iPROCEEDS

Targeting Crime Proceeds on the Internet in South-Eastern Europe and Turkey

EAP III

Public/Private Cooperation under the Programmatic Cooperation Framework for Eastern Partnership countries

Cybercrime Coordination and Partnership Exercise

Provided under iPROCEEDS and Cybercrime@EAP III projects

Tbilisi, Georgia, 24-28 April 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 be organized from 24 to 28 April 2017 in Tbilisi, in close partnership between the Cybercrime Programme Office of the Council of Europe (through joint action by the Cybercrime@EAP III and iPROCEEDS projects) and the Data Exchange Agency of the Ministry of Justice of Georgia. The exercise will bring together prosecutors, investigators, financial investigation/intelligence and cyber security specialists from 12 countries of the regions of Eastern Partnership and West Balkans as well as Turkey, and will be managed by a multinational team of experts from France, Ireland, Romania and the United Kingdom acting, together with CERT.GOV.GE, as a command and control center throughout the five-day exercise. Representatives of private sector companies from Georgia will also participate in the exercise to bring in the industry viewpoints in the solution of exercise scenarios.

Both CyberCrime@EAP III and iPROCEEDS projects have strong focus on public-private cooperation in cybercrime and electronic evidence.

The workplan for CyberCrime@EAP III envisages the "Regional meeting: Coordination and partnership exercise involving a wide array of stakeholders" on the week of 24-28 April 2017. During the exercise, both strategic (tabletop) coordination and technical ways to identify, process and act on electronic evidence should be practiced.

The workplan of iPROCEEDS envisages a similar case simulation exercise on cybercrime and financial investigations, which is planned for April 2017; bringing in financial intelligence and investigation units into the fold will lead to inclusion of other potential partners into the reach of the public-private cooperation and eventually will lead to wider partnerships.

Expected outcome

Carried out under Result/Immediate Outcome 2 of the Cybercrime@EAP III project (*A structured process of public/private cooperation on cybercrime underway and agreements concluded*) and Result/Immediate Outcome 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, cyber-security 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 cybersecurity incident handling and criminal/financial investigations on the basis of internationally accepted standards, such as the Council of Europe Convention on Cybercrime.

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

- Detect cyber security incidents against critical infrastructure;
- 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, cybersecurity players and financial intelligence/investigation officers in a real-time environment. If proven successful, this approach will be further developed and replicated in future activities of the Council of Europe that aim to improve states' capacities in detecting and investigating cybercrime.

Participants

The event will be attended by the following participants:

- International experts on cybercrime and electronic evidence;
- Project country team members;
- Cybercrime investigators;
- Cybercrime prosecutors;
- Financial investigators;
- Financial intelligence specialists;
- CSIRT/national CERT experts;
- C-PROC staff.

Administrative arrangements and location

The event will take place at the Radisson Blu Iveria Hotel, 1 Rose Revolution Square, Tbilisi, Georgia.

Programme

Monday, 24 April 2017

9h00	*Registration*
10h00	Opening address (plenary) • Government of Georgia • European Union • Council of Europe
10h30	Introduction to the exercise: goals, timeline, administration (plenary) • C-PROC and Council of Europe experts
11h30	*Coffee break*
12h00	Exercise day I: first injects and feeds (plenary)
13h00	*Lunch*
14h00	Exercise day I: practical work (workshops)
15h30	*Coffee break*
16h00	Exercise day I: practical work (workshops)
18h00	End of day 1
19h00	*Social dinner hosted by iPROCEEDS*

Tuesday, 25 April 2017

9h00	Exercise day II: practical work (workshops)
11h30	*Coffee break*
12h00	Exercise day II: practical work (workshops)
13h00	*Lunch*
14h00	Exercise day II: practical work (workshops)
15h30	*Coffee break*
16h00	Exercise day II: practical work (workshops)
18h00	End of day 2

Wednesday, 26 April 2017

9h00	Exercise day III: practical work (workshops)
11h30	*Coffee break*
12h00	Exercise day III: practical work (workshops)
13h00	*Lunch*
14h00	Exercise day III: practical work (workshops)
15h30	*Coffee break*
16h00	Exercise day III: practical work (workshops)
18h00	*End of day 3*

Thursday, 27 April 2017

9h00	Exercise day IV: practical work (workshops)
11h30	*Coffee break*
12h00	Exercise day IV: practical work (workshops)
13h00	*Lunch*
14h00	Exercise day IV: report to the plenary, case solutions (plenary)

	• Coordinated by Council of Europe experts
15h30	*Coffee break*
16h00	Exercise day IV: report to the plenary, case solutions (plenary) • continued
18h00	End of day 4

Friday, 28 April 2017

9h30	*Welcome coffee*
10h00	Exercise day V: lessons learned (plenary) • Coordinated by Council of Europe experts
11h00	Exercise day V: way forward for current and future projects (plenary) • C-PROC and Council of Europe experts
11h40	Conclusions and closing session (plenary) • Data Exchange Agency • Council of Europe experts • C-PROC
12h00	End of event (formal part)
12h00	*Lunch*
13h00	*Social programme hosted by Cybercrime@EAP III*

Contacts

Giorgi JOKHADZE
Project Manager (CyberCrime@EAP III)
Cybercrime Programme Office of the
Council of Europe (C-PROC)
giorgi.jokhadze@coe.int

Mariana CHICU
Project Manager (iPROCEEDS)
Cybercrime Programme Office of the
Council of Europe (C-PROC)
Email: mariana.chicu@coe.int
www.coe.int/cybercrime