Une vulnérabilité dans les Cartes bancaires connue et exploitée discrètement | Le Net Expert Informatique

Une vulnérabilité dans les Cartes bancaires connue et exploitée discrètement

Des chercheurs viennent de publier un rapport d'étude sur l'exploitation concrète mais discrète d'une vulnérabilité affectant les cartes EMV et connue depuis plus de 5 ans.

Combien de cas réellement constatés ? Combien de cas non constatés ? C'est la question que soulève l'étude que viennent de publier Houda Ferrradi, Rémi Géraud, David Naccache et Assia tria, de l'Ecole normale supérieure et du CEA-TEC Paca.

Dans celle-ci, les quatre chercheurs se penchent des cartes bancaires EMV modifiées pour permettre leur utilisation sans en connaître le code PIN, en toute discrétion, grâce à deux puces câbles l'une sur l'autre, sur la puce d'origine : « la première puce est clipsée sur une carte authentique volée. La seconde puce joue le rôle d'intermédiaire et communique directement avec le terminal de point de vente. L'ensemble est intégré au corps en plastique d'une autre carte également volée ».

Le concept est connu depuis début 2010. C'est le chercheur Steven J. Murdoch, de l'université de Cambridge qui avait levé le voile sur une vulnérabilité potentiellement grave des cartes bancaires à puces dites EMV. Une faille qui « permet à un fraudeur d'utiliser une carte de paiement à puce volée pour régler un achat, via un terminal de paiement électronique non modifié, sans connaître le code PIN du porteur légitime de la carte bancaire ». Ainsi, un dispositif électronique intercepte et modifie les communications entre la carte à puce et le terminal de paiement électronique. Lorsque celui-ci demande à la carte de vérifier le code PIN saisi par l'utilisateur, le dispositif du pirate intercepte la requête et se charge, à la place de la carte, de répondre au TPE que le code a été vérifié et confirmé. Voilà ce que décrivait alors, par le menu, le chercheur britannique dans un rapport d'étude préliminaire.

Lors d'un entretien téléphonique avec LeMagIT, Steven J. Murdoch évoquait alors l'ampleur de la menace : « le reçu indique que la transaction a été autorisée par code PIN », du moins était-ce le cas lors de ses tests au Royaume-Uni, pour des transactions de type offline comme online – à savoir, avec ou sans connexion aux serveurs de contrôle des transactions. Un détail lourd de conséquences : même armé d'une déclaration de perte ou de vol, comment le porteur légitime de la carte pourra-t-il dégager sa responsabilité face à un banquier qui ne manquera pas de lui rappeler qu'il est responsable de la confidentialité de son code PIN ? Pour Steven J. Murdoch, le risque était notamment que « d'autres aient découvert la faille avant nous ».

La lecture du rapport des quatre chercheurs français nous apprend qu'environ 40 modifications frauduleuses de cartes, exploitant la vulnérabilité dévoilée par Murdoch, ont été découvertes en 2011 : « en mai 2011, le GIE Cartes Bancaires a relevé qu'une dizaine de cartes EMC, volées en France quelques mois plus tôt, étaient utilisées en Belgique. Une enquête de police a été ouverte ». Le montant de la fraude liée à cette opération : un peu moins de 600 000 € sur plus de 7 000 transactions.

Début 2010, sans surprise, le GIE Cartes Bancaires minimisait toutefois la menace, estimant qu'elle « nécessitait des équipements qui ne sont pas très discrets ». Certes, la carte frauduleuse présente une puce d'apparence plus épaisse que la normale. Mais au moins dans le cas de cette fraude ayant fait l'objet d'une enquête, cela n'a pas éveillé de soupçons.

Source :
http://www.lemagit.fr/actualites/4500256061/Cartes-bancaires-une-vulnerabilite-connue-exploitee-discretement
par Valéry Marchive