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

Version 23 March 2022

International law enforcement training course on *investigating ransomware attacks*

Organised jointly by the CyberSouth, CyberEast, iPROCEEDS-2, Octopus and GLACY+ projects

3-4 of May 2022 10:00-13:30 (Bucharest time)

-on-line activity-

Outline

BACKGROUND

Cybercrime – that is, offences against and by means of computer systems – has evolved into a significant threat to fundamental rights, democracy and the rule of law, as well as to international peace and stability, and has a major social and economic impact.

Therefore, cybercrime as a transnational phenomen by its nature, continues to attract high interest from criminals and is "taking the place" of other domestic crimes and creates a huge economic impact by fraud, phishing and ransomware.

COVID-19 forced societies to rely even more on computer systems to communicate, shop, share and receive information and otherwise mitigate the impact of social distancing and other measures taken in response to the pandemic. Teleworking and virtual meetings have become the norm.

The pandemic has not only increased the reliance on information and communication technology and accelerated the digital transformation of societies, but also offered criminals new opportunities to exploit them, in the form of phishing campaigns and malware distribution, ransomware attacks (including against health facilities), fraud schemes, disinformation or increased online sexual violence against children[1]. These are not necessarily new forms of cybercrime, but the focus might be a bit different than before the pandemic, in the sense that they are targeting health care infrastructures, medicines, medical equipment, financial institutions or public information system.

The Cybercrime Programme Office of the Council of Europe (C-PROC) through its mandate on capacity building has been trying to address these new challenges faced by the criminal justice authorities, by adapting the activities as to respond to the new realities in the countries.

[1] This has been confirmed by EUROPOL, INTERPOL and reports of numerous other public and private sector organisations, including the COVID-19 Cyber Threat Coalition. An online resource by C-PROC provides further information.

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

An important focus of our capacity building support is the reinforcement of the capacities of law enforcement authorities, as they need to be equiped with the proper legal and technical tools.

The Council of Europe, within the framework of different capacity building projects, developed over the years guides and tools based on international standards and best practices on conducting cybercrime investigations and handling of e-evidence, in support to the national efforts for enhancing criminal justice capacities.

These tools are accessible to any law enforcement agency interested in using them and, together with the Budapest Convention on Cybercrime, could be successfully used in addressing the new international cybercrime trends and threats.

Moreover, to respond to the need for increased knowledge and practical skills of LEA representatives, training courses on cybercrime investigations and e-evidence were deployed to different countries, based on the training materials developed in house or by other partners.

To this end, a new training course on conducting cybercrime investigations on ransomware attacks will be put together with the support of international experts in the field.

OBJECTIVE

The aim of this training course is to provide LEA representatives from the priority countries of the following projects: CyberSouth, CyberEast, GLACY+, iPROCEEDS-2 and Octopus an understanding on the international dimension and impact of ransomware attacks. Furthermore, best practices on conducting criminal investigations on ransomware attacks, legal and technical tools to be used, as well as different investigative techniques, will be shared with the participants.

EXPECTED RESULTS

This training course is expected to:

- increase the knowledge of participants on the impact of ransomware attacks and international cooperation mechanism;
- develop practical skills of the LEA representatives on conducting criminal investigations on ransomware attacks.

PARTICIPANTS

The training course will be attended by the representatives of the priority countries of CyberEast, CyberSouth, iPROCEEDS-2, Octopus and GLACY+ projects coming from the following institutions:

- Two investigators of the Specialised Cybercrime Units from Ministry of Interior/Police/Gendarmerie;
- Two specialists of the Computer Forensic Unit/Lab from Ministry of Interior/Police/Gendarmerie.

ADMINISTRATIVE ARRANGEMENTS

The activity will take place online by using the Bluejeans videoconferencing platform. The official language of the event will be English and no interpretation or translation of materials is envisaged.

The access of the participants to the virtual meeting room will be facilitated by the project team and further instructions will be provided before the meeting.

PROGRAMME

Tuesday, 3 May 2022	
10.00 – 10.10	**Introductory remarks** Council of Europe (COE) representative and experts
10.10 – 11.40	**General overview of ransomware attacks** • Forms of ransomware and its evolution • Ransomware "as a service" • Legal aspects • Distribution of ransomware COE experts
11.40 -12.00	**Break**
12.00 – 13.30	**Conducting criminal investigation on ransomware attacks** • Tools and techniques • Malware analysis • Collection of e-evidence • Practical demonstration COE experts
13.30	**Closing of the first day**
Wednesday, 4 May 2022	
10.00 – 11.30	**Exploring different investigative leads** • TOR hidden services and encrypted communication • Ransomware platforms • Cryptocurrencies • OSINT COE experts
11.30 – 11.45	**Break**
11.45 -12.30	**Case study**
12.30 – 13.15	**International cooperation on ransomware attacks** • Preservation requests • MLA process • Cooperation with on-line service providers COE experts
13.15	**Closing**

CONTACT

Council of Europe

Virgil SPIRIDON
Head of Operations
Cybercrime Programme Office (C-PROC)
Directorate General of Human Rights and Rule of Law
virgil.spiridon@coe.int

Ioana LAZAR
Senior Project Officer
Cybercrime Programme Office (C-PROC)
Bucharest, Romania
ioana.lazar@coe.int

Monica CIMPEANU
Project Assistant
Cybercrime Programme Office (C-PROC)
Bucharest, Romania
monica.cimpeanu@coe.int

Felicia NICA
Project Assistant
Cybercrime Programme Office (C-PROC)
Bucharest, Romania
felicia.nica@coe.int