Date: Vendredi 14 octobre 2005 à 09:25:41
Sujet: 9 News informatiques

Le virus Sober ouvre la porte au spam politique en allemand

Apparu en juin 2004, le virus Sober est revenu à la mi-mai. Il déclenche l'arrivée de pourriels d'extrême-droite rédigés en allemand.

« Tu seras réduit en esclavage ! » , « Multiculturel = multicriminel » , « La Turquie dans l'Europe » . Depuis le 14 mai, une vague de messages portant des intitulés de ce type, rédigés en allemand, envahissent les boîtes aux lettres électroniques. Il s'agit de l'effet de la propagation d'un virus de type cheval de Troie, Sober.Q. Ce virus n'est pas inconnu puisqu'il avait déjà sévi en juin 2004, selon le même procédé. A savoir une attaque en deux temps.

Description :
D'abord, un spam contenant un fichier attaché circule. Si l'utilisateur ouvre le message et clique sur le fichier, un virus (appelé Sober.N) s'installe sur l'ordinateur. « Il n'y a pas de destruction sur le PC. Le virus est là, sur la machine, c'est tout , explique Mathieu Tarnus, directeur marketing de l'éditeur Goto Software. Mais il est programmé pour aller chercher une autre souche de virus. » En l'occurrence Sober.Q, qui envoie automatiquement des courriers à contenu politique en allemand. Ce qui ne rend pas cette attaque facile à détecter avant qu'elle ne soit effectivement déclenchée. Mais en tout état de cause, insiste Stéphan Roux, responsable avant-vente chez Sophos, « Si vous n'êtes pas infectés par Sober.N, vous avez une probabilité qui tend vers zéro d'être touché par Sober.Q ».
Un virus qui fait la promotion de son auteur

En elle-même, l'attaque n'est pas très dommageable, comme le montre par exemple la synthèse faite par Symantec . Pour la société de sécurité, ce virus a fait l'objet d'une alerte de niveau 2 sur une échelle de 5. « Sober.N était beaucoup plus méchant. Il arrêtait l'antivirus, par exemple », ajoute Stéphan Roux. Et même s'il y a ouverture d'un port de communication, comme c'est le cas avec les chevaux de Troie, aucune porte dérobée n'est installée par Sober.Q.

En fait, la vocation de cette attaque serait surtout, pour leurs auteurs, de se faire connaître. Sober.Q est en effet accompagné d'un fichier TXT disant « Je ne suis pas un spammeur, mais je pourrais le devenir » et contenant un lien Internet qui liste l'historique de toutes les versions de Sober...

En revanche, cette attaque confirme une tendance. Celle de la convergence des auteurs de virus et des spammeurs inaugurée par le virus Mydoom début 2004. Comme il y a toujours un enjeu commercial derrière le spam, tous les moyens de propager un message sont bons. « En juin 2004, on a vu des choses encore plus poussées avec l'utilisation du peer-to-peer », rappelle Stéphan Roux.

Correctif et Protection :

Télécharger l'utilitaire de désinfection du virus Sober.
Il détecte et élimine les virus Sober.A, Sober.B, Sober.C, Sober.D, Sober.E, Sober.F, Sober.G, Sober.I, Sober.L, Sober.N et Sober.O.

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
http://www.zmaster.fr

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=131