**Convention de Budapest – Étude de cas**

**Contexte**

La Terre du Milieu est un petit pays fictif en voie de développement. Situé en Afrique et voisin de deux autres pays, le Rohan et le Mordor, il est membre de l'OMC et de l'ONU et il est également partie à la Convention de Budapest sur la cybercriminalité. La Terre du Milieu abrite traditionnellement un secteur bancaire et financier florissant. Sa plus grande banque, la Middle Earth National Bank (« MENB »), possède plusieurs succursales dans la région et à l'étranger. La langue officielle de la Terre du Milieu est le termilian.

Vous êtes un agent des services répressifs de la Terre du Milieu chargé d'enquêter sur des cybercrimes commis dans cette juridiction.

.

**Partie 1 - Droit matériel**

Vous recevez un rapport anonyme indiquant que des cybercriminels ont piraté le serveur principal de la MENB. Les cybercriminels ont installé un logiciel malveillant qui modifie de façon aléatoire la taille du curseur de la souris et le fond d'écran de tous les ordinateurs connectés au serveur principal. Votre enquête suggère que ledit logiciel a été créé par un groupe de hackers connu sous le nom de « DarkHacker ».

Dans le cadre de votre enquête, vous identifiez le site officiel de DarkHacker comme étant www.darkhacker.com. Vous observez qu'un logiciel apparemment conçu pour traduire des textes du termilian vers l'anglais et vendu sur ce même site web est également commercialisé comme permettant aussi de pirater des ordinateurs.

Votre enquête révèle également que des données d'empreintes digitales permettant d'accéder à des ordinateurs portables et à des smartphones sont vendues sur [www.darkhacker.com](http://www.darkhacker.com). Pour tenter d'identifier les personnes exploitant DarkHacker, vous menez une opération sous couverture et achetez des données de ce type sur www.darkhacker.com.

**Questions :**

* Quel(s) cybercrime(s) a (ont) été commis par piratage et installation subreptice d'un logiciel malveillant sur le serveur de la MENB ?
* Quel(s) cybercrime(s) pouvez-vous identifier comme ayant été commis par DarkHacker ?
* Avez-vous commis une infraction relevant de la cybercriminalité en achetant des données d'empreintes digitales à DarkHacker ?

**Partie 2 – Droit procédural**

Dans le cadre de l'opération d'infiltration visant à acheter des données d'empreintes digitales à DarkHacker, vous êtes invité à saisir votre adresse électronique pour recevoir des instructions de paiement. Vous recevez du compte de messagerie [criminal@scammail.com](mailto:criminal@scammail.com) un courriel contenant des instructions sur la façon d'effectuer le paiement au moyen de bitcoins.

Votre enquête initiale révèle que le fournisseur de services de messagerie pour [criminal@scammail.com](mailto:criminal@scammail.com) est Scam Mail Inc. Vous identifiez son site web comme étant [www.scammailinc.com](http://www.scammailinc.com). Vous apprenez sur le même site que le siège social et le seul centre de données de Scam Mail Inc se trouvent en Terre du Milieu. Vous apprenez également que Scam Mail Inc. ne conserve les données que pendant sept jours et les détruit une fois ce délai écoulé.

Vous envisagez d'utiliser les adresses électroniques pour identifier les personnes qui se cachent derrière DarkHacker.

Vous envisagez également d'obtenir des détails sur les autres personnes contactées par le biais du compte e-mail [criminal@scammail.com](mailto:criminal@scammail.com) au cours des sept derniers jours.

**Questions :**

* Quelles mesures initiales devez-vous prendre pour vous assurer que le processus d'enquête ne sera pas entravé ?
* De quel type d'informations auriez-vous besoin pour identifier la personne qui utilise [criminal@scammail.com](mailto:criminal@scammail.com) ? Comment pourriez-vous obtenir ces informations auprès de Scam Mail Inc ?
* Comment pourriez-vous obtenir des informations 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**

Après avoir effectué le paiement en bitcoins, vous recevez d'un compte de messagerie [fraud@hackmail.com](mailto:fraud@hackmail.com) un autre courriel auquel sont jointes les données d'empreintes digitales.

Vous envisagez à nouveau d'utiliser l'adresse électronique pour identifier les personnes à l'origine de DarkHacker. Votre enquête initiale révèle que Hack Mail Inc (siège social en Mordor) n'a pas de bureau ou de centre de données en Terre du Milieu, mais a récemment publié des annonces concernant ses services gratuits en termilian. Hack Mail Inc stocke les informations relatives aux abonnés sous forme de données informatiques.

Vous apprenez que plusieurs personnes du Mordor ont dénoncé sur différents forums en ligne des incidents de fraude prétendument perpétrés par l'utilisateur de fraud@hackmail.com. Vous souhaitez utiliser ces plaintes comme preuves dans une procédure ultérieure. De plus, vous contactez ces personnes pour obtenir des informations et celles-ci se déclarent disposées à vous laisser accéder à leurs comptes de messagerie et à leurs courriels.

**Questions :**

* De quel type d'informations auriez-vous besoin pour identifier la personne utilisant [fraud@hackmail.com](mailto:fraud@hackmail.com) ?
* Quelle est la manière la plus expéditive d'obtenir ces informations de Hack Mail Inc ?
* Quelle est la mesure la plus expéditive pour obtenir les courriels envoyés par l'utilisateur de [fraud@hackmail.com](mailto:fraud@hackmail.com) aux victimes résidant au Mordor ?

**Partie 4 – Entraide judiciaire**

Après analyse des informations reçues de Hack Mail Inc. et Scam Mail Inc. vous identifiez un individu faisant partie du groupe DarkHacker : Boris Smith, un ressortissant de la Terre du Milieu.

Vous arrêtez Boris Smith en Terre du Milieu et il vous révèle l'emplacement du système informatique utilisé par DarkHacker au Rohan. L'arrestation de Boris n'ayant pas été rendue publique, il n'y a aucune raison de croire que les données du système informatique de DarkHacker risquent d’être perdues ou modifiées.

Smith 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 transaction à grande échelle pour la vente de codes PIN de cartes de débit est prévue le lendemain à 17 h via le même compte de messagerie.

* Quelles mesures pouvez-vous prendre pour que HackMail Inc. préserve les données relatives au compte [fraud@hackmail.com](mailto:fraud@hackmail.com) ?
* Quelles mesures pouvez-vous prendre pour identifier les autres fournisseurs de services impliqués dans la transmission des communications liées à l'escroquerie de DarkHacker ?
* Quelles mesures pouvez-vous prendre pour obtenir des données informatiques du système informatique de DarkHacker ?
* Quelles mesures pouvez-vous prendre pour localiser le client de DarkHacker prévoyant d'acheter des codes PIN de cartes de débit ?