Symantec, les anti-virus factices, distribution et communication organisÃ©e
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 21/10/2009 15:00:00

Les cybercriminels ont dÃ©veloppÃ© sur Internet des dispositifs de distribution et de communication pointus, performants et offrant des rÃ©munÃ©rations gÃ©nÃ©reuses (prÃ¨s de trois fois le salaire de Barack Obama).

Les internautes, bernÃ©s par un faux sentiment de sÃ©curitÃ© sâ□□exposent Ã des risques plus importants.

Symantec prÃ©sente aujourdâ□□hui les rÃ©sultats de son rapport sur les anti-virus factices, ou Â« facticiels Â», rÃ©alisÃ© Ã partir des donnÃ©es collectÃ©es mondialement par les 240.000 capteurs de Symantec, de juin 2008 Ã juin 2009. Ces anti-virus factices, ou facticiels, sont des programmes qui ont lâ□□apparence dâ□□une solution de sÃ©curitÃ© informatique rÃ©elle, mais qui nâ□□offre peu voire aucune protection Ã son utilisateur et peut mÃªme, dans certains cas, installer des codes malveillants ou rÃ©duire lâ□□ensemble de la sÃ©curitÃ© de lâ□□ordinateur. Lâ□□Ã©tude prÃ©sentent les ressorts utilisÃ©s par les cybercriminels en termes de communication, de distribution, de rÃ©munÃ©ration et bien sÃ»r dâ□□ingÃ©nierie sociale pour inciter les internautes Ã acheter leurs solutions de sÃ©curitÃ© factice.

Pour attirer de nouvelles victimes, les cybercriminels dÃ©veloppent des publicitÃ©s sur Internet ou des sites Web qui gÃ©nÃ¨re une certaine anxiÃ©tÃ© chez lâ□□internaute. Avec des messages tels que Â« si ce message apparaÃ®t, votre ordinateur court un risque ou est infectÃ© Â», ils encouragent lâ□□internaute Ã scanner son ordinateur ou Ã acheter le logiciel en question afin dâ□□Ã©liminer toute menace. Ainsi, 93% des installations des 50 faux antivirus les plus rÃ©pandus ont Ã©tÃ© effectuÃ©es de faÃ§on volontaire par les internautes. En juin 2009, Symantec avait dÃ©tectÃ© plus de 250 anti-virus factices.

CoÃ»t initial et coÃ»t cachÃ© pour les internautes

Le coÃ»t initial pour les internautes qui tÃ©lÃ©chargent ces facticiels varie de 30$ Ã 100$. NÃ©anmoins, les coÃ»ts liÃ©s Ã lâ□□exploitation de leurs donnÃ©es par les cybercriminels sont

nettement plus Ã©levÃ©s : les informations collectÃ©es telles que les numÃ©ros de carte bancaire peuvent Ãªtre lâ□□objet dâ□□une utilisation frauduleuse, ou bien Ãªtre revendues sur le marchÃ© noir. De plus, certains facticiels installent des codes malveillants qui placent lâ□□utilisateur face Ã un risque encore plus Ã©levÃ© devant de nouvelles menaces. Certains anti-virus factices demandent par exemple Ã lâ□□utilisateur de rÃ©duire ou de supprimer les paramÃ¨tres de sÃ©curitÃ© de son ordinateur lorsquâ□□il sâ□□enregistre, voire mÃªme lâ□□empÃªchent dâ□□accÃ©der Ã des sites lÃ©gitimes sur la sÃ©curitÃ© informatique aprÃ¨s leur installation.

Par consÃ©quent, lâ□□installation de ces programmes peut abaisser le niveau de sÃ©curitÃ© de lâ□□ordinateur alors quâ□□ils prÃ©tendent faire prÃ©cisÃ©ment lâ□□inverse.

Des publicitÃ©s mensongÃ¨res aux messages anxiogÃ¨nes pour dÃ©clencher lâ□□achat dâ□□ un anti-virus factice

Les cybercriminels utilisent diffÃ©rentes mÃ©thodes pour inciter les internautes Ã acheter un anti-virus factice ; la plupart dâ□□entre elles repose sur la gÃ©nÃ©ration immÃ©diate dâ□□une crainte dâ□□Ãªtre exposÃ© Ã un risque, ainsi que sur

dâ□□autres mÃ©canismes dâ□□ingÃ©nierie sociale.

Les annonces proposant ce type de programmes se trouvent sur des sites crÃ©dibles et lÃ©gaux comme des blogs, des forums, des rÃ©seaux sociaux ou des sites pour adultes. Alors que les sites Internet nâ□□ont aucun rapport avec ces activitÃ©s frauduleuses, leur rÃ©putation et leur image peuvent se trouver compromises par la prÃ©sence dâ□□annonces pour des logiciels de sÃ©curitÃ© factices. Les faux antivirus peuvent Ã©galement apparaÃ®tre en tÃªte des rÃ©sultats des outils de recherche si les cybercriminels ont travaillÃ© sur leur rÃ©fÃ©rencement.

Pour augmenter leur chance de Â« succÃ¨s Â», les crÃ©ateurs de facticiels conÃ§oivent leurs programmes pour que ceux-ci apparaissent comme le plus crÃ©dible possible. Ils prennent en effet lâ□□aspect graphique des vrais logiciels de sÃ©curitÃ© conÃ§us par les Ã©diteurs du marchÃ©, ou bien porte des noms trompeurs comme SpywareGuard 2008, AntiVirus 2008

ou encore Nortel 2009. Ils sont par ailleurs distribuÃ©s sur des sites qui jouissent dâ□□une bonne rÃ©putation et permettent Ã lâ□□utilisateur un tÃ©lÃ©chargement facile. Certains vont mÃªme jusquâ□□Ã utiliser des moyens de paiement usuels sur Internet et Ã envoyer Ã leurs victimes un reÃ§u par email, avec numÃ©ro de sÃ©rie et service client.

Un rÃ©seau de distribution trÃ¨s organisÃ© autour â□¦ du profit

Les cybercriminels tirent profit dâ□□un business model particuliÃ¨rement bien organisÃ© en rÃ©seau et avec, comme logique, la rÃ©munÃ©ration Ã la performance. Selon le rapport de Symantec, les 10 premiers affiliÃ©s pour le site

distributeur de faux antivirus ont dÃ©clarÃ© gagner 23.000 $ par semaine pendant les 12 mois de lâ□□enquÃªte, soit prÃ¨s de trois fois le salaire de Barack Obama11.

Ces pratiques de distribution sont similaires Ã celles des programmes dâ□□affiliation des e-commerÃ§ants les plus frÃ©quentÃ©s. Ces programmes rÃ©compensent les affiliÃ©s ou les membres pour chaque visiteur quâ□□ils dirigent vers leur site de e-commerce. A travers ce modÃ¨le, les affiliÃ©s des escrocs concepteurs de facticiels gagnent entre 0.01$ et 0.55$ pour chaque installation rÃ©ussie. Ce sont les Etats-Unis, puis le Royaume-Uni, le Canada et lâ□□Australie qui rÃ©munÃ¨rent le mieux ces affiliÃ©s. Certains sites offrent Ã©galement Ã leurs affiliÃ©s des incentives sous la forme de primes pour un certain nombre dâ□□installations, ainsi que des points VIP et des prix comme du matÃ©riel Ã©lectronique et des voitures de luxe.

Citations :

Â« *Les rÃ©sultats de notre rapport sur les facticiels montrent que les cybercriminels sont trÃ¨s bien organisÃ©s et particuliÃ¨rement dÃ©cidÃ©s Ã duper les internautes* Â», explique **Stephen Trilling**, Senior Vice President du Symantec

Security Technology Response. Â« *Pour Ã©viter quâ□□ils ne soient des victimes de ces escrocs, Symantec conseille vivement aux internautes dâ□□utiliser les derniÃ¨res solutions de protection et de sâ□□Ã©quiper auprÃ¨s de distributeurs Internet reconnus et lÃ©gaux* Â».

Â« *Les crÃ©ateurs de facticiels peuvent duper des milliers dâ□□internautes en investissant un minimum dâ□□argent et de temps, et rÃ©aliser ainsi des profits considÃ©rables* Â», commente David Wall, Professeur Ã la Criminal Justice et Information Society de lâ□□UniversitÃ© de Leeds en Angleterre. Â« *Ce type dâ□□arnaque est efficace car les utilisateurs pensent quâ□□ils courent un risque informatique immÃ©diat que seul le programme qui leur est prÃ©sentÃ© Ã lâ□□Ã©cran peut rÃ©soudre. Au final, câ□□est une escroquerie. Je recommanderais aux internautes dâ□□Ãªtre prudents sur Internet et de ne tÃ©lÃ©charger que depuis une site digne de confiance* Â».

Informations complÃ©mentaires

- Les 5 premiÃ¨res fausses applications de sÃ©curitÃ© sont les suivantes : SpywareGuard 2008, AntiVirus 2008, AntiVirus 2009, SpywareSecure et XP AntiVirus

- Parmi les sites de distribution observÃ©s par Symantec, les affiliÃ©s sont payÃ©s 0.55$ pour chaque installation de faux antivirus aux Etats-Unis, 0.52$ au Royaume-Uni et au Canada, et 0.50$ en Australie. Les rÃ©munÃ©rations chutent ensuite Ã 0.16$ en France, Espagne, Irlande et Italie. Cette rÃ©munÃ©ration varie selon la probabilitÃ© des utilisateurs dâ□□un pays Ã tÃ©lÃ©charger et payer pour un faux antivirus.

- 93% des faux antivirus font lâ□□objet dâ□□un site Internet dÃ©diÃ© et 52% sont promus par de la publicitÃ© online

- Sur les 50 faux antivirus les plus rÃ©pandus observÃ©s par Symantec, 61% ciblaient lâ□□AmÃ©rique du Nord, 31% la zone EMEA (Europe, Moyen-Orient, Afrique), 6% lâ□□Asie-Pacifique et 2% lâ□□AmÃ©rique latine et du Sud.

Le pourcentage plus Ã©levÃ© en AmÃ©rique du Nord et dans la zone EMEA reflÃ¨te le niveau dâ□□activitÃ©s malveillantes dans ces zones gÃ©ographiques et peut sâ□□expliquer par les rÃ©munÃ©rations plus attractives des affiliÃ©s dans ces rÃ©gions.