SÃ©curitÃ© : Botnets, la menace est lÃ
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 2/2/2016 13:00:00

Parmi les diffÃ©rents types de logiciels malveillants, les botnets sont en passe de devenir l'une des plus graves cyber-menaces. Dans le dernier rapport technique de l'ENISA (European Union Agency for Network and Information Security), les botnets sont considÃ©rÃ©s comme une menace absolue pour la cyber-sÃ©curitÃ©, aprÃ¨s les diffÃ©rentes attaques du Web et de code malveillant. Aujourd'hui, aucune entreprise, aucune administration, aucun individu ne peut prÃ©tendre Ãªtre Ã l'abri de lâ□□effet des botnets sur les systÃ¨mes connectÃ©s Ã Internet.

Â
Vous avez dit botnet ?

Le botnet (contraction de Â« robot Â» et Â« rÃ©seau Â» en anglais) est dÃ©fini comme une ensemble ou un rÃ©seau de machines hÃ´tes compromises - les bots - passÃ© sous le contrÃ´le d'un opÃ©rateur malveillant. Les botnets sont utilisÃ©s pour des activitÃ©s illicites comme le lancement dâ□□une attaque DDoS, la diffusion dâ□□un malware, une fraude bancaire au clic, un vol dâ□□informations ou de ressources informatiques, la production et la propagation de SPAM, lâ□□hÃ©bergement d'opÃ©rations de phishing, lâ□□extorsion dâ□□argentâ□¦

Le botnet se distingue dâ□□autres formes de logiciels malveillants par sa capacitÃ© Ã Ã©tablir un canal de communication â□□Command and Controlâ□□ (C & C) par lequel il peut Ãªtre surveillÃ© et mis Ã jour. Il fournit ainsi l'occasion aux crÃ©ateurs de malwares de contrÃ´ler simultanÃ©ment un grand nombre de systÃ¨mes infectÃ©s et dâ□□utiliser automatiquement plus de ressources Ã des fins malveillantes.

Un peu dâ□□histoire

Les botnets sont responsables d'un grand nombre de piratages et de malveillances dont nous pouvons lire les mÃ©faits dans les colonnes des journaux. Malheureusement lâ□□attention du public nâ□□est pas encore attirÃ©e sur ce danger.
Tout a commencÃ© Ã la fin du siÃ¨cle dernier avec ce que lâ□□on a appelÃ© les bots IRC qui Ã©taient trÃ¨s apprÃ©ciÃ©s par les utilisateurs dâ□□Internet Relay Chat (discussion relayÃ©e par Internet).

Ils les utilisaient comme programme indÃ©pendant pour se connecter Ã IRC en tant que client. PrÃ©tendant envoyer des messages privÃ©s, ils envoyaient en faitâ□¦ des liens malveillants. Depuis lors, les botnets ont considÃ©rablement Ã©voluÃ© dans les architectures HTTP et P2P qui fournissent tout autant des services spÃ©cialisÃ©s que la possibilitÃ© de gÃ©nÃ©rer des attaques ciblÃ©es.

La guerre est dÃ©clarÃ©e

La guerre contre les perturbations dues aux botnets est principalement menÃ©e par des organismes publics ou des agences de droit international, qui associent Ã leurs projets le monde universitaire et les fournisseurs de sÃ©curitÃ©. Cependant, le nombre de machines actives reste important, en dÃ©pit de la puissance et de l'efficacitÃ© combinÃ©e des experts juridiques et techniques.

Il existe quelques outils - dont certains sont en ligne - qui fournissent une plate-forme pour vÃ©rifier si votre machine fait partie d'un botnet particulier. Mais l'Ã©volution de l'infrastructure de ces rÃ©seaux de machines zombies rend difficile la dÃ©tection de leur prÃ©sence. Cerise sur ce gÃ¢teau, rÃ©cemment de nouveaux signes d'activitÃ© de botnets sur des ordinateurs domestiques et sur des routeurs de petites entreprises ont montrÃ© la nÃ©cessitÃ© d'une solution de surveillance totale pour les prÃ©venir et les dÃ©tecter.

La lutte anti-botnet

La lutte contre les botnets est un dÃ©fi permanent sur le plan de la cybersÃ©curitÃ© pour les chercheurs et les entreprises spÃ©cialisÃ©es.

En fonction de l'architecture C & C utilisÃ©e par le botnet, diffÃ©rentes approches sont proposÃ©es. La dÃ©tection rÃ©seau est utilisÃ©e pour identifier des zones avec un grand nombre de machines potentiellement compromises. Cette dÃ©tection rÃ©seau implique le suivi des donnÃ©es du trafic DNS Ã la pÃ©riphÃ©rie d'un rÃ©seau, afin de dÃ©tecter certains modÃ¨les particuliers de trafic rÃ©seau.

En partant des anomalies dÃ©tectÃ©es dans le trafic, on peut classer les botnets en botnets P2P ou botnets DGA. Dans les botnets P2P, les bots communiquent directement les uns avec les autres, sans serveur centralisÃ© pour contrÃ´ler et commander lâ□□Ã©mission. Une des solutions pour lutter contre ce type de botnet est la production dynamique de listes noires interdisant le trafic en provenance des machines zombies du botnet.

Comme au jeu du chat et de la souris, lorsque lâ□□on cherche Ã mettre en Å□uvre des moyens pour diminuer les activitÃ©s malveillantes, les acteurs malveillants affinent leur approche pour surmonter les obstacles et atteindre leurs objectifs nÃ©fastes. Ainsi, des botnets basÃ©s sur lâ□□algorithme de gÃ©nÃ©ration de domaine (DGA) ont Ã©tÃ© dÃ©veloppÃ©s pour contrer les systÃ¨mes de dÃ©tection des listes noires dynamiques dÃ©ployÃ©s par de nombreux fournisseurs de sÃ©curitÃ©. Ces botnets DGA veulent Ã©viter la dÃ©tection et la neutralisation en misant sur la technique de flux de domaine.

Chaque utilisateur de bot-machine gÃ©nÃ¨re une liste unique de noms de domaine chrono-dÃ©pendante fondÃ©e sur un algorithme prÃ©dÃ©fini.

Tous les domaines produits sont ensuite interrogÃ©s jusqu'Ã ce qu'un serveur DNS rÃ©ponde avec un enregistrement de ressource non-NXDOMAIN.
Seul l'opÃ©rateur du botnet connaÃ®t le moment prÃ©cis oÃ¹ les bots interrogeront un domaine existant, quâ□□il a prÃ©alablement enregistrÃ© au registre des domaines et qui deviendra son serveur C & C, Ã partir duquel les bots seront commandÃ©s et mis Ã jour.

Les mÃ©thodes de dÃ©tection

Les approches pour dÃ©tecter les botnets Ã algorithme de gÃ©nÃ©ration de domaine se fondent sur la reconnaissance de certains modÃ¨les de trafic ou sur la rÃ©tro-ingÃ©nierie du vÃ©ritable algorithme du malware. Ce dernier implique lâ□□obtention du code exact et sa modification pour rediriger le trafic vers les serveurs lÃ©gitimes. Une approche hautement laborieuse qui produit habituellement peu de rÃ©sultats ; au moment dâ□□un rÃ©sultat notable, l'opÃ©rateur malveillant pourrait avoir dÃ©jÃ changÃ© son propre algorithme de gÃ©nÃ©ration.

La zone d'investigation du trafic DNS a suscitÃ© plus d'intÃ©rÃªt ces derniers temps, en raison de certaines caractÃ©ristiques du trafic contrÃ´lÃ© produit.

On peut constater un grand nombre de rÃ©ponses NXDomain produites du fait que l'opÃ©rateur malveillant n'a pas officiellement enregistrÃ© tous les domaines gÃ©nÃ©rÃ©s par les bots. Les

serveurs DNS rÃ©pondent en effet en indiquant quâ□□un tel nom de domaine nâ□□est pas enregistrÃ©. En rassemblant toutes ces rÃ©ponses sur une pÃ©riode donnÃ©e, les chercheurs peuvent dÃ©duire quâ□□il est fort probable que l'hÃ´te produisant ces requÃªtes fasse en rÃ©alitÃ© partie d'un botnet.

La seconde zone principale de surveillance et dâ□□examen du trafic rÃ©seau vient du fait que les caractÃ¨res alphanumÃ©riques des noms de domaine gÃ©nÃ©rÃ©s par des bots diffÃ¨rent de maniÃ¨re significative de ceux des noms de domaine gÃ©nÃ©rÃ©s par une personne physique.

Autrement dit, quand un humain enregistre un domaine en ligne, lâ□□objectif est une mÃ©morisation facile ou lâ□□adÃ©quation avec une activitÃ©, une marque, etc. Or, les caractÃ¨res des domaines gÃ©nÃ©rÃ©s automatiquement par les botnets reflÃ¨tent un niveau de hasard Ã©levÃ©. Ces caractÃ©ristiques linguistiques combinÃ©es Ã des mÃ©thodes statistiques appropriÃ©es permettent lâ□□obtention de rÃ©sultats significatifs dans la dÃ©tection.

Quid pour l'avenir ?

Le monde universitaire, les Ã©diteurs de sÃ©curitÃ© Ã travers le monde et des organismes publics ont collaborÃ© avec succÃ¨s dans le passÃ© Ã des opÃ©rations de dÃ©montage de botnets. Mais le sujet nÃ©cessite des recherches supplÃ©mentaires car de nouvelles variantes apparaissent aprÃ¨s le dÃ©mantÃ¨lement dâ□□un botnet particulier.

En outre, la communautÃ© des acteurs de la sÃ©curitÃ© a besoin d'une nouvelle gÃ©nÃ©ration de systÃ¨mes de dÃ©tection de botnets DGA, en mesure dâ□□examiner et de traiter rapidement dâ□□importants volumes de donnÃ©es en temps rÃ©el, avec un taux de faux positifs acceptable. En raison de la course aux armements dans la sÃ©curitÃ© informatique, les nouveaux systÃ¨mes ont sans cesse besoin de rester Ã jour et d'utiliser les techniques et les mÃ©thodes les plus avancÃ©es.

LogPoint travaille dans ce sens en allouant des ressources spÃ©cifiques pour la surveillance sur le rÃ©seau, avec un modÃ¨le de traitement continu qui donne des rÃ©sultats en temps rÃ©el, rapides et efficaces, confirme. Dimitrios Larisis Graduate Researcher chez LogPoint Danemark.