

Comment prévenir les menaces ransomnelles de type MitB ?

Internet

Posté par : JulieM

Publié le : 21/2/2012 15:00:00

Le détournement d'un navigateur Web par des malwares n'a rien de nouveau. Depuis une dizaine d'années, les cybercriminels ont causé de nombreux dégâts à l'aide de ZeuS, un cheval de Troie qui s'attaque à tout, depuis les comptes bancaires jusqu'aux réseaux gouvernementaux.

Ce qui suscite de plus en plus d'attention, c'est l'ampleur et l'ingéniosité dites des attaques dites à l'«Man-in-the-Browser» (MitB), qui menacent les banques en ligne. Jusqu'alors responsables de quelques exploits occasionnels, elles constituent aujourd'hui un véritable marché du cyber-crime, qui pèse plusieurs millions de dollars à l'échelle mondiale.

Les attaques MitB se multiplient, devenant plus difficiles à contrer et coûteuses à gérer. Quant aux mécanismes de défense en ligne traditionnellement déployés, ils échouent, car ces attaques évoluent constamment. Aucune méthode de sécurité particulière ne s'est révélée suffisamment robuste pour se prémunir contre des malwares sophistiqués. Ainsi, une attaque MitB peut atteindre ses objectifs, quelle que soit la méthode d'authentification mise en place.



En effet, le malware est capable de contrôler l'application utilisée pour effectuer une transaction en ligne, le navigateur Web par exemple, plutôt que le mécanisme d'authentification. De plus, l'architecture des navigateurs Web standards n'est pas conçue pour s'adapter au flux continu de ce nouveau type de malware. Enfin, les firewalls et les antivirus ne suffisent pas pour se protéger contre des attaques massives sur le PC de l'utilisateur final.

Afin de contrer la fraude bancaire en ligne, il convient de prévenir la modularité des attaques via les malwares. Les banques le reconnaissent : leur service en ligne peut être un outil efficace à la disposition du client, mais celui-ci a un prix en matière de sécurité. En effet, leurs clients ne suivent pas toujours les procédures recommandées et la plupart d'entre eux n'acceptent pas un niveau de sécurité renforcé s'il est synonyme d'une expérience utilisateur moins riche. Les banques doivent donc fournir une protection efficace et multi-couches, qui peut être active sans nécessiter la participation de l'utilisateur et/ou sans procédures particulières.

La solution 4TRESS Authentication Appliance permet de créer une infrastructure cohérente multi-couches et proactive pour garantir la sécurité du point d'accès comme de l'utilisateur, ce dont les banques ont besoin pour combattre les menaces qui passent actuellement sur leurs systèmes en ligne, mais aussi celles qui pourraient apparaître.

L'identification en temps réel du terminal utilisé et les services mobiles de localisation, associés à une authentification forte suivant plusieurs méthodes et à une vérification OOB (out-of-band) permettent de prévenir les attaques de malwares, tout en garantissant le confort d'utilisation via un niveau de sécurité adaptable et transparent, calibré en fonction du profil de risque. Si l'on renforce également le point d'accès et l'application, grâce à un navigateur sécurisé par exemple, qui peut communiquer avec le microprogramme de l'équipement d'authentification et assurer la connexion avec les sites Web de la banque figurant sur sa liste blanche uniquement, les cybercriminels devront alors redoubler d'efforts pour voir leurs attaques aboutir.