Europol et consorts débranchent le botnet Beebone

Dit « polymorphe » de par sa capacité à changer régulièrement de forme pour échapper aux programmes antivirus, le malware **AAEH** a du plomb dans l'aile : le botnet **Beebone**, qui constituait son principal vecteur de propagation, a été démantelé ce 8 avril.

Sous la houlette d'Europol et du J-CAT (Joint Cybercrime Action Taskforce), la plupart des Etats membres de l'Union européenne se sont associés à des partenaires du secteur privé (Intel Security, Kaspersky et Shadowserver). Avec le soutien du FBI et des autorités néerlandaises, cette coalition a saisi ou fait suspendre tous les domaines Internet avec lesquels AAEH communiquait. Des alertes vont être diffusées dans les prochains jours par les fournisseurs d'accès.

AAEH n'est pas le plus répandu des logiciels malveillants. Il serait actuellement présent sur environ 12 000 machines, loin de son pic à plus de 100 000 infections. Ce qui retient l'attention, c'est sa complexité… et donc ce caractère polymorphe : plus de 2 millions d'échantillons lui sont associés – Intel évoque même 5 millions de signatures.

D'après la description qui en est fait par le CERT-US, AAEH affecte les principaux OS Windows sur desktop (95, 98, Me, 2000, XP, Vista, 7, 8) et sur serveur (2003, 2008, 2008 R2, 2012). Codé en Visual Basic, il se propage via le réseau, mais aussi par des médias amovibles (CD, DVD, clés USB), souvent caché dans des archives (.zip, .rar).

La plupart des cas d'infection sont liés au manque de vigilance d'utilisateurs qui ont cliqué sur un lien malveillant depuis un réseau social, un outil de messagerie instantanée ou tout simplement un site Internet. Souvent dans l'intention de télécharger un générateur de clés destiné à débloquer la version complète d'un logiciel, selon ITespresso.

Un scan et ensuite une mutation pour entrer

Une fois sa cible atteinte, AAEH vérifie si certains modules sont chargés en mémoire ; auquel cas il ne s'exécute pas. C'est le cas de *dbghelp.dll* (débogage), *sbiedll.dll* (sandbox) et *snxhk.dll* (antivirus Avast). Il consulte également, dans le registre Windows, l'entrée *HLKM\System\ControlSet001\Services\Disk\Enum\0* pour s'assurer de ne pas se trouver dans une machine virtuelle.

Une fois ces vérifications effectuées, AAEH engage un « cycle de renouvellement » : il change de forme à quelques heures d'intervalle pour brouiller les pistes. Lorsque la voie est libre, il tente de se connecter à un serveur parmi plusieurs dizaines (Microsoft a repéré *checktech.eu*, *noip1.com*, *sh3.net* ou encore *selfip.me*).

Dès lors, il peut transmettre des informations, recevoir des commandes… mais surtout télécharger d'autres logiciels malveillants. En tête de liste, ZBot (espionnage des transactions bancaires), Necurs (rootkit) et Cutwail (spambot). Mais aussi de faux antivirus et des rançongiciels, qui chiffrent des fichiers et demandent une rançon pour y restaurer l'accès.

En plus de tenter de désactiver les logiciels antivirus, AAEH bloque les connexions vers les sites Internet des éditeurs spécialisés en sécurité informatique. Lorsqu'il a terminé son travail, il se supprime avec la commande *cmd.exe /c tasklist&&del*. Ses cibles se situent essentiellement aux Etats-Unis, en Amérique du Sud et en Asie.

A lire aussi :

Europol coupe le sifflet au botnet Ramnit

Des serveurs Linux enrôlés sur les botnets IptabLes et IptabLex

crédit photo: Oleksandr Lysenko – shutterstock