Funded by the European Union and the Council of Europe

Implemented by the Council of Europe

CyberCrime@IPA and CyberCrime@EaP
Public/private cooperation against cybercrime and criminal money on the Internet

Session 2: Introducing the issues

Criminal money flows on the Internet

International workshop, Istanbul, Turkey, 26-28 November 2012

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

www.coe.int/cybercrime

1

MONEYVAL / Global Project on Cybercrime: Typology study

Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction

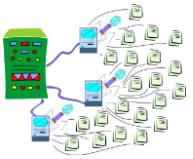
Start: Octopus Conference & MONEYVAL Plenary 2009
End: Adopted/published March 2012

(see: www.coe.int/cybercrime (reports)

2

Study: Cybercrime tools, infrastructure, platforms

- Malware
  - Viruses, worms, trojans ►remove security applications, download additional malware, infect files, steal login and account credentials and other data
  - Web remains main vehicle for malware ►infections by visiting infected sites
  - Email threats ► spam as vector for malware and fraud
- Botnets
  - Main tool for cybercrime and
  - Main risk for cybersecurity (DDOS)
  - Organising for cybercrime



- Criminal domains ►anonymous and „bullet proof“ hosting of criminal domains
- Organising for cybercrime
  - Underground economy
  - Organised crime
  - Persistent threats against political or economic targets
  - Financing of terrorism
- Money mules
- Technology/context
  - Social networking platforms
  - Cloud computing

3

Study: Cybercrime and predicate offences on the Internet

- Fraud
  - identify theft
  - man-in-the-middle-attacks
  - payment card fraud
  - account take over
  - mass-marketing fraud
  - pyramid schemes
  - confidence and action fraud
- Child abuse materials
- Counterfeit medicines
- IPR
- Extortion
- Many other forms of traditional crimes committed on the Internet

4

Study: Typologies and case studies

1. Money remittance providers
2. Wire transfers and account take-over
3. Cash withdrawals
4. Internet payment services
5. Money mules
6. International transfers
7. Digital electronic currency
8. Purchase through the Internet
9. Shell companies
10. Prepaid cards
11. Online gaming and online trading platforms

Study: Red flags and indicators for potential money laundering

- Persons holding large number of accounts with the same Internet payment services provider
- Discrepancies between submitted customer identification and IP address
- Suspicious IP addresses, and suspicious usernames
- Log-ins or attempting log-ins from non trusted IP addresses or from user's ID previously identified as associated with suspicious activity
- Unusual conditions and complexity of the transaction: high frequency of money transfers in a short time, large and diverse source of funds, large and diverse payment methods for the beneficiaries
- Etc.

Study: Countermeasures – The way ahead

- Research and other measures to prevent/mitigate AML/TF and cybercrime risks
- AML/CTF and anti-cybercrime strategies
- Legislation (harmonised with Budapest Convention and Convention 198)
- Reporting mechanisms
- Guidance and typologies for financial and non-financial institutions
- Specialised cybercrime units
- Inter-agency cooperation and parallel financial investigations when pursuing cybercrime and money laundering
- Public-private cooperation and information exchange on criminal money flows on the Internet
- Training of criminal justice and AML authorities in cybercrime and electronic evidence matters
- International cooperation between FIUs and Cybercrime Units

Criminal money @ IPA and EAP projects

- Workshop on criminal money flows, Serbia, March 2011 (CyberCrime@IPA)
- Workshop on criminal money flows, Ukraine, February 2012 (CyberCrime@IPA and CyberCrime@EAP)

Criminal money @ IPA and EAP projects

Recommendations from previous events:

- Albania: legislative reforms, training, rules on info exchange with ISPs, public awareness and reporting, legal obligations for private entities, strengthening technical infrastructure
- BiH: interagency cooperation for cybercrime and financial investigations, financial investigations in parallel with cybercrime investigations, FIU, legislation on crime proceeds, law on ISPs (data regention)
- Croatia: specialised cybercrime units, centralised body for cybercrime, involve academia, rules on cybercrime reporting (also for financial sector), judicial training, public awareness

Criminal money @ IPA and EAP projects

Recommendations from previous events:

- Montenegro: guidelines for judges and prosecutors; resources for cybercrime division within Police; create CERT; interagency, international and public/private cooperation
- Serbia: faster information exchange and access to databases; LEA/ISP MoUs, training on criminal money on Internet; rules on LEA access to private sector data; international info exchange on criminal money

Criminal money @ IPA and EAP projects

Recommendations from previous events:

- "The former Yugoslav Republic of Macedonia": Public/private cooperation on suspicious transactions; capacity building on criminal money flows on Internet; cooperation with multi-national ISPs
- Turkey: Asset recovery centre at Chief Prosecutor's Office; Internet portal for reporting; link IT systems of high-tech crime, LEA, FIU, ISPs to accelerate communications; interagency taskforce to enhance public/private (financial sector) cooperation; info flow between MASAK and ISPs; create Cyber Consultative Forum
- Kosovo*: -

Criminal money @ IPA and EAP projects

Recommendations from previous events:

- Armenia: promote interagency and public/private cooperation; awareness raising of new types of financial crime; international cooperation with off-shore countries; legislation to facilitate LEA/ISP cooperation
- Azerbaijan: Specialisation of LEA, prosecutors, judges; joint LEA/private sector training; LEA access to data bases of financial service providers; harmonise AML/CFT legislation with international standards; interagency cooperation; trusted fora; National Cybercrime Centre
- Belarus: online platform for complaint reporting, interagency cooperation, FATF recommendations in domestic legislation

Criminal money @ IPA and EAP projects

Recommendations from previous events:

- **Georgia: international cooperation, interagency taskforce to improve cooperation, PPP**
- **Moldova: amend AML legislation and CPC, expand AML reporting obligations, laws on e-payment and e-money, awareness raising at private sector, National Cybercrime Investigation Centre**
- **Ukraine: FATF Recommendations, analyse problems hindering search, seizure, confiscation of digital assets, international cooperation, website for prevention and reporting of complaints**

Criminal money @ IPA and EAP projects

For discussion in Istabul workshop:

- **What follow up has been given to previous recommendations?**
- **What additional recommendations can be made?**
- **What would be strategic priorities regarding criminal money flows on the Internet?**

Thank you

Alexander.seger@coe.int

15