Affaire United : selon le FBI, un hacker a modifié en vol la puissance d’un réacteur – Le Monde Informatique | Le Net Expert Informatique

Un hacker a modifié en vol la puissance d’un réacteur

Selon une note du FBI, en trois ans, le chercheur en sécurité Chris Roberts a réussi à pirater une vingtaine de fois les systèmes informatiques d'avions de ligne. Le dernier en date, sur un vol d'United Airlines entre Denver et Chicago, a entraîné son interpellation à la sortie de l'avion le 15 avril 2015.

Le FBI soupçonne aujourd'hui le chercheur en sécurité Chris Roberts, fondateur et CTO de One World Labs, d'avoir modifié la puissance d'un des réacteurs du vol d'United Airlines du 15 avril dernier entre Denver vers Chicago. M. Roberts avait été interpellé par le FBI à sa descente d'avion suite à un tweet suggérant qu'il avait scanné les systèmes informatiques (EICA) d'un Boeing 737. Cette arrestation et la saisie de tout son matériel informatique semblent faire suite à des dysfonctionnements relevés par United Airlines. Interrogé par le FBI, le chercheur, justement spécialisé dans les failles de sécurité des systèmes embarqués en aéronautique, a indiqué avoir réussi à accéder une vingtaine de fois aux systèmes informatiques d'avions de ligne.

Le 17 avril, l'agence fédérale américaine a obtenu un mandat pour perquisitionner les locaux du chercheur. Dans sa demande de mandat, le FBI révèle des informations provenant des trois interrogatoires de M. Roberts. Il n'a pas encore été accusé d'un crime, même si United Airlines l'a interdit de vol sur ses avions. On ne sait pas encore si l'incident impliquant le moteur de l'avion a eu lieu ou si l'avion aurait pu être en danger à la suite de celui-ci.

Un tweet dévastateur

Dimanche dernier, M. Roberts a écrit sur Twitter que «au cours des cinq dernières années, mon seul but a été d'améliorer la sécurité des avions … compte tenu de la situation actuelle, on m'a conseillé de ne pas en dire plus. » La défense du chercheur en sécurité est assurée par Nate Cardozo, un avocat travaillant avec l'Electronic Frontier Foundation. M. Cardozo a déclaré que son client n'était pas disponible pour commenter autre chose que ce qu'il a écrit sur Twitter.

En ce qui concerne l'incident de moteur, l'agent spécial Mark S. Hurley a écrit dans la demande de mandat que M. Roberts a indiqué qu'il avait connecté son PC portable au système de divertissement en vol (In Flight Entertainment System ou IFE) de l'avion United Airlines en utilisant le Seat Electronic Box (SEB), qui se trouve sous certains sièges passagers. Après le piratage du système IFE, il a accédé aux autres systèmes de l'avion, précise l'agent spécial. M. Roberts « a déclaré qu'il avait modifié le code du Thrust Management Computer (TMC) de l'avion pour modifier la puissance des moteurs », ajoute M. Hurley. « Il a déclaré qu'il a commandé avec succès le système pour consulter et modifier les commandes de vol (CLB ou climb command). Un des moteurs de l'avion a commencé à augmenter sa puissance, « entrainant un mouvement latéral ou sur le côté de l'avion lors d'un de ces vols », précise le mandat de perquisition. L'agent Hurley écrit encore que M. Roberts a précisé qu'il avait compromis 15 à 20 fois des systèmes IFE de 2011 à 2014. Selon l'agent spécial, les systèmes IFE compromis sont fabriqués par Thales et Panasonic (les moniteurs vidéo installés à l'arrière de sièges passagers), .

Un boitier SEB forcé sous le siège passager

Les problèmes judiciaires de Chris Roberts ont vraiment commencé le 15 avril quand il a écrit un tweet suggéré qu'il sondait les systèmes d'un Boeing 737/800 d'United Airlines lors d'un vol Denver/Chicago. Il a ensuite poursuivi son voyage de Chicago vers Syracuse (dans l'état de NY). Entretemps le département Cyber Security Intelligence d'United Airlines qui avait vu ce tweet faisant référence au système EICAS, a envoyé une équipe de sécurité interpeller M. Roberts à sa sortie de l'avion pour le remettre au FBI.
Après son interpellation, un agent spécial a examiné la cabine de première classe où avait voyagé M. Roberts vers Chicago. Les boitier SEB sous les sièges 2A et 3A montraient des signes d'effraction. « Le SEB sous le siège 2A a été endommagé » indique le mandat de perquisition. « L'enveloppe extérieure de la boîte a été ouverte d'environ 1,27 cm, et une des vis de fixation était manquante ». Redevenu très prudent, M. Roberts a affirmé aux agents du FBI qu'il n'avait pas compromis le réseau de l'avion sur le vol à destination de Chicago, selon le mandat. En février et mars dernier, le FBI avait déjà interrogé Chris Roberts qui avait également affirmé avoir réussi à pirater les systèmes IFE à bord d'avions.
Cette affaire devrait en n'en pas douter, impacter le monde de la sécurité aérienne dans les prochains mois, voire années, et aboutir au renforcement des règles dans ce domaine.

Source : http://www.lemondeinformatique.fr/actualites/lire-affaire-united%C3%82%C2%A0-selon-le-fbi-un-hacker-a-modifie-en-vol-la-puissance-d-un-reacteur-61170.html
Par Serge Leblal avec IDG NS