Yahoo Mail et Hotmail également piratés par la Chine

Selon l'éditeur de sécurité Trend Micro, Yahoo Mail et Hotmail ont été victimes du même type d'attaques que celles visant les comptes Gmail. Google révélait la semaine dernière que les comptes Gmail de militants chinois, de journalistes, de dirigeants de pays asiatiques et de membres de l'administration américaine étaient victimes d'attaques sous forme de phishing.

Le moteur de recherche précisait que les intrusions dans son webmail provenaient de la ville de Jinan (centre de la Chine), mais en prenant un soin tout diplomatique de ne pas accuser directement les autorités chinoises.

Trend Micro se garde de son côté de révéler d'où proviennent les intrusions sur les webmails de Yahoo et de Microsoft. *« Bien que les attaques semblent avoir été conduites de façon séparées, elles présentent des similarités significatives »*, cite *ITespresso.fr*.

Après avoir récupéré les mots de passe de leurs victimes grâce à des messages de phishing très ciblés (semblant provenir d'une adresse légitime), les pirates réglaient les paramètres de transfert automatique des différents webmails pour que tout le courrier de transit leur soit renvoyé. Du coup, l'attaquant pouvait espionner toute l'activité épistolaire de sa victime.

Mais TrendMicro révèle que les pirates utilisaient également des failles du protocole res://, permettant de connaître les programmes et antivirus installés sur la machine. Ils organisaient ensuite des attaques taillées sur mesure pour les vulnérabilités de l'ordinateur ciblé (PDF, documents Excel…). Le taux de succès en était logiquement très élevé, et c'est alors l'ordinateur entier et tous ses documents, sans compter le réseau auquel il est connecté, qui était compromis.

Des attaques contre des vulnérabilités des webmails eux-même ont aussi été tentées. Par exemple un pirate a essayé de récupérer les cookies de Yahoo pour se connecter au compte de sa victime. Mais la tentative aurait échoué. Une autre passant par Facebook et utilisant une faille du protocole MHTML aurait connu plus de succès.

Le Parti Communiste Chinois a de son côté nié toute implication dans ces attaques. L'édition française du *Quotidien du Peuple*, un organe de presse officiel du PCC, a tout de même publié un article très dur envers le moteur de recherche, accusant Google de les diffamer : *« [Google] ne devrait pas venir se plaindre aux autres Etats avec des mots vides de sens et des rêveries mais plutôt en possession de faits avérés. »*

Les sentiments du gouvernement Chinois envers le géant américain du Net ne sont pas très tendres depuis leur conflit il a un peu plus d'un an, qui a abouti à la fin de la censure volontaire par Google de son moteur chinois.