Outlook victime d'une attaque de l'homme du milieu en Chine

Le week-end dernier, les utilisateurs de Microsoft Outlook (et probablement d'autres clients e-mail SMTP et IMAP tels Mozilla Thunderbird ou Apple Mail) sur le territoire chinois ont été victimes d'un piratage de leurs comptes **par… les services gouvernementaux chinois**. *« Le 17 janvier, nous avons reçu des rapports signalant que […] Outlook a été l'objet d'une attaque de type Man-in-the-Middle »*, rapporte le site GreatFire.org, un service dédié à la collecte de données sur le filtrage de l'Internet chinois (qui reste sous la coupe du Great Firewall de Pékin). *« L'attaque a duré une journée et a maintenant cessé »*, ajoute l'organisation qui indique par ailleurs que les services de webmail Outlook.com et Login.live.com n'ont pas été affectés.

Rappelons que les attaques de l'homme du milieu (Man-in-the-middle) consistent à s'interposer dans une communication entre deux équipements afin d'intercepter les échanges, voire de les détourner et les modifier. *« Cette forme d'attaque est particulièrement sournoise car les messages que les utilisateurs reçoivent de leur client e-mail sont nettement moins percutants que les alertes qu'ils peuvent recevoir de leur navigateur »*, indique GreatFire.org. En l'occurrence, les victimes de l'attaque de ce week-end se voyaient signifier, par un simple pop-up, que le système ne pouvait vérifier l'identité du serveur et les invitait alors à 'Annuler' ou 'Continuer l'opération'. Les utilisateurs leurrés (notamment par l'idée qu'il pouvait s'agir d'un simple problème de connexion réseau) et qui ont cliqué sur 'Continuer' ont probablement fourni l'accès de leurs messages, identifiants/mots de passe, et contacts aux attaquants.

Les attaques vont s'intensifier

Cette opération succède au blocage de Gmail constaté en décembre dernier en Chine et toujours en place à ce jour. Blocage qui interdit aux applications tierces type Outlook et Mail se connectant à la messagerie de Google d'accéder aux messages. En octobre 2014, les services d'iCloud étaient aussi victimes des indiscrétions des autorités chinoises qui avaient mis en place des adresses web de redirection.

L'organisation à but non lucratif GreatFire.org s'appuie sur les méthodes d'attaques similaires constatées pour accuser, une nouvelle fois, les services chinois de l'administration du cyberespace (Cyberespace Administration). *« Si nos accusations sont correctes, cette nouvelle attaque montre que les autorités chinoises ont l'intention d'accentuer leurs méthodes de piratage des communications qu'elles ne surveillent pas encore »*, souligne GreatFire.org. La Chine montre ainsi qu'elle ne cède pas un octet sur le contrôle des communications électroniques du pays.

Lire également
Le gouvernement allemand ciblé par des attaques DDoS
Pour FireEye, la Chine finance une razzia sur les données de santé US
Google enquête sur les attaques manuelles ciblées des comptes

crédit photo © Gil C – shutterstock