Délits sur les GAB

Vue d'ensemble de la situation en Europe et règles d'or pour les éviter

enisa
European Network and Information Security Agency

Au sujet de l'ENISA

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est une agence européenne qui a été créée afin d'améliorer le fonctionnement du marché intérieur. L'ENISA est un centre d'excellence en matière de sécurité des réseaux et de l'information pour les États membres et les institutions de l'Union. Elle prodigue conseils et recommandations et agit comme une centrale d'informations en matière de bonnes pratiques. En outre, elle facilite les contacts entre les institutions européennes, les États membres, les entreprises privées et les acteurs de l'industrie.

Coordonnées:

Pour toute information générale ou concernant la sensibilisation à la sécurité de l'information, veuillez nous contacter à l'adresse électronique suivante:

Courriel: Isabella Santa, Responsable Sensibilisation — awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Délits sur les GAB:
Vue d'ensemble de la situation en Europe et règles d'or pour les éviter

Août 2009

Remerciements

Plusieurs personnes ont soutenu ce travail et y ont contribué directement ou indirectement de diverses façons. Les informations comprennent des contributions de différents membres de la communauté de la sensibilisation (*AR Community*) de l'ENISA.

L'ENISA tient à remercier les membres de l'*AR Community* et leurs organisations, ADICAE, Arjen de Landgraaf d'E-Secure-IT, Daniel Blander d'InfoSecurityLab Inc., David Barroso de S21sec, Fabio Guasconi de @ Mediaservice.net S.r.l., Fabrizio Cirilli, Gerasimos Ntouskas de KPMG Limited, INTECO, Joao Brites Moita, Lachlan Gunn de European ATM Security Team Ltd, Neal Ysart de PwC, Sissel Thomassen d'InfoSecure, William Beer de PwC, Yves Le Roux de CA, qui ont apporté à l'élaboration de ce document de précieuses contributions, de la documentation et un soutien diligent.

Enfin, nous tenons à remercier toutes les personnes qui ont contribué à l'élaboration de ce document par leurs analyses informelles, leur perspective intéressante, leurs observations, suggestions et solutions. Nous souhaitons notamment remercier les membres de la European ATM Security Team. Bien que cette liste ne soit évidemment pas exhaustive, le contenu présenté ici ne pourrait être ni complet ni correct sans leur contribution.

Table des matières

Résumé

Le nombre de guichets automatiques bancaires (GAB) augmente chaque année en Europe. On en trouve de plus en plus dans de nombreux endroits autres que les banques, comme les commerces de proximité, les aéroports, les stations-service, les gares ferroviaires, les grands magasins, etc. Avec la hausse du nombre de GAB en Europe, une augmentation considérable du nombre total de délits sur les GAB a été observée, les pertes totales se montant à 485,15 millions d'euros en 2008. Le crime organisé est à l'origine d'un grand nombre de ces attaques, et la récession est considérée comme un facteur probable de cette augmentation. Par conséquent, l'industrie des GAB a fait de la sécurité des utilisateurs et de la protection contre la fraude une priorité majeure afin de maintenir la confiance à l'égard du système.

Le présent livre blanc vise à offrir une série de recommandations afin de sensibiliser les utilisateurs aux différents types de risques auxquels ils s'exposent lorsqu'ils recourent à un GAB, ainsi que des conseils sur la manière de les identifier et de les contrer. L'ENISA estime que la sensibilisation des utilisateurs aux risques constitue le premier moyen de défense dans la lutte contre les délits sur les GAB, et qu'elle peut entraîner une réduction significative des attaques et des fraudes sur les GAB. Il convient de former et de conseiller les citoyens sur les moyens de réduire ces risques en prenant les précautions nécessaires lors de l'utilisation d'un distributeur automatique (comme composer leur code confidentiel à l'abri des regards) et en étant attentifs aux moindres signes d'altération ou d'activité suspecte à proximité d'un GAB.

Les délits sur les GAB sont en constante évolution, au même titre que les mesures requises pour les contrôler. Le présent document ne peut couvrir tous les risques liés à l'utilisation des GAB, pas plus qu'il ne peut offrir des conseils complets sur la manière de les utiliser en toute sécurité. Il doit au contraire être vu comme un point de départ utile et nécessaire à la sensibilisation générale des utilisateurs aux risques auxquels ils s'exposent en utilisant les GAB, dans l'Union européenne comme ailleurs dans le monde, à la sécurité des données et aux bonnes pratiques de l'industrie. L'ENISA s'engage à fournir aux utilisateurs de GAB des informations instructives sur les vulnérabilités potentielles et invite instamment les banques, les institutions financières, les systèmes de paiement et les services chargés de faire appliquer la loi à fournir des informations et des conseils supplémentaires à l'échelon national dans les États membres de l'UE.

Le présent document ne porte aucunement sur les conditions légales régissant l'installation, l'exploitation et la maintenance des GAB, le traitement des opérations effectuées sur les GAB ou la circulation et la distribution des billets de banque.

Enfin, le présent document ne contient aucun avis ou conseil en matière de conformité, de disponibilité et d'efficacité des systèmes ou dispositifs susceptibles d'être utilisés pour prévenir ou empêcher les attaques sur les GAB.

PARTIE 1: LES GAB ET LEURS IMPLICATIONS EN TERMES DE SECURITE

GAB

Définition

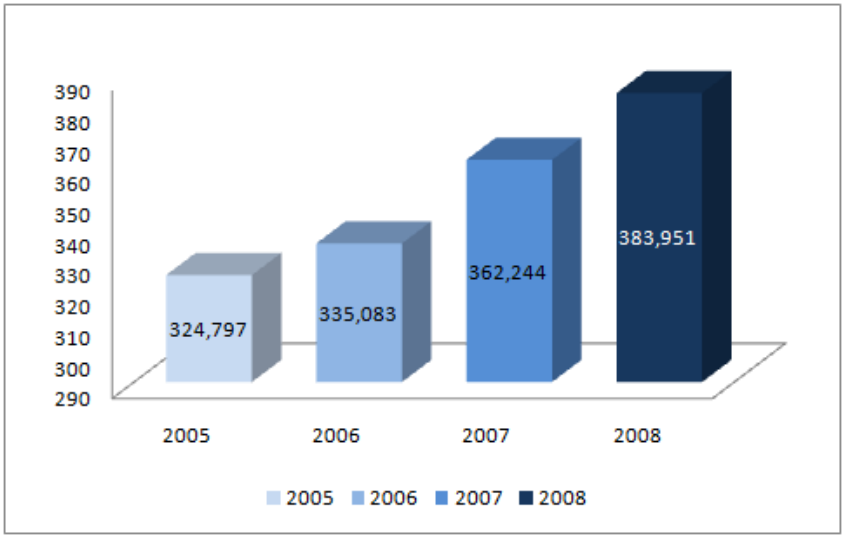
Un guichet automatique bancaire (aussi appelé GAB, DAB ou distributeur automatique de billets) est un dispositif informatisé qui offre aux clients d'une institution financière la possibilité d'effectuer des opérations bancaires sans avoir à passer par un employé de banque ou un préposé au guichet.

La plupart des GAB actuels identifient l'utilisateur par le biais de la carte en plastic que celui-ci insère dans l'appareil. La carte peut contenir une bande magnétique ou une puce indiquant un numéro de carte unique et diverses informations de sécurité, telles qu'une date d'expiration et un code d'authentification de la carte (CVC, de l'anglais *card validation code*). L'utilisateur s'identifie en composant un code confidentiel (PIN).

Au moyen d'un guichet automatique, les utilisateurs peuvent accéder à leurs comptes bancaires afin d'effectuer des retraits d'espèces (éventuellement avec une carte de crédit). Ils peuvent aussi vérifier le solde de leurs comptes, acheter des crédits téléphoniques prépayés, payer leurs factures, etc.

Utilisation des distributeurs automatiques: le panorama européen

En 2008, l'EAST (*European ATM Security Team*) a estimé à 383 951 et à plus de 1,5 million le nombre de GAB en Europe et dans le monde respectivement ([1]). Soixante-douze pour cent du nombre total de GAB européens se situent dans cinq pays: Royaume-Uni, Espagne, Allemagne, France et Italie. Le nombre total de GAB européens a grimpé de 6 % par rapport à l'année précédente.

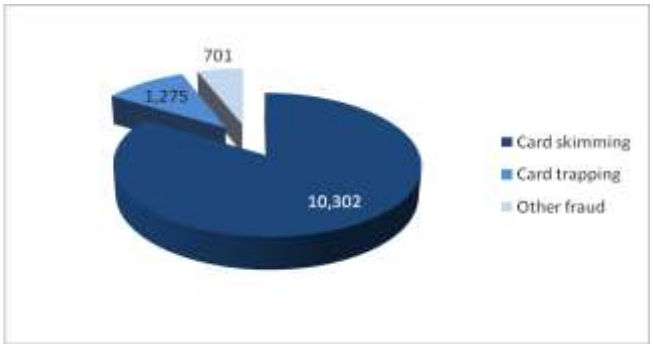


Graphique 1: Nombre de GAB en Europe. Source: EAST & EPC.

([1]) *https://www.european-atm-security.eu/Welcome%20to%20EAST/*
Selon un sondage réalisé en mai-juin 2009 par l'EAST sur l'utilisation des GAB, 49% des personnes interrogées avaient une connaissance basique des risques et dangers probables mais avaient besoin de davantage d'informations, tandis que 14% n'étaient pas sûrs des risques et dangers et apprécieraient de recevoir des conseils sur la manière de les identifier.

Délits sur les GAB et leur impact financier en Europe

Avec la hausse du nombre de distributeurs automatiques, une augmentation considérable du nombre de délits sur les GAB a été observée. Un récent rapport de l'EAST affirme qu'en 2008, les délits liés à la fraude au GAB en Europe ont grimpé de 149% comparativement à l'année précédente. D'après le rapport, cette augmentation de la fraude aux GAB est liée avant tout à une croissance spectaculaire des attaques de type *skimming*. En 2008, un total de 10 302 cas de vol de données a été signalé en Europe. Plus grave encore, de récents rapports signalent des délits qui s'appuient sur des logiciels malveillants sophistiqués et aisément disponibles ([2]) qui ont infecté les réseaux de distributeurs automatiques et les GAB directement.

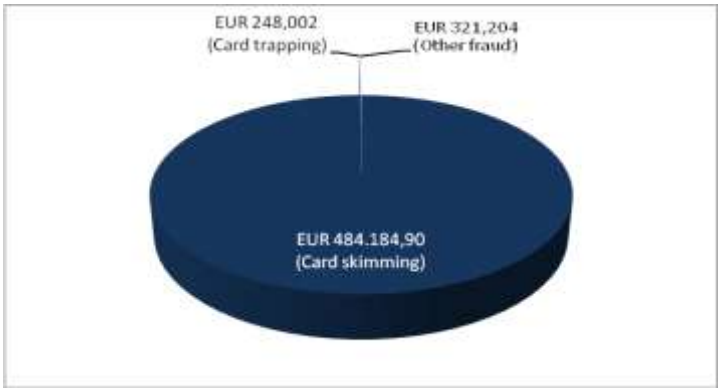


Selon ce même rapport, les agressions physiques sur les utilisateurs de distributeurs automatiques en Europe ont chuté de 29%, essentiellement en raison d'une baisse du nombre de vols signalés. Par contre, les cas d'agressions physiques sur les GAB mêmes ont augmenté de 32%. Si les pertes financières dues à ces attaques sont inférieures à celles provoquées par d'autres délits sur les GAB, lesdites attaques continuent de préoccuper vivement l'industrie.

Graphique 2: Attaques frauduleuses liées aux GAB par nombre d'incidents en 2008 (année complète). Source: EAST & EPC

Malgré l'augmentation spectaculaire du nombre d'incidents, les pertes réelles dues à la fraude n'ont progressé que de 11% par rapport à l'année précédente. Les pertes dues à la fraude au GAB sont restées significatives et une perte totale de quelque 500 millions d'euros a été signalée l'an dernier en dépit des mesures prises dans tous les pays d'Europe. La figure 3 illustre de façon détaillée la répartition de ces pertes.

Sur cette perte, près de 400 millions d'euros sont dus à des pertes internationales, qui sont le résultat de fraudes commises en dehors des frontières nationales par des criminels qui utilisent des données de cartes volées. Ces pertes ont lieu essentiellement hors d'Europe en raison principalement du déploiement de la technologie EMV ([3]) en Europe.



Graphique 3: Attaques frauduleuses liées aux GAB par pertes totales signalées en 2008 (année complète). Source: EAST & EPC

([2]) Un logiciel malveillant est un logiciel conçu pour infiltrer ou endommager un système informatique sans le consentement en connaissance de cause du détenteur.
([3]) EMV est une norme d'interopération de cartes à CI et de terminaux de point de vente capables et de GAB, destinée à authentifier les paiements par carte de crédit et de débit. Le sigle EMV se compose des initiales d'*Europay*, *MasterCard* et *VISA*, les trois sociétés qui ont coopéré afin de mettre au point la norme.

Pertes estimées dans le monde entier

Les services secrets américains estiment que les pertes annuelles dues à la fraude au GAB se montent à un total d'environ 1 milliard de dollars, ou 350 000 USD par jour, en 2008.

En 2007, le coût de la fraude à la carte de crédit et de débit au Royaume-Uni a atteint le niveau record de 535 millions de livres. L'APACS signale que la fraude à la carte a augmenté de 14% en 2008, pour atteindre près de 610 millions de livres. La fraude spécifique au GAB a grimpé de 31% et représentait 45,7 millions de livres de pertes en 2008.

Quelques incidents récents dans le monde

Les délits sur les GAB continuent de se produire dans le monde entier. Des incidents sont signalés non seulement en Europe, mais aussi en Asie-Pacifique, dans les Amériques, en Afrique, en Russie et au Moyen-Orient. Quelques exemples:

- ✓ 500 000 USD ont été volés dans une banque australienne au moyen d'un dispositif de copie installé sur un distributeur automatique de Melbourne ([4]);
- ✓ des dispositifs capables de scanner les données des cartes bancaires et de crédit ont été installés sur des GAB à l'extérieur d'un supermarché du Royaume-Uni ([5]);
- ✓ à Melbourne, dix GAB ont été utilisés pour cloner des cartes et voler plus d'un million d'USD sur différents comptes bancaires ([6]);
- ✓ à Staten Island, 500 000 USD ont été volés à plus de 250 victimes en plaçant des caméras directement sur le clavier du distributeur et en filmant les victimes pendant qu'elles composaient leur code confidentiel ([7]);
- ✓ environ 4 000 pages de données relatives à des cartes de crédit chypriotes ont été trouvées sur un ordinateur appartenant à des voleurs ([8]).

Types de délits sur les GAB

Définition

Les guichets automatiques attirent les criminels parce qu'ils offrent un accès direct à des devises, sous la forme de billets de banque, voire, dans certains cas, aux informations personnelles de l'utilisateur, qui peuvent être mises à profit en vue d'un vol d'identité. Si un GAB peut contenir un montant important de devises, les cartes bancaires, elles, peuvent donner aux voleurs l'accès aux

([4]) «*ATM scam nets Melbourne thieves $ 500,000*» [Melbourne: une arnaque aux distributeurs rapporte 500 000 dollars aux escrocs], 24 mars 2009, disponible sur *http://www.atmmarketplace.com/article.php?id=10808* (dernière visite le 20 avril 2009).
([5]) «*Shoppers are targeted in ATM scam*» [Les acheteurs pris pour cible dans une fraude aux distributeurs automatiques], BBC News, 11 mars 2006, disponible sur *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.*stm (dernière visite le 20 avril 2009).
([6]) «*Australian police suspect Romanian gang behind $ 1 million ATM scam*» [Un million de dollars détournés aux distributeurs: la police australienne soupçonne une bande de Roumains], 14 avril 2009, disponible sur *http://www.atmmarketplace.com/article.php?id=10883* (dernière visite le 20 avril 2009).
([7]) «*ATMs on Staten Island rigged for identity theft; bandits steal $500G*» [Distributeurs de Staten Island trafiqués pour vol d'identité: les escrocs détournent 500 000 dollars], 11 mai 2009, disponible sur http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D
([8]) «*ATM scam targets hundreds of credit cards*» [Des centaines de cartes de crédit victimes d'une arnaque aux distributeurs], New Europe, n° 793, 4 août 2008, disponible sur *http://www.neurope.eu/articles/89221.php* (dernière visite le 20 avril 2009).

comptes bancaires, lesquels peuvent aisément dépasser la valeur des devises contenues dans un seul GAB. Pour autant qu'ils aient aussi obtenu le code confidentiel, les criminels peuvent utiliser une carte volée pour retirer de l'argent d'un compte bancaire à hauteur du retrait maximal journalier autorisé, ou jusqu'à ce que la banque émettrice bloque la carte. Si les voleurs continuent de s'en prendre aux distributeurs automatiques et aux devises qu'ils contiennent, ils se sont de plus en plus concentrés sur les manières de recueillir les données des cartes bancaires et d'accroître leurs gains.

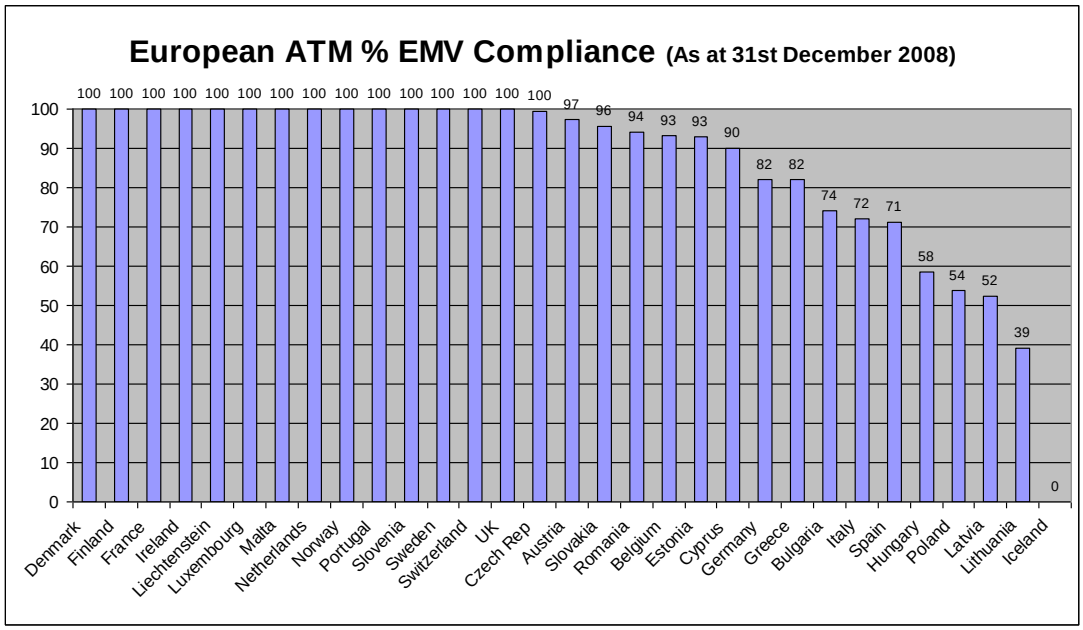
Il existe trois types fondamentaux d'attaques sur les GAB:

- ✓ les tentatives de vol visant les données de la carte bancaire d'un utilisateur;
- ✓ les attaques informatiques et réseau contre les GAB afin de recueillir les données des cartes bancaires;
- ✓ les attaques physiques sur le GAB.

Vol des informations contenues sur la carte bancaire

La principale finalité des délits sur les GAB est le vol des données enregistrées sur les cartes bancaires. Jusqu'il y a peu, les cartes bancaires utilisaient une bande magnétique pour conserver des informations permettant d'identifier le titulaire et un code confidentiel permettant de les authentifier et d'effectuer des opérations au guichet automatique. Malheureusement, les informations contenues dans la bande magnétique sont faciles à copier et falsifier. En conséquence, les voleurs se sont concentrés sur les moyens de recueillir ces informations.

Cette lacune a été partiellement comblée par l'introduction en Europe des cartes intelligente EMV (aussi appelées cartes à puce). Selon l'EAST, 90 % des distributeurs européens répondent à présent aux normes EMV.



Graphique 4: Part (en %) des GAB européens répondant aux normes EMV. Source; EAST & EPC.

Bien que ces cartes contiennent aussi une bande magnétique, cette dernière seule ne suffit pas à permettre qu'une opération ait lieu à un GAB au moyen d'un lecteur de carte modifié afin de lire les puces EMV (excepté si l'émetteur de la carte autorise une telle opération). Les copies frauduleuses de ces cartes EMV ne peuvent donc pas être utilisées pour retirer du liquide sur des distributeurs aux normes EMV.

Comme les cartes aux normes EMV seront utilisées dans la plus grande partie de l'Europe d'ici à la fin 2010, il s'ensuit que les criminels devront utiliser les cartes falsifiées en dehors de l'Europe et dans les pays où les distributeurs automatiques ne sont pas équipés de lecteurs aux normes EMV. D'ici là toutefois, la menace des cartes bancaires falsifiées reste réelle.

Card skimming

Le *card skimming* (vol de données par copie frauduleuse de carte) consiste à prélever au GAB les données contenues sur la bande magnétique et le code confidentiel au moyen d'un lecteur de carte modifié appelé «*skimming device*». Ce dispositif de copie frauduleuse est placé sur le distributeur de telle sorte que sa présence est cachée mais qu'il peut capturer les informations contenues sur la bande magnétique de la carte et le code confidentiel de l'utilisateur. L'utilisateur insère sa carte dans le distributeur sur lequel un dispositif de copie frauduleuse a été placé, effectue une opération normale et reprend sa carte. Il quitte le GAB sans savoir que sa carte a été «forcée». Les informations subtilisées sont utilisées afin de produire des cartes falsifiées et d'effectuer ensuite des retraits de devises frauduleux. Le titulaire de la carte ne prend conscience des faits que lorsque des opérations ou des retraits non autorisés sont effectués sur son compte bancaire. Comme les dispositifs de copie sont très sophistiqués et souvent difficiles à détecter, ils compromettent de nombreuses cartes.

Les criminels utilisent plusieurs méthodes différentes, et le code confidentiel est obtenu soit grâce à une petite caméra de surveillance, soit au moyen d'une fausse grille recouvrant le clavier. La technologie sans fil Blue Tooth ([9]) est de plus en plus utilisée pour transmettre les détails de la carte bancaire et le code confidentiel à un ordinateur portable situé à distance. Ces informations peuvent ensuite être envoyées facilement partout dans le monde afin de permettre la production rapide de cartes falsifiées.

Méthodes classiques de vol de données

Un petit dispositif de copie frauduleuse (*skimming device*) placé à l'entrée du lecteur de carte (ou un faux panneau placé sur le lecteur de carte), avec une fausse grille sur le clavier (ou une petite caméra de surveillance) pour voler le code confidentiel.

([9]) La technologie Blue Tooth permet aux dispositifs électroniques de communiquer entre eux au moyen d'une liaison radio de courte portée.

Illustration 5: reproduite avec l'autorisation d'EAST

Illustration 6: reproduite avec l'autorisation d'EAST

Un faux panneau frontal complet est placé sur le tableau du GAB.

Illustration 7: reproduite avec l'autorisation d'EAST

Un dispositif de copie frauduleuse est placé dans un lecteur de carte conçu pour ouvrir la porte du vestibule d'une banque (en général, la caméra utilisée pour recueillir les codes PIN sera située au-dessus des GAB, dans le vestibule).

Illustration 8: reproduite avec l'autorisation d'EAST

Les dispositifs de copie frauduleuse peuvent également être montés à côté du vrai lecteur de carte du distributeur, avec un petit panneau disant «Insérez d'abord votre carte ici»; cela n'est toutefois pas très fréquent en Europe.

Illustration 9: reproduite avec l'autorisation de la police de Naples

Faux distributeurs de billets

Les criminels placent de faux distributeurs dans les centres commerciaux et à proximité, ainsi que dans d'autres lieux publics. Ils ressemblent à de vrais guichets automatiques, et certains distribuent même des billets. Toutes les cartes utilisées sur ces machines sont copiées, et le code confidentiel est obtenu à partir du clavier. Ces machines n'étant reliées à aucun réseau, les criminels peuvent les placer partout où il existe une source d'électricité.

Cas récent de card skimming

En avril 2009, un employé de Microsoft âgé de 33 ans vivant à New York City s'est arrêté à la banque Chase la plus proche pour y retirer du liquide afin de payer son coiffeur. Au moment d'insérer sa carte, il a remarqué une légère résistance. L'écran l'a informé que la machine ne pouvait pas lire sa carte. Il a donc réessayé. Mais la seconde fois aussi, le distributeur a affiché un message d'erreur.
Il était sur le point de renoncer, lorsqu'une pensée l'a effleuré. Il avait entendu parler de dispositifs que les fraudeurs placent à l'extérieur des lecteurs de carte sur les GAB et, même si cela lui paraissait peu probable, il s'est demandé si ce n'était pas la cause de son problème. En tirant sur le plastique vert entourant la goulotte d'introduction de carte, il s'est aperçu qu'il se détachait facilement. Derrière un miroir supplémentaire à proximité de la machine, il a également trouvé une caméra dissimulée dirigée droit sur le clavier, afin d'enregistrer les codes confidentiels saisis par les utilisateurs ([10]).

Illustration 10: Vol de données magnétiques.

Card trapping

Le *card trapping* (piégeage de carte) consiste à capturer physiquement la carte dans le GAB, tout en subtilisant le code confidentiel de l'utilisateur au moyen de diverses méthodes. Lorsque l'utilisateur quitte le GAB sans sa carte, celle-ci est ensuite récupérée par les voleurs et utilisée pour effectuer des retraits frauduleux ou des achats (en magasin, par téléphone ou en ligne). En général, une seule carte est perdue dans chaque attaque, et les criminels doivent récupérer tout le dispositif chaque fois

([10]) http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

qu'une carte est piégée. Récemment toutefois, on a retrouvé un dispositif de piégeage de carte pouvant rester en place pendant un certain temps et permettant de récupérer les cartes piégées sans avoir à être enlevé.

La variante la plus fréquente est appelée «collet marseillais» (ou «*Lebanese Loop*» en anglais). Les voleurs placent un dispositif muni d'une boucle de ruban adhésif, de câble ou de fil résistant sur le lecteur de carte d'un distributeur automatique. La carte peut de la sorte être insérée et lue par le GAB, mais pas restituée. Les criminels obtiennent le code confidentiel en regardant par-dessus l'épaule de l'utilisateur lorsqu'il saisit son code (*shoulder surfing*). Ils récupèrent ensuite la carte après que la victime a quitté le GAB en étant convaincu que la machine a retenu sa carte pour d'autres raisons.

Diverses techniques sont utilisées pour subtiliser le code confidentiel du titulaire de la carte, comme recourir à des caméras vidéo, offrir des conseils et distraire l'utilisateur pendant qu'il saisit son code. Un autre type de piège à carte est appelé «*Algerian V*».

Vol par distraction ou vol «manuel»

La pratique est semblable à celle du *card trapping*, à la différence qu'au lieu d'être capturée par un collet ou autre type de piège, la carte est retirée du lecteur par les criminels eux-mêmes. Après avoir observé la saisie du code confidentiel, un groupe de criminels distrait l'utilisateur et annule l'opération. Pendant que deux complices distraient l'utilisateur (souvent en laissant tomber un billet et en lui demandant s'il lui appartient), un troisième criminel presse la touche Stop et prend la carte de l'utilisateur. Lorsque ce dernier reporte son attention sur le distributeur, il se voit informer que la machine est défectueuse et ne peut lui restituer sa carte.

Shoulder surfing

La méthode du *shoulder surfing* est utilisée par les criminels pour obtenir un code confidentiel, en général lorsqu'ils piègent ou volent les cartes en distrayant l'utilisateur. Se tenant derrière la victime, le criminel lit le code confidentiel que ce dernier saisit; il le mémorise, le note ou l'enregistre aussitôt dans un téléphone mobile.

Quitter une opération en cours

Dans ce cas, le voleur termine une opération inachevée après que la victime a quitté le guichet automatique. En général, le criminel persuade la victime, pendant une opération, que le distributeur est hors service, ou il éloigne la victime du distributeur par différents moyens alors qu'elle était sur le point de retirer de l'argent.

Un incident récent aux États-Unis

Deux hommes ont volé 1 800 USD en liquide à des utilisateurs sans méfiance moins d'une demi-heure après leur avoir subtilisé leur carte bancaire au milieu d'une opération. Dans l'un des trois vols connus, la police pense que les criminels ont parcouru moins de deux mètres jusqu'à un distributeur proche et ont retiré 900 USD en trois opérations distinctes, avant que les victimes fassent bloquer leur carte par la banque. Ailleurs, les deux criminels ont volé 900 USD à travers des opérations par carte de crédit et des retraits de liquide dans la demi-heure qui a suivi le vol de la carte.

La police pense que le premier complice observe utilisateur du GAB saisir son code, qu'il l'enregistre aussitôt dans un téléphone mobile. Le second délinquant distrait ensuite la victime en laissant tomber un billet de 20 USD à ses pieds et en lui tapant sur l'épaule pour l'avertir. Pendant ce temps,

le premier vole la carte éjectée par la machine. La carte volée est utilisée dans une autre machine. La victime ne comprend pas pourquoi le distributeur automatique n'a pas restitué la carte ([11]).

Cash trapping

Les criminels placent sur la goulotte de sortie des billets un dispositif qui bloque ces derniers à l'intérieur lorsqu'un utilisateur tente d'effectuer un retrait. L'utilisateur s'en va en pensant que la machine est défectueuse ou entre dans la banque pour signaler l'incident, et pendant ce temps les voleurs viennent récupérer les billets.

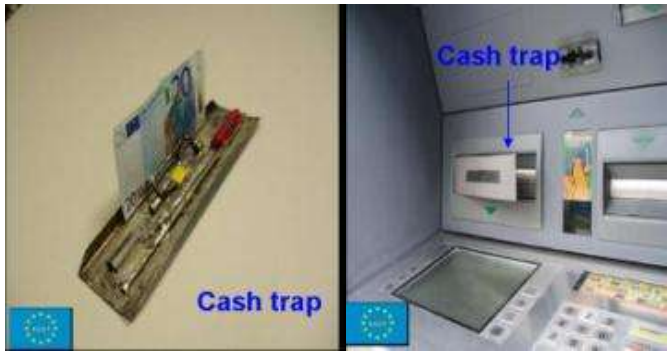


Illustration 11: reproduite avec l'autorisation d'EAST

Attaques informatiques et via réseau

L'internet offre accès et connectivité dans le monde entier. Il permet à chacun de nous d'être en contact avec des personnes du monde entier. Il permet aussi aux voleurs d'accéder aux systèmes et aux individus. Cette menace se manifeste de la même façon.

Attaques sur les distributeurs via le réseau

Les GAB communiquent avec les systèmes bancaires au moyen d'une connexion réseau. Certaines de ces connexions utilisent des réseaux privés et des protocoles de réseau propres, mais le plus souvent ces connexions se font à présent par l'internet au moyen de protocoles de réseau standard. Les voleurs utilisent des programmes informatiques (logiciels malveillants) pour attaquer le GAB afin d'y accéder à travers une faille du logiciel ou de l'ordinateur. Une fois qu'ils ont accès au GAB, les voleurs installent un logiciel qui recueille les données des cartes et les codes confidentiels. Un distributeur qui a été trafiqué n'est pas physiquement différent d'un autre qui ne l'a pas été et, souvent, les utilisateurs n'auront pas conscience du danger.

Virus et logiciels malveillants

Les GAB utilisent aujourd'hui des systèmes d'exploitation disponibles largement et du matériel vendu dans le commerce. Par conséquent, ils sont susceptibles d'être infectés par des virus et autres logiciels malveillants. Le logiciel malveillant est injecté dans le GAB à travers des attaques via réseau ou au moyen d'autres dispositifs infectés. Une fois installé sur le GAB, le logiciel malveillant recueille les données des cartes et les codes confidentiels.

Incident récent

En avril 2009, on a découvert que les GAB de Russie avaient été infectés au moyen d'un logiciel malveillant sophistiqué. Celui-ci était capable non seulement de recueillir les données des cartes mais aussi le code confidentiel. Si la machine d'un seul vendeur de GAB spécifique a été attaquée avec succès, des rapports des services de renseignements reçus en mars ont fait état de tentatives visant à infecter les distributeurs d'autres vendeurs ([12]).

([11]) Robinson G., «*Bondi banks scam: ATM alert*» [Fraude dans les banques de Bondi: alerte dans les distributeurs automatiques], *The Sydney Morning Herald*, octobre 2008, disponible sur http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950 (dernière visite le 2 juillet 2009).
([12]) http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html

Hameçonnage

La fraude et les arnaques recourant à la communication par courrier existent depuis de nombreuses années. Avec l'apparition du courrier électronique et de l'internet, ce type de fraude s'est diffusé rapidement dans le monde entier sous le nom de «*phishing*» (hameçonnage). La fraude par hameçonnage vise à persuader l'utilisateur de communiquer le numéro et le code confidentiel de sa carte bancaire. Les voleurs envoient un courrier électronique en se faisant passer pour une banque et en prétendant que les données relatives au compte sont incomplètes ou que l'utilisateur doit mettre à jour les données relatives à son compte afin d'éviter la fermeture de celui-ci. L'utilisateur est invité à cliquer sur un lien et à suivre les instructions données. Or, le lien est frauduleux et dirige l'utilisateur vers un site créé par les criminels et conçu de manière à ressembler à un site de la banque de l'utilisateur. Sur le site, l'utilisateur est invité à saisir des données sensibles telles que le numéro et le code confidentiel de la carte. Les informations sont recueillies par les voleurs et utilisées pour créer des cartes falsifiées, retirer des fonds du compte de la victime et effectuer des achats.

Vols de codes confidentiels

Les voleurs recourent à des techniques de programmation sophistiquées ([13]) pour forcer l'accès aux sites internet hébergés sur le réseau d'une institution financière. Grâce à cet accès, les voleurs pénètrent dans les systèmes de la banque pour localiser la base de données des GAB. Ils recueillent les numéros de carte et, si nécessaire, modifient les codes confidentiels des cartes qu'ils comptent utiliser. Les voleurs revendent ensuite les cartes et leurs données à d'autres criminels. Ceux-ci créent des cartes au moyen des informations subtilisées et les utilisent pour retirer de l'argent des comptes liés. Les premiers voleurs reçoivent en général un pourcentage des gains.

Incident récent

En janvier et février 2008, les services secrets américains ont révélé qu'ils enquêtaient sur deux effractions – l'une à l'encontre d'OmniAmerican Credit Union et l'autre contre Global Cash Card. En avril et mai 2008, des délits de même nature ont été découverts à l'encontre de Symmetrex, processeur d'opérations, et la 1st Source Bank. Les cartes de Symmetrex étaient utilisées par MetaBank. À elles seules, ces deux enseignes ont enregistré des pertes réelles de plus 4 millions de dollars ([14]).

Attaques physiques contre les GAB

Les attaques physiques contre les GAB visent à forcer l'accès aux devises contenues dans le coffre du distributeur ou le boîtier de sécurité du GAB. Les méthodes les plus fréquentes sont notamment les attaques par voiture, les explosifs (gaz et autres) et la découpe (p.ex. scie circulaire, chalumeau, lance thermique, foreuse à couronne diamanteuse). Le vol peut également avoir lieu au moment du réapprovisionnement ou de l'entretien du distributeur. Le personnel est braqué alors qu'il apporte des devises dans un distributeur ou qu'il les emporte, ou lorsque le coffre du GAB est ouvert et les tiroirs-caisse remplacés.

Implications en termes de sécurité

Que se passe-t-il lorsque les données d'un utilisateur ont été subtilisées?

([13]) *Les voleurs utilisent des techniques d'injection SQL.*
([14]) http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

Les numéros de carte et les codes confidentiels subtilisés peuvent être utilisés de multiples façons par les voleurs. Les données des cartes concernées peuvent être utilisées soit pour faire des retraits du compte bancaire lié, soit pour effectuer des achats dans des points de vente au détail, sur l'internet ou par téléphone. De fausses cartes de crédit et de débit peuvent être fabriquées et utilisées par d'autres individus.

Les criminels agissent en général en bandes hautement organisées, et parfois pour le compte de vastes organisations criminelles. On note une augmentation récente du nombre d'associations de malfaiteurs venant de l'étranger pour se livrer à ces fraudes.

Risques et dangers

Résumer les risques et dangers potentiels susceptibles de se poser aux citoyens à la suite d'un délit perpétré avec succès sur un distributeur automatique est une tâche ambitieuse. En effet, un tel délit peut non seulement donner aux criminels un accès non autorisé au compte bancaire de la victime, mais il peut aussi offrir aux criminels les informations et outils nécessaires pour commettre une gamme étendue de délits allant de la simple usurpation d'identité à des fraudes d'identité plus complexes telles que le piratage de compte.

Pour illustrer cela, il y a lieu de considérer l'éventail croissant de services généralement offerts à travers le compte bancaire utilisé via un GAB. Si, par exemple, les données ainsi que le code confidentiel de votre carte de débit sont subtilisés, le criminel peut alors être en mesure non seulement d'accéder aux fonds de votre compte, mais aussi d'effectuer diverses opérations de gestion de compte visant spécifiquement à lui permettre de commettre d'autres délits.

Par conséquent, le nombre de risques et de dangers est presque illimité, même si, au niveau le plus élevé, deux grandes catégories de risques et de dangers doivent être envisagées.

La première catégorie de risques porte sur des formes d'attaques plus immédiates telles que les pièges à billets, le collet marseillais qui permet au criminel de subtiliser directement la carte de la victime ou les agressions physiques directes sur les utilisateurs du distributeur automatique ou sur le distributeur lui-même, par exemple les voleurs à la tire ou les attaques consistant à défoncer la structure au moyen d'un véhicule.

La seconde catégorie de risques, ciblée sur des préjudices à plus long terme, est sans doute la plus fréquente du fait du large éventail de modalités d'attaque. Ce type de délit débouche invariablement sur l'exploitation ultérieure des informations et de l'identité de la victime, même s'il y a souvent aussi des gains primaires tels que l'accès immédiat aux fonds. Diverses formes de fraude peuvent s'ensuivre, dont le vol d'identité, le piratage de compte et l'extorsion, et, outre une perte financière, la victime subit souvent un préjudice sous la forme d'une baisse de son degré estimé de solvabilité ou des condamnations judiciaires.

À l'avenir, les délits sur les GAB devraient se faire encore plus intéressants pour les criminels, à mesure que les types de services et de produits offerts à travers la dernière génération de distributeurs continuent de se développer et d'évoluer. De même qu'un nombre croissant de GAB sont conçus pour accepter différents types de dépôts (p.ex. en devises ou par chèque), beaucoup sont à présent utilisés pour distribuer d'autres produits qui attireront également les criminels, comme les timbres-poste. Dans ces conditions, il est raisonnable de penser que les types d'attaques continueront également d'évoluer et que les différentes formes de délits commis sur les GAB resteront une source de préoccupation, ce qui renforce la nécessité de sensibiliser la population.

Implications pour les titulaires de carte en termes de sécurité

La fraude aux distributeurs automatiques est de plus en plus sophistiquée et les criminels ont trouvé des manières nouvelles et innovantes de retirer de l'argent des comptes au moyen de fausses cartes ou de cartes falsifiées contenant de vraies données. Si les méthodes des criminels pour faire main basse sur l'argent se sont affinées sur le plan technique, les enjeux pour les titulaires de carte restent les mêmes qu'à l'époque où la fraude aux GAB a commencé à poser sérieusement problème.

L'objectif principal des titulaires de compte est de conserver leur argent à l'abri sur leur compte. La sécurité des informations s'est trop longtemps focalisée sur les solutions techniques pour renforcer au maximum la protection. S'agissant des incidents de sécurité sur les distributeurs automatiques survenus ces dernières années, l'élément humain attire de plus en plus l'attention. Les titulaires de carte doivent avoir conscience des risques auxquels ils s'exposent et de la manière de prévenir la fraude, ou savoir ce qu'il convient de faire pour limiter les préjudices au cas où les données de leur carte tomberaient entre de mauvaises mains.
Les GAB sont utilisés par les criminels à la fois pour recueillir des informations relatives aux cartes bancaires et pour effectuer des retraits frauduleux sur les comptes des utilisateurs. Les titulaires de carte doivent garder en permanence ces deux aspects à l'esprit lorsqu'ils utilisent leur carte, observent d'autres personnes qui retirent de l'argent ou contrôlent leurs relevés bancaires.

Protection de carte

Les titulaires de carte doivent être conscients des risques pour leurs cartes, ainsi que des moyens de contribuer à empêcher les retraits frauduleux sur les comptes d'autres titulaires de carte.

Le premier indice que quelque chose ne va pas se perçoit lorsqu'un titulaire de carte se rend au distributeur automatique. Il importe que les titulaires de carte aient conscience de ce qui se passe autour d'eux, qu'ils se tiennent près de la machine et cachent le clavier afin d'empêcher quiconque de les voir saisir leur code confidentiel. Le meilleur moyen pour les titulaires de carte de protéger leur carte et ses données consiste à rester vigilants lorsqu'ils utilisent un GAB. Par exemple, en utilisant régulièrement le même appareil, ils connaîtront l'aspect normal du distributeur concerné et seront à même d'observer le comportement normal escompté. Au moindre détail inhabituel concernant la machine, les titulaires de carte veilleront à ne pas l'utiliser et à informer leur banque de leurs observations et soupçons.

Protection personnelle

Si les titulaires de carte observent un comportement suspect à proximité des GAB, il est primordial qu'ils en informent immédiatement la banque si possible. Il importe qu'ils n'essaient jamais d'examiner de plus près un distributeur à l'allure suspecte ou qui ne fonctionne pas comme il le devrait; souvent les fraudeurs ne sont pas loin et peuvent tenter d'intervenir, si quelqu'un se met à examiner l'appareil de plus près. Dans certains cas, les titulaires de carte ont été agressés alors qu'ils tentaient de découvrir la cause du problème de la machine. Soyez attentifs aux autres personnes autour du GAB; si vous notez un comportement suspect ou si vous n'êtes pas à l'aise pour utiliser un distributeur, faites part de vos soupçons et observations à la banque et utilisez un autre appareil.

Protection du code confidentiel

Les fraudeurs utilisent des méthodes nombreuses et diverses pour obtenir les données relatives aux cartes. Aussi le premier moyen d'assurer la sécurité et de protéger les titulaires de carte contre l'escroquerie consiste-t-il à faire en sorte que personne d'autre n'en connaisse le code confidentiel. Si des fraudeurs apprennent le code confidentiel, ils peuvent facilement avoir accès à l'argent. Les GAB n'appliquent pas les mêmes mesures de sécurité dans le monde entier: il est donc conseillé aux titulaires de carte de changer de code chaque fois qu'ils ont voyagé à l'étranger. Les fraudeurs essaieront également le code confidentiel en leur possession pour accéder aux comptes liés à d'autres cartes, aussi est-il conseillé d'utiliser un code différent pour chaque carte.

Détails des cartes bancaires et l'internet

Un autre moyen d'accéder aux données bancaires et d'identification personnelles (p.ex. code confidentiel) passe par l'internet. Une fois ces informations obtenues, des copies des cartes peuvent être produites. Les cas de hameçonnage, où les titulaires de carte reçoivent un courrier électronique les invitant à cliquer sur les liens et à communiquer leurs données bancaires et personnelles, sont en augmentation. Les courriers électroniques proviennent souvent de sources aux apparences légales, car les fraudeurs ont trouvé des moyens très sophistiqués pour simuler la correspondance entre les banques et leurs clients, de sorte qu'il peut être parfois difficile de reconnaître un message frauduleux. Une bonne règle consiste à ne jamais cliquer sur les hyperliens reçus par courrier électronique et invitant à confirmer les données bancaires. Un autre moyen de se protéger est d'installer un bon programme anti-virus et pare-feu sur l'ordinateur utilisé pour effectuer des opérations bancaires en ligne.

Autres précautions de sécurité

Une autre précaution de sécurité pourrait être d'envisager l'utilisation de cartes bancaires rechargeables sur lesquelles des montants restreints d'argent sont stockés. Cela permettrait d'éviter que les fraudeurs retirent une somme d'argent importante qu'un titulaire de carte aurait déposée sur un compte.

De plus, les consommateurs doivent également rester vigilants lorsqu'ils communiquent leurs données bancaires par téléphone, car quelqu'un pourrait être à l'écoute non loin. Efforcez-vous toujours de trouver un endroit tranquille lorsque vous téléphonez à votre banque.

Pour déceler les retraits frauduleux, les titulaires de carte doivent contrôler régulièrement leurs opérations bancaires et leurs relevés de compte.

Conservez le numéro d'urgence de la banque à portée de main

Après avoir obtenu les données et le code confidentiel d'une carte, les fraudeurs essaieront sans doute de retirer de l'argent aussi rapidement que la technique le leur permet. Il est primordial d'informer la banque dans les meilleurs délais et, parfois, les forces de police locales lorsqu'un titulaire de carte soupçonne que son code confidentiel et/ou les données de sa carte ont été divulgués, afin de permettre à la banque de bloquer le(s) compte(s) et, partant, d'éviter les retraits frauduleux. Il est crucial de conserver à portée de main le numéro d'appel d'urgence de la banque. Rappelez-vous que, lorsqu'une carte est égarée, le numéro d'urgence sera également perdu s'il n'est pas noté dans un endroit sûr. De même, sachez quel numéro il convient d'appeler depuis l'étranger, car il est possible que le numéro utilisé à l'intérieur des frontières ne fonctionne pas à partir d'un hôtel.

PARTIE 2: RÈGLES D'OR

Règles d'or pour réduire les délits sur les GAB

Ces conseils de sécurité s'appuient sur l'analyse des données et les recherches existantes. La présente section du document vise à formuler, rassemblées en un seul endroit, des recommandations en vue de sensibiliser la population aux différents types de délits commis, ainsi que des conseils sur la manière de les reconnaître.

Ces règles offrent une protection maximale à moindre effort. En observant ces règles, les parties concernées accroîtront leur protection lors de l'utilisation d'un GAB.

Catégorie	#	Recommandations	Description
Choisissez un GAB sûr	1.	N'utilisez pas de GAB vous rappelant de manière excessive de rester vigilant	N'utilisez pas de GAB vous rappelant de manière excessive de rester vigilant au moyen de signaux et d'avertissements placés sur la machine, car ils sont souvent utilisés par les fraudeurs pour tenter de convaincre les utilisateurs que des GAB trafiqués sont sans danger. Méfiez-vous notamment des instructions inhabituelles sur la manière d'utiliser le distributeur.
	2.	Utilisez un GAB à l'intérieur d'une banque	Si possible, utilisez les GAB à l'intérieur des banques, d'autres bâtiments et d'espaces fermés, plutôt que dans la rue. Les GAB situés dans la rue sont plus faciles d'accès pour les criminels.
	3.	N'utilisez pas de GAB autonome	Évitez les GAB autonomes placés dans la rue. Évitez les GAB qui ne sont pas fixés dans le mur d'un bâtiment ou à l'intérieur d'une infrastructure. Si la machine ne fait pas payer les opérations mais est attachée à un bâtiment et que les opérations se déroulent sans problème, vous ne courez sans doute aucun risque.
Observez les alentours	4.	Restez vigilant au cadre environnant	Restez toujours vigilant à votre cadre environnant. Utilisez un GAB qui est bien en vue et bien éclairé. Méfiez-vous en particulier des machines situées dans l'ombre ou dans des endroits qui ne semblent pas bien gardés et surveillés.
	5.	Assurez-vous que les autres personnes dans la file d'attente se tiennent à une distance raisonnable	Assurez-vous que les autres personnes dans la file d'attente se tiennent à une distance raisonnable de vous. Méfiez-vous si un inconnu vous propose de l'aide au distributeur, même si votre carte est coincée ou si vous avez des difficultés. Ne vous laissez distraire par personne.
	6.	Protégez votre code confidentiel des regards indiscrets en vous tenant près de la machine et en cachant le clavier	Cachez le clavier avec votre main lorsque vous saisissez votre code confidentiel afin d'empêcher toute caméra dissimulée ou toute personne de subtiliser vos informations. Ne révélez jamais à personne votre code confidentiel.

Observez le GAB	7.	Soyez attentif à l'avant des machines	Si l'avant de la machine est différent de celui des autres distributeurs de la région (par exemple parce qu'il y a un miroir supplémentaire sur la façade), qu'il présente des résidus de colle (provenant sans doute d'un dispositif qui y avait été attaché) ou des avertissements supplémentaires, utilisez un autre appareil et faites part de vos inquiétudes à la direction de la banque.
	8.	Faites attention au lecteur dans lequel vous insérez votre carte	Si vous vous rendez à un GAB inhabituel qui n'est pas situé à l'intérieur d'une banque, examinez-le soigneusement pour déceler tout dispositif. Même si vous connaissez bien un GAB, soyez attentif à toute différence ou caractéristique inhabituelle du lecteur de carte. Si la goulotte d'introduction de carte vous semble bizarre ou volumineuse, essayez d'exercer une pression dessus avec la main. Si un dispositif a été collé par-dessus le vrai lecteur de carte, il bougera ou se détachera. Les dispositifs de capture des billets ou des cartes doivent être collés ou scotchés au lecteur de carte ou au distributeur de billets. Si le GAB semble présenter un élément collé sur le lecteur de carte ou le clavier, ne l'utilisez pas. Annulez l'opération et éloignez-vous. N'essayez jamais d'enlever les dispositifs suspects.
	9.	Vérifiez attentivement le clavier du guichet automatique	Même si vous connaissez bien un GAB, vérifiez attentivement que le clavier ne présente aucune différence ou caractéristique inhabituelle. Si un faux clavier a été collé par-dessus le vrai clavier, il se révélera «mal fixé» si vous le remuez légèrement.
	10.	Vérifiez qu'il n'y a pas de caméra supplémentaire	Assurez-vous qu'il n'y a pas de caméra «supplémentaire» dans le GAB, en dehors de la caméra de sécurité classique et généralement apparente.
	11.	Signalez immédiatement les cartes retenues dans la machine	Signalez immédiatement les cartes retenues dans la machine. Si possible, ne vous éloignez pas de la machine. Appelez plutôt la banque depuis le GAB où votre carte a été retenue. N'acceptez pas l'aide de personnes inconnues pour récupérer une carte retenue. En outre, prévenez les forces de police locales.
	12.	Méfiez-vous des GAB qui ne donnent pas d'argent ou qui font ne pas payer les opérations bancaires	Si vous utilisez un GAB qui ne donne pas d'argent, il est plus que probable qu'il s'agit d'un faux, et il convient d'avertir votre banque du risque potentiel pour votre compte. Si vous utilisez un GAB qui n'est pas lié à une banque (par exemple dans une station-service ou un bar), méfiez-vous s'il ne vous fait pas payer les opérations bancaires. Les GAB privés qui ne sont pas liés directement à une banque font payer les services qu'ils fournissent. Si les services d'un tel GAB sont gratuits, c'est un indice que l'appareil est sans doute frauduleux.

Vérifiez vos relevés	13.	Vérifiez régulièrement vos relevés de compte	Vérifiez régulièrement vos relevés de compte pour déceler toute activité inhabituelle. Si la plupart des actes de fraude se produisent rapidement, certains peuvent avoir lieu des semaines, voire des mois après que les données de votre carte ont été subtilisées. Vérifier régulièrement ses relevés de compte contribue à limiter l'impact potentiel de toute fraude.
Signalez toute activité suspecte	14.	Signalez immédiatement les cartes retenues dans la machine	Signalez immédiatement les cartes retenues dans la machine. Si possible, ne vous éloignez pas de la machine. Appelez plutôt la banque depuis le GAB où votre carte a été retenue. N'acceptez pas l'aide de personnes inconnues pour récupérer une carte retenue. En outre, prévenez les forces de police locales.
	15.	Signalez immédiatement toute activité suspecte	En cas de perte ou de vol de votre carte bancaire, ou si vous remarquez une activité frauduleuse sur votre compte, signalez-le immédiatement afin d'éviter toute perte supplémentaire.

Conclusions

Les GAB font partie intégrante du commerce dans toute l'Europe et offrent un service précieux aux utilisateurs. L'utilisation croissante des GAB s'est accompagnée d'une multiplication spectaculaire des attaques et des fraudes aux guichets automatiques. Des techniques telles que le vol des données par copie frauduleuse, le hameçonnage et les attaques via réseau contre des GAB ont entraîné des pertes de près de 500 millions d'euros en Europe l'an dernier. Ces techniques, de plus en plus sophistiquées, ont donné lieu à une hausse de 149% des attaques sur les GAB en 2008.

Ce document présente les multiples façons dont les attaques sur les GAB sont perpétrées, ainsi que des techniques et conseils simples que les utilisateurs peuvent appliquer pour déceler et prévenir ces agressions.

L'ENISA pense qu'un moyen important de réduire les fraudes et attaques sur les GAB consiste à informer la population des risques potentiels et des façons de les combattre. Cette information peut réduire significativement la fréquence et l'impact financier des attaques perpétrées sur les guichets automatiques, et renforcer la confiance à l'égard de l'utilisation des GAB.

ANNEXE

Utilisation des GAB et fraude: études de cas

L'ENISA a recueilli, dans différents pays d'Europe, plusieurs études de cas et expériences relatives à diverses formes d'utilisation et de fraude aux GAB, afin de permettre aux lecteurs de connaître les principaux problèmes, les enjeux et les solutions. Ces exemples accroissent l'efficacité des règles suggérées et les présente de diverses manières concrètes.

Chypre

Actuellement sur l'île (dans la République de Chypre), quelque 560 GAB sont installés. On ne dispose d'aucune information sur le nombre ou le type de GAB installés dans la partie de l'île occupée par la Turquie. La majorité des 560 guichets automatiques installés sont des appareils «à travers le mur». Deux ou trois autres sont des «*cash-kiosks*» (bornes à devises). Un grand nombre des GAB installés sur l'île sont équipés de protections spéciales en plastique au niveau du lecteur de carte, ainsi que d'un dispositif anti-copie frauduleuse afin d'empêcher le placement de *skimmers* (et le vol consécutif des informations stockées dans la bande magnétique), ce qui pourrait fortement contribuer à éliminer les cas de fraude aux GAB par vol des données magnétiques ([15]).

Incidents récents survenus à Chypre

Les informations suivantes ont été enregistrées par le système de suivi des fraudes de JCC Payments System Ltd.

Cas n° 1

Certaines personnes utilisaient des cartes rechargeables falsifiées et recodées aux guichets automatiques. Vingt-six cartes ont été utilisées, et 2 310 euros ont été retirés. Le système de suivi des fraudes a décelé les activités frauduleuses et en a informé les services de police chypriotes. L'un des fraudeurs a été arrêté à l'aéroport.

Cas n° 2

Deux individus utilisaient des cartes rechargeables falsifiées aux guichets automatiques. Cent trente et une cartes ont été utilisées, et 15 830 euros ont été retirés. Identifiés par le système de suivi des fraudes, les individus ont été arrêtés par la police alors qu'ils utilisaient des cartes falsifiées.

Cas n° 3

Un individu utilisait des cartes rechargeables falsifiées aux guichets automatiques. Quarante-trois cartes ont été utilisées, et 1 860 euros ont été retirés. Le système de suivi des fraudes a décelé les activités frauduleuses et en a informé les services de police chypriotes. Le fraudeur a été arrêté.

Cas n° 4

Deux individus utilisaient des cartes rechargeables falsifiées aux guichets automatiques. Soixante-seize cartes ont été utilisées, et 7 950 euros ont été retirés. Le système de suivi des fraudes a décelé les activités frauduleuses et en a informé les services de police chypriotes. Les fraudeurs ont été arrêtés.

Cas n° 5

([15]) Toutes ces informations ont été transmises par le service de gestion des risques de JCC Payments Systems Ltd, l'unique acquéreur/processeur de Chypre pour VISA, MasterCard, AMEX et Diners.

Plusieurs individus utilisaient des cartes rechargeables falsifiées aux guichets automatiques. Cinquante-trois cartes ont été utilisées, et 10 700 euros ont été retirés. Le système de suivi des fraudes a décelé les activités frauduleuses et en a informé les services de police chypriotes. L'un des fraudeurs a été arrêté.

Cas n° 6

Deux individus utilisaient des cartes rechargeables falsifiées aux guichets automatiques. Cent vingt-deux cartes ont été utilisées, et 21 980 euros ont été retirés. Identifiés par le système de suivi des fraudes, les individus ont été arrêtés par la police alors qu'ils utilisaient les cartes falsifiées.

Cas n° 7

Un individu utilisait des cartes rechargeables falsifiées aux guichets automatiques. Quarante et une cartes ont été utilisées, et 28 340 euros ont été retirés. Identifié par le système de suivi des fraudes, l'individu a été arrêté par la police alors qu'il utilisait les cartes falsifiées.

Cas n° 8

Un individu utilisait des cartes rechargeables falsifiées aux guichets automatiques. Quatre-vingt-deux cartes ont été utilisées, et 12 330 euros ont été retirés. Le système de suivi des fraudes a décelé les activités frauduleuses et en a informé les services de police chypriotes. Le fraudeur a été arrêté.

Cas n° 9

Deux individus utilisaient des cartes rechargeables falsifiées aux guichets automatiques. Vingt et une cartes ont été utilisées, et 10 980 euros ont été retirés. Le système de suivi des fraudes a décelé les activités frauduleuses et en a informé les services de police chypriotes. Les fraudeurs ont été arrêtés.

Risques et dangers

Évolution de la fraude aux GAB

Les activités de fraude aux GAB vont décroissant de manière constante en 2009, principalement en raison du déploiement de la puce EMV en Europe et des mesures efficaces et proactives de lutte contre la fraude prises à Chypre.

Un nombre accru de fraudeurs ont été identifiés. La principale raison en est qu'ils croient à tort que Chypre est un pays peu avancé sur le plan technologique (terminaux EMV limités et systèmes de contrôle des cartes faibles) et qu'en tant qu'île ultrapériphérique de l'Europe, Chypre est un endroit où les fraudeurs ne risquent pas d'être pris. En fait, comme il n'y a qu'un acquéreur à Chypre, il est nettement plus facile d'identifier les fraudeurs, par rapport au Royaume-Uni ou à la Grèce, qui comptent cinq ou six acquéreurs différents qui ne partagent pas les données et où, par conséquent, il est nettement plus difficile de les prendre.

Capacités de fraudeurs

Les fraudeurs identifiés sur l'île se caractérisaient par une approche intelligente des actes de fraude et ont fait preuve d'une adresse remarquable pour contourner les systèmes de sécurité des banques. Ils se montrent également pleins de ressources et semblent bien organisés. En outre, les technologies de vol de données des fraudeurs supplantent les technologies des vendeurs de GAB (p.ex. «Jitter», «FDI»).

Impact de la fraude aux GAB

La fraude porte atteinte à l'intégrité des marques et à la confiance des titulaires de carte. Elle est toutefois compensée par les actions des systèmes de carte, qui déjouent efficacement les actions des fraudeurs lors d'une fraude à la carte de crédit.

Italie

En Italie, les GAB sont principalement utilisés avec des cartes de débit, qui permettent le retrait immédiat de liquide du compte bancaire et proposent des services de paiement et d'information tels que les recharges téléphoniques, la consultation des comptes personnels, les dons, etc. Le circuit BANCOMAT (principal circuit italien de cartes de débit) et ses protocoles ont été conçus il y a plus de vingt ans et, bien qu'aujourd'hui ils évoluent vers de nouveaux concepts, les questions de sécurité continuent de se poser au niveau des choix de conception et des solutions appliquées aux technologies actuellement abandonnées en faveur de plus modernes.

Les premières cartes de ce type, encore largement utilisées, sont équipées d'une bande magnétique où sont stockées diverses informations. Le titulaire de carte s'identifie au moyen d'un code confidentiel de cinq chiffres, communiqué directement par la banque. Toutefois ces dernières années, les sociétés gestionnaires du circuit tentent de remplacer ces cartes par celles de la nouvelle génération, équipées d'une puce (cartes intelligentes), qui résistent mieux aux tentatives de clonage. Tout l'environnement évolue: les anciens GAB fondés sur des systèmes locaux sont remplacés et les nouveaux proposent des fonctions avancées, comme les contenus multimédias, les paiements avec reconnaissance automatique des billets, les écrans tactiles, le clavier et des possibilités étendues de personnaliser le logiciel d'exploitation.

Tous les dispositifs de distribution automatique sont contrôlés par du matériel de surveillance vidéo en circuit fermé afin de prévenir les attaques physiques comme l'utilisation de grues pour arracher les GAB à leur base, l'utilisation de voitures volées comme béliers ou la pose d'explosifs. Les systèmes de fraude sophistiqués recourent à une fausse face avant équipée d'un dispositif permettant de cloner les cartes. Pour limiter l'ampleur des vols (outre le coût du système des GAB, qui est encore élevé), les banques italiennes n'approvisionnent les GAB que des montants strictement nécessaires, et les équipent de dispositifs qui endommagent définitivement les billets (encres de couleur, etc.).

À ce jour, les fraudes perpétrées en Italie se sont essentiellement limitées aux catégories décrites ci-dessus, car aucune attaque logique sur les GAB n'a été signalée. Il est toutefois permis de supposer que cette tendance évoluera considérablement dans un avenir proche.

L'un des principaux problèmes rencontrés sur le plan de la sécurité des GAB concerne le nombre d'acteurs dans le domaine: souvent la communication entre ces parties est faible et il n'est pas facile de déterminer si un *bug* est dû au constructeur du matériel (vendeur du GAB), au fabricant du logiciel, aux protocoles utilisés ou à la configuration de l'infrastructure de distribution automatique elle-même.

Méthodes utilisées lors des attaques

La dernière génération de GAB se compose, fondamentalement, de PC industriels dotés de connexions sérielles spécifiques ou de dispositifs USB (clavier PIN, distributeur de billets, claviers plus ou moins personnalisés, etc.), communiquant avec la banque via des protocoles IP ou SNA (à présent encapsulés sur IP). Les banques ont

également réalisé des économies en réduisant les investissements dans des lignes spéciales pour les données qui diminuent la sécurité des systèmes GAB. Il a maintes fois été souligné que ces dispositifs sont directement liés au réseau interne (LAN) de la banque ou au réseau des agences et sont rarement coupés du segment de réseau où se trouvent d'autres systèmes d'entreprise (du poste de travail au système de serveur).

En règle générale, les systèmes de GAB sont utilisés en tant qu'équipements industriels et non comme des ordinateurs ordinaires. Il s'ensuit que, une fois installés, ils sont rarement mis à jour et peu entretenus. En outre, en tant que produits industriels, les corrections au système d'exploitation (le plus souvent Microsoft Windows) doivent d'abord être testées, recevoir une licence et être distribuées par le fabricant, ce qui constitue un obstacle supplémentaire. Ce choix expose les systèmes de GAB à divers types de dangers bien connus, comme les vers et les virus, susceptibles de compromettre l'infrastructure et de la rendre indisponible (p.ex. crash massif des GAB Diebold en 2003, à cause du ver Slammer). Un facteur externe ou interne de danger pour la banque pourrait également attaquer les systèmes en tirant profit des faiblesses du système d'exploitation, du logiciel ou de la gestion du mot de passe (souvent, «connu») pour accéder aux GAB et modifier le logiciel afin de fournir davantage de liquide, si certaines conditions spécifiques sont remplies.

En outre, les protocoles de communication analysés ont révélé de nombreux problèmes de sécurité. Bien que, dans un passé récent, de nouvelles spécifications réputées plus sûres ont été mises en circulation, en général, elles ne sont pas entièrement mises en œuvre. Par exemple, souvent les communications entre le GAB et l'unité finale (macroordinateur, etc.) ne sont pas cryptées et aucun élément ne garantit l'authenticité des données. Pendant certaines attaques, il a été démontré qu'il est possible d'intercepter et de modifier ces notifications, permettant ainsi au criminel de retirer davantage d'argent que n'en contient le compte concerné, ou de modifier le montant retiré.

Les différentes analyses effectuées révèlent un autre problème sérieux (qui exacerbe également ce qui se passait auparavant), à savoir le placement de systèmes de GAB: dans le cas de distributeur automatiques situés dans des zones non protégées, les connexions électriques et les liaisons réseau sont souvent accessibles à l'utilisateur final (même si le GAB est situé à l'intérieur de la banque). Une coupure de courant provoquée entraînerait une réinitialisation du système, livrant ainsi plusieurs informations à l'auteur de l'attaque; d'un autre côté, la possibilité d'accéder au câblage de réseau permettrait l'installation d'un système TAP à même d'intercepter le trafic réseau et de le transférer par un réseau sans fil.

Afin de mieux se rendre compte du nombre de problèmes de sécurité qui peuvent se poser, pas seulement lié à la technologie, nous pouvons réfléchir à la manière dont les systèmes de GAB sont déployés. Ils sont distribués dans tout le pays, souvent sans passer par le siège central des banques, et installés directement dans les agences ou en d'autres lieux d'intérêt par des tierces parties qui se voient remettre des clés de chiffrement.

Les procédures de gestion relatives à ces systèmes sont en général moins détaillées que celles des systèmes informatiques, même s'ils utilisent de plus en plus souvent des plateformes similaires: nous voulons parler des tests de sécurité après déploiement, de la gestion des mots de passe, des contrôles et alertes de sécurité, de la gestion des vulnérabilités et des corrections de programme, de la protection contre les logiciels malveillants, etc.

Il convient de souligner avec insistance que nombre de ces attaques ne visent pas seulement les cartes de débit, mais peuvent également être efficaces avec les cartes de crédit utilisées dans les GAB, même si les répercussions spécifiques doivent encore être évaluées pleinement.

Trop souvent, les enjeux de sécurité liés aux GAB ne sont pas reconnus. Très rares sont les banques qui ont réalisé une évaluation formelle et complète des risques pour la sécurité de leurs infrastructures GAB. Le recours à la notion de «sécurité par l'obscurité», qui a longtemps été

appliquée aux dispositifs spécialisés, est erroné sur le plan conceptuel, et s'avère l'être aussi sur le plan concret à mesure que la tendance mondiale de la fraude bancaire s'accentue. De plus en plus d'individus étudient ces infrastructures afin d'y déceler des failles de sécurité susceptibles de leur donner accès aux distributeurs automatiques et à l'objectif final réel de ces nouvelles formes de crime organisé: les billets.

À l'avenir, les attaques logiques sur les GAB se multiplieront certainement: si l'on néglige ces risques en cette période délicate de transition, on risque dans la pratique de commencer à perdre une bataille tout à fait cruciale, capitale pour la sécurité nationale de tous les pays et systèmes économiques du monde.

Portugal

Le Portugal présente l'un des taux de pénétration des GAB par habitant les plus élevés d'Europe. Cela s'explique en grande partie par les fonctions avancées qui sont offertes à la population en général, comme le paiement de services publics et privés (tels que le gaz, l'eau, les impôts ou la téléphonie mobile) ou la possibilité d'acheter des billets de concert, en plus des services financiers plus traditionnels comme le retrait d'argent ou la consultation des comptes.

Dans les paragraphes qui suivent, nous vous présentons une vue générale du réseau de GAB au Portugal, des principaux dangers et types de fraude, ainsi que des efforts en cours et de ceux qui s'imposent afin d'améliorer la sécurité de l'environnement des GAB.

Le réseau de GAB

Le réseau de GAB au Portugal est géré par SIBS, une société détenue par la majorité des banques présentes sur le marché. SIBS est la sixième plus grande chambre de compensation automatisée (CCA) d'Europe. Elle traite plus de deux milliards d'opérations par an, pour un total d'environ 6 000 000 de millions d'euros, et est à l'origine de la mise sur pied d'un réseau intégré des GAB et des POS (points de vente) commun à toutes les banques sur le marché.

S'agissant de l'utilisation des cartes de débit et de crédit, les indicateurs portugais sont supérieurs à la moyenne de l'UE, pour les cartes comme pour les GAB et les terminaux POS par habitant. De même, le Portugal présente le taux d'utilisation de carte le plus élevé d'Europe, par rapport à d'autres formes de paiement, avec plus de 60% des transactions.

Tous les GAB du pays sont à présent compatibles avec EMV (Europay, Mastercard et Visa), de même que 83% des terminaux POS. Les institutions financières s'efforcent également à offrir des cartes de crédit et de débit aux normes EMV, qui représentent environ 44% des cartes dans le pays en 2008.

Sur le plan des communications, le réseau des GAB repose sur des lignes de communication spéciales (RPV) par SSL, dotées de mécanismes de sécurité complémentaires tels que le codage 3DES et le code d'authentification de message (MAC). En outre, la philosophie sous-jacente au développement du réseau de GAB s'appuie sur une approche de sécurité en vertu de laquelle aucun appareil ne peut entamer une communication directement avec un GAB; ce sont au contraire les GAB qui engagent la communication avec les autres équipements (y compris les systèmes SIBS).

PayWatch

À la fin 2008, une nouvelle société a été créée – Paywatch –, chargée de contrôler en permanence le réseau des GAB, d'identifier les modes d'utilisation de carte et de déceler les formes de fraude aux guichets automatiques et aux terminaux POS.
Cela permettra à Paywatch d'identifier en temps réel les fraudes commises avec des cartes portugaises et/ou sur le réseau GAB / POS et de limiter rapidement les préjudices. Cela n'est

possible qu'en raison du fait, mentionné ci-dessus, que le réseau est intégré et peut être vu comme un tout, plutôt que comme un réseau fragmenté. Il n'y a pas très longtemps, le grand public voyait dans ces activités de contrôle une sorte de «Big Brother», et les gens ne pouvaient comprendre pourquoi leurs opérations personnelles étaient surveillées. Toutefois, probablement en raison du fait qu'un nombre croissant de cas sont rendus publics chaque année (non seulement au Portugal, mais dans le monde entier), les mentalités ont changé depuis quelques années, et les gens y voient à présent un avantage pour le système et une protection pour eux-mêmes et leur argent.

PayWatch est à même de détecter en temps réel l'utilisation d'une carte clonée sur le réseau de GAB, à travers l'analyse de cryptogrammes – une caractéristique propre aux cartes et aux GAB portugais. En gros, si une carte est censée être aux normes EMV, mais que seule la piste magnétique est utilisée (*fallback* ou fonctionnement dégradé), il est plus que probable que la carte en cause est un clone, et l'opération est refusée.

PayWatch a une vue d'ensemble de toutes les utilisations des cartes de crédit et de débit portugaises, dans le réseau GAB national comme à l'étranger. Cela permet à PayWatch et SIBS de bloquer l'utilisation de certaines cartes, voire de bloquer les opérations dans une région donnée du monde, si une augmentation des utilisations frauduleuses est décelée – par exemple, les transactions de toute carte portugaise effectuées depuis la ville de Barcelone peuvent être bloquées.

Si PayWatch détecte en temps réel une carte clonée ou toute autre utilisation frauduleuse, SIBS ou la banque peut contacter le client immédiatement et prendre les mesures qui s'imposent afin de limiter les risques.

Risques et niveaux de fraude

Les niveaux de fraude dans le pays sont, en règle générale, faibles, avec un ou deux cas signalés par an. La principale menace réside dans les attaques physiques sur les GAB: elles ont augmenté très nettement en 2008, en raison de la spécialisation dans ce type d'attaques d'un groupe d'individus originaires d'Europe orientale.

Cependant, le nombre d'attaques ratées croît aussi plus rapidement, car de plus en plus de guichets automatiques sont désormais équipés de systèmes de maculage des billets et sont ancrés dans le sol.

S'agissant des attaques sur les cartes, le vol/exploitation (*skimming*) des données reste le principal danger. La carte est copiée sur le GAB même, ou dans le vestibule d'une banque où sont installés des GAB, et dont l'accès requiert que les utilisateurs glissent leur carte dans un lecteur pour en ouvrir les portes, cette dernière forme de fraude représentant de 10 à 20 %. Le code confidentiel est en général «volé» au moyen d'une caméra placée au sommet du guichet automatique, d'un faux clavier ou en observant par-dessus l'épaule de l'utilisateur (*shoulder surfing*).

Tous les GAB du pays sont à présent équipés de mécanismes anti-*skimming*. Le plus fréquent consiste en l'utilisation d'un lecteur qui ralentit l'entrée de la carte et la rend difficile à lire pour un faux lecteur.

D'un point de vue technologique, une caméra pourrait être intégrée aux GAB afin de tenter de déceler si quelqu'un place un faux équipement par-dessus le guichet automatique, mais cela n'est pas possible au Portugal, pour des raisons de protection de la vie privée, comme le souligne la Commission nationale de la protection des données.

Si la relation entre SIBS et les services de police est très coopérative et repose sur la confiance mutuelle, il n'en va pas de même avec la justice. Les auteurs de fraudes récidivistes ne sont parfois condamnés que pour un fait précis, et le fait qu'ils soient récidivistes n'est pas pris en considération.

De même, la législation portugaise ne condamne que les personnes prises avec des cartes de crédit clonées et non des cartes de débit, ce qui est perçu comme un problème vu le nombre de cartes de ce type (Visa Electron) dans le pays.

Au niveau des tendances, depuis l'introduction des cartes EMV l'on prévoit une augmentation de l'utilisation des cartes portugaises clonées à l'étranger, dans des pays où le système EMV n'a pas encore été entièrement déployé.

Vers un environnement plus sûr

SIBS publie sur son site internet les précautions que doivent prendre les citoyens lorsqu'ils utilisent un GAB ou un terminal POS, notamment, mais pas uniquement: ne pas perdre de vue la carte, ne pas répéter une opération à moins que le terminal n'affiche un message les informant que la première tentative a échoué, et ne pas communiquer le code confidentiel à des tiers. Sur ce dernier point, le guichet automatique lui-même invite l'utilisateur à protéger et cacher le clavier lorsqu'il saisit son code confidentiel.
L'introduction de systèmes de maculage des billets a contribué à prévenir les attaques physiques sur les GAB, et les commerçants se voient informer qu'un billet de banque taché d'encre ou de teinture est un billet volé – à ce jour, un seul cas a été enregistré, où un billet maculé a été utilisé chez un commerçant.

Étant donné les mécanismes actuellement mis en œuvre sur les GAB, les criminels concentrent leurs efforts sur les portes des vestibules des banques où sont installés des distributeurs. N'importe quelle carte à bande magnétique ouvre la porte, ce qui rend le mécanisme inutile en termes de contrôle d'accès au vestibule, tout en créant un nouveau point vulnérable au vol de données. L'ouverture des portes au moyen d'un bouton offre le même niveau de contrôle qu'actuellement, mais permettrait d'éliminer le point vulnérable précité. Tant que la carte est nécessaire pour accéder au vestibule, il est conseillé d'utiliser une carte pour ouvrir la porte et une autre pour effectuer l'opération sur le GAB.

Il est également conseillé, chaque fois que possible, d'utiliser toujours le même distributeur, afin de déceler les anomalies éventuelles (telles que de faux claviers ou lecteurs de carte).

Une hausse des niveaux de fraude dans le monde virtuel est également prévue. Afin de faire face à ce problème, SIBS a mis au point un système – MBNet – permettant aux utilisateurs de lier un compte MBNet à un compte bancaire, une opération qui peut être réalisée auprès d'une banque. Ainsi, quand une personne souhaite payer un achat en ligne, elle peut accéder au site internet de MBNet et générer un numéro de carte Visa virtuel, qui met à sa disposition un montant limité et a une durée de vie d'un mois.

Références et lectures conseillées

«*ATM scam nets Melbourne thieves $ 500,000*» [Melbourne: une arnaque aux distributeurs rapporte 500 000 dollars aux escrocs], 24 mars 2009, disponible sur http://www.atmmarketplace.com/article.php?id=10808 (dernière visite le 20 avril 2009).

«*ATM scam targets hundreds of credit cards*» [Des centaines de cartes de crédit victimes d'une arnaque aux distributeurs], New Europe, n° 793, 4 août 2008, disponible sur *http://www.neurope.eu/articles/89221.php* (dernière visite le 20 avril 2009).

«*ATMs on Staten Island rigged for identity theft; bandits steal $500G*» [Distributeurs de Staten Island trafiqués pour vol d'identité: les escrocs détournent 500 000 dollars], 11 mai 2009, disponible sur http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html#ixzz0J8qBVdar&D

«*Australian police suspect Romanian gang behind $ 1 million ATM scam*» [Un million de dollars détournés aux distributeurs: la police australienne soupçonne une bande de Roumains], 14 avril 2009, disponible sur http://www.atmmarketplace.com/article.php?id=10883 (dernière visite le 20 avril 2009).

http://abcnews.go.com/Technology/Business/story?id=7434509&page=1

http://cert.inteco.es

http://garwarner.blogspot.com/2009/03/bank-hacking-exposed-analyzer-affadavit.html

http://www.adicae.net/

http://www.atmsecurity.com/monthly-digest/atm-security-monthly-digest/atm-fraud-and-security-digest-march-2009.html

http://www.computerworld.com/securitytopics/security/story/0,10801,111158,00.html

http://www.denverpost.com/headlines/ci_12276447 (dernière visite le 5 mai 2009).

http://www.europol.europa.eu/index.asp?page=news&news=pr090731_2.htm

http://www.mydigitallife.info/2006/09/25/atm-hacking-and-cracking-to-steal-money-with-atm-backdoor-default-master-password/

http://www.theregister.co.uk/2006/11/18/mp3_player_atm_hack/

http://www.wired.com/threatlevel/2009/04/pins/

https://www.european-atm-security.eu/Welcome%20to%20EAST/

Marks P., «*Cash machines hacked to spew out card details*» [Distributeurs piratés pour révéler les données des cartes], *NewScientist magazine*, n° 2713, disponible sur

http://www.newscientist.com/article/mg20227135.700-cash-machines-hacked-to-spew-out-card-details.html?full=true (dernière visite le 8 juillet 2009).

McGlasson L., «*ATM Fraud: 7 Growing Threats to Financial Institutions*» [Fraude aux GAB: 7 menaces croissantes pour les institutions financières]*, BankInfoSecurity*, disponible sur http://www.bankinfosecurity.com/articles.php?art_id=1523 (dernière visite le 9 juin 2009).

Peretti K. K., «*Data Breaches: What The Underground World of «Carding» Reveals*» [Vols de données: dans le monde souterrain de la fraude à la carte], *Santa Clara Computer & High Technology Law Journal*, volume 25, n° 2, disponible sur http://www.chtlj.org/volumes/v25 (dernière visite le 2 juillet 2009).

Reuters, «*Cyberthieves steal millions from banks*» [Des cybervoleurs subtilisent plusieurs millions aux banques], mai 2009, disponible sur http://uk.reuters.com/article/idUKTRE54I6CK20090520 (dernière visite le 20 mai 2009).

Robinson G., «*Bondi banks scam: ATM alert*» [Fraude dans les banques de Bondi: alerte sur les distributeurs automatiques], *The Sydney Morning Herald*, octobre 2008, disponible sur http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950 (dernière visite le 2 juillet 2009).

«*Shoppers are targeted in ATM scam*» [Les acheteurs pris pour cible dans une fraude aux distributeurs automatiques], *BBC News*, 11 mars 2006, disponible sur *http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.stm* (dernière visite le 20 avril 2009).

SIBS, «*Relatório e Contas 2008*» [Rapport et comptes 2008], *SIBS*, 2009, disponible sur http://www.sibs.pt/export/sites/sibs_publico/pt/documentos/relatorioecontas/Contas_SA_2008.pdf (dernière visite le 5 mai 2009).

Sydney Morning Herald, octobre 2008, disponible sur http://www.smh.com.au/news/national/bondi-banks-scam-atm-alert/2008/10/09/1223145514492.html?sssdmh=dm16.338950

Trustwave, «*Automated Teller Machine (ATM) Malware Analysis Briefing*» [Logiciel malveillant aux distributeurs automatiques: information et analyse], 28 mai 2009, disponible sur https://www.trustwave.com/pressReleases.php (dernière visite le 13 juillet 2009).

VISA Business News, «*Data Security Alert – Compromise of ATM PIN Transactions*» [Alerte à la sécurité des données – Risque pour les transactions sur distributeur avec code confidentiel], 3 juin 2009.

Zetter K., «*ATM Vendor Halts Researcher's Talk on Vulnerability*» [Le vendeur des distributeurs automatiques suspend l'exposé d'un chercheur sur la vulnérabilité du système], *WIRED*, juin 2009, disponible sur http://www.wired.com/threatlevel/2009/06/atm-vendor-halts-talk/ (dernière visite le 8 juillet 2009).

Délits sur les GAB: Vue d'ensemble de la situation en Europe et règles d'or pour les éviter

ISBN-13: 978-92-9204-043-7

Numéro de catalogue: TP-80-09-736-FR-N

DOI : 10.2824/18027

TP-80-09-736-FR-N

enisa
European Network and Information Security Agency

ISBN-13 978-92-9204-043-7

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu