**Renforcement des compétences en matière de cybercriminalité**

**Étude de cas "Qui suis-je ?**

**1. "Qui suis-je ?"**

1.1

Les services de police du pays A ont commencé à recevoir de nombreuses plaintes de citoyens concernant des cas étranges de jeux primés organisés sur les réseaux de médias sociaux par des marques connues dans différents domaines commerciaux. Les prix remportés sont différents et alléchants, allant de coupons de réduction du marché à des téléphones portables ou des ordinateurs portables coûteux. Les jeux sont organisés sur les réseaux de médias sociaux de la même manière que sur les canaux de communication générale les plus populaires. Les équipes de marketing des marques publient les annonces des jeux et des prix gagnés en invitant toutes les personnes intéressées à y participer en cliquant sur le lien qui ouvre le canal de médias sociaux dédié au jeu. Des centaines et même des milliers de personnes sont attirées, et elles suivent le lien et commencent à participer au jeu.

1.2

Après quelques questions plus ou moins habituelles qui sont présentées sous la forme d'un bref quiz sur la chaîne du jeu, ainsi que le paiement de frais de participation peu élevés, les personnes aspirant à un prix obtiennent l'information qu'elles ont gagné le prix et qu'aux fins de la réclamation, des données personnelles doivent être fournies. Au lieu d'appeler le numéro de téléphone ou d'envoyer un e-mail au service des prix de la marque, la procédure est simplifiée dans la mesure où seule une photographie du recto et du verso de la carte d'identité personnelle ou du passeport du gagnant, avec lui en main, suffira pour l'identification positive et la réclamation du prix, à condition que toutes les données d'identification personnelle soient clairement visibles et que le visage de la personne qui le tient et la photo sur le document soient les mêmes et clairement reconnaissables. Les prix sont élevés, les questions sont faciles, tout le monde gagne, des centaines et des milliers de personnes envoient volontiers des photos d'elles en possession d'une pièce d'identité personnelle sans poser de question.

1.3

Cependant, quelque chose ne fonctionne pas correctement. Les heureux gagnants, bien qu’ayant tout fait selon les instructions, ne sont pas contactés par le service des prix de la marque et ne reçoivent pas non plus de prix par courrier. Les jours passent et les questions se multiplient. Certains des gagnants commencent à s'inquiéter du partage de leurs données personnelles et à vérifier leurs comptes bancaires et autres comptes financiers. Cependant, il semble que tout soit en ordre : pas un seul centime n'a été volé ou transféré sans raison valable. Ils commencent à vérifier les autres services qu'ils utilisent, et tout semble en ordre. Rien n'a changé.

La situation commence à devenir frustrante. Rien n'est volé ou retiré et les prix ne sont pas remis. Que peut-il y avoir de mal ? Pour le savoir, les gagnants commencent à appeler le siège de Brands, qui est basé dans leur pays, et à demander ce qui se passe.

1.4

Les services de relations clientèle des marques prennent les appels et répondent immédiatement aux gagnants : nous sommes désolés, nous n'organisons pas de jeu gagnant pour le moment. De plus, lorsque de tels jeux sont organisés, ils le sont conformément à la loi du pays concerné régissant les jeux d'argent, qui garantit la protection des données personnelles, ce qui signifie que la marque ne demandera jamais l'affichage public de la carte d'identité.

Les gagnants commencent à se rendre compte qu'ils ont été fraudés d'une manière ou d'une autre, mais on ne sait pas exactement comment et pourquoi. Tous les comptes bancaires et autres sont inchangés et rien ne manque. Jusqu'à présent, il semble que seules des données personnelles aient été recueillies et rien de plus. Pourtant, les "gagnants" sont en colère parce qu'ils n'ont pas reçu de prix et que quelqu'un a leurs données personnelles, ou pire encore, des photos de leurs documents personnels. Ils veulent des réponses et les médias commencent à y prêter attention.

La police commence son enquête préliminaire.

**2. Suivez les données**

2.1

La police se rend compte que des milliers de citoyens du pays A ont maintenant participé à une version du jeu primé. Les marques sont différentes, nationales ou étrangères, mais toutes sont basées dans le pays A d'une manière ou d'une autre. Les comptes bancaires et autres comptes financiers ou de propriété sont vérifiés et rien ne manque en effet. Les réseaux de médias sociaux sont hébergés à la fois dans le pays et à l'étranger. Il semble qu'il n'y ait pas de règle à ce sujet, si ce n'est qu'ils doivent être populaires. Une demande a été envoyée aux réseaux avec certaines questions et demandes d'action. La police commence à recevoir des résultats et les premiers indices apparaissent. Les fournisseurs de services Internet sont désormais inclus dans l'enquête. Les résultats de certaines actions de la police donnent des résultats. Les premiers suspects sont identifiés.

2.2

Certaines mesures et ordonnances procédurales du ministère public et de la Cour sont acquises et en cours d'exécution. Les preuves sous forme régulière ou électronique commencent à être acquises. Un doute raisonnable quant à la perpétration d'un crime est établi. Les preuves et les interrogatoires montrent qu'un groupe de personnes qui ne sont pas nécessairement connectées affiche des informations sur les jeux gagnants sur des canaux de médias sociaux originaux ou faux des marques. L'accès aux canaux originaux est rendu possible par l'acquisition illégale des identifiants de connexion. Si les canaux sont faux, des copies de l'étiquetage original de la marque sont utilisées. Les données personnelles acquises frauduleusement sont en fait une marchandise. Elles sont vendues à des personnes sur le marché noir hébergé dans le pays A qui paient entre 15 et 50 euros par photographie, selon la qualité. L'argent est transféré tantôt sur des comptes bancaires, tantôt en monnaie de cryptologie.

**3. Suivre l'argent**

3.1

Des informations complémentaires sont acquises. Les suspects suivants dans la chaîne sont identifiés et des mesures et actions supplémentaires sont entreprises sur ordre du ministère public ou du tribunal. Les actions et mesures de preuve donnent des résultats. Les preuves et les interrogatoires électroniques montrent que les données personnelles achetées sur le marché noir sont effectivement utilisées pour l'ouverture de comptes de paiement auprès de sociétés de paiement en ligne résidant dans le pays B, qui approuvent la coopération volontaire. Les comptes de paiement sont ouverts au nom de la personne dont la carte d'identité et la photographie ont été utilisées. La photographie est l'une des conditions d'ouverture du compte. Une enquête plus approfondie montre que les comptes nouvellement ouverts reçoivent dans les 24/48 heures des dépôts de 1000 EUR chacun payés en monnaie cryptographique. Comme des centaines ou des milliers de comptes sont utilisés, il commence à être clair que des sommes importantes sont en jeu.

3.2

Une enquête plus approfondie montre que les comptes de paiement en ligne dans le pays B sont liés aux comptes du pays C auprès d'une société de paris en ligne, qui n'approuve pas la coopération volontaire. Il semble que les mêmes noms et les mêmes identifiants personnels soient utilisés pour l'ouverture des comptes de paris en ligne dans le pays C. Des enquêtes complémentaires montrent que très peu de temps après le versement initial de l'acompte de 1000 EUR sur le compte dans le pays B, celui-ci est transféré sur le compte de paris dans le pays C. Le flux net de trésorerie est complet, ce qui signifie que rien ne reste dans le pays B et que tout l'argent est transféré dans le pays C.

La série suivante d'actions d'enquête a lieu et les résultats montrent que l'argent est effectivement versé sur les comptes dans le pays C mais pas pour longtemps. Dans les 24 à 48 heures, l'argent est à nouveau transféré sur les comptes à partir desquels le premier paiement a été effectué. Après le transfert, les comptes de la société de paris en ligne sont fermés et supprimés définitivement.

**4. Suivre le leader**

4.1

L'enquête porte à présent sur le pays B et les comptes auprès de la société de paiement en ligne. Tous les comptes à partir desquels les premiers paiements ont été effectués et qui étaient vides ont à nouveau 1000 EUR sur eux sous le nom des personnes "gagnantes" du pays A.

Une analyse plus poussée des preuves montre que, dans un court laps de temps, des transactions sont effectuées entre les comptes de paiement en ligne et, cette fois, les comptes bancaires des personnes du pays A. Le transfert est complet et les 1000 euros sont tous transférés. Une fois le transfert effectué, les comptes sont fermés et supprimés sur la plate-forme du pays B. Les forces de police du pays A poursuivent leur enquête. Des informations et des preuves supplémentaires sont recueillies et montrent qu'un certain nombre d'individus dans le pays A reçoivent des paiements du pays B. Il semble qu'un certain niveau de coordination existe entre eux puisque, le même jour, ils se rendent dans des banques ou utilisent des distributeurs automatiques pour retirer des sommes presque identiques.

4.2

Ce qui semble intéressant, c'est que sur certains comptes, tout l'argent n'a pas été retiré et que 5 à 10% reste. Toutefois, la communication entre les personnes est maintenue d'une certaine manière, puisque ce type d'action se poursuit jusqu'à ce que tout l'argent soit retiré ou qu'un certain pourcentage reste.

La police poursuit l'enquête. Des ordres supplémentaires du ministère public et du tribunal sont obtenus et le jour de l'action est fixé. Au cours de l'action sur le terrain, un certain nombre d'individus sont arrêtés et des preuves électroniques et régulières sont obtenues. Il semble qu'une grande partie de l'argent n'ait pas été saisie. Les dossiers d'interrogatoire montrent que les suspects utilisent les médias sociaux et les services VOIP pour contacter une personne du pays E. Certains des messages montrent que les suspects s'attendent à remettre de l'argent liquide à cette personne soit lorsqu'il arrivera dans le pays A, soit lorsqu'ils se rendront dans le pays E qui est voisin.