BitDefender : Ã□lection amÃ©ricaine, un malware grand gagnant
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 22/1/2010 0:00:00

Les recherches web portant sur lâ□□Ã©lection du sÃ©nateur du Massachusetts pourraient entraÃ®ner lâ□□installation de malwares Câ□□est un faux logiciel antivirus qui sort gagnant de la confrontation entre la dÃ©mocrate **Martha Coakley** et le rÃ©publicain **Scott Brown** .

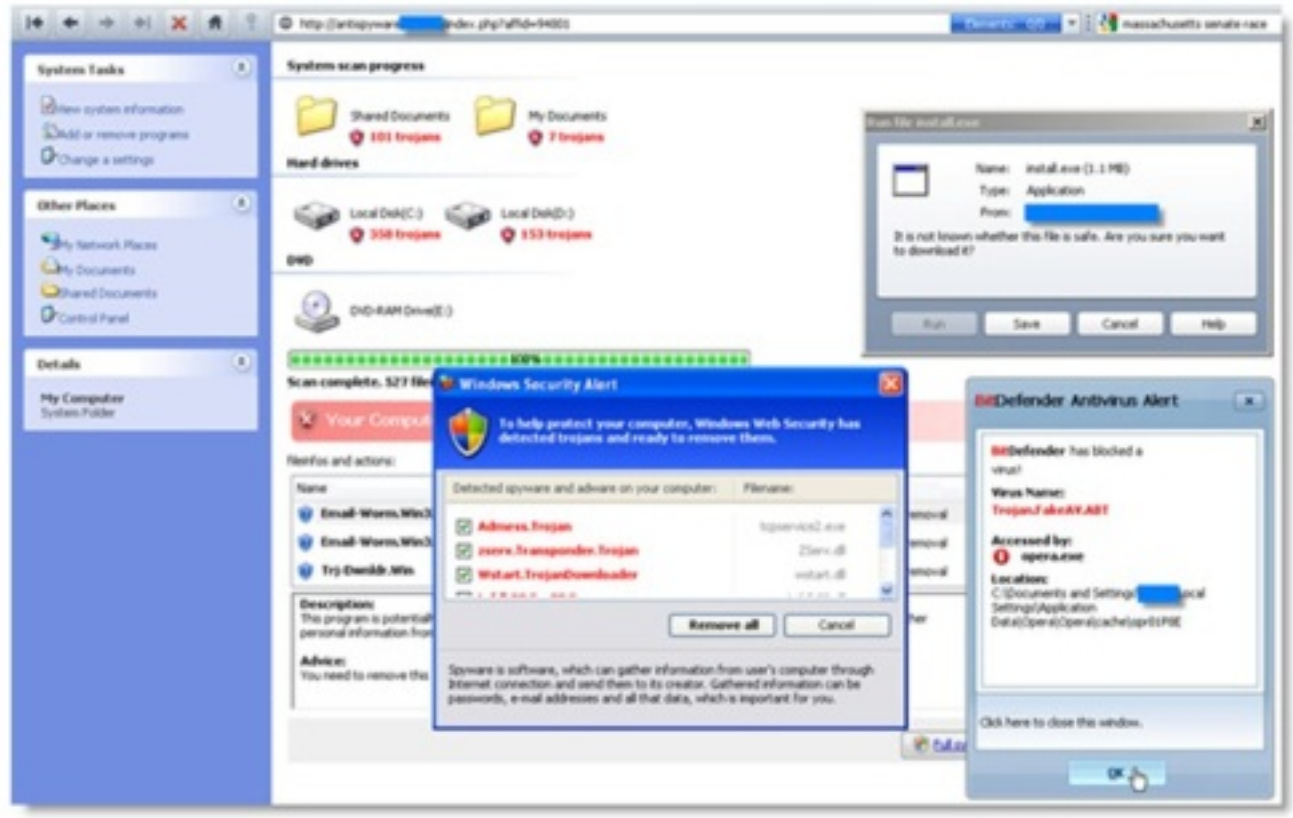
Les crÃ©ateurs de malwares continuent Ã exploiter les mÃªmes techniques dâ□□ingÃ©nierie sociale, et notamment la curiositÃ©, afin que leurs victimes exposent leurs donnÃ©es. Les internautes curieux, utilisant des systÃ¨mes non protÃ©gÃ©s pourraient Ãªtre menacÃ©s en cliquant simplement sur des liens Ã lâ□□apparence anodine, concernant les Ã©lections sÃ©natoriales amÃ©ricaines.

Le mode opÃ©ratoire est classique : un clic sur un lien dâ□□un site Internet semblant lÃ©gitime dans une page de rÃ©sultats de recherche, qui redirige automatiquement le navigateur vers une page Web et qui infecte lâ□□utilisateur avec une variante du faux antivirus System Security (dÃ©tectÃ© par BitDefender sous le nom de Trojan.FakeAV.ABT.)

Son action est similaire Ã celle de ses prÃ©dÃ©cesseurs (les faux antivirus XP Antivirus, Antivirus 2009, AV360, Personal Antivirus et Total Security) : une fois sur une page Web diffusant des malwares, la fenÃªtre du navigateur est automatiquement rÃ©duite et un message dâ□□avertissement sâ□□affiche, informant lâ□□utilisateur de la prÃ©sence de plusieurs infections sur son ordinateur et lui proposant dâ□□utiliser System Security.

Que lâ□□utilisateur clique sur le bouton Â« OK Â» ou sur Â« Annuler Â» dans lâ□□une des fenÃªtres pop-up Ã lâ□□Ã©cran, le rÃ©sultat est le mÃªme : il lance un faux processus d'analyse sâ□□affichant dans la fenÃªtre du navigateur qui a Ã©tÃ© restaurÃ©e. Ce processus est censÃ© dÃ©tecter les trÃ¨s nombreux malwares prÃ©sents sur le systÃ¨me alors que dâ□□autres fausses fenÃªtres pop-up incitent lâ□□utilisateur Ã tÃ©lÃ©charger le programme malveillant.

System Security essaie de convaincre lâ□□utilisateur dâ□□enregistrer le faux logiciel antivirus en lui signalant de nouvelles (fausses) dÃ©tections toujours plus nombreuses Ã chaque simulation dâ□□analyse. Une fois sur la machine, il modifie ou endommage irrÃ©mÃ©diablement le contenu de plusieurs fichiers systÃ¨me et dÃ©clenche lâ□□affichage de nombreuses fenÃªtres pop-up avertissant de problÃ¨mes systÃ¨me et dâ□□infections (imaginaires).



Il demande aussi constamment Ã lâ□□utilisateur dâ□□acheter/de renouveler une licence et, pour Ãªtre encore plus persuasif, il supprime le fond dâ□□Ã©cran du bureau de lâ□□utilisateur et bloque de nombreuses applications.

Afin de protÃ©ger vos systÃ¨mes et donnÃ©es et Ã©viter de les compromettre, veuillez suivre les cinq conseils ci-dessous :

â□¢ Installez et activez une solution pare-feu et antimalware fiable ainsi quâ□□un filtre antispam, comme celles proposÃ©es par BitDefender.

â□¢ Mettez Ã jour votre antimalware, votre pare-feu et votre filtre antispam aussi souvent que possible avec les derniÃ¨res dÃ©finitions de virus et signatures de fichiers et dâ□□applications

suspectes.

â□¢ Analysez votre systÃ¨me frÃ©quemment.

â□¢ VÃ©rifiez rÃ©guliÃ¨rement votre systÃ¨me dâ□□exploitation : tÃ©lÃ©chargez et installez les derniÃ¨res mises Ã jour de sÃ©curitÃ© et les outils permettant de supprimer des malwares, ainsi que les autres patches et fixes disponibles.

â□¢ Ne tÃ©lÃ©chargez pas et nâ□□enregistrez pas de fichiers provenant de sources inconnues ; Ã©vitez dâ□□ouvrir et de copier sur votre systÃ¨me des fichiers, mÃªme sâ□□ils proviennent dâ□□une source fiable, sans avoir lancÃ© auparavant une analyse antimalware complÃ¨te.

Visitez le site de BitDefender