'S ACTION ENCYCLOPAEDIA

NUMBER OF SOURCES & USERS

- Millions of webpage offer information: Difficult to identify illegal information
- Popular Services do often have millions of user

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: WWW.SKYPE.COM

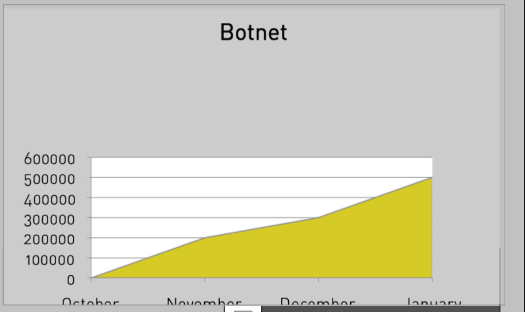
RESOURCES

- Current analysis indicate that up to a quarter of all private computer connected to the internet could be used by criminals as they belong to "botnets"

  Souce: BBC report "Criminals 'may overwhelm the web"

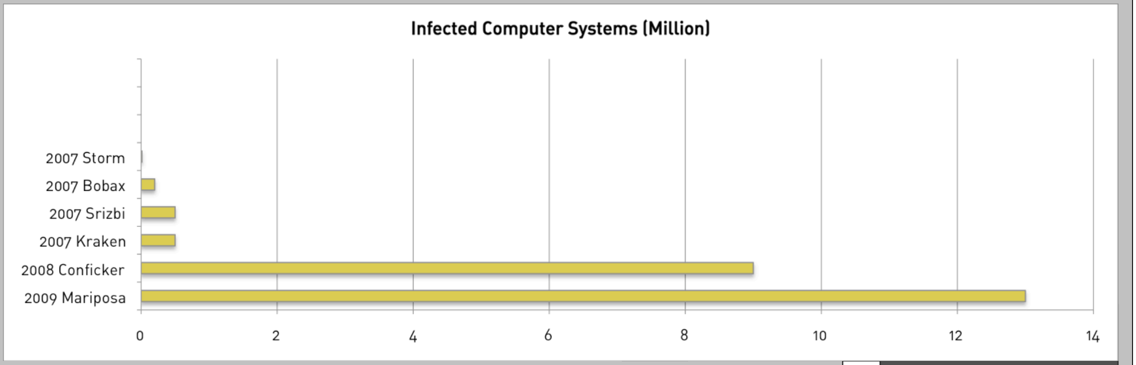
- Despite the fact that the estimation is not based on a scientifically reliable basis the growing size of detected botnets highlight the challenge

- Debate about legal response just started



WWW.SHADOWSERVER.ORG

ECONOMIC IMPORTANCE



Sources: Various

RESOURCES

- Critical mass is already reached
- Attacks in the context of the Wikileaks discussion highlight that a relatively small number of people can affect large businesses
- This underlines the threat level

LANGUAGES

- Internet enables access to content in various languages
- Number of sources is much higher compared to traditional print publication
- Fight against illegal content requires language skills of the investigator

Picture removed in print version
Bild zur Druckoptimierung entfernt

WWW.ALIAZEERA.NET

MISSING CONTROL

- Internet was developed as a military network
- Consequences: **Strategic** and **military aspects** dominated the development of the technology - not the needs of a global mass communication network
- Resistant against nearly any form of **centralised control**

Decentralised concept was a necessary element to protect the network against malfunctions caused attacks against single elements. Missing control instruments makes the implementation of investigation routines, that are necessary for a mass communication system difficult.

DECENTRALISED CONCEPT

MISSING CONTROL

Major consequences

- Very few possibilities to protect a territory against attacks from the outside
- Very few possibilities to disconnect a territory from internet services

Additional consequences

- Independence of place of action an place of the result
- International Dimension

INDUSTRY APPROACH

- Not only states and law enforcement are trying to re-territorialise the Internet
- Industry has undertaken several approaches
- Outside the Internet region codes on DVD are a well known example
- Today several Internet services are trying to limit access to content to certain regions

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: HULU

WIKILEAKS

- Another example highlighting the limited ability of governments to control information is the platform WIKILEAKS
- Controversial discussion about the advantages and disadvantages of such platforms
- Approaches of major governments to remove the website from the web in 2010 failed

Picture removed in print version
Bild zur Druckoptimierung entfernt

WIKILEAKS

INDEPENDENCE

- Technical requirements to commit Cybercrime are rather low
- Offenders can act from any place in the world
- By choosing their place of action they can take into account the status criminalisation and the capabilities of the law enforcement authorities
- Threat of “save havens”

Picture removed in print version
Bild zur Druckoptimierung entfernt

INDEPENDENCE

INDEPENDENCE

Example “Hacking”

- In the 1970th an offender needed physical access to obtain information from the victims computer system
- In the 1980th local networks enabled offenders to access computer systems remotely
- With the creation of the Internet in the 1990th connected computer systems can be accessed globally

INTERNATIONAL DIMENSION

- One of the most fundamental functions of the TCP/IP (Transfer Control Protocol and Internet Protocol) protocols is the identification of the most efficient routing
- This leads in an nearly uncontrollable way to international dimensions within data exchange processes

Picture removed in print version
Bild zur Druckoptimierung entfernt

INDEPENDENCE

SPEED OF DATA TRANSFER

- The transfer of an E-Mail normally only takes seconds
- Key information that are necessary to identify an offender are often available only for a short period of time (eg. traffic data)
- Independence between place of action an the result
- Traditional investigation instruments are not able to catch up with the speed of the information exchange.

Often important traffic information are deleted within several hours after the end of use. After several days investigations might only effective in countries with data retention.

DELETION OF INFORMATION

SPEED OF DATA TRANSFER

- Data transfer speed enables quick move of data
- Offenders can make use of the speed of data transfer processes to hinder the removal of information

Picture removed in print version
Bild zur Druckoptimierung entfernt

MOVEMENT WEBSITE

SPEED OF THE DEVELOPMENT

- Computer technology is becoming more and more complex
- Development is continuing
- Users are expecting “easy to use” software and hardware devices
- Comfort vs. Security (Open systems)
- Systems are becoming more and more **powerful** on the one hand side and **vulnerable** on the other hand side.
- **Monoculture** with regard to the operation systems

IMPORTANCE OF UPDATES

- Constant training is necessary as technology is changing
- Experts working in this field need to be aware about the consequences of the latest technical trends for investigations
- Example: Advice to unplug cord from computer can lead to an encryption of the hard drive if the suspect activated whole disc encryption

Picture removed in print version
Bild zur Druckoptimierung entfernt

US FIRST RESPONDER GUIDE 3RD ED.

DECENTRALISED SERVICES

- Availability of high-speed Internet connections and server infrastructure today enables the development of storage concepts that are not anymore based on local but decentralised storage
- „cloud computing“ and „cloud storage“

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

FAILURE OF INVEST. INSTR.

- Traditional investigation instruments are not necessary efficient enough to carry out sophisticated Internet investigation
- Significant technical and legal changes are required
- Despite the importance of specific investigation instruments traditional instruments remain important