Comment prÃ©venir les menaces rÃ©elles de type MitB ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 21/2/2012 15:00:00

Le dÃ©tournement dâ□□un navigateur Web par des malwares nâ□□a rien de nouveau. Depuis une dizaine dâ□□annÃ©es, les cybercriminels ont causÃ© de nombreux dÃ©gÃ¢ts Ã lâ□□aide de ZeuS, un cheval de Troie qui sâ□□attaque Ã tout, depuis les comptes bancaires jusquâ□□aux rÃ©seaux gouvernementaux.

Ce qui suscite de plus en plus dâ□□attention, câ□□est lâ□□ampleur et lâ□□ingÃ©niositÃ© inÃ©dites des attaques dites â□□Man-in-the-Browserâ□□ (MitB), qui menacent les banques en ligne. Jusquâ□□alors responsables de quelques exploits occasionnels, elles constituent aujourdâ□□hui un vÃ©ritable marchÃ© du cyber-crime, qui pÃ¨se plusieurs millions de dollars Ã lâ□□Ã©chelle mondiale.

Les attaques MitB se multiplient, devenant plus difficiles Ã contrer et coÃ»teuses Ã gÃ©rer. Quant aux mÃ©canismes de dÃ©fense en ligne traditionnellement dÃ©ployÃ©s, ils Ã©chouent, car ces attaques Ã©voluent constamment. Aucune mÃ©thode de sÃ©curitÃ© particuliÃ¨re ne sâ□□est rÃ©vÃ©lÃ©e suffisamment robuste pour se prÃ©munir contre des malwares sophistiquÃ©s. Ainsi, une attaque MitB peut atteindre ses objectifs, quelle que soit la mÃ©thode dâ□□authentification mise en place.

En effet, le malware est capable de contrÃ´ler lâ□□application utilisÃ©e pour effectuer une transaction en ligne, le navigateur Web par exemple, plutÃ´t que le mÃ©canisme dâ□□authentification. De plus, lâ□□architecture des navigateurs Web standards nâ□□est pas conÃ§ue pour sâ□□adapter au flux continu de ce nouveau type de malware. Enfin, les firewalls et les antivirus ne suffisent pas pour se protÃ©ger contre des attaques massives sur le PC de lâ□□utilisateur final.

Afin de contrer la fraude bancaire en ligne, il convient de prÃ©venir la modularitÃ© des attaques via les malwares. Les banques le reconnaissent : leur service en ligne peut Ãªtre un outil efficace Ã la disposition du client, mais celui-ci a un prix en matiÃ¨re de sÃ©curitÃ©. En effet, leurs clients ne suivent pas toujours les procÃ©dures recommandÃ©es et la plupart dâ□□entre eux nâ□□acceptent pas un niveau de sÃ©curitÃ© renforcÃ© sâ□□il est synonyme dâ□□une expÃ©rience utilisateur moins riche. Les banques doivent donc fournir une protection efficace et multi-couches, qui peut Ãªtre activÃ©e sans nÃ©cessiter la participation de lâ□□utilisateur et/ou sans procÃ©dures particuliÃ¨res.

La solution 4TRESS Authentication Appliance permet de crÃ©er une infrastructure cohÃ©rente multi-couches et proactive pour garantir la sÃ©curitÃ© du point dâ□□accÃ¨s comme de lâ□□utilisateur, ce dont les banques ont besoin pour combattre les menaces qui pÃ¨sent actuellement sur leurs systÃ¨mes en ligne, mais aussi celles qui pourraient apparaÃ®tre.

Lâ□□identification en temps rÃ©el du terminal utilisÃ© et les services mobiles de localisation, associÃ©s Ã une authentification forte suivant plusieurs mÃ©thodes et Ã une vÃ©rification OOB (out-of-band) permettent de prÃ©venir les attaques de malwares, tout en garantissant le confort dâ□□utilisation via un niveau de sÃ©curitÃ© adaptable et transparent, calibrÃ© en fonction du profil de risque. Si lâ□□on renforce Ã©galement le point dâ□□accÃ¨s et lâ□□application, grÃ¢ce Ã un navigateur sÃ©curisÃ© par exemple, qui peut communiquer avec le microprogramme de lâ□□Ã©quipement dâ□□authentification et assurer la connexion avec les sites Web de la banque figurant sur sa â□□liste blancheâ□□ uniquement, les cybercriminels devront alors redoubler dâ□□efforts pour voir leurs attaques aboutir.