COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/moneyval
www.coe.int/cybercrime

2010 Joint EAG/MONEYVAL Typology Meeting

Criminal money on the internet: workshop findings

Workshop on criminal money flows on the Internet and misuse of e-money

Moscow, Russian Federation, 9-10 November 2010

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

1

Workshop on criminal money flows on the Internet and misuse of e-money

Presentations/discussions on:

- Session 1 – Scene setting
  - Alexander Seger (Council of Europe), Ivan Uvarov (Russian Federation), Eugene Kaspersky (Kaspersky Lab, Russian Federation)
- Session 2 – Detection, investigation, financial investigation of Internet crime and related money laundering
  - Dimitri Rudadov (Estonia), Frederic Van Leeuw (Belgium), Vladimir Kopytin (Russian Federation), Nedko Krumov (Bulgaria), Zhang Yang (China), Nurbek Ashirov (Kyrgyzstan)
- Session 3 – Cooperation and shared responsibilities
  - Svetlana Poddubskaya (Belarus), Ioana Albani (Romania), Aleksandar Naumov (Association of Russian Banks), Bertrand Lathoud (PayPal, Luxembourg), Andrey Masalovich (Scientific expert, Russian Federation), Galina Tivinskaya (Belarus))

1 Session 1 - Scene setting

In relation to criminal money flows:

- Cybercrime as
  - Attacks against computer data and systems
  - Offences by means of computer data and systems
  - Categories of Budpest Convention
- Tools, infrastucture, platforms
  - malware, botnets, criminal domains,
  - underground economy ►organised crime,
  - context of social networks and cloud computing
- Proceeds generating crime/predicate offences ►Fraud, child abuse materials, theft of digital goods and services, other crime
- Money flows ► weakest link for offenders: disposing of proceeds ► mules?
- World is online ► everybody a target ► DDOS and high-tech catastrophies
- Multi-national criminal activities
- Cyber –hacktivists, -criminals, -combatants
- Internet passports? Global Internet police?

2 Session 2 - Detection, investigation, financial investigation of Internet crime and related money laundering

In relation to criminal money flows:

- Combination of high-tech and financial investigations
- Follow the money ► Investigate also minor amounts ► Money mules ► Link money mules (1st and 2nd level, mone y collectors): trace phones (Skype), bank accounts, money transfers (Western Union)
- Close loopholes to prevent conversion of e-money to real money
- Prosecution to prosecution cooperation
- Problem of IP addresses: difficult to identify access points
- Use of Internet for phishing ► Misuse of personal data to receive, withdraw and send money via money transmitters ► Offender? Mule? Victim?
- Problem of servers based abroad for illegal activities (e.g. Online gambling) and dual criminalitity How to obtain international cooperation
- Combination with alternative remittance systems

3 Session 3 - Cooperation and shared responsibilities

In relation to criminal money flows:

- Legislation based on Budapest Convention
- Problem of understanding by judges and prosecutors
- Prosecution and court prosecutor unpredictable
- Risk management
  - Security risks
  - Reputational risks
  - Legal risks
  - Trans-border risks
- Managing and controlling risks
  - Security policies and risks (problem: protection of hardware not information)
  - Policies and procedures to detect, report suspicious activity
  - Role of regulators and supervisors
- Threat intelligence
- Public-private cooperation and information sharing (European Financial Coalition, Information Sharing and Analysis Centres (ISACS) for the financial sector
- Make use of publicly available information on the internet for intelligence purposes
- Protect information not only hardware

4 Techniques

In relation to criminal money flows:

- Use of money mules structures (1st/2nd level mules, blind mules, affiliate mules, collectors etc.)
- Use of fictitious companies to establish accounts and hire mules
- Use of bank accounts of „financial agents“
- Theft of digital goods and services (VOIP and digital goods in virtual worlds)
- Phishing and infection through fake/contaminated websites
- ATM manipulation
- Skimming/carding
- Transfer to accounts of off-shore/fake companies
- Misuse of POS terminals for payment with stolen cards
- Use of keyloggers
- ZEUS malware

5 Further points

- How far can FIUs go in internet analysis, investigations and sharing of information?
- Focus on money mules, collectors etc.
- Domestic interagency cooperation : ► What cooperation FIUs – high-tech crime units?
- How to convince police and prosecutors to follow the money ?
- Training of judges and prosecutors
- International cooperation ►How to get quicker access to international financial information?
- Create positive framework for use of ICT and only financial activities: risk of overregulation?
- Create public-private interfaces for cooperation and specific information exchange.
- From checking boxes to risk-based approaches in private sector

6 Countermeasures

1. Mechanisms for reporting on fraud and other proceeds generating offences on the internet
2. Prevention and public awareness
3. Regulation/licensing and supervision
4. Risk management in the private sector
5. Creation of a legal framework based on international standards
6. Establishment of specialised units for high-tech crime
7. Interagency cooperation, in particular between authorities responsible for financial investigations, money laundering and cybercrime
8. Public-private cooperation and information exchange.
9. Training

7 Typology study on criminal money flows: state and steps

- Finalise study for adoption by MONEYVAL in May 2011
- Document and share good practices
- Follow up through capacity building projects

8 Conclusions

- AML/CFT and anti-cybercrime worlds are converging
- After this workshop cyber criminals can rely less on keeping their proceeds than before the workshop