A Conthey, un bancomat piégé fait une trentaine de victimes

PIRATAGE En piégeant le bancomat de la Coop-Bassin, des malfrats ont dupliqué des cartes bancaires, puis retiré indûment de l'argent aux USA.
HIGH-TECH Les bandes internationales incriminées recourent à des caméras et scanners miniaturisés pour voler codes NIP et infos des cartes.
QUE FAIRE? Quelques précautions simples suffisent pour se prémunir de tels prélèvements frauduleux. Les conseils de la police.

CONTHEY Plusieurs cas de skimming ont été relevés récemment au bancomat du magasin Coop Bassin. Les prélèvements frauduleux ont ensuite été effectués aux USA.

Arnaqueurs sans frontière

DAVID VAQUIN

«J'ai failli ne pas m'en rendre compte. Plusieurs retraits aux Etats-Unis étaient inscrits sur mon relevé bancaire alors que je n'ai jamais visité ce pays. J'ai immédiatement pris contact avec ma banque pour l'aviser du problème.» Mélina, comme une trentaine d'autres personnes, a été victime de skimming. Le skimming? *«C'est une fraude sophistiquée qui consiste à voler de l'argent directement depuis un compte. Pour cela, les arnaqueurs se procurent illégalement des informations sur vos cartes bancaires puis retirent de l'argent à votre insu»*, précise Jean-Marie Bornet, chef de l'information et de la prévention de la police cantonale valaisanne. *«Concernant l'affaire de Conthey, nous pensons que le dispositif frauduleux a été installé à la fin avril. Pour l'instant, une trentaine de lésés se sont annoncés»*, relève l'inspecteur David Fumeaux de la section financière.

Système bien rodé

Comment les malfrats ont-ils fait pour pirater le bancomat contheysan? *«Concrètement, le skimming consiste à installer des dispositifs qui collectent les données bancaires. Deux choses intéressent les fraudeurs: le code NIP et les informations de débit ou de crédit contenues dans la bande magnétique. Il existe plusieurs systèmes. Des caméras miniatures permettent de filmer le code tandis que des dispositifs pirates placés sur la fente d'introduction scannent les données. Données qui sont ensuite collectées au moyen d'une clé USB ou alors transmises immédiatement plus loin par WiFi. Il ne reste ensuite plus qu'à fabriquer une fausse carte avec ces informations pour pouvoir faire des prélèvements»*, détaille Olivier Glassey, inspecteur de la section financière en charge de la coordination cantonale pour le skimming.

Comment l'argent fait ensuite pour transiter de Conthey aux USA? *«En Suisse et en Europe, les cartes bancaires sont munies d'une puce EMV qui n'est pas falsifiable. Ce n'est par contre pas le cas des*

USA et de différents autres pays dans le monde. Les voleurs transmettent donc les données à des complices dans d'autres pays. En moyenne, 40% des prélèvements frauduleux surviennent aux USA, 10% au Brésil, 10% également en Russie et le reste dans différentes autres nations, notamment en Asie.»

Mafias internationales

Le système est donc bien rodé? *«Extrêmement! En 2011, nous avons démantelé une filière qui sévissait depuis la Bulgarie. D'autres cas ont aussi été relevés en Roumanie. Les malfrats opèrent souvent depuis les anciens blocs de l'Est. Au niveau organisationnel, tout est extrêmement cloisonné. Dans le cas de 2011, les malfrats ne se connaissaient pas entre eux. Un homme gérait les piratages pour tout le canton. Un autre installait les dispositifs et un troisième venait les récupérer. Dispositifs qui étaient de surcroît livrés par une tierce personne»*, explique David Fumeaux.

Ne pas dramatiser

L'inspecteur tient cependant à ne pas dramatiser la situation: *«En Valais, les cas restent assez limités. Les différentes arnaques sur internet représentent notamment des montants nettement plus importants. Sur les dernières années, il y a eu 1 cas de skimming en 2009, 0 en 2010, 21 installations frauduleuses en 2011, trois cas dont deux tentatives en 2012 et trois cas pour l'instant en 2013. Il faut savoir que l'on parle bien de situations où nous avons constaté des appareils frauduleux. Il est très difficile de connaître le nombre de personnes lésées car les banques n'ont aucun intérêt à communiquer sur ces problèmes. Elles préfèrent rembourser les personnes touchées.»*

Des banques qui sont conscientes du problème et qui prennent des mesures. *«Les bancomats sont renforcés. Des employés contrôlent chaque jour les distributeurs sans oublier tous les systèmes d'alerte. Les montants sont limités à l'étranger et un retrait effectué à Miami quelques heures après un achat d'essence à Sion déclenchera une alarme»*, détaille Jean-Marie Bornet.

Hélas, les malfrats ont l'habitude de s'adapter et ils visent de plus en plus d'autres distributeurs, dans les gares ou les stations-service.

Conséquence directe, le lésé aura aussi moins de chances de se faire rembourser dans de telles installations. ◎

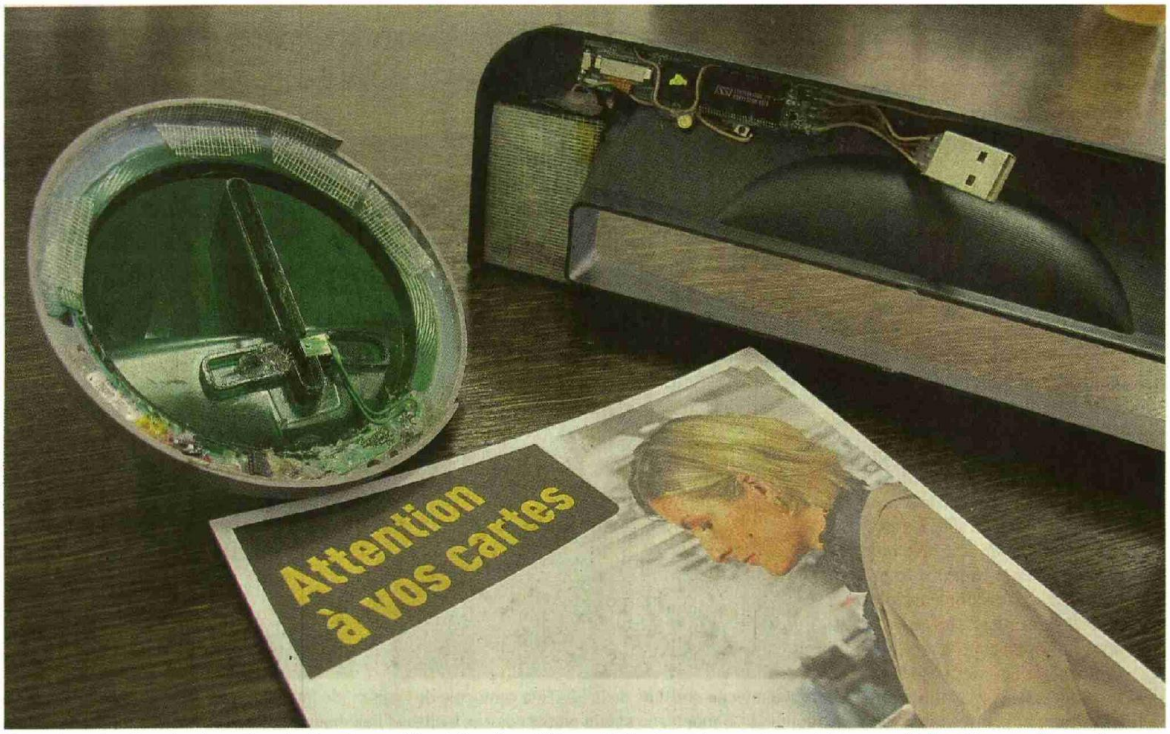
VIDÉO

Retrouvez notre vidéo sur ce sujet

iPad Le Nouvelliste + Epaper

«Le système est extrêment bien rodé. Les malfrats opèrent depuis les anciens pays de l'Est.»

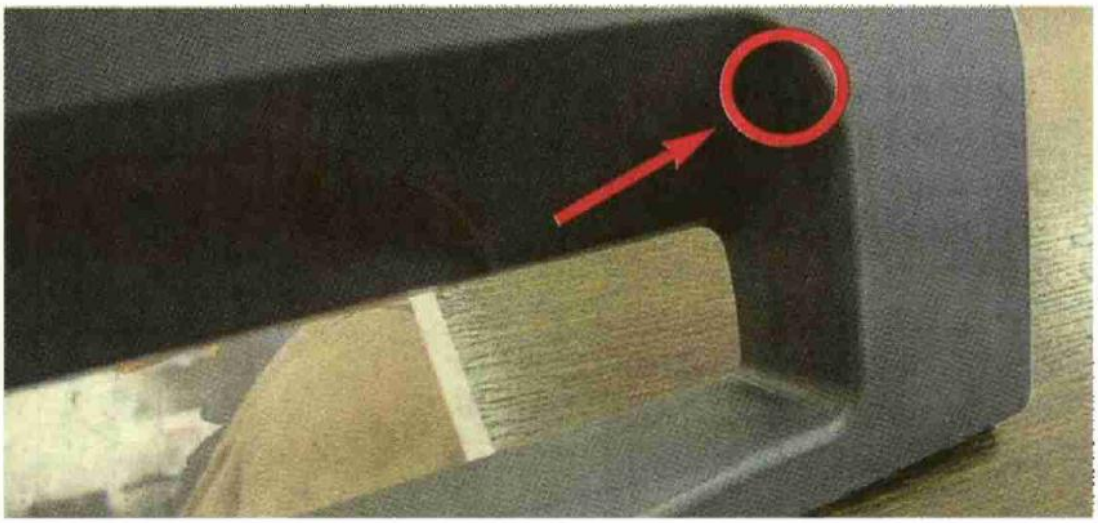
OLIVIER GLASSEY INSEPCTEUR À LA SECTION FINANCIÈRE DE LA POLICE CANTONALE



Pour pirater les données bancaires, les fraudeurs utilisent des dispositifs sophistiqués et des caméras miniatures qu'ils installent par-dessus les distributeurs. Ils viennent ensuite récupérer les engins avec les données ou alors la transmission se fait par WiFi. Il ne reste ensuite plus qu'à fabriquer une fausse carte et à prélever l'argent. LE NOUVELLISTE

LES CONSEILS DE PRÉVENTION

- Au niveau national, le nombre de vols par skimming a fortement augmenté en Suisse ces dernières années. Dans de nombreux cas, les malfaiteurs profitent du manque de méfiance des victimes. «Pourtant, quelques précautions suffisent pour protéger des retraits frauduleux», prévient Jean-Marie Bornet, chef de la cellule information et prévention de la police cantonale.
- Le code NIP est confidentiel, il ne doit jamais être transmis à des tiers, conservé avec la carte ou noté sur la carte.
- Il faut saisir son code à l'abri des regards, en cachant le clavier avec sa main ou en demandant aux personnes qui s'approchent trop près de reculer.
- Si vous découvrez qu'un automate a été piraté, qu'une pièce bouge ou que quelque chose n'est pas normal, il faut immédiatement aviser la banque qui gère le distributeur ou la police.
- Pensez à contrôler régulièrement vos comptes en banque et à prévenir immédiatement votre établissement bancaire en cas d'anomalies. **DV**



Les systèmes utilisés sont très astucieux. Ci-dessus, un faux cache installé sur un distributeur. Le petit trou (flèche) est l'objectif de la caméra. NF