**Convention de Budapest – Étude de cas**

**Contexte**

Vous êtes un agent des services de répression de Middle Earth, un petit pays voisin de deux autres pays : Rohan et Mordor. Vous êtes chargé d'enquêter sur des cybercrimes commis dans ce pays.

**Partie 1 Droit matériel**

Vous recevez un rapport d'information qui indique queldes lecteurs de données des systèmes informatiques d'une institution financière de renom ont été piratés par des cybercriminels inconnus et que des logiciels malveillants qui augmentent la taille du curseur de souris ont été installés sur ces systèmes. Votre enquête suggère que le logiciel malveillant a été créé par un groupe de « hackers » exploitant un forum appelé « DarkHacker ».

Une enquête plus poussée révèle que le logiciel de traduction principalement conçu pour pirater les ordinateurs est également vendu par DarkHacker sous le slogan « Achetez notre logiciel de traduction et demandez à des amis de l'installer : vous pourrez ainsi accéder à leurs ordinateurs sans autorisation! »

Pour tenter d'identifier les personnes qui exploitent DarkHacker, vous montez une opération « secrète » visant à obtenir des codes d'accès aux systèmes informatiques.

**Questions :**

* Quelle est la nature du ou des cybercrimes commis en installant des logiciels malveillants dans les systèmes informatiques de l'institution financière de renom ?
* Quelle est la nature du ou des cybercrimes qui ont été commis par les personnes qui exploitent le forum DarkHacker ?
* Avez-vous commis une infraction de cybercriminalité en achetant des codes d'accès aux systèmes informatiques sur DarkHacker ?

**Partie 2 Droit procédural**

Dans le cadre de l'opération secrète, vous obtenez des codes d'accès et des informations de paiement auprès d'un agent de DarkHacker. Vous recevez un message provenant d'un compte électronique payant [criminal@scammail.com](mailto:criminal@scammail.com) ainsi qu’un lien de téléchargement vers les codes d'accès.

Votre enquête initiale révèle que le prestataire de services qui gère la messagerie [criminal@scammail.com](mailto:criminal@scammail.com) est Scam Mail Inc., une société dont le siège social et le centre de données se trouvent sur le territoire de Middle Earth.

Vous apprenez sur son site internet que la politique de Scam Mail Inc. est de conserver les données pendant une période de 7 jours et de les supprimer après ce délai.

Vous envisagez d'utiliser les adresses de messagerie électronique pour identifier l'agent de DarkHacker.

Les renseignements que vous obtenez suggèrent que l’ampleur des opérations est beaucoup plus importante que prévu. Vous pensez qu'il est désormais nécessaire d'obtenir des informations auprès des autres personnes inconnues contactées par le biais du compte [criminal@scammail.com](mailto:criminal@scammail.com) au cours des 7 derniers jours.

**Questions :**

* Quelles mesures initiales devez-vous prendre pour que le processus d'enquête ne soit pas mis en échec ?
* De quel type d'informations avez-vous besoin pour identifier la personne qui utilise [criminal@scammail.com](mailto:criminal@scammail.com) ? Comment pouvez-vous obtenir ces informations auprès de Scam Mail Inc ?
* Comment allez-vous faire pour obtenir des renseignements auprès de Scam Mail Inc. concernant d'autres personnes contactées par [criminal@scammail.com](mailto:criminal@scammail.com) au cours des sept derniers jours ?

**Partie 3 Autres formes de coopération**

Cliquez sur le lien pour télécharger le code d'accès : vous recevez un autre message électronique à partir d'un compte de messagerie gratuit **fraud@hackmail.com** ainsi que des coordonnées bancaires.

Vous envisagez à nouveau d'utiliser l’adresse de messagerie électronique pour identifier l'agent de DarkHacker. Votre enquête initiale révèle que Hack Mail Inc. (dont le siège social est à Mordor) n'a ni bureau ni centres informatiques sur le territoire de Middle Earth, mais que cette société y a récemment diffusé des publicités en langue locale sur ses services gratuits.

Hack Mail Inc. stocke des informations sur les abonnés sous forme de données informatiques.

Vous avez parallèlement appris que plusieurs personnes de Mordor ont déclaré dans différents forums publics qu’elles avaient été victimes de fraudes qui auraient été commises par l'utilisateur du compte **fraud@hackmail.com**.

Vous souhaitez utiliser ces plaintes comme preuve dans des poursuites ultérieures. Pour ce faire, vous entrez en contact avec ces personnes pour obtenir des informations. Ces personnes sont disposées à vous donner accès à leurs comptes de messagerie et à leurs messages électroniques.

**Questions :**

* De quel type d'informations avez-vous besoin pour identifier la personne qui utilise [criminal@scammail.com?](mailto:fraud@hackmail.com)
* Quelle est la mesure la plus rapide pour obtenir de telles informations auprès de Hack Mail Inc. ?
* Quel est le moyen le plus rapide d’obtenir des messages électroniques envoyés aux victimes par l’utilisateur du compte [fraud@hackmail.com?](mailto:fraud@hackmail.com)

**Partie 4 Entraide judiciaire**

L'analyse des données obtenues vous permet d’identifier une personne chargée de la vente de données et de la prestation de services : il s’agit de Boris Smith, un ressortissant de Middle Earth.

Vous arrêtez Boris Smith dans ce pays et cette personne révèle le lieu où se trouve le système informatique utilisé par DarkHacker au Rohan. L’arrestation de Boris n'étant pas publique, il n'y a aucune raison de penser que les données sont susceptibles d’être perdues ou modifiées.

Boris vous informe que le compte [fraud@hackmail.com](mailto:fraud@hackmail.com) a été utilisé pour contacter d'autres agents de DarkHacker. Il vous informe également qu’une vaste opération de vente de codes PIN bancaires est prévue le lendemain à 17 heures en utilisant le même compte de messagerie.

* Quelles mesures pouvez-vous prendre pour contraindre HackMail Inc. à conserver les données relatives au compte [fraud@hackmail.com?](mailto:fraud@hackmail.com)
* Quelles mesures devriez-vous prendre pour identifier d'autres prestataires de services impliqués dans la transmission de communications liées à l'arnaque DarkHacker ?
* Quelles mesures pouvez-vous prendre pour obtenir des données informatiques provenant du système informatique DarkHacker ?
* Quelles mesures pouvez-vous prendre pour localiser le client de DarkHacker qui envisage d'acheter des codes PIN bancaires?