Un virus «World Trade Center» est en circulation

Un nouveau virus prend avantage des événements du 11 septembre dernier pour faire de nouvelles victimes, par Internet cette fois. Il s'agit d'un ver informatique qui, une fois téléchargé sur un ordinateur, y sème la zizanie. C'est part un courriel déguisé en appel à la paix entre l'Amérique et l'Islam qu'on amène l'utilisateur à laisser la méfiance de côté...

Puis, un dossier intitulé «WTC.exe» provoque les dégâts dès qu'il est activé. Vous pouvez donc recevoir un courriel portant la mention «Fwd:Peace BeTweeN AmeriCa and IsLaM!», dont le corps du message sera :

Hi
iS iT A waR Against AmeriCa Or IsLaM !?
Let's Vote To Live in Peace!

En plus de se répandre par le biais d'un carnet d'adresses Outlook Express, le virus W32.Vote.A@mm peut effacer des fichiers, les corrompre et même menacer la sécurité du système. Ce message sera porteur d'un fichier joint, WTC.EXE, un exécutable qui permettra au virus de s'installer dans l'ordinateur de l'usager. Il s'attaque aux ordinateurs ayant Windows 95, Windows 98, Windows ME ou DOS.

C'est à partir de l'exécution du fichier qu'un cheval de Troie est placé dans le système, donnant ainsi l'accès d'un ordinateur à un pirate. Finalement, le ver ira effacer tous les fichiers de certains dossiers, notamment les dossiers d'installation d'antivirus, rendant ainsi sa détection difficile.

Malgré qu'il ne se soit pas encore répandu à grande échelle, les dommages qu'il peut causer sont importants. Symantec, le fabricant d'antivirus, le décrit comme un ver aux risques élevés.

Une fois que le ver se sera introduit dans l'ordinateur de l'utilisateur, deux fichiers .vbs sont installés. Un premier fichier s'exécutera dès son installation pour effacer tous les fichiers .htm ou .html qu'il trouvera. Un deuxième s'exécutera au redémarrage, pour effacer tous les fichiers des dossiers système. Un de ces fichiers corrompus aura pour fonction de reformater le disque dur, rendant l'ordinateur inopérant.

Par ailleurs, l'installation d'un cheval de Troie sur un ordinateur ouvre la porte à une série d'intrusion dans les données personnelles, notamment: le vol de mots de passe, des logiciels d'accès extérieur, la reconfiguration des pare-feu, le vol d'informations bancaires et l'envoi de courriels personnels et d'information stratégique à des correspondants.

Pour se débarrasser du virus, le site de Symantec contient toutes les informations nécessaires. Par Jean-francois Parent

Source & infos complémentaires :
Mmedium

Par

Publié sur Cafeduweb - Archives le mardi 25 septembre 2001
Consultable en ligne : http://archives.cafeduweb.com/lire/358-virus-world-trade-center-en-circulation.html