Regional Seminar on Cyber Preparedness
– Cyber Crime Challenges from a Law Enforcement Perspective –

Dr. Philipp Amann, MSc
Senior Strategic Analyst, EC³
18 May 2015
Outline

• Introduction to Europol’s European Cybercrime Centre (EC3)

• Relevant Developments and Challenges

• EC3 – ‘Walking the Walk’

• Q&A
**Connected Life**

- **7,27 bn** current world population
- **3,01 bn** Internet users worldwide
- **7 bn** mobile devices worldwide
- **70%** Internet penetration in Europe
- **51%** of employees connect to unsecured wireless networks with their smartphones
- **2 mln** blog posts written today
- **90 bn** Google searches so far this year
- **24 bn** total connected devices by 2020
- **12 bn** mobile connected devices
- **423 mln** Tweets sent today
- **1,4 bn** monthly active users
- **115 bn** Emails sent today
- **7 bn** mobile devices worldwide
- **24 bn** total connected devices
- **12 bn** mobile connected devices
- **70%** Internet penetration in Europe
- **51%** of employees connect to unsecured wireless networks with their smartphones
19% Android users encountered a mobile threat

38% of user computers subjected to at least one web attack

15,577,912 malicious mobile apps worldwide

123,054,503 unique malicious objects detected

12,100 mobile banking Trojans

1,432,660,467 attacks launched from online resources

Cybercrime costs annually $445 billion or ~1% of global income

Over 307 new cyber threats every minute, more than 5 every second

Europol Unclassified - Basic Protection level / Europol Public Information
EC3 – Who We Are and What We Do

European Cybercrime Centre
The Road to Europol’s EC3

2011-2012
RAND Corporation Europe: Feasibility Study for a European Cybercrime Centre

28 March 2012
Communication of the Commission on the establishment of a European Cybercrime Centre at Europol

8 June 2012
European Council of Ministers endorsement

12 June 2012
First EC³ Programme Board
- Advisory Board created to help the strategic decision-making process of the EC³
- Members: EUCTF, CIRCAMP, ENISA, ECTEG, CEPOL, EUROJUST, CERT-EU, INTERPOL, EU Commission, EEAS, EU Council

11 January 2013
EC³ inauguration

1 January 2013
EC³ is live

23 October 2012
Second EC³ Programme Board

1 July 2012
EC³ Implementation Team starts its activities

18 June 2012
EC³ Blueprint
EC3’s Mandate

Cybercrimes committed by Organised Groups, particularly those generating large criminal profits such as online fraud (FP Terminal)

Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation (FP Twins)

Cybercrimes (including cyber attacks) affecting critical infrastructure and information systems in the Union (FP Cyborg)
EC3’s Organisational Structure

Head of EC3

MANAGEMENT SUPPORT TEAM

Head of Operations

Head of Strategy

CYBER INTELLIGENCE

OUTREACH & SUPPORT

CYRORG

------------------------

STRATEGY & DEVELOPMENT

TERMINAL

-------------

FORENSIC EXPERTISE

TWINS

(incl. Forensic Lab)
E3’s Governance Model

Programme Board
Advisory Board created to help the strategic decision-making process of E3

Assisted by 2 Advisory Groups

Financial services

Internet security
Multi-Stakeholder Approach
Core Functions

• EU cybercrime information and intelligence focal point

• Pool EU cybercrime expertise to support Members States in capacity building

• Provide coordination & support to Member States' cybercrime investigations

• Collective voice of European cybercrime investigators across law enforcement and the judiciary
**Products and Services**

- Operational, Technical and Forensic Support
- Cross-Matching of Crime-related Information
- Mobile Office & On-the-Spot Deployment
- Digital Forensic IT Lab
- Decryption Platform
- Europol Malware Analysis System
- Large File Exchange
- SPACE
  - Cyber Intelligence Knowledge Products
- Strategic Analysis Products
- Training
- Counterfeit Currency & Documents
Cooperation Mechanisms

EC3's existing cooperation mechanisms

- EMPACT OAPs
- EC3 Programme Board
- EC3 Advisory Groups
  - Internet Security
  - Financial Services
- EUCTF
- ECTEG
- EUFCC
- Forensic Expert Forum
- Cybercrime Prevention Network
- EC3 Academic Advisory Network
- Internet Governance Law Enforcement Activities
Joint Cybercrime Action Taskforce (J-CAT)

Staged Approach of the J-CAT

1. Identification of Cases
2. Preparation of Prioritised Cases
3. Investigation and Operational Activities
4. Prosecution of Investigated Cases
Cyber Challenges

- Increased Connectivity, Blurred lines between the physical & virtual life
- New Payment Systems, Electronic Money, Crypto Currencies
- Anonymisation, Obfuscation, Encryption Techniques
- Underground Cybercriminal Markets, Illegal Trade on Online Markets

Cyber-Crime

- Lack of Security by Design
- Risk of Unpatched Systems
- Borderlessness of the Internet
- Cloud-based & Mobile Devices as Targets
- Targeted Threats
- Industrialisation of Cybercrime, Cybercrime-as-a-Service
Cybercrime-as-a-Service

THE CYBERCRIME BUSINESS MODEL

- Organisation
- Cooperation
- Command

- Hackers
- Coders
- Scammers

- e-Launderers
- Recruiters
- e-Mules

PHASE 1: Building the Bots
- Execute hacks
- Develop Malware
- Build Botnets

PHASE 2: Identity theft
- Compromise users
- Commit ID Theft
- Collect Info

PHASE 3: Commit the e-Crimes
- Execute scams
- Target e-Banking
- Target e-Commerce

PHASE 4: Money laundering
- Set up e-Mule networks
- Layer money flows
- Cash out

Underground economy
Trade of stolen goods, stolen information, malware, tools, expertise and skills.
Predictions for 2015/16

New mobile payment methods (e.g. NFC) and the rise of POS, ATM attacks

Rise of the Internet of (Every)Things

Continuous penetration of mobile phones

Growing number of Internet users on a daily basis

Banking and healthcare sectors’ transition to cyberspace

Widespread use of open source code

Sophistication of malware going beyond Android and Windows

A merger between cybercriminals and APT groups

Cloud-based hosting services

Social media emerging as a new hotbed for cybercriminality
Predictions for 2015/16

Expected increase in the size, scope and sophistication of cyber threats and the emergence of new attack vectors, posing new challenges for law enforcement.
Financial Sector – Trends and Challenges

• Attacks against financial institutions directly

• Payment card fraud in the EU dominated by well structured and globally active Organised Criminal Groups

• PCF migrating to countries with no/less successful countermeasures and cooperation

• Increase in online fraud (CNP fraud) – data breaches main source of stolen data
Financial Sector – Trends and Challenges

• Physical ATM/POS Skimming on the rise – specialization by OCGs
  • Professional production of skimming devices e.g. using 3-D printers

• Attacks against the chip – ATM/POS Shimmer and Man-in-the-Middle cards

• Mobile banking and ATM malware
Financial Sector – Trends and Challenges

- Increasing activities by Asian OCGs in the EU
- Increased (ab)use of cryptocurrencies and ‘underground’ banking systems e.g. Hawala, Hund, ...
- ...
Challenges for Law Enforcement

- Cross-border cooperation and PPPs
  - Transnational crime
  - Most relevant data/evidence held by private sector
  - R&D

- Attribution
  - ‘Putting a person in front of the keyboard’
  - Who’s behind an IP address or a nickname?
  - Criminal abuse of encryption & anonymity services

- Legislation
  - Evidence physically stored in different jurisdictions
  - Identification of relevant legal framework
  - Chain of custody and admissibility of evidence
  - Timeliness, ...
Challenges for Law Enforcement

• Technical challenges
  • Digital forensics – ever increasing no. and variety of connected devices (IoE, Big Data)
  • Volatility of electronic evidence
  • Encryption, obfuscation, anti-forensics
  • Timestamps, timelines, ...

• Tools, skills and expertise
  • First responder (LE but also industry)
  • Live Data Forensics
  • Virtual infrastructure forensics
  • Remote storage and Cloud forensics, ...
EC3 – Walking the Walk...

European Cybercrime Centre
Europol-Coordinated International Botnet Takedowns

- Dec 2013: Zero Access
- May 2014: Game Over Zeus
- July 2014: Shylock
- Feb 2015: Ramnit
- April 2015: Beebone
Operation Onymous targeted marketplaces running as hidden services on the Tor network. The action aimed to stop the sale, distribution and promotion of illegal and harmful items.
Operation Onymous

Objectives:
- Stop the sale, distribution and promoting of illegal and harmful items
- Convey the message that criminals abusing TOR are not beyond the reach of law enforcement

Figures:
- 17 arrests of vendors and administrators
- 410 hidden services taken down
- Bitcoins worth approximately 1 million USD and 180,000 Euros in cash, drugs, gold and silver seized
Global Airline Action Day

Coordination centres:
Europol, The Hague, The Netherlands
Interpol, Singapore
Ameripol, Bogota, Colombia

Over 60 airlines
Over 80 airports
45 countries
EC3 Intelligence/Knowledge Products

**CYBER-INTEL**

- **Cyber Bits**
  - **Trends:** Modus operandi, tool or technique used by cyber criminals. Emerging patterns and crime series.
  - **Knowledge:** Offer guidance and raise awareness.
  - **Technology:** Technical developments having impact law enforcement work.
  - **Tools:** Presentation of tailored tools to support operational activities.

- **OSINT Dashboard**

- **Strategic Assessments of Operations**

**STRATEGY**

- **iOCTA**

- **Project 2020: Scenarios for the Future of Cybercrime**

- **Police Ransomware Threat Assessment, Review of Criminal Forums, etc.**

- **Strategic Assessments of Operations (e.g. Onymous)**

- **Quantitative Quarterly Report on Cybercrime, CC Dependencies Map**

- **ICANN Guide for Dummies, Assessment of Bitcoin, Top 10 External Cyber Threats, etc.**
iOCTA – Internet Organized Crime Threat Assessment

- EC3’s flagship strategic product
- Informs EU decision makers at strategic, policy and tactical levels
- In-house expertise and contributions from EU law enforcement, third parties, private sector, and academia
iOCTA – Internet Organized Crime Threat Assessment

- Assessment of the three main mandated cybercrime areas of EC3
- Set of key recommendations for EU law enforcement and policy makers
- Release date next version: September 2015
- https://www.europol.europa.eu/ec3
EC3 Academic Advisory Network

- Establishment of a cross-disciplinary academic advisory network of thought leaders and leading academic experts
- Advising the EC3 on key cybersocietal issues
- Forward-looking research and thought leadership
- Strategic and policy-related input
- Platform for networking
Training Competency Framework

Matrix of Required Knowledge and Skills for LE Actors

<table>
<thead>
<tr>
<th>Discussed Category</th>
<th>Management Skills</th>
<th>Technical Skills</th>
<th>Investigation Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political and Strategic Decision Makers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Enforcement Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heads of Cybercrime Units and Team Leaders</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Criminal Investigators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intermediate and Advanced Investigators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybercrime Analysts and Intelligence Officers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online Investigators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Forensic Investigators and Examiners</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Relevant Cybercrime Training:
- Basic level
- Expert level
EC3 Capacity Building & Training Coordination

Forensic Expert Training on Examination of Skimming Devices

Training course on Combating the Sexual Exploitation of Children on the Internet

Training Course on Open Source IT Forensics
Cybercrime Prevention, Communication & Events Management

- EU Cybercrime Prevention and Communication Strategy
- EU Cybercrime Network of Prevention Contact Points
- Communication and awareness-raising activities
- Events management
The Cyber Dichotomy

- Need to protect the privacy of citizens, provide a secure online environment for industry and create a safe cyberspace for everyone to enjoy

- Need for law enforcement to be able to investigate criminal activity online, including the criminal abuse of encryption and anonymity services

- The role of EC3 (platform for cooperation, pooling of expertise, tool support, R&D, training, highlighting of operational/legal issues, ...)

37