ASSEMBLÉE NATIONALE

14ème législature

sécurité

Question écrite n° 41995

Texte de la question

Mme Sandrine Doucet attire l'attention de M. le ministre de l'intérieur sur les vols et escroqueries à la carte bancaire. Récemment, plusieurs villes de l'agglomération bordelaise ont été les victimes de bandes spécialisées dans le « *cash-trapping* ». Cette technique, qui peut s'adapter à tous les distributeurs automatiques de billets (DAB), consiste à piéger les billets au niveau de la trappe de sortie. Le système a l'avantage d'être rapidement et facilement installé, puisqu'il ne demande aucune connaissance en informatique, ce qui permet aux malfaiteurs de multiplier les arnaques. Cette nouvelle technique n'est malheureusement qu'une des multiples escroqueries à la carte bancaire déjà existantes. Si la plupart des DAB de dernière génération sont équipés de nouvelles technologies permettant aux policiers d'obtenir les éléments nécessaires à leurs enquêtes, il n'en reste pas moins que ces arnaques coûtent très cher, tant économiquement qu'en termes de sécurité des riverains. En effet, les malfaiteurs utilisent parfois des méthodes plus dangereuses, comme l'introduction dans le DAB d'un mélange gazeux explosif. On estime d'ailleurs qu'une centaine de DAB auraient été attaqués de cette façon au cours de ces derniers mois en France. L'arsenal législatif pour répondre à ce type de méfaits semble aujourd'hui trop imprécis pour faire face à la recrudescence des vols. Il apparaît dès lors nécessaire qu'une réflexion soit menée afin de renforcer les normes de sécurité existantes. Elle souhaite donc savoir comment le ministère entend s'emparer de cette question. Elle le remercie de bien vouloir la tenir informée des suites données à ce dossier.

Texte de la réponse

L'action de l'Etat et des professionnels du secteur a permis de renforcer la sécurité des distributeurs automatiques de billets (DAB) comme celle des « dabistes » chargés de leur alimentation et de leur maintenance. Le taux d'échec des attaques visant les « dabistes » (60 % en 2013) et le niveau de sécurisation élevé des appareils ont conduit les délinquants à modifier leurs techniques. De nouveaux modes opératoires sont apparus, en particulier les attaques physiques par explosif. Près de 50 % des attaques de DAB constatées en 2013 ont été commises par l'explosion d'un mélange au préjudice d'établissements bancaires situés en zone rurale et environ 8 % ont été commises avec des explosifs au détriment d'établissements bancaires implantés en zone urbaine ou péri-urbaine. Face à cette criminalité violente, les forces de l'ordre recourent à tous les moyens d'investigation spécifiques prévus par le code de procédure pénale en matière de criminalité organisée et de délinquance spécialisée (infiltration, sonorisation de lieux et de véhicules, etc.). La réglementation relative à la protection des transports de fonds a également été adaptée (décrets du 1er octobre 2012 et du 25 octobre 2013 ayant modifié le décret du 28 avril 2000 relatif à la protection des transports de fonds) : renforcement des parois des bâtiments abritant un DAB ; mise en place de systèmes de surveillance à distance des DAB ; généralisation des dispositifs de neutralisation des billets, etc. L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire est impliqué dans les mesures de sécurisation technique des DAB et des terminaux de paiement électronique, en coopération avec la fédération bancaire française (FBF) et l'Observatoire de la sécurité des cartes de paiement. S'agissant des fraudes à la carte bancaire, elles relèvent de diverses techniques : capture

de données bancaires confidentielles via Internet (« carding »1, « phishing »2, « pharming »3) ou falsification et contrefaçon des cartes de paiement. Dans cette dernière catégorie, les attaques de DAB par un dispositif de « skimming » sont les plus répandues : elles consistent à fabriquer des systèmes de piratage de DAB ou de terminal de paiement électronique en vue de capturer les pistes magnétiques et les codes secrets des utilisateurs. La fraude dite du « cash-trapping », quant à elle, est un mode opératoire apparu en 2012. Il s'agit d'un dispositif qui empêche l'éjection des billets de l'automate bancaire, laissant supposer au client que l'appareil est en panne. Après son départ, les malfaiteurs récupèrent les billets bloqués. Dans l'agglomération bordelaise par exemple, sept faits de cette nature ont été constatés en 2012 en zone police, ayant conduit à l'interpellation de deux personnes, et trois faits ont été constatés en 2013, ayant conduit à l'interpellation de sept personnes. Les enquêteurs de la sûreté départementale de la direction départementale de la sécurité publique de la Gironde sont activement engagés dans la lutte contre cette délinquance, qui fait aussi l'objet d'un suivi particulier assuré par le service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée (SIRASCO) de la police judiciaire de la Gironde. Face à ces nouvelles menaces en constante évolution, un plan de lutte a été mis en place sous l'égide de l'OCLCTIC. Sur le plan opérationnel, la convocation de « bureaux de liaison » regroupant l'ensemble des acteurs concernés a permis de renforcer la sensibilisation des services sur ces fraudes. Des documents techniques à destination des services de police, de gendarmerie et des douanes ont été diffusés et des actions de sensibilisation ont été menées, notamment auprès des services du ministère de la justice. La formation et le déploiement des investigateurs en cybercriminalité (ICC) de la police nationale se sont intensifiés pour répondre aux réalités du terrain, la plupart des perquisitions s'accompagnant dorénavant de recherches informatiques. En matière de prévention, l'OCLCTIC a renforcé son partenariat avec les professionnels chargés de la production d'automates, la fédération bancaire française et le groupement d'intérêt économique des cartes bancaires. L'OCLCTIC siège, en outre, au sein de l'Observatoire de la sécurité des cartes de paiement, présidé par le gouverneur de la Banque de France, qui regroupe des parlementaires, des représentants des administrations concernées, des émetteurs de cartes de paiement et des associations de commerçants et de consommateurs. Par ailleurs, le directeur général de la police nationale organise deux fois par an, en liaison avec la fédération bancaire française, le groupement d'intérêt économique des cartes bancaires et plus largement avec les représentants du secteur industriel et bancaire, une réunion de coordination et de remontée d'informations particulièrement efficace. Ce partenariat concerne également les professionnels de la production d'automates afin d'améliorer la protection des équipements, la détection des dispositifs de captation et la remontée de l'information vers les services de police. Dans sa dimension internationale, la lutte contre cette criminalité fait l'objet d'une coopération renforcée en particulier avec la Roumanie, qui a détaché un officier de liaison au sein de l'OCLCTIC. La France s'investit également activement dans les travaux d'Europol. Sur le plan juridique, la répression de l'utilisation d'instruments de paiement falsifiés (cartes de paiement, etc.), si elle est commise en bande organisée, est plus sévère (dix ans d'emprisonnement et un million d'euros d'amende) depuis la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui a par ailleurs créé une incrimination relative à l'utilisation frauduleuse de données à caractère personnel de tiers sur Internet. La mobilisation des pouvoirs publics a par exemple contribué à l'éradication récente, en France, des escroqueries à la « Yes Card » (carte à puce, vierge à l'origine, dans laquelle des données spécifiques sont générées par calcul ou programmées par un « pirate », à partir du contenu d'une carte bancaire trouvée ou périmée). La lutte contre ce type de fraude relève plus largement de la lutte contre la cyberdélinquance, dont le ministre de l'intérieur a fait une priorité. L'année 2014 sera à cet égard une année d'initiatives et d'avancées, avec l'élaboration en cours d'un plan d'action du ministère de l'intérieur en matière de lutte contre la cybercriminalité. Il sera finalisé d'ici à la fin du trimestre, en lien étroit avec la réflexion que mène le ministère de la justice sur ces mêmes questions. 1) Le « carding » concerne le trafic de données de cartes de paiement, aisément utilisables ou négociables pour le commerce en ligne. 2) Le « phishing » vise à recueillir les informations confidentielles liées à un compte bancaire via des envois massifs de mels ou « pourriels » censés provenir de banques, d'organismes publics, etc. Les victimes, trompées par la qualité supposée de l'expéditeur, fournissent elles-mêmes leurs données bancaires et/ou personnelles. 3) Le « pharming » consiste à contraindre un serveur à rediriger une requête d'accès non pas sur l'adresse IP correspondant au vrai site bancaire mais vers le faux site qu'une personne mal intentionnée aura défini en piratant le serveur.

Données clés

Version web : https://www.assemblee-nationale.fr/dyn/14/questions/QANR5L14QE41995

Auteur : Mme Sandrine Doucet
Circonscription : Gironde (1re circonscription) - Socialiste, écologiste et républicain
Type de question : Question écrite
Numéro de la question : 41995
Rubrique : Banques et établissements financiers
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 12 novembre 2013, page 11767
Réponse publiée au JO le : 13 mai 2014, page 3895