***BitDefender : Des attaques DDOS envoyÃ©es depuis un simple tÃ©lÃ©phone portable***
**SÃ©curitÃ©**
PostÃ© par : JerryG
PubliÃ©e le : 18/5/2010 0:00:00

**BitDefender publie une mise Ã  jour dâ□□urgence contre un kit de dÃ©veloppement** (SDK) permettant de crÃ©er un botnet contrÃ´lÃ© via Twitter

Le terme Â« botnet Â» (contraction de Robot et dâ□□Internet) Ã©voque gÃ©nÃ©ralement dâ□□Ã©normes armÃ©es dâ□□ordinateurs zombies exÃ©cutant ensemble les commandes envoyÃ©es par leur Â« maÃ®tre Â» le BotMaster. Heureusement, crÃ©er un Â« bot Â» est une tÃ¢che fastidieuse qui requiert des connaissances approfondies en programmation. Ainsi, lâ□□on ne devient pas â□□botmasterâ□□ du jour au lendemain, malgrÃ© lâ□□attrait financier que cela peut reprÃ©senter.

**BitDefender a publiÃ© une mise Ã  jour dâ□□urgence** destinÃ©e Ã  fournir une protection contre une pandÃ©mie potentielle qui pourrait Ãªtre provoquÃ©e par un kit de dÃ©veloppement logiciel (SDK) permettant de crÃ©er un botnet dirigÃ© Ã  partir du cÃ©lÃ¨bre service de mÃ©dias sociaux TwitterÂ®.

Pour crÃ©er un bot personnalisÃ©, lâ□□attaquant doit simplement lancer le SDK, indiquer un nom dâ□□utilisateur Twitter qui agira comme centre de commande et de contrÃ´le, et modifier le nom du bot et son icÃ´ne pour lâ□□adapter Ã  la mÃ©thode de distribution de son choix.


**Le bot ainsi crÃ©Ã© interroge constamment le profil Twitter** spÃ©cifiÃ© Ã  la recherche de posts ressemblant aux commandes spÃ©cialement conÃ§ues pour lui. Lâ□□attaquant dispose ensuite de commandes relativement simples Ã  utiliser pour paramÃ©trer les actions de son Bot.

Il sâ□□agit assurÃ©ment de lâ□□une des premiÃ¨res tentatives de crÃ©ation dâ□□un bot automatisÃ© Ã  utiliser avec Twitter. Cependant, lâ□□intention de lâ□□outil TwitterNET Builder est expÃ©rimentale : le crÃ©ateur nâ□□a pas particuliÃ¨rement veillÃ© Ã  protÃ©ger les bots gÃ©nÃ©rÃ©s contre le reverse engeneering ou contre leur dÃ©tection et leur arrÃªt. Cette faille ne les rend pas pour autant moins dangereux pour les Â« utilisateurs moyens Â».

Notons quâ□□une observation plus attentive de ces fichiers rÃ©vÃ¨le que le botmaster en herbe

nâ□□est pas le seul Ã  contrÃ´ler le rÃ©seau. Il existe un nom de compte Twitter secondaire, codÃ© en dur, appelÃ© @Korrupt, qui peut transmettre des commandes Ã  tout bot gÃ©nÃ©rÃ© avec cet outil. MÃªme si, Ã  ce stade de nos recherches le compte ne contient pas, jusquâ□□Ã  maintenant, de trace dâ□□activitÃ© criminelle.

**Si diriger un botnet** via un compte Twitter prÃ©sente des inconvÃ©nients spÃ©cifiques (par exemple une fois le compte Twitter incriminÃ© supprimÃ©, lâ□□ensemble du botnet est dÃ©truit), lâ□□avantage est le suivant : un botmaster peut dÃ©clencher une vague de malwares Ã  grande Ã©chelle (en tÃ©lÃ©chargeant et en exÃ©cutant silencieusement des malwares sur tous les systÃ¨mes zombies) ou une attaque de type DDOS en tapant simplement une ligne de texte sur Twitter Ã  partir dâ□□un tÃ©lÃ©phone portable.

Afin de protÃ©ger les utilisateurs, **BitDefender assure la dÃ©tection de Trojan.TweetBot.A** et a publiÃ© un outil de dÃ©sinfection gratuit tÃ©lÃ©chargeable.

Pour plus dâ□□informations concernant cette alerte nâ□□hÃ©sitez pas Ã  vous connecter sur **Malwarecity**