****

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Division Protection des données et Cybercriminalité Direction générale des droits de l’homme et de l’État de droit Strasbourg, France  Version mars 2018 |

**Cybercriminalité et preuves électroniques : formation complémentaire pour les juges et les procureurs**

**2018**

*Présentation de l’étude de cas pour l’exercice d’investigation*

*et Guide des formateurs*



**Sommaire**

**1. Introduction ..………………………………………………………………………………………………………..3**

**2. Investigations ………………………………………………………………………………………………….……4**

**2.1 Établissement des faits initiaux**

**2.2 Établissement du début probable de l’infraction pénale**

**3. Éléments financiers…………………………………………….………………………………………………….6**

**4.** **Début des faits répréhensibles et moment clé pour les investigations.…….…………………..7**

**5.** **Fin de la perpétration et ouverture de l’affaire ………………………….………………………………9**

**6.** **Grandes étapes des investigations et preuves électroniques clés..……………………..………10**

**7. Annexes………………………………………………….….……………………………………………………….11**

**1. Introduction**

Le scénario de l’étude de cas correspond à un phénomène récemment arrivé sur le devant de la scène : les escroqueries dites « BEC », pour « Business E-mail Compromise » (piratage de la messagerie d’entreprise), dérivées des escroqueries « au président » ou « au faux intermédiaire » déjà connues. L’ampleur de ces escroqueries est énorme.

Les victimes subissent des dommages substantiels et en augmentation constante, malgré les efforts continus engagés par les pouvoirs publics et par le secteur privé dans de nombreux pays du monde pour tenter de sensibiliser les entités publiques et privées. Malheureusement, les dernières informations sur le préjudice financier total dans le monde n’amènent pas à conclure que des progrès auraient été réalisés dans ce domaine.

*Note aux formateurs :* **Pour commencer, le scénario présente la Federal Bank of Atlantis (FBA) comme une banque ancienne et à la réputation bien établie. La description devrait amener les participants à penser que ce type de banque est à l’abri des problèmes, *a fortiori* tels que ceux qui seront décrits plus loin.**

Ce sont pourtant les banques de ce type, précisément, qui sont aujourd’hui régulièrement visées par les escroqueries BEC, peut-être en raison de leur réticence à adapter leurs procédures de sécurité aux nouveaux risques ou d’un faux sentiment de sécurité dû à leur importance et à leur présence mondiale.

**À la fin de la formation, les participants devraient avoir pris conscience que même les banques et institutions financières renommées peuvent être les cibles et les victimes d’escroqueries.** Dans ce cas, les investigations révéleront aussi que la BEC s’appuie sur la menace persistante avancée (MPA), sur la manipulation psychologique et sur le recours aux crypto-monnaies.

*Note aux formateurs :* **L’idée derrière cet exercice est d’approfondir l’approche juridique investigative, en amenant les participants à utiliser étape par étape les outils juridiques à leur disposition pour mener une investigation très proche du réel et monter un dossier pénal.** L’exercice combine des articles de la Convention de Budapest et des dispositions juridiques internes permettant de résoudre l’affaire avec succès, de la phase d’investigation à la décision finale en passant par les poursuites et le procès. Il englobe aussi des mesures importantes qui peuvent, et devraient, être prises dans le cadre du processus d’entraide judiciaire conformément à la Convention.

Des pays fictifs ont été créés aux fins de la formation. Ce sont notamment Atlantis, Norland, Ostland et Westland. **On considère que tous ont ratifié la Convention du Conseil de l’Europe sur la cybercriminalité (« Convention de Budapest »).** Cette approche devrait permettre d’organiser la formation dans différents pays sans devoir modifier notablement les supports de formation.

*Note aux formateurs :* **À l’issue de cette session, les participants devraient savoir :**

* **identifier les personnes morales et physiques présentes dans le scénario ;**
* **expliquer la structure de l’affaire et les faits initiaux ;**
* **suivre et expliquer l’enchaînement et l’évolution des investigations ;**
* **établir comment et par où les investigations pénales devraient commencer, et selon quelles procédures.**

**2. Investigations**

**2.1 Établissement des faits initiaux**

*« La Federal Bank of Atlantis (FBA) est une banque européenne bien connue, sérieuse et prospère. Elle dispose de nombreux établissements et succursales dans plusieurs pays en Europe et dans le reste du monde. Ses activités bancaires et commerciales sont réputées fiables et solides. Sa politique semble lui attirer plus de clients que les banques concurrentes, aussi bien pour l’ouverture de comptes que pour l’utilisation d’autres produits bancaires.*

*À l’occasion des 100 ans de la banque, le Conseil d’administration de la FBA décide d’émettre une obligation « spéciale anniversaire ». Le Conseil charge le Département de la logistique et des opérations (DLO) de préparer l’impression des obligations, et notamment de trouver un imprimeur à même de fournir toutes les prestations nécessaires.*

*Le DLO trouve un fournisseur, bien connu dans le domaine des produits et services d’impression. Il s’agit d’United Bank Printing (UBP), dont le siège se trouve à Atlantis, avec une succursale européenne en Norland. En interne, le DLO est également en contact à ce sujet avec le Département des finances de la FBA ».*

**Les principaux faits :**

* la Federal Bank of Atlantis (FBA) est une banque bien connue, sérieuse et prospère ;
* la FBA souhaite émettre une obligation spéciale pour son anniversaire ;
* le Département de la logistique et des opérations (DLO) est en charge de l’organisation logistique dans le cadre de ce projet ;
* United Bank Printing (UBP) fournira le matériel d’impression ;
* le DLO associe le Département des finances de la FBA à la logistique de l’opération.

*Note aux formateurs :* **Les participants doivent identifier les principaux faits, ainsi que les départements et décideurs clés des entreprises, pour cerner l’étendue et la composition du milieu professionnel dans lequel les faits vont se dérouler.**

**Supports d’étude de cas à utiliser :**

* *Dossier « 2e jour/2.2.2, Introduction à l’exercice d’investigation/Lectures préalables » :*
* Synopsis de l’étude de cas ;
* Présentation de l’étude de cas et Guide des formateurs sur l’étude de cas pour l’exercice d’investigation ;
* *Dossier « 2e jour/2.23, Exercice d’investigation/Preuves/Profils » :*
* Profil de l’entreprise Federal Bank of Atlantis ;
* Profil de l’entreprise United Bank Printing ;
* Profil de l’entreprise Docklands Security Bank of Norland.
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Documents et rapports » :*
* Annonce de l’obligation anniversaire par la FBA ;
* Obligation anniversaire.
* *Dossier « 2e jour/2.2.3, Exercice d’investigation/Preuves/E-mails » :*
* 1er e-mail ;
* 2e e-mail.

**Exemples de questions à poser aux participants :**

*- Quelles autorités et quels types d’outils juridiques seront utilisés au niveau local pour établir les principaux faits susmentionnés ?*

*- Quelle influence ces faits auront-ils sur l’évolution ultérieure des investigations ?*

**2.2 Établissement du début probable de l’infraction pénale**

*« En raison des congés d’été, les effectifs du DLO sont clairsemés, si bien que le chef adjoint du département confie à des employés fraîchement recrutés la tâche de travailler à ce projet (passer des appels, coopérer avec leurs collègues du Département des finances) ».*

*Note aux formateurs :* **L’exposé du fait qu’en raison des congés d’été, une opération aussi délicate a été confiée à de nouvelles recrues devrait vite éveiller l’attention des participants.** L’élément clé est qu’un de ces nouveaux employés est en fait membre d’un groupe criminel organisé. Il s’est porté candidat pour un poste subalterne au DLO en vue d’obtenir un accès direct aux ordinateurs de la FBA. Son but était de lancer un logiciel espion capable de transmettre à un ordinateur et à un utilisateur spécifiques (en l’occurrence lui-même – principal suspect), des copies des courriers électroniques entre le DLO et le Département des finances de la FBA et les entreprises partenaires. Ce type d’accès permet d’étudier et de repérer la cible possible d’une attaque BEC.

**Supports d’étude de cas à utiliser :**

* *Dossier « 2e jour/2.2.3, Exercice d’investigation/Preuves/E-mails » :*
* 1er e-mail ;
* 2e e-mail ;
* 5e e-mail ;
* 7e e-mail.

**Exemples de questions à poser aux participants :**

*- Quelles actions devraient être lancées, et par quelles autorités, pour établir l’identité de l’auteur présumé ?*

*- Comment déterminer le type de logiciel malveillant utilisé ?*

*- Comment déterminer les effets de ce logiciel, les traces de communication entre ce logiciel et des points de contact extérieurs, et à quels autres faits importants les investigations devraient-elles s’intéresser à ce stade ?*

**3. Éléments financiers**

*« La FBA commande à UBP 20 000 impressions sur papier spécial pour un montant de 300 000 euros. Les départements concernés au sein de la FBA et d’UBP entament les démarches logistiques et financières.*

*La FBA et UBP échangent des détails sur la facturation et le paiement, dont les identifiants SWIFT et IBAN. UBP demande le versement d’un paiement anticipé de 100 000 euros sur son compte à la Docklands Security Bank of Norland. Le versement est effectué dans les 24 heures suivant l’acceptation de l’ordre de virement ».*

Outre l’exposé des éléments financiers, les faits principaux s’enrichissent de quelques informations :

*- L’entrée dans le cercle des entreprises concernées de la Docklands Security Bank of Norland, banque désignée par UBP pour le transfert de fonds ;*

*- le versement réussi du paiement anticipé de 100 000 euros de la FBA à UBP sur le compte à la DSBN ;*

*- le fait que l’opération ait nécessité l’usage d’identifiants SWIFT et IBAN.*

*Note aux formateurs :* **Ces éléments montrent que le premier virement bancaire a été réalisé sans problème ; la mention des identifiants SWIFT et IBAN indique qu’il s’agissait d’un virement international, et non national.** De ce fait, les participants devraient commencer à envisager le recours aux articles de la Convention de Budapest sur l’entraide judiciaire internationale.

**Supports d’étude de cas à utiliser :**

* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Documents et rapports » :*
* Contrat FBA-UBP.
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Relevés bancaires » :*
* facture pro forma d’UBP ;
* relevé bancaire de la FBA ;
* relevé bancaire d’UBP.
* *Dossier « 2e jour/2.23, Exercice d’investigation/Preuves/E-mails » :*
* 3e e-mail ;
* 4e e-mail ;
* 6e e-mail ;
* 7e e-mail ;
* 8e e-mail.

**Exemples de questions à poser aux participants :**

* *Quelles sont les principales clauses de fond du contrat ?*
* *Comment et quand le paiement anticipé a-t-il été effectué ?*
* *Ce virement s’est-il fait sans problème ? Pourquoi ?*
* *Le virement a-t-il pu être suivi par un tiers indésirable ?*
* *Si oui, comment ?*

**4.** **Début des faits répréhensibles et moment clé pour les investigations**

*« Le contrat prévoit la réalisation de 20 000 impressions sur papier spécial dans un délai de sept jours. UBP remplit cette obligation un jour avant le délai. Le Département commercial signale au Département des finances d’UBP que les impressions sont prêtes et seront expédiées dès l’encaissement du paiement définitif.*

*Le Département des finances d’UBP envoie un e-mail à son homologue de la FBA pour l’informer que la commande est prête est que le paiement final de 200 000 euros est dû dans les 48 heures. Ce soir-là, la FBA reçoit un e-mail d’UBP l’informant que le compte bancaire de l’entreprise en Norland sera inaccessible dans les trois jours à venir en raison de la fête nationale en Norland. L’e-mail demande que le solde soit versé sur le compte d’UBP à la Docklands Security Bank of Norland en Ostland ».*

*Note aux formateurs :* **Il faut situer ici l’élément déclencheur de la perpétration des faits répréhensibles.** Le membre déjà mentionné du groupe criminel organisé, à l’aide du logiciel espion, a pu détecter et suivre les échanges entre la FBA et UBP sur cette opération. Il ne lui reste plus qu’à réagir rapidement au moment du paiement définitif, c’est-à-dire dès qu’UBP signale à la FBA que les impressions demandées sont terminées.

Lorsque le Département des finances d’UBP a notifié à son homologue à la FBA que le paiement était dû, l’« infiltré » a intercepté l’e-mail et averti le reste du groupe criminel. Avec ses complices, il était prêt à envoyer de fausses factures établies au préalable, avec des en-têtes d’e-mail presque identiques à ceux du Département des finances d’UBP, en utilisant un serveur SMTP libre loué avant le début de la perpétration de l’infraction.

**Variante du scénario :** si les formateursconstatent que les participants ont des connaissances techniques limitées, ils peuvent expliquer que la véritable adresse électronique de l’employé du Département des finances d’UBP a été légèrement modifiée, sans évoquer l’utilisation d’un serveur SMTP libre ; cela permettra d’éviter des problèmes dans le déroulé de l’exercice d’investigation.

Le groupe criminel a spécialement ouvert dans l’autre pays (Ostland dans l’exercice) un compte pour une entreprise prête-nom, portant le même nom que l’originale (UBP dans ce cas), dans une succursale de la banque mère : c’est donc un compte bancaire frauduleux qui a été ouvert dans la succursale de la Docklands Security Bank of Norland en Ostland. Le compte bancaire est resté dormant jusqu’au virement de la FBA et ses coordonnées étaient connues de l’auteur principal de l’infraction et de ses complices. Le compte a été enregistré avec des données falsifiées presque identiques aux originales, fondées sur les coordonnées des employés du Département des finances de la FBA.

Un sentiment d’urgence est venu s’ajouter à tout ce montage, via l’annonce de la fête nationale en Norland. Les criminels ont utilisé ce prétexte pour justifier le changement de compte bancaire. Il ne leur manquait plus qu’à passer à l’acte.

**Principaux faits :**

* *les impressions sur papier spécial ont été réalisées et UBP le signale à la FBA en demandant le versement du solde ;*
* *via le logiciel espion, le membre infiltré du groupe criminel organisé détecte le moment de clôture imminente de l’opération ;*
* *le groupe a enregistré une entreprise prête-nom en Ostland et ouvert un compte bancaire au nom de cette entreprise dans une succursale de la banque habituelle d’UBP en Norland ;*
* *de faux documents, dont une fausse facture, un serveur de courrier électronique et des e-mails, ont été préparés ;*
* *un serveur SMTP libre a été réservé et testé en vue d’envoyer de faux e-mails (on peut aussi simplifier l’exemple en mentionnant la création d’une adresse électronique très proche de l’originale) ;*
* *la location du serveur SMTP libre a été payée en bitcoins (pas de paiement si le scénario retient l’utilisation d’une fausse adresse électronique) ;*
* *de faux e-mails ont été préparés, avec les noms des véritables employés, des détails sur le contrat et des formulations déjà utilisées auparavant.*

**Supports d’étude de cas à utiliser :**

* *Dossier « 2e jour/2.2.3, Exercice d’investigation/Preuves/E-mails » :*
* 9e e-mail ;
* 10e e-mail.
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Relevés bancaires » :*
* fausse facture d’UBP
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Documents et rapports » :*
* enregistrement de l’entreprise prête-nom UBP en Ostland ;
* enregistrement du compte de l’entreprise prête-nom UBP à la DSBN en Ostland ;
* rapport des résultats du scan anti-logiciel espion ;
* rapport d’établissement du réseau de serveurs SMTP ;
* rapport du paiement en bitcoins auprès du prestataire de serveurs SMTP.
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Dépositions de témoins » :*
* Déposition du chef du Département informatique de la FBA.

**Exemples de questions à poser aux participants :**

* *Comment les informations sur la finalisation de l’opération ont-elles été acquises et comment les récupérer, si possible ?*
* *Comment trouver des informations sur l’entreprise prête-nom et sur ses coordonnées bancaires en Ostland ?*
* *Quels types d’informations devraient être demandés à l’Ostland et de quelle manière ?*
* *Certaines de ces informations devraient-elles être récupérées en urgence, justifiant l’activation du Point de contact 24/7 du Réseau CdE ?*
* *Comment obtenir des preuves de la copie/falsification de documents et comment les analyser ?*
* *Comment recueillir des informations sur le serveur SMTP libre (ou sur le prestataire de courrier électronique) et que peuvent-elles révéler ?*
* *Qu’est-ce que le bitcoin, comment a-t-il été utilisé et comment peut-il être utilisé comme preuve électronique ?*
* *En récapitulant, quelles sont les preuves électroniques qui peuvent être obtenues ?*

**5.** **Fin de la perpétration et ouverture de l’affaire**

*« Le lendemain, le Département des finances de la FBA est prêt à transférer les fonds. La directrice financière autorise le virement des 200 000 euros restants, qui sont versés sur le compte bancaire d’UBP en Ostland.*

*Le matin suivant l’expiration du délai de 48 heures, le Département des finances d’UBP contacte son homologue à la FBA pour demander le paiement immédiat du solde. La FBA informe UBP que les fonds ont déjà été versés et qu’elle attend la livraison de la commande. Elle en profite pour souhaiter à UBP une bonne fête nationale.*

*Le Département des finances d’UBP vérifie son compte bancaire et répond à la FBA qu’aucun paiement n’a été reçu. Il demande également pourquoi la FBA lui souhaite une bonne fête nationale alors qu’elle aura lieu dans deux mois ».*

*Note aux formateurs :* **le montage trouve sa conclusion lorsque la directrice financière de la FBA autorise le virement bancaire sur la base des documents présentés ci-dessus : faux e-mail d’UBP accompagné d’une fausse facture, renvoyant vers un compte bancaire qui n’est connu ni de la FBA ni d’UBP.**

L’escroquerie se noue à ce moment précis. 200 000 euros ont été virés sur le compte frauduleux. En fonction du scénario retenu, les formateurs peuvent poursuivre en évoquant les mouvements entre le compte bancaire en Ostland et des comptes situés dans d’autres pays, ayant ratifié ou non la Convention de Budapest. L’exercice porte alors à la fois sur le suivi du cheminement des fonds et des transactions à travers une investigation financière, et sur les connaissances en matière de procédure d’entraide judiciaire.

Au gré des formateurs, les fonds peuvent être acheminés dans un pays atteignable ou non au moyen de la Convention de Budapest. Dans le second cas, les traces et les preuves finales vont probablement se perdre ou devenir irrécupérables. Cependant, les deux exemples peuvent être utiles aux fins de la formation.

**Principaux faits :**

* *la directrice financière de la FBA autorise le virement sur la base des documents présentés plus haut ;*
* *ces documents sont un faux e-mail d’UBP accompagné d’une fausse facture contenant les coordonnées d’un compte bancaire frauduleux ;*
* *200 000 euros sont transférés. En fonction des besoins en formation, les virements bancaires peuvent se poursuivre dans d’autres pays ou s’arrêter là. Le dernier virement peut s’effectuer vers un pays ayant ratifié ou non la Convention de Budapest.*

**Supports d’étude de cas à utiliser :**

* *Dossier « 2e jour/2.2.3, Exercice d’investigation/Preuves/E-mails » :*
* 9e e-mail ;
* 10e e-mail ;
* 11e e-mail.
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Dépositions de témoins » :*
* déposition du chef du Département de la logistique de la FBA ;
* déposition de la directrice financière de la FBA ;
* déposition du chef du Département informatique de la FBA ;
* déposition du responsable de l’audit de DSBN Ostland.
* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Preuves/Relevés bancaires » :*
* relevé bancaire de DSBN Ostland.

**Exemples de questions à poser aux participants :**

* *Pourquoi la directrice financière a-t-elle autorisé l’opération ?*
* *Sur quel compte les fonds ont-ils été virés ?*
* *L’Ostland ayant ratifié la Convention de Budapest, quelles mesures les forces de l’ordre vont-elles prendre ?*
* *Quels documents devraient être recueillis auprès de la FBA et sous quelle forme ?*
* *Quels documents devraient être recueillis auprès d’UBP et sous quelle forme ?*
* *Quelle banque convient-il de contacter au cours des investigations, selon quelles modalités et via quel type de demande ?*
* *Comment les fonds peuvent-ils être récupérés, si possible ?*
* *Quels types de demandes et/ou injonctions peuvent-ils être adressés aux différentes banques et entreprises ?*
* *Sur quoi les actions de ce type se fondent-elles ?*
* *Quels articles de la Convention de Budapest vont-ils être utilisés ?*

**6.** **Grandes étapes des investigations et preuves électroniques clés**

Les participants présumeront que le premier contact entre la FBA et les forces de l’ordre a lieu le jour du virement, à réception de l’e-mail d’UBP signalant que les fonds ne sont pas arrivés et s’interrogeant sur la fête nationale. L’investigation commence à ce moment, avec des variations en fonction du cadre juridique local. Le scénario peut s’adapter et inclure la police, les procureurs, les juges d’instruction et d’autres entités si nécessaire. Toutes les institutions peuvent jouer un rôle, leurs actions poursuivant un but commun à travers des approches différentes.

Toutefois, voici ce que devraient être les **grandes étapes des investigations**:

* *recueillir les dépositions des possibles suspects ;*
* *recueillir les dépositions des représentants de la FBA ;*
* *obtenir des preuves électroniques et autres auprès de la FBA ;*
* *recueillir les dépositions des représentants d’UBP ;*
* *obtenir des preuves électroniques et autres auprès d’UBP ;*
* *recueillir les dépositions des représentants de la DSBN en Norland et en Ostland ;*
* *obtenir des preuves électroniques et autres auprès des deux établissements bancaires ;*
* *obtenir des preuves auprès de l’autorité compétente pour l’enregistrement des entreprises en Ostland ;*
* *assurer la coopération entre la police, les procureurs et le cas échéant, les juges d’instruction ;*
* *passer par l’entraide judiciaire internationale dans le cadre des dispositions de la Convention de Budapest ;*
* *autres actes d’investigation importants reconnus et définis par les participants avec l’aide des formateurs.*

**Preuves électroniques clés :**

* *archives informatiques de la FBA ;*
* *logiciel espion utilisé à la FBA ;*
* *serveur SMTP pour l’envoi de faux e-mails et archives associées ;*
* *crypto-monnaie (bitcoin), chaîne de blocs, registre de la chaîne de blocs ;*
* *e-mails légitimes ;*
* *faux e-mails avec en-tête complet ;*
* *fausse facture ;*
* *archives informatiques d’UBP ;*
* *relevés de compte et coordonnées bancaires de la DSBN ;*
* *registres de l’entreprise ;*
* *rapports de surveillance ;*
* *autres preuves électroniques.*

Ces deux listes ne sont pas exhaustives et peuvent être modifiées ou mises à jour pour englober les étapes d’investigation et les preuves électroniques nécessaires.

**Autres supports d’étude de cas à utiliser :**

* *Dossier « 2e jour/2.2.3 Exercice d’investigation/Glossaire » :*
* Menace persistante avancée ;
* Crypto-monnaies ;
* Manipulation psychologique en ligne ;
* Logiciel espion ;
* Serveur SMTP libre et arnaques aux e-mails.

**7. Annexes**