

**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 paramÃªtres DNS du systÃªme Windows infectÃ©. En modifiant ces paramÃªtres 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 paramÃªtres systÃªme. Il peut aussi accÃ©der Ã certains modÃªles 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 d'utilisateurs (environ 4 millions selon le FBI) utilisent actuellement des configurations DNS non conformes et qui ne seront plus disponibles lorsque le FBI arrÃtera ces serveurs. L'arrÃt est prÃvu le 8 mars 2012.



«Supprimer seulement le code malveillant DNSChanger du systÃme ne suffit pas Ã rÃsoudre tous les problÃmes», explique **Ralf BenzmÃller**, Directeur du G Data SecurityLabs. « Dans le cas d'une infection par ce code malveillant, les utilisateurs doivent aussi vÃrifier les paramÃtres de connexion Internet de leur ordinateur ainsi que les paramÃtres de leur routeur ADSL afin de les corriger en cas de modification frauduleuse. Cela afin de garantir une connexion Internet normale mÃme aprÃs le 8 Mars. »

### VÃrifier ses configurations

La premiÃre Ãtape consiste Ã vÃrifier sa configuration DNS Ã partir de cette page de test : [dns-ok.fr](http://dns-ok.fr). En cas de problÃme, le G Data SecurityLabs dÃtaille : [gdata.fr/qui-sommes-nous/centre-de-presse/communiqués-de-presse/news-details/article/2558-infection-dnschanger-ver.html](http://gdata.fr/qui-sommes-nous/centre-de-presse/communiqués-de-presse/news-details/article/2558-infection-dnschanger-ver.html) ) toutes les manipulations nÃcessaires afin de vÃrifier et rÃparer son systÃme.

### Conseils de sÃcuritÃ gÃnÃraux pour les utilisateurs d'Internet

â€¢ G Data recommande d'utiliser une solution de sÃcuritÃ complÃte qui surveille en permanence le trafic HTTP. En plus de la protection Internet, un logiciel de sÃcuritÃ doit Ãgalement avoir un filtre antispam pour Ãliminer les courriers indÃsirables.

â€¢ Le systÃme d'exploitation, le navigateur, ainsi que tous les autres programmes installÃs doivent toujours Ãtre tenus Ã jour. Sinon, les criminels peuvent exploiter les failles de sÃcuritÃ non corrigÃes.

â€¢ Pour les pÃriphÃriques tels que les routeurs, les mots de passe dÃfinis par dÃfaut doivent Ãtre changÃs.

â€¢ Si un ordinateur a ÃtÃ infectÃ par un logiciel malveillant, tous les mots de passe, y compris ceux des comptes de courrier Ãlectronique, de banque ou de boutiques en ligne ou encore de rÃseaux sociaux doivent Ãtre immÃdiatement changÃs.

**[Vous trouverez les solutions G-Data chez GS2i.](#)**