

Gmail détecte désormais les attaques informatiques émanant de gouvernements

La messagerie électronique Gmail mettra désormais systématiquement en garde ses utilisateurs en cas de soupçons d'attaques informatiques commanditées par des « gouvernements renégats » ou perpétrées à l'initiative d'un individu agissant pour le compte d'un État.

La révélation au grand jour du malware **Flame** au potentiel dévastateur a rappelé Google à son devoir de protection des internautes, face à la recrudescence d'actes de piratage susceptibles d'engendrer la compromission de données, voire l'usurpation d'identité. À l'appui d'une analyse interne des intrusions de tiers et d'une consultation concomitante des rapports d'utilisateurs affectés au préalable, le groupe Internet de Mountain View différenciera les actions individuelles des opérations à grande échelle et établira en conséquence une échelle des risques.

Les victimes potentielles d'une action d'État se verront adresser un avertissement concis, sous la forme d'un bandeau au liseré rouge affiché en haut de l'interface web de Gmail. Les applications mobiles nécessiteront une mise à jour pour exploiter à ces fins la barre de notifications des systèmes d'exploitation mobiles. L'utilisateur sera invité à initier la procédure de rigueur, soit la modification de son mot de passe et l'adoption d'une méthode d'identification plus stricte, en deux étapes, pour une intégrité renforcée face aux robots.

Mieux vaut prévenir que guérir

Vice-président sécurité pour le compte de Google, **Eric Grosse** vante les mérites de ce système, mais rappelle que les rapports qui en découlent ne constituent en aucun une preuve irréfutable. « *Cela signifie simplement que nous pensons que vous êtes une cible, de phishing ou de malware par exemple, et que vous devriez ainsi prendre des mesures immédiates pour sécuriser votre compte* », résume l'intéressé. Et d'interrompre là son propos « *pour ne pas donner d'indice aux cybercriminels quant au mode opératoire de Google* ».

Proche cousin des vers industriels **Stuxnet** et **Duqu** de par ses origines, le malware Flame, considéré comme la plus sophistiquée des souches virales qui ait jamais été, a agi tel un détonateur. Avec à son tableau de chasse l'industrie pétrolière iranienne, il s'est fait le catalyseur d'une angoisse généralisée quant à l'immunité des données personnelles de tout un chacun. Google a pris le taureau par les cornes, mais certains internautes ont déploré un manque de flexibilité dans la démarche. Plutôt que de développer des outils capables de bloquer ou d'ignorer des tentatives d'identification par force brute, les soins sont curatifs plus que proactifs.