Le code source d'Adobe retrouvé sur un serveur de hackers

Le code source volé à Adobe était disponible sur un site de hackers, non protégé. Suite à une faille sur son réseau exploitée par des hackers, l'éditeur avait reconnu, le 3 octobre, le vol de 2,9 millions d'enregistrements de cartes de crédit de ses clients et la copie illicite du code source d'**Acrobat**, de **ColdFusion**, **ColdFusion Builder** et d'autres produits maison.

Lors de cette alerte, Adobe avait remercié **Brian Krebs** ainsi que le chercheur en sécurité **Alex Holden**, de Hold Security, pour leur aide. En fait, c'est ce dernier qui a découvert le code source volé sur un serveur utilisé par un groupe de hackers russophones, sous la forme d'une série de fichiers compressés déposés sans sécurité particulière sur la machine.

Vers de nouveaux exploits zero day ?

Le même serveur avait déjà été utilisé pour stocker des données volées à trois grands fournisseurs d'informations sur les habitudes de consommation des Américains, **LexisNexis**, **Dunn & Bradstreet** et **Kroll Background America**. L'affaire avait été révélée par Brian Kreks, sur son blog.

Selon Alex Holden, interrogé par nos confrères de *CIO*, le même groupe de hackers serait toujours actif et le serveur renfermerait des données volées à d'autres organisations.

La fuite des codes source d'Adobe pourrait aboutir à la découverte de nouvelles failles *zero day* exploitées par des organisations criminelles afin de pénétrer les systèmes des clients de l'éditeur ou dérober de l'information. Pour l'instant, aucun nouvelle attaque exploitant le code dérobé n'a été signalé.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes