GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

2 février 2021

Activité 2.4.2

INTERPOL Webinaires Techniques en Français: Crypto pour les Autorités de Justice Pénale

15-25 février 2021

dans le cadre du projet GLACY+

Aperçu

CONTEXTE ET JUSTIFICATION

Comme l'utilisation et la dépendance aux technologies de l'information deviennent de plus en plus répandues dans la société, le ciblage et l'exploitation des systèmes informatiques est également devenue de plus en plus répandus. Les infractions qui impliquent des ordinateurs ont connu une croissance rapide, tant en nombre qu'en complexité, et les autorités de justice pénale sont appelées à faire face à un nombre croissant de défis afin d'assurer une enquête efficace et des poursuites fructueuses pour les crimes connexes. Ces dernières années, de nombreux pays ont entrepris des efforts pour établir des unités spécialisées dans la cybercriminalité au niveau des autorités de police, ainsi que des unités chargées de la criminalistique numérique.

La cryptographie est l'un des principaux outils technologiques qui permet à la technologie de l'information d'être si largement accueillie par le public. Sans cela, le faible niveau de confiance dans l'Internet aurait empêché le réseau de prendre une

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

telle ampleur. Toutefois, les connaissances en cryptographie n'ont pas été suffisamment étudiées dans le cadre de la formation des forces de l'ordre.

Dans le cadre du projet GLACY+, ce thème de formation a été testé pour la première fois dans la formation des premiers intervenants, organisée par le Groupe européen de formation et d'éducation en matière de cybercriminalité (ECTEG) et INTERPOL en septembre 2020 dans le cadre du programme E-First.

RÉSULTAT ATTENDU

La formation vise à fournir des connaissances et une compréhension conceptuelle de la cryptographie nécessaire aux responsables de l'autorité de justice pénale, notamment :

PART I. CONCEPTS DE LA CRYPTO

- Caractéristiques et capacités d'une bonne fonctionnalité de hachage cryptographique ;
- Comment les mots de passe sont stockés et volés ;
- Orientation conceptuelle des algorithmes dans le contexte de la cryptographie ancienne ;
- La cryptographie symétrique par blocs modernes et les capacités qu'elle fournit ;
- Comment deux parties peuvent partager une clé secrète en présence d'un espion/intercepteur (Internet) ;
- Pourquoi les clés publiques réutilisables sont utiles pour un réseau avec beaucoup de participants ;
- Comment le concept de clé publique a été réalisé (exemple de RSA) ;
- Capacités de non-répudiation du chiffrement à clé publique.

PART II. CRYPTOGRAPHIE APPLIQUÉE

- Comment le cryptage à clé publique a été appliqué pour devenir l'icône de cadenas (HTTPS) dans la barre d'adresse du navigateur Web ;
- Quel degré de confiance pouvons-nous accorder aux certificats, et pourquoi (HTTPS : qui vérifie l'entité et comment?) ;
- Comment le hachage et le cryptage à clé publique sont appliqués dans les transactions de Blockchain et de crypto-monnaie dans Bitcoin.

PARTICIPANTS

La participation est envisagée de la part des services chargés de l'application de la loi et d'autres services publics concernés par le sujet, impliqués en fonction des compétences et des responsabilités requises dans l'ordre du jour.

Les participants recommandés comprendraient :

- Les officiers des services de police dont le travail quotidien implique la cybercriminalité et les preuves électroniques ;
- Les procureurs et les juges qui sont intéressés à apprendre et participer à ces thèmes ;
- Les formateurs des institutions gouvernementales responsables de la formation sur le même sujet.

PROGRAMME PRÉLIMINAIRE (projet)

Date et l'heure	Thème
Lun. 15 Février 13:00 UTC 21:00 SGT	**Webinaire 1. Essentiels du hachage et cryptographie** - Fonctionnalité de hachage cryptographique, mots de passe - Algorithmes de cryptographie ancienne
Mer. 17 Février 13:00 UTC 21:00 SGT	**Webinaire 2. Cryptographie symétrique** - Cryptographie symétrique: chiffrement par bloc - Partage de clé secrète en présence d'espionnage
Lun. 22 Février 13:00 UTC 21:00 SGT	**Webinaire 3. Cryptographie asymétrique** - Pourquoi les clés publiques réutilisables sont utiles pour un réseau avec beaucoup de participants - Comment le concept de clé publique a été réalisé (exemple de RSA) - Capacités de non-répudiation du chiffrement à clé publique
Mer. 24 Février 13:00 UTC 21:00 SGT	**Webinaire 4. Confiance en Internet - certificats numériques** - Comment le cryptage à clé publique a été appliqué pour devenir l'icône de cadenas (HTTPS) dans la barre d'adresse du navigateur Web - Quelle confiance pouvons-nous accorder aux certificats, et pourquoi (HTTPS: qui vérifie l'entité et comment?)
Jeu. 25 Février 13:00 UTC 21:00 SGT	**Webinaire 5. Fondamentaux des crypto-monnaies** - Comment le hachage a permis la vérification de l'intégrité des données (exemple de blockchain) - Comment le cryptage par clé publique a permis les transactions Bitcoin

CONTACT

Au Conseil de l'Europe:

Matteo LUCCHETTI
Chef du projet GLACY+
Bureau du programme de cybercriminalité du Conseil de l'Europe (C-PROC)
Bucarest, Roumanie
Tel: +40-21 201 7832
Email: matteo.lucchetti@coe.int

À INTERPOL:

Donguk KIM
Officier spécialisé, Projet GLACY+
INTERPOL Direction de la cybercriminalité
Singapour
Tel: +65 9679 4719
Email: d.kim@interpol.int