Sécurité : le gouvernement US infiltré via une faille dans Adobe ColdFusion

Selon le FBI, des activistes liés au collectif des Anonymous sont parvenus à accéder à des ordinateurs appartenant à plusieurs agences gouvernementales américaines et à y **dérober des informations sensibles**. La campagne des hackers exploitait une faille dans un logiciel d'Adobe, afin de lancer une série d'attaques démarrées en décembre dernier. Les assaillants ont ensuite laissé des backdoors sur les ordinateurs infectés afin de les visiter régulièrement. Ces activités ont duré jusqu'au mois dernier, explique le FBI dans un mémo qu'a pu consulter Reuters.

Le mémo, qui décrit l'épisode comme *« un problème généralisé »*, explique que l'attaque a touché **l'armée, le département de l'Energie, celui de la Santé** et peut être d'autre organisations du gouvernement américain. Le document précise également aux administrateurs système les points à surveiller pour déterminer si leur organisation est infectée.

ColdFusion : le code source dans la nature

Reuters cite aussi un e-mail du responsable RH du ministère de l'Energie expliquant que le vol d'informations concerne notamment **les données personnelles de 104 000 employés**, sous-traitants, membres de leurs familles ou personnes associées au département. Ainsi que plusieurs milliers de comptes bancaires.

Les enquêteurs pensent que l'affaire est reliée au cas de **Lari Love**, un citoyen britannique accusé le 28 octobre de piratage d'ordinateurs appartenant notamment au département de l'Energie, à l'armée US et au département de la Santé. Selon eux, les assaillants ont exploité une faille de l'éditeur HTML d'Adobe, ColdFusion.

A Reuters, l'éditeur s'est contenté d'indiquer que la majorité des attaques exploitant des failles de ses produits concernaient en réalité souvent **des versions anciennes de ses logiciels**, qui n'avaient pas été mis à jour avec les patchs de sécurité qu'il propose.

Remarquons que ColdFusion fait partie des logiciels dont **le code source a été dérobé** par des hackers sur les propres serveurs d'Adobe. L'éditeur avait reconnu le 3 octobre avoir découvert des accès illégaux aux codes sources de certaines de ses applications, dont l'éditeur de site Web. Adobe n'avait toutefois pas précisé à quand remontaient ces intrusions et combien de temps elles avaient duré.

Crédit photo : © drc / Fotolia.com

Voir aussi

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