G-Data : Infection DNSChanger - Attention Ã votre navigation Internet
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 16/2/2012 14:00:00

Les experts du G Data SecurityLabs font un point sur cette situation et donne quelques conseils.

PrÃ¨s de 4 millions dâ□□internautes Ã travers le monde pourraient se voir privÃ© de **navigation Internet Ã partir du 8 mars 2012**. Suite Ã lâ□□Operation Ghost Click menÃ©e en novembre 2011 par le FBI amÃ©ricain, des serveurs DNS compromis sont maintenant sous le contrÃ´le des autoritÃ©s. Mais leur arrÃªt programmÃ© le 8 mars pourrait empÃªcher tous les internautes infectÃ©s par le cheval de Troie DNSChanger de naviguer sur Internet. ***Lâ□□opÃ©ration Ghost Click*** menÃ©e en novembre 2011 par le FBI et d'autres entitÃ©s internationales a Ã©tÃ© une rÃ©ussite. Le responsable de lâ□□infection DNSChanger a Ã©tÃ© mis sous les verrous et ses serveurs DNS compromis sont maintenant sous le contrÃ´le du FBI.

Quelles sont les actions de DNSChanger ?

Ce cheval de Troie modifie les paramÃ¨tres DNS du systÃ¨me Windows infectÃ©. En modifiant ces paramÃ¨tres de connexion, le cybercriminel est alors capable de rediriger Ã sa convenance la navigation Internet de tous les ordinateurs infectÃ©s. Affichage de publicitÃ©s spÃ©cifiques (menant par exemple vers des produits pharmaceutiques douteux), redirection vers un site dâ□□hameÃ§onnage pour la collecte dâ□□information bancaire, etc. Le contrÃ´le total de la navigation Internet de lâ□□utilisateur ciblÃ© donne accÃ¨s Ã un trÃ¨s large panel dâ□□attaques. Ce code nâ□□est pas seulement capable de modifier les paramÃ¨tres systÃ¨me. Il peut aussi accÃ©der Ã certains modÃ¨les de routeur Internet (en utilisant les mots de passe courants) et en modifier les adresses DNS.

Que se passera-t-il le 8 Mars 2012 ?

Le FBI contrÃ´le aujourdâ□□hui les serveurs DNS compromis. Ces serveurs redirigent actuellement toute la navigation des personnes infectÃ©es normalement vers les sites demandÃ©s. Cela signifie

que beaucoup dâ□□utilisateurs (environ 4 millions selon le FBI) utilisent actuellement des configurations DNS non conformes et qui ne seront plus disponibles lorsque le FBI arrÃªtera ces serveurs. Lâ□□arrÃªt est prÃ©vu le 8 mars 2012.

Â«*Supprimer seulement le code malveillant DNSChanger du systÃ¨me ne suffit pas Ã rÃ©soudre tous les problÃ¨mes*Â», explique **Ralf BenzmÃ¼ller**, Directeur du G Data SecurityLabs. Â« *Dans le cas d'une infection par ce code malveillant, les utilisateurs doivent aussi vÃ©rifier les paramÃ¨tres de connexion Internet de leur ordinateur ainsi que les paramÃ¨tres de leur routeur ADSL afin de les corriger en cas de modification frauduleuse. Cela afin de garantir une connexion Internet normale mÃªme aprÃ¨s le 8 Mars.* Â»

VÃ©rifier ses configurations

La premiÃ¨re Ã©tape consiste Ã vÃ©rifier sa configuration DNS Ã partir de cette page de test : dns-ok.fr . En cas de problÃ¨me, le G Data SecurityLabs dÃ©taille : gdata.fr/qui-sommes-nous/centre-de-presse/communiques-de-presse/news-details/article/2558-infection-dnschanger-ver.html) toutes les manipulations nÃ©cessaires afin de vÃ©rifier et rÃ©parer son systÃ¨me.

Conseils de sÃ©curitÃ© gÃ©nÃ©raux pour les utilisateurs d'Internet

â□¢ G Data recommande d'utiliser une solution de sÃ©curitÃ© complÃ¨te qui surveille en permanence le trafic HTTP. En plus de la protection Internet, un logiciel de sÃ©curitÃ© doit Ã©galement avoir un filtre antispam pour Ã©liminer les courriers indÃ©sirables.

â□¢ Le systÃ¨me d'exploitation, le navigateur, ainsi que tous les autres programmes installÃ©s doivent toujours Ãªtre tenus Ã jour. Sinon, les criminels peuvent exploiter les failles de sÃ©curitÃ© non corrigÃ©es.

â□¢ Pour les pÃ©riphÃ©riques tels que les routeurs, les mots de passe dÃ©finis par dÃ©faut doivent Ãªtre changÃ©s.

â□¢ Si un ordinateur a Ã©tÃ© infectÃ© par un logiciel malveillant, tous les mots de passe, y compris ceux des comptes de courrier Ã©lectronique, de banque ou de boutiques en ligne ou encore de rÃ©seaux sociaux doivent Ãªtre immÃ©diatement changÃ©s.

Vous trouverez les solutions G-Data chez GS2i.