Financé
par l'Union européenne
et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Mis en œuvre
par le Conseil de l'Europe

Version 23 mars 2022

Cours international de formation des forces de l'ordre pour les *enquêtes sur les attaques par ransomware*

Organisé conjointement par les projets CyberSud, CyberEast, iPROCEEDS-2, Octopus et GLACY+

3-4 mai 2022 10h00-13h30 (heure de Bucarest)

-activité en ligne-

Aperçu

CONTEXTE

La cybercriminalité - c'est-à-dire les infractions commises contre et au moyen de systèmes informatiques - est devenue une menace importante pour les droits fondamentaux, la démocratie et l'État de droit, ainsi que pour la paix et la stabilité internationales, et a un impact social et économique majeur.

Par conséquent, la cybercriminalité, phénomène transnational par nature, continue de susciter un grand intérêt de la part des malfaiteurs et « prend la place » d'autres infractions nationales et crée un énorme impact économique par la fraude, le phishing et le ransomware.

COVID-19 a contraint les sociétés à s'appuyer encore davantage sur les systèmes informatiques pour communiquer, faire des achats, partager et recevoir des informations et atténuer l'impact de la distanciation sociale et des autres mesures prises en réponse à la pandémie. Le télétravail et les réunions virtuelles sont devenus la norme.

La pandémie a non seulement accru la dépendance à l'égard des technologies de l'information et de la communication et accéléré la transformation numérique des sociétés, mais elle a également offert aux criminels de nouvelles possibilités d'exploitation, sous la forme de campagnes de phishing et de diffusion de logiciels malveillants, d'attaques par ransomware (y compris contre des établissements de santé), de systèmes de fraude, de désinformation ou d'une augmentation des violences sexuelles en ligne à l'encontre des enfants[1] . Il ne s'agit pas nécessairement de nouvelles formes de

[1] Cela a été confirmé par EUROPOL, INTERPOL et les rapports de nombreuses autres organisations des secteurs public et privé, dont la Coalition contre les cybermenaces COVID-19. Une ressource en ligne du C-PROC fournit de plus amples informations.

Financé
par l'Union européenne
et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Mis en œuvre
par le Conseil de l'Europe

cybercriminalité, mais l'objectif est peut-être un peu différent de celui d'avant la pandémie, dans le sens où les infrastructures de soins de santé, les médicaments, les équipements médicaux, les institutions financières ou les systèmes d'information publics sont visés.

Le Bureau du Programme sur la cybercriminalité du Conseil de l'Europe (C-PROC), par le biais de son mandat sur le renforcement des capacités, a tenté de relever ces nouveaux défis auxquels sont confrontées les autorités de justice pénale, en adaptant les activités afin de répondre aux nouvelles réalités dans les pays.

Le renforcement des capacités des services répressifs constitue un axe important de notre soutien au renforcement des capacités, car elles doivent être dotées des outils juridiques et techniques appropriés.

Le Conseil de l'Europe, dans le cadre de différents projets de renforcement des capacités, a élaboré au fil des ans des guides et des outils fondés sur les normes et les meilleures pratiques internationales en matière d'enquêtes sur la cybercriminalité et de traitement des preuves électroniques, afin de soutenir les efforts nationaux visant à renforcer les capacités de la justice pénale.

Ces outils sont accessibles à toute entité chargée de l'application de la loi souhaitant les utiliser et, avec la Convention de Budapest sur la cybercriminalité, ils pourraient être utilisés avec succès pour faire face aux nouvelles tendances et menaces internationales en matière de cybercriminalité.

En outre, pour répondre au besoin d'accroître les connaissances et les compétences pratiques des représentants des services répressifs, des cours de formation sur les enquêtes en matière de cybercriminalité et les preuves électroniques ont été déployés dans différents pays, sur la base des supports de formation développés en interne ou par d'autres partenaires.

À cette fin, un nouveau cours de formation sur la conduite d'enquêtes en matière de cybercriminalité sur les attaques par ransomware sera mis en place avec le soutien d'experts internationaux dans ce domaine.

OBJECTIF

L'objectif de ce cours de formation est de fournir aux représentants de LEA des pays prioritaires des projets suivants : CyberSud, CyberEast, GLACY+, iPROCEEDS-2 et Octopus une compréhension de la dimension internationale et de l'impact des attaques par ransomware. En outre, les participants partageront les meilleures pratiques en matière d'enquêtes criminelles sur les attaques par ransomware, les outils juridiques et techniques à utiliser, ainsi que les différentes techniques d'enquête.

RÉSULTATS ATTENDUS

Ce cours de formation est censé :

- accroître les connaissances des participants sur l'impact des attaques par ransomware et le mécanisme de coopération internationale ;
- développer les compétences pratiques des représentants des services répressifs en matière de conduite d'enquêtes pénales sur les attaques par ransomware.

PARTICIPANTS

Le cours de formation sera suivi par les représentants des pays prioritaires des projets CyberEast, CyberSud, iPROCEEDS-2, Octopus et GLACY+ provenant des institutions suivantes :

- deux enquêteurs des unités spécialisées dans la cybercriminalité du Ministère de l'Intérieur/de la Police/Gendarmerie ;
- deux spécialistes de l'Unité/Laboratoire de criminalistique numérique du Ministère de l'Intérieur/de la Police/Gendarmerie.

ARRANGEMENTS ADMINISTRATIFS

L'activité se déroulera en ligne en utilisant la plateforme de vidéoconférence Bluejeans. La langue officielle de l'événement sera l'anglais et aucune interprétation ou traduction des documents n'est prévue. L'accès des participants à la salle de réunion virtuelle sera facilité par l'équipe du projet et des instructions supplémentaires seront fournies avant la réunion.

PROGRAMME

Mardi 3 mai 2022	
10h00 - 10h10	**Remarques introductives** Représentant et experts du Conseil de l'Europe (CdE)
10h10 - 11h40	**Aperçu général des attaques par ransomware** • Formes de ransomware et leur évolution • Ransomware « en tant que service » • Aspects juridiques • Distribution de ransomware Experts du CdE
11h40 -12h00	**Pause**
12h00 - 13h30	**Conduite d'une enquête pénale sur les attaques par ransomware** • Outils et techniques • Analyse des logiciels malveillants • Collecte de preuves électroniques • Démonstration pratique Experts du CdE
13h30	**Clôture de la première journée**
Mercredi 4 mai 2022	
10h00 - 11h30	**Explorer différentes pistes d'investigation** • Termes de référence - services cachés et communication cryptée • Plateformes de ransomware • Crypto-monnaies • Renseignements de source ouverte

	Experts du CdE
11h30 - 11h45	**Pause**
11h45 -12h30	**Étude de cas**
12h30 - 13h15	**Coopération internationale en matière d'attaques par ransomware** • Demandes de conservation • Processus d'entraide judiciaire • Coopération avec les fournisseurs de services en ligne Experts du CE
13h15	**Clôture**

CONTACT

Conseil de l'Europe

Virgil SPIRIDON
Chef des opérations
Bureau du programme sur la cybercriminalité (C-PROC)
Direction générale des droits de l'homme et de l'État de droit
virgil.spiridon@coe.int

Ioana LAZAR
Chargée de projet expérimentée
Bureau du programme sur la cybercriminalité (C-PROC)
Bucarest, Roumanie
ioana.lazar@coe.int

Monica CIMPEANU
Assistante de projet
Bureau du programme sur la cybercriminalité (C-PROC)
Bucarest, Roumanie
monica.cimpeanu@coe.int

Felicia NICA
Assistante de projet
Bureau du programme sur la cybercriminalité (C-PROC)
Bucarest, Roumanie
felicia.nica@coe.int