



**Observatoire  
de l'évolution  
des moyens  
de paiement**

Faits, Tendances et Analyses



## ÉTAT DES LIEUX

**LUTTE CONTRE LA FRAUDE**

*SECURITE DES DONNEES*

*LES MENACES QUI PERSISTENT*

Inspiré par l'actualité récente, le présent cahier a été conçu pour proposer un état des lieux en matière de sécurité des données. Il se fait l'écho de cas particulièrement marquants : les attaques à l'encontre d'un certain nombre de distributeurs de renom dont, notamment, le géant américain Target.

Ce dossier ne se veut pas exhaustif mais se présente comme un outil d'accompagnement, susceptible d'être mis à jour pour accueillir des développements futurs, au fil de l'eau.

Outre une synthèse des éléments rendus publics quant aux affaires de fraudes qui ont fait les grandes lignes ces dernières semaines, ce document comprend, à titre d'illustration, quelques brèves Moyens de paiement ayant trait à l'actualité de la lutte contre la fraude. Extraites de notre **Observatoire de l'évolution des moyens de paiement**® publié mensuellement, elles analysent un certain nombre de solutions ou d'évolutions que nous avons jugées pertinentes.

Spécialiste de l'innovation liée aux métiers de la monétique et, plus globalement, des services financiers, ADN'co mobilise ses consultants pour vous aider à appréhender les enjeux qui façonnent déjà l'industrie des paiements de demain.

Consciente de la nécessité d'une bonne appropriation de sujets tels que celui de la sécurité des données et de la lutte contre la fraude, notre société peut vous accompagner dans vos réflexions et projets (diagnostic, recherche de solutions, POC, gestion de projet, etc.). Enfin, en tant qu'organisme de formation, nous pouvons aussi vous guider, vous apporter des éclairages et contribuer à sensibiliser vos équipes à ces problématiques.

<b>SÉCURITÉ DES DONNÉES – LES MENACES QUI PERSISTENT...</b>	<b>5</b>
<b>INTRODUCTION</b>	<b>6</b>
<b>AFFAIRE TARGET : UN GEANT SOUS LES FEUX DES PROJECTEURS</b>	<b>6</b>
<b>DE LONGUE DATE DES CIBLES PRIVILEGIEES</b>	<b>7</b>
<b>SECURITE DES DONNEES : LES NORMES QUI S'APPLIQUENT</b>	<b>8</b>
<b>CONCLUSION</b>	<b>9</b>
<b>ANNEXES – Extraits <i>Observatoire de l'Évolution des moyens de paiement</i>®</b>	<b>10</b>
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : DECEMBRE 2013</b>	<b>11</b>
JP Morgan attaquée	11
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : NOVEMBRE 2013</b>	<b>12</b>
PCI-DSS et PA-DSS : versions 3	12
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : OCTOBRE 2013</b>	<b>13</b>
Les points de vente sud-africains attaqués	13
DataCash améliore les performances de GateKeeper:2.0	14
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : AOUT 2013</b>	<b>15</b>
Les membres présumés d'un réseau criminel devant les tribunaux	15
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : JUILLET 2013</b>	<b>16</b>
Nouvelle évolution de la fraude en 2012	16
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : DECEMBRE 2012</b>	<b>17</b>
TPE : un nouveau malware ciblant les points de vente	17
<b>OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT® : NOVEMBRE 2012</b>	<b>18</b>
Vols de données : collaboration internationale contre les réseaux de <i>carders</i>	18



# **SÉCURITÉ DES DONNÉES**

—

## **LES MENACES QUI PERSISTENT...**

## INTRODUCTION

Les grands titres de la fin d'année 2013 ont fait la part belle au récent cas de fraude à l'encontre de l'un des géants américains de la distribution, Target. Un incident à l'ampleur « historique » dans le sillage duquel d'autres affaires font surface et qui éveille des attaques antérieures également marquantes.

### Quand sécurité des données et image ne font plus bon ménage

Des cas d'autant plus impactants que leurs retombées financières peuvent s'avérer dramatiques et que rétablir l'image de sociétés victimes n'est jamais chose aisée : état des lieux sur ces affaires ainsi que sur les mesures et normes auxquelles les distributeurs sont tenus de se conformer...

## AFFAIRE TARGET : UN GEANT SOUS LES FEUX DES PROJECTEURS



Le vol d'un grand nombre de données stockées par Target au niveau de ses TPE fait aujourd'hui l'objet de toutes les attentions. Aux dires de la chaîne de distribution, près de **40 millions de numéros de cartes de débit et de crédit** auraient été subtilisés suite à l'exploitation d'une brèche dans ses systèmes peu avant Thanksgiving. Des chiffres qui ne cessent d'évoluer et font désormais état de **70 millions de noms, adresses, numéros de téléphone et courriels** dans la nature.

Dès le mois de décembre, Target indiquait que les noms des porteurs ainsi que les numéros, dates d'expiration, CVx de leurs cartes et codes PIN chiffrés avaient peut-être été affectés.

Enquête oblige, Target reste très évasif quant à la nature de la faille incriminée et au mode opératoire de l'attaque proprement dite. Les comptes-rendus les plus récents évoquent cependant un **malware**, surnommé **BlackPOS**, présent sur les dispositifs d'encaissement. Connu des chercheurs en sécurité (société PSC) depuis début janvier 2013, il se distingue de la plupart des « *RAM scraper* » : il ne se « contente » pas de passer en revue la mémoire des terminaux pour exfiltrer et transmettre les données qui y circulent. Conçu pour cibler avec précision les dispositifs qu'il infecte, il saurait où chercher et sélectionnerait l'information. L'installation de ce logiciel aura impliqué l'accès par des attaquants au réseau du commerçant.

Visa faisait état de ce type de menaces sous forme d'alerte en avril et août 2013. L'histoire ne dit pas encore si Target avait mis en œuvre les mesures de protection décrites alors par le réseau international. Le distributeur explique avoir fait appel à un prestataire externe pour auditer ses systèmes et remédier aux risques résiduels.

**Un coup de marteau pour Target.** Outre l'aspect financier (une première estimation de Forrester indique la somme de 100 millions de dollars en frais juridiques et réparations), côté porteurs, un sentiment légitime d'**insécurité** prédomine alors que les premières victimes se font entendre. Les centres d'appels de Target seraient assaillis depuis l'attaque et ses ventes auraient régressé de 2 à 6 % selon les estimations.

Rappel: Target faisait également partie des sociétés victimes de l'attaque menée en 2007 par Albert Gonzalez (hacker américain accusé en août 2009 d'avoir organisé une fraude touchant 135 millions de numéros de cartes)

Quoi qu'il en soit, toutes ces informations ont peut-être déjà intégré les circuits d'un marché noir sur lequel se reposent les campagnes de *phishing* et autres industries frauduleuses des réseaux de *carders*. Dans tous les cas, les autorités compétentes (Secret Service et DoJ, notamment) ont déjà ouvert l'enquête. Selon le blog spécialisé krebsonSecurity, les numéros ainsi récupérés se monnaient fin décembre par lots d'un million de 20 à 100 dollars par carte.

## DE LONGUE DATE DES CIBLES PRIVILEGIEES

Également affecté en ce début d'année, **Neiman Marcus** (spécialisé dans le secteur du luxe) qui explique avoir pris connaissance de la fuite de données le concernant au mois de décembre dernier. Les éléments dérobés incluraient des numéros de cartes ainsi que diverses données porteurs sensibles. Confirmation n'a pas été faite que cette affaire est en lien avec celle de Target.



Ces attaques porteraient cependant à environ un quart la proportion de citoyens américains potentiellement touchés... Le bruit court aussi que des annonces supplémentaires seraient imminentes et que **plusieurs grands noms** risquent bientôt de s'ajouter à cette liste (les rumeurs en date de mi-janvier laissent entendre qu'au moins six distributeurs seraient concernés).

### Ces incidents rappellent des cas identifiés antérieurement :

**Octobre 2013** – les **infrastructures d'acceptation sud-africaines** sont frappées par l'une des plus vastes cyberattaques de leur histoire : un grand nombre de points de vente compromis : magasins, hôtels, restaurants (dont la chaîne de fast-foods KFC), etc. Les pertes sont estimées à plusieurs dizaines de millions de rands. Toutes les banques sud-africaines auraient été indirectement affectées.

**Juillet 2013** – les autorités fédérales américaines inculpent cinq suspects russes et ukrainiens en lien avec l'affaire Heartland. Un cas de fraude qui avait conduit à la compromission de plus de 160 millions de cartes dérobés aux processeurs **Global Payments** et **Heartland Payment Systems** entre autres. Coût : plus de 300 millions de dollars pour trois des sociétés victimes. 7-Eleven et Carrefour font partie des distributeurs impactés.

**Décembre 2012** – l'Israélien Seculert met au jour un malware surnommé Dexter, conçu pour infecter les terminaux de paiement. Un outil qui aurait servi au cours du dernier trimestre 2012 dans **une quarantaine de pays**. Les systèmes compromis incluraient indistinctement des distributeurs, des hôteliers, des gestionnaires de parc de stationnement, etc.

**Novembre 2012** – les forces de police australiennes et roumaines démantèlent un gang international de *carders* supposé avoir mené la plus vaste opération de vol de données cartes jamais conduite en **Australie** : une centaine de points de vente impactés, les informations de près de 500 000 porteurs exposées et 30 000 exploitées pour un préjudice estimé à 30 millions de dollars.

**Mars 2007** – TJX annonce avoir été victime d'une attaque susceptible d'avoir impacté 46 millions de ses clients (cartes MasterCard et Visa). Ce chiffre sera revu à la hausse la même année, portant à 94 millions le nombre de victimes potentielles.

## SECURITE DES DONNEES : LES NORMES QUI S'APPLIQUENT

Ces attaques et leurs conséquences soulignent l'intérêt d'audits réguliers et la mise en place de mesures adaptées aux risques encourus. En matière de normes, le PCI-SSC a récemment publié la version 3 de PCI- et PA-DSS. Des mises à jour qui cadrent avec l'évolution des contextes transactionnels.

Ces bonnes pratiques s'appliquent à l'ensemble des acteurs susceptibles de gérer, stocker ou faire transiter des données transactionnelles ; elles font une grande place au monde de la distribution. Parmi les « nouveaux » ajouts à PCI-DSS, la **nécessité d'améliorer la gestion des alertes en cas de modification des systèmes**, etc. et l'obligation pour les fournisseurs de services de garantir par écrit la sécurité des données clients qu'ils gèrent.

Target dit avoir fait réaliser un audit PCI environ trois mois avant que l'incident ne se produise. Il explique aussi investir lourdement dans son programme de mise en conformité EMV et compte sur une migration rapide de tous ses terminaux (et de ses cartes REDcards). Ces changements, attendus d'ici début 2015, représenteraient 100 millions de dollars.

Dans tous les cas, il convient de rappeler que le PCI-SSC recommande de ne pas stocker les pistes, CVx et PIN :

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data <sup>2</sup>	Full Track Data <sup>3</sup>	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID <sup>4</sup>	No	Cannot store per Requirement 3.2
		PIN/PIN Block <sup>5</sup>	No	Cannot store per Requirement 3.2

Source : PCI-DSS, version 3.0 (page 8)



Autre point : bien que dans le cas de Target une mise en conformité EMV seule, sans mesures complémentaires, n'aurait pas suffi à prémunir le distributeur contre ce type d'attaques, la migration américaine vers la norme internationale pourrait progressivement changer la donne pour les commerçants. Les réseaux internationaux continuent de faire pression pour cette mise en place.

Néanmoins, ces affaires mettent en relief l'intérêt de la mise en œuvre de plusieurs normes et solutions complémentaires. Il y a fort à penser que l'adoption d'outils de chiffrement de bout en bout par les différents acteurs des paiements constituerait aussi un début de réponse pour augmenter les chances de prévenir de nouveaux écueils.

## CONCLUSION

Loin d'être closes, ces nouvelles affaires et les enquêtes auxquelles elles donnent lieu ne connaîtront leur dénouement qu'au bout de plusieurs mois, voire plusieurs années. L'origine de telles opérations frauduleuses, souvent menées par des réseaux criminels internationaux organisés, reste en effet difficile à cerner.

Les processeurs, banques et réseaux dont les données ont été exposées risquent aussi de demander réparation. Des imbroglios dont le monde de la distribution, comme les autres parties prenantes des transactions de paiement doivent se prémunir.

D'ici là, il convient, pour les distributeurs victimes, de s'assurer de la conformité et de la pertinence de leurs politiques de sécurité pour éviter d'autres dommages et regagner la confiance de leurs clients, également victimes. Considérer l'ensemble des technologies désormais disponibles pour garantir une protection renforcée est pour eux nécessaire. L'organisme international de normalisation EMVCo s'attache d'ailleurs en ce moment à étendre le champ de ses travaux pour plébisciter la tokenisation : de nouvelles spécifications englobant divers équipements (mobiles, tablettes, ordinateurs, etc.) seraient en cours de préparation pour compléter sa documentation EMV.

En effet, la multiplication des supports mobiles et de leur implication dans le paiement, tant côté émission qu'acquisition, est une source exponentielle de nouvelles menaces. Les distributeurs qui choisiront ces supports devront opter pour des solutions présentant des niveaux de sécurité exemplaires au risque de voir des attaques de grande envergure se produire sur ces moyens de paiement mobiles.

# ANNEXES

—

## Extraits

### *Observatoire de l'Évolution des moyens de paiement<sup>®</sup>*

## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT<sup>®</sup> :

### DECEMBRE 2013

## JP Morgan attaquée

**JP Morgan a annoncé avoir été victime d'une attaque susceptible d'avoir impacté 465 000 de ses cartes prépayées UCard, autant d'informations pouvant d'être utilisées pour créer de faux comptes cartes.**

Les cartes prépayées UCards servent notamment à des entreprises et agences gouvernementales pour les versements des salaires et allocations chômage. Les données relatives à ces cartes auraient, selon la banque, été dérobées entre juillet et septembre dernier suite à une attaque ayant pris pour cible les serveurs du site [www.ucard.chase.com](http://www.ucard.chase.com).

La technique utilisée et la faille mise en cause n'ont pas été décrites. Cette fuite aurait néanmoins permis la récupération de données personnelles en clair, bien que, selon la banque, ces informations n'incluraient pas d'éléments critiques (*Social Security Number*, date de naissance, etc.). Une enquête officielle est en cours.

### Notre analyse

### Les cartes prépayées cibles idéales pour les contrefacteurs ?

Cette attaque pourrait avoir porté atteinte à 2 % des 25 millions de cartes UCard émises par JP Morgan Chase. La banque consent à un geste commercial mais indique que les cartes ne seront pas remplacées. Pour l'heure, il n'a pas été fait état de pertes financières, mais l'image de la banque a, quant à elle, bien été atteinte.

Cette annonce met en lumière les risques liés à l'appropriation des données cartes à des fins de contrefaçon.

L'année 2013 a connu d'autres incidents du même ordre et plusieurs mises en examen en mai et novembre derniers : affaires dans lesquelles 45 millions de dollars auraient été détournés grâce à des numéros de cartes prépayées volés. Les cartes impactées auraient été émises par des banques basées aux Emirats Arabes Unis et dans le sultanat d'Oman (voir *l'Observatoire de mai 2013*).

**Pays :** Etats-Unis

**Tags :** prépayé, cartes, vol de données, contrefaçon

**Source :** Reuters

**Date :** 5 décembre 2013

## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT<sup>®</sup> : NOVEMBRE 2013

### PCI-DSS et PA-DSS : versions 3

Le PCI-SSC fait évoluer ses publications pour cadrer avec l'évolution des contextes transactionnels. Très attendus, ces documents prendront effet, pour les procédures de mise en conformité, dès le 1<sup>er</sup> janvier 2014.



Les nouvelles exigences de la norme PCI-DSS incluent notamment :

- l'évaluation des menaces en regard des systèmes jugés peu ciblés,
- un contrôle plus poussé des accès du personnel aux départements sensibles,
- une meilleure protection des outils servant à capturer les données cartes,
- une meilleure gestion des alertes en cas de modification des systèmes, etc.
- l'obligation pour les fournisseurs de services de garantir par écrit la sécurité des données clients qu'ils gèrent.

PA-DSS, pour sa part, insiste notamment sur le rôle des développeurs, avec :

- pour les éditeurs, l'obligation de s'assurer de l'intégrité des codes source pendant le processus de développement,
- pour les éditeurs d'applications de paiement, l'intégration de techniques d'évaluation du risque dans leurs processus de développement.

Eveiller les consciences : c'est l'objectif de ces nouveaux documents qui font une large place à l'information et à l'éducation des parties prenantes. Les acteurs concernés disposent d'un an pour faire auditer leurs systèmes, s'assurer de leur conformité et apporter, le cas échéant, les modifications nécessaires.

#### Notre analyse

### Des normes qui se doivent d'être exhaustives

Cet ensemble de bonnes pratiques intègre les retours de spécialistes des industries concernées. En accord avec l'évolution des technologies, des menaces et des risques, le PCI-SSC complète ses recueils de recommandations en visant l'exhaustivité.

A titre d'exemple, face à l'émergence des supports mobiles et à leur adoption par l'industrie des paiements, le Conseil a publié en 2012 et 2013 plusieurs recommandations dédiées à l'acceptation mobile ; des documents qui prennent en compte l'essor du multicanal et mettent en lumière des menaces émergentes et la complexité des mesures de sécurisation à appliquer.

**Pays :** Monde

**Tags :** normes, sécurité des données

**Source :** communiqué de presse

**Date :** 7 novembre 2013

## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT<sup>®</sup> :

### OCTOBRE 2013

### Les points de vente sud-africains attaqués

**Les infrastructures d'acceptation sud-africaines ont été frappées par l'une des plus vastes cyberattaques de leur histoire. Les autorités locales font le point sur un malware qui s'est propagé au sein des logiciels des points de vente.**

Selon la *Payment Association of South Africa* (PASA), un grand nombre de magasins, hôtels, restaurants (dont la chaîne de fast-foods KFC), etc. auraient été compromis, engendrant des pertes estimées à plusieurs dizaines de millions de rands. Toutes les banques sud-africaines auraient été indirectement affectées.

**Premiers cas de fraude identifiés en début d'année.** Les fraudeurs auraient utilisé une variante d'un malware baptisé Dexter conçu pour skimmer et retransmettre les informations contenues sur les pistes magnétiques des cartes.

L'attaque aurait été lancée depuis l'Europe, sans que l'association ait pour l'heure pu identifier son origine exacte. Les enquêtes se poursuivent au niveau international, mobilisant les services de police sud-africains (SAPS), Interpol et Europol.

Notre  
analyse

### Les points de vente très menacés

Identifiée fin 2012 par le spécialiste israélien Seculert, la version précédente du code malveillant avait alors impacté plusieurs pays, avec pour cibles principales le Royaume-Uni et les États-Unis (voir l'*Observatoire de décembre 2012*).

Cette affaire illustre à nouveau l'intérêt des fraudeurs pour les points de vente. Une situation pré-occupante alors que, selon Trusteer, le nombre de malwares ne cesse d'augmenter. Cette année, Dexter, vSkimmer, BlackPOS et Alina ont été identifiés (tous récupèrent les données cartes).

**Pays :** Afrique du Sud

**Tags :** malware, points de vente

**Source :** Bloomberg

**Date :** 15 octobre 2013

## DataCash améliore les performances de GateKeeper:2.0

Le fournisseur de services de paiement, DataCash (filiale de MasterCard) annonce l'intégration de deux produits à sa solution de détection et de prévention de fraude GateKeeper:2.0 : *Expert Monitoring System Fraud Scoring for Merchants* et *Lost-Stolen Account List API* de MasterCard.

Deux outils qui, ajoutés à sa plate-forme GateKeeper:2.0, doivent aider les commerçants à mieux gérer leurs stratégies de lutte contre la fraude.

Grâce à l'API *Lost-Stolen Account List*, GateKeeper:2.0 bénéficiera d'un système de référencement croisé portant sur plus de 30 millions de données cartes volées ou perdues au niveau international. Le but : aider les commerces clients à détecter les tentatives frauduleuses et améliorer le service fourni aux consommateurs légitimes.

*Expert Monitoring System Fraud Scoring for Merchants* leur procure un outil de scoring proactif pour mieux appréhender les comportements d'achat et l'usage des cartes de paiement par les porteurs.

### Notre analyse

#### Détection de fraude : une lutte proactive

Cette intégration réaffirme l'engagement des grands réseaux internationaux dans la détection proactive des transactions suspectes. Lancée en avril dernier, la plate-forme GateKeeper:2.0 s'adresse particulièrement aux commerces et aux acquéreurs (*Voir l'Observatoire d'avril 2013*). Elle traite chaque mois plus de 30 millions de transactions pour environ 30 000 commerçants dans 180 pays.

Autre signe de l'investissement des réseaux sur ce point, Visa, de son côté, annonce avoir apporté des améliorations à *Advanced Authorization* (VAA). Là encore, l'intérêt pour les commerçants réside dans la possibilité d'identifier et proscrire les transactions frauduleuses en amont. *Advanced Authorization* intègre désormais un outil d'analyse repensé ainsi qu'un plus grand nombre de données sur les historiques transactionnels. Objectif : proposer un outil de scoring et de gestion de risque plus complet. Parmi les secteurs concernés par ces améliorations : les stations-service dont les automates sont toujours très ciblés par les fraudeurs (*Automated Fuel Dispensers*).

**Pays :** International

**Tags :** détection de fraude

**Source :** communiqué de presse

**Date :** 8 octobre 2013



## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT<sup>®</sup> :

### AOUT 2013

## Les membres présumés d'un réseau criminel devant les tribunaux

**Les autorités fédérales américaines ont inculpé cinq suspects russes et ukrainiens en lien avec l'affaire Heartland. Un cas de fraude de grande envergure qui aurait conduit à la compromission de plus de 160 millions de cartes dérobées aux processeurs Global Payments et Heartland Payment Systems notamment.**

L'organisation (surnommée *Shadowcrew*), supposément active durant sept ans, aurait coûté plus de 300 millions de dollars à trois des sociétés victimes.

Parmi les sociétés impactées, des réseaux, des établissements financiers et des distributeurs : le NASDAQ, 7-Eleven, Carrefour S.A., Dexia Bank Belgique, Dow Jones Inc., Euronet, Visa Jordan Card Services, ou bien encore Diners Club Singapour.

**Chefs d'inculpation : vol et recel.** Les suspects auraient été chargés de la conception des malwares utilisés pour exfiltrer les données et les compromettre.

#### Notre analyse

### Internationalisation de la fraude

Cette affaire illustre à nouveau la portée désormais internationale des organisations criminelles dont les victimes se répartissent ici sur trois continents. Parmi elles, le distributeur français Carrefour pour qui la fuite aurait porté sur deux millions de numéros de cartes, dérobés à partir d'octobre 2007.

Les cas d'Heartland (130 millions de cartes dérobées pour environ 200 millions de dollars de pertes) et Global Payments (950 000 cartes pour 92,7 millions de dollars) ont été particulièrement médiatisés ainsi que les règlements qui en ont découlé. Ces attaques rappellent la vulnérabilité des processeurs et réseaux ainsi que la nécessité pour eux de se conformer aux normes internationales de sécurité.

Les numéros volés étaient ensuite vendus : de 10 dollars pour les données américaines à 50 dollars pour les cartes européennes.

**Pays :** Etats-Unis / Monde

**Tags :** fuite de données, vol, recel, contrefaçon

**Source :** *Second Superseding Indictment*

**Date :** juillet 2013

## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT<sup>®</sup> : JUILLET 2013

### Nouvelle évolution de la fraude en 2012



La Banque de France publie son *Observatoire de la sécurité des cartes de paiement* pour l'exercice 2012 : état des lieux et nouvelle progression de la fraude en France.

La BdF constate une nouvelle augmentation du taux de fraude carte global : 0,080 %, pour 450,7 millions d'euros en 2012, contre 0,077 % en 2011 (413,2 millions d'euros).

Les cas de fraude au niveau national ont augmenté de 7,1 % ; cette augmentation concerne surtout les retraits. Ainsi les attaques de DAB ont augmenté de 73 % par rapport à 2011 et les cas de compromissions aux points de vente étaient 2,5 fois plus nombreux qu'en 2011.

Au niveau international le taux de fraude augmente de 11,2 %. Principaux responsables : les vols de cartes et compromissions par skimming des moyens de paiement des porteurs en voyage d'une part, la fraude en ligne à partir de sites basés à l'étranger d'autre part.

#### Notre analyse

### Des efforts qui doivent se maintenir

Ce dixième rapport note le rôle des solutions d'authentification forte pour lutter contre la fraude en ligne. Bien que sa part atteigne 27,5 % du montant (contre 23 % en 2011), le taux de fraude sur les paiements en ligne passe à 0,290 % contre 0,341 % en 2011. Signe que les travaux en cours s'avèrent utiles et doivent se poursuivre.

L'Observatoire plébiscite également les efforts de mise en conformité, notamment la généralisation d'EMV au niveau européen.

En ce qui concerne les transactions sans contact, la Banque de France estime que, compte tenu des « modalités techniques » requises et du « faible intérêt financier » de ce type d'attaques pour les fraudeurs, les risques sont aujourd'hui peu élevés. Les émetteurs se doivent de rassurer leurs porteurs en leur fournissant les moyens d'empêcher la récupération des données (cages de Faraday) et de pouvoir désactiver à distance le mode sans contact. Comme indiqué par la CNIL, les porteurs doivent aussi pouvoir refuser cette fonctionnalité.

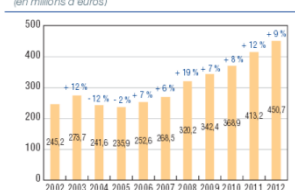
Pays : France

Tags : cartes

Source : communiqué de presse

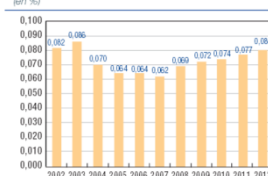
Date : 2 juillet 2013

Graphique 2  
Évolution du montant de la fraude  
(en millions d'euros)



Source : Observatoire de la sécurité des cartes de paiement

Graphique 3  
Évolution du taux de fraude  
pour tous types de cartes et transactions  
(en %)



Source : Observatoire de la sécurité des cartes de paiement



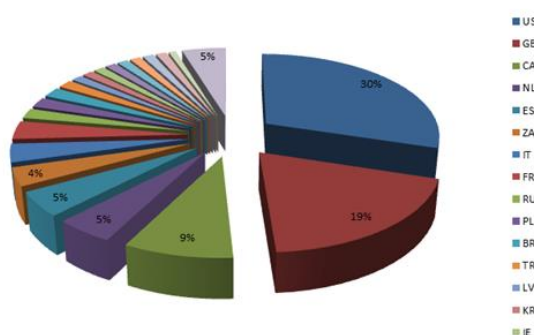
## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT © : DECEMBRE 2012

### TPE : un nouveau malware ciblant les points de vente

Le spécialiste israélien Seculert a récemment mis au jour un malware (surnommé Dexter) conçu pour infecter les terminaux de paiement. Selon les chercheurs, l'outil aurait servi au cours du dernier trimestre 2012 dans une quarantaine de pays.

Les systèmes compromis incluraient indistinctement des distributeurs, des hôteliers, des gestionnaires de parc de stationnement, etc. Les régions les plus affectées seraient les États-Unis (42 %) et la Grande-Bretagne (19 %) – voir schéma pour cette répartition.

Dexter s'approprierait les journaux des terminaux infectés et récupérerait aussi les pistes 1 et 2 des cartes : autant de supports pouvant être dupliqués ensuite par les fraudeurs.



Répartition des TPE compromis par pays

<http://blog.seculert.com/2012/12/dexter-draining-blood-out-of-point-of.html>

#### Notre analyse

### Prévenir les compromissions aux points de vente

Seculert rappelle que les attaquants s'en prennent aujourd'hui davantage aux systèmes mis en place aux points de vente : leur compromission s'avèrerait plus simple que l'installation de dispositifs de skimming (qui impliquent quant à eux la présence physique d'un manipulateur pour pouvoir être déployés).

Les points de vente ont été particulièrement ciblés ces derniers temps, avec, par exemple, les récentes attaques relevées en Australie : une centaine de systèmes compromis auraient permis aux fraudeurs d'accéder aux informations d'environ 500 000 clients (dont 30 000 auraient été exploitées). La coopération de forces internationales aura néanmoins permis le démantèlement d'un réseau de *carders* présumés à l'origine de cette opération (voir l'*Observatoire de novembre 2012*).

Pays : Monde

Tags : vol de données, points de vente

Source : Blog Seculert

Date : 11 décembre 2012

## OBSERVATOIRE DE L'ÉVOLUTION DES MOYENS DE PAIEMENT<sup>®</sup> : NOVEMBRE 2012

### Vols de données : collaboration internationale contre les réseaux de *carders*

**Les forces de police australiennes et roumaines viennent conjointement de démanteler un gang international de *carders* supposé avoir mené la plus vaste opération de vol de données cartes jamais conduite en Australie.**

Seize attaquants présumés ont été interpellés en Roumanie. Ils auraient eu accès à une centaine de points de vente ainsi qu'aux informations de près de 500 000 porteurs. Parmi ces données, 30 000 auraient été exploitées, engendrant un préjudice estimé à 30 millions de dollars.

Les forces de police peuvent déjà confirmer la compromission des systèmes de 46 points de vente (pour l'essentiel de petits commerces, dont des stations-service).

Si l'ensemble des informations potentiellement récupérées avaient été ainsi utilisées, le préjudice aurait pu s'élever à près de 750 millions de dollars (environ 1 500 dollars par carte).

Les données cartes auraient permis la fabrication de fausses cartes utilisées en Europe, à Hong Kong, en Australie ainsi qu'aux États-Unis.

#### Notre analyse

L'enquête policière était lancée en juin 2011. Les commerçants impactés ont pris les mesures nécessaires pour prévenir de nouvelles attaques et, bien que tous les clients n'aient pas encore été informés de l'exposition de leurs informations, les fonds éventuellement perdus leur seront restitués. Ces attaques ont déjà coûté 30 millions de dollars aux banques australiennes qui procèdent aujourd'hui au remboursement des sommes dérobées aux victimes.

Ce démantèlement est le fruit d'une collaboration internationale réussie ayant mis à contribution les services d'environ 13 pays (dont le MI-5 et le FBI). Selon l'AFP (Australian Federal Police), les établissements bancaires ont également permis à l'enquête de progresser et ont mis en place des mesures de prévention plus robustes.

L'AFP recommande toutefois aux porteurs, aux banques ainsi qu'aux commerçants de rester vigilants. Les clients se doivent de suivre attentivement leurs comptes et de remonter toutes transactions suspectes (aux forces de l'ordre, puis à leur banque). Les commerces doivent pour leur part protéger les données de leurs clients et s'assurer de la pertinence comme de la conformité de leurs mesures de sécurité, qui doivent être tenues à jour.

**Pays :** Australie

**Tags :** vol de données, points de vente

**Source :** Herald Sun

**Date :** 29 novembre 2012



Votre partenaire face aux nouveaux enjeux des paiements



#### Notre mission à vos côtés :

- Analyser et interpréter les tendances, nouveautés et inflexions à l'échelle internationale
- Vous aider à optimiser vos solutions et vos offres, choisir les bons partenaires et saisir les opportunités les plus en phase avec votre stratégie et vos objectifs.

#### Angelo Caci

angelo.caci@adn-conseil.com  
Tél. : +33 (0)1 44 71 90 04  
Fax. : +33 (0)1 44 71 01 03



#### Luc Boucey

luc.boucey@adn-conseil.com  
Tél. : +33 (0)1 44 71 90 04  
Fax. : +33 (0)1 44 71 01 03



- Connaissance approfondie des services de paiement en France, en Europe et dans le monde
- Vision globale des enjeux et opportunités business et industriels
- Multiples secteurs d'activité (banque / finance, retail, e-commerce, telco, services, etc.)
- Relations au long cours avec nos clients
- Offre complète de la stratégie à l'accompagnement opérationnel (conseil, veille, études, gestion de projet, assistance marketing, etc.)
- Expertise sur les chaînes de valeur acceptation, acquisition et émission, sur les produits cartes et les services innovants (Internet, mobile, wallet, data, etc.)

**Contactez le Pôle Veille et Innovation au**  
**+33 (0)1 44 71 90 04**  
[commercial@adn-conseil.com](mailto:commercial@adn-conseil.com)