COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Cybercrime and identity theft: the challenges

Conference on Identity Fraud and Theft : the Logistics of Organised Crime - Tomar, Portugal, November 2007

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

1 Cybercrime – current challenges

Dependency of societies on information and communication technologies. This dependency makes societies highly vulnerable to cybercrimes

Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

Child pornography and sexual exploitation on the internet increasingly commercial

Spam nuisance and carriers of malware

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

Many challenges related to ID theft

Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)

Offenders increasingly organising for crime aimed at generating illicit profits

Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)

Growing risk of cyber-attacks against critical infrastructure

2

2

2 Cybercrime and identity theft

Definitions

- The misuse of the identity (name, date of birth, address, financial information or other personal details) of another person without knowledge or consent
- Asssuming the identity of another person by stealing personnally identifiable information (PII) to commit fraud
- "Identity theft" may be used to describe the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive

3

3

Cybercrime and identity theft

- Physical methods (bin raiding, dumpster diving etc)
- Search engines
- Insider attacks
- Attacks from the outside (illegal access, trojans, key-loggers, spyware and other malware)
- Phishing and other social engineering techniques

Forms/ Methods

Obtaining identity information → **Fraud and other offences**

Sale of ID data. Goods available on underground servers:
1 Credit cards (22%) US$ 0.50 – 1
2 Bank accounts (21%) US$ 30-400
3 Email passwords (8%) US$ 1-350
7 Full identity (6%) US$ 10-150
(Symantec data for Jan – June 2007)

Assume another person's identity to:
- Exploit bank accounts, credit cards
- Create new accounts
- Take out loans and credit
- Order goods and services
- Disseminate malware

4

3 Responses

Prevention

- Measures to be taken by individuals
- Data security in public sector
- Data security in private sector
- Privacy and protection of personal data (vs authentication/data retention?)

Legislation

- Criminalise illegal access, interception, data and system interference, misuse of devices, computer-related forgery and fraud
- Make identity theft a separate offence?
- Liability for data security
- Civil remedies

Enforcement

- Facilitate reporting
- Investigate and prosecute ID theft
- Build law enforcement capacities
- Coordinaton, intelligence and analysis
- Public-private cooperation

International cooperation

- Facilitate international cooperation
- Ratify the Convention on Cybercrime

5

5

4 The Convention on Cybercrime

- Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
- Opened for signature in Budapest in November 2001
- In force since July 2004
- Now becoming a global treaty

The Protocol on Xenophobia and Racism Committed through Computer Systems

- Opened for signature in January 2003
- In force since March 2006

6

6

Structure and content of the Convention

Chapter I: Definitions

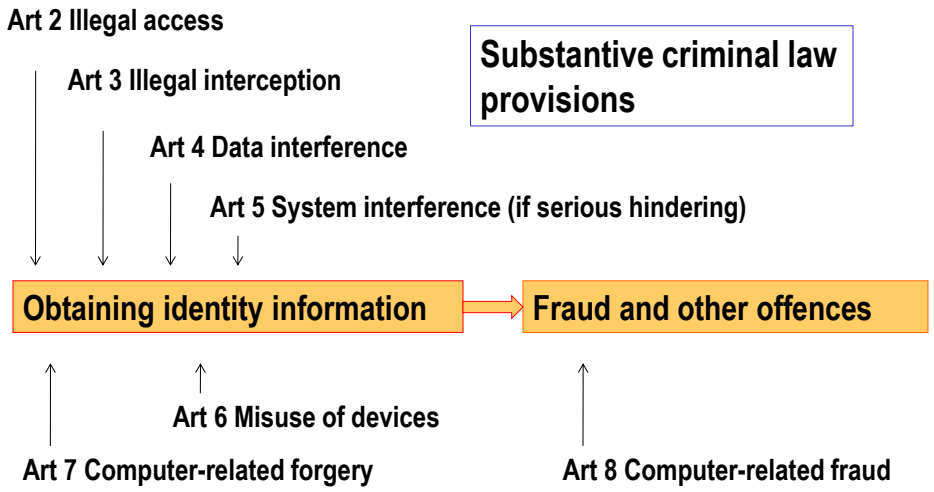
Chapter II: Measures at national level
- Section 1 - Substantive criminal law (offences to be criminalised)
- Section 2 - Procedural law
- Section 3 - Jurisdiction

Chapter III: International cooperation
- Section 1 - General principles
- Section 2 - Specific provisions

Chapter IV: Final provisions

7

7



8

8

Procedural law provisions

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

These apply to all criminal offences!

International cooperation - general and specific provisions:

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data (public/with consent)
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance re interception of content data
- Art 35 - 24/7 network

The Convention on Cybercrime

Ratified:

- Bulgaria
- Cyprus
- Denmark
- Estonia
- France
- Hungary
- Latvia
- Lithuania
- Netherlands
- Romania
- Slovakia
- Slovenia

State of implementation in European Union Member States

Signed:

- Austria
- Belgium
- Czech Rep
- Finland
- Germany
- Greece
- Ireland
- Italy
- Luxembourg
- Malta
- Poland
- Portugal
- Spain
- Sweden
- United Kingdom

11

5 Panel 2: Cybercrime and ID fraud and theft

Defining the problem, situation and trends

What are the current forms of identity theft and fraud on the internet, what is their scope and impact, what developments are to be expected?

The legal response

Are existing cybercrime and fraud provisions sufficient or should identity theft be made a separate criminal offence?

The role of service providers and the private sector

What preventive measures can be undertaken by service providers and the private sector to protect their systems and their users?

12

12