iPROCEEDS

Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey

Version 06 November 2017

Cybercrime Coordination and Partnership Exercise

Provided under iPROCEEDS project

Pristina, 13-16 November 2017

Outline

Background and Justification

In the world of today, the increasing number of attacks against computer systems and data is a growing concern for both cyber security professionals and the law enforcement. Cybercrime of today is driven mostly by financial gain and thus rapid detection and action on illegal money flows on the Internet often a necessity to identify and minimize damages from the criminal activity. The growing threat of cybercrime is further exacerbated by difficulties of access to and securing of electronic evidence, especially if information vital for criminal investigations is in the hands of private companies and is found beyond national borders. However, even where realization of these threats and challenges by policy makers and professional communities is as strong as ever, successful response to these is often hampered by lack of coordination and common approach of these communities to what should be the ultimate common goal – ensuring safer cyberspace for all.

In order to address the problems of coordination and cooperation in the most practical way, the Cybercrime Coordination and Partnership Exercise will bring together prosecutors, investigators, financial investigation/intelligence and digital forensics specialists and will be managed by a team of experts, as a command and control center.

Expected Outcome

Carried out under Result 3 of the iPROCEEDS project *Cybercrime Units, financial investigators and financial intelligence units cooperate with each other at the domestic level in the search, seizure and confiscation of online crime proceeds*, the exercise aims to strengthen the understanding of the need to exchange information between different professional communities, sometimes even in real time. The need for persons designated as contact points to coordinate efforts in an event of attack should become an accepted practice.

The goal is also to demonstrate the need for public-private partnerships in cybercrime and financial investigations in order to get access to data held by private companies, and to encourage the use of common approaches and methods for processing electronic evidence in both criminal and financial investigations on the basis of internationally accepted standards, such as the Council of Europe Convention on Cybercrime.

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

More specifically, the exercise will involve the following major themes:

- Investigate cybercrime;
- Apply digital forensics skills to identify potential perpetrators and collect potential evidence;
- Detect and handle suspicious financial transactions and money laundering; and
- Recover data through international cooperation channels.

By the end of the workshop, the participants will be able to establish closer links between professional communities of cybercrime investigators and financial intelligence/investigation officers in a real-time environment.

Participants

The event will be attended by the following participants:

- International experts on cybercrime and electronic evidence;
- Cybercrime investigators;
- Cybercrime prosecutors;
- Digital forensics specialists;
- Financial investigators;
- Financial intelligence specialists.

Administrative arrangements and location

Hotel Nartel, Kalabria Bll B2, Pristina

DRAFT Programme

Monday, 13 November 2017

9h00	Registration
09h30	Opening address • European Union • Council of Europe
09h50	Introduction to the exercise: goals, timeline, administration (plenary) • Council of Europe experts
11h00	*Coffee break*
11h30	Exercise day I: Initial intelligence feeds and crime prevention exercise
13h00	*Lunch*
14h00	Exercise day I: practical work
15h30	*Coffee break*
16h00	Exercise day I: practical work
18h00	End of day 1

Tuesday, 14 November 2017

9h00	Exercise day II: Morning briefing and practical work
11h30	*Coffee break*
12h00	Exercise day II: practical work
13h00	*Lunch*
14h00	Exercise day II: practical work

15h30	*Coffee break*
16h00	Exercise day II: practical work (workshops)
18h00	End of day 2

Wednesday, 15 November 2017

9h00	Exercise day III: Morning briefing and practical work
11h30	*Coffee break*
12h00	Exercise day III: practical work
13h00	*Lunch*
14h00	Exercise day III: practical work
15h30	*Coffee break*
16h00	Exercise day III: practical work
18h00	*End of day 3*

Thursday, 16 November 2017

9h00	Exercise day IV: Morning briefing and practical work
11h30	*Coffee break*
12h00	Exercise day IV: Presentation preparations for exercise debrief
13h00	*Lunch*
14h00	Exercise day IV: Participant preparations, report, case solutions Coordinated by Council of Europe experts
15h30	*Coffee break*
16h00	Exercise day IV: Course feedback and lessons learned (plenary) Coordinated by Council of Europe experts
17h30	Conclusions and closing
18h00	End of day 4

Contact:

Liliana TROFIM
Project Officer
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel: +40-21-201-7840
Email: liliana.trofim@coe.int
www.coe.int/cybercrime