SOPHOS

simple + secure

Les botnets: Le côté obscur de l'informatique dans le cloud

Par **Angelo Comazzetto,** Senior Product Manager

Les botnets représentent une sérieuse menace pour votre réseau, vos activités, vos partenaires et vos clients. Les botnets rivalisent avec les plateformes de "cloud computing" dans le cloud les plus puissantes d'aujourd'hui. Ces nuages « noirs », contrôlés par des cybercriminels, sont conçus pour infecter votre réseau en toute discrétion. S'ils ne sont pas détectés, ils utilisent votre réseau pour servir des intérêts malveillants.

Ce document indique en détail comment vous protéger contre le risque d'une infection par un botnet, à l'aide de passerelles de sécurité offrant une gestion des menaces unifiée (UTM) complète.

Tous les nuages ne sont pas bons

De quoi est constitué un nuage informatique ? Il s'agit d'un grand ensemble d'ordinateurs ou de processeurs, de mémoire, d'espace de stockage, d'applications et d'autres ressources informatiques connectées au Web. Ces ressources sont disponibles simultanément pour des millions de clients et peuvent être hébergées n'importe où dans le monde. Le nuage offre de nombreux avantages aux entreprises, notamment la réduction des dépenses en capital et de fonctionnement liées à la possession de matériel et de logiciels et à la maintenance.

D'un autre côté, les cybercriminels contrôlent certaines des plateformes d'informatique dans le cloud les plus redoutables qui existent. Ces réseaux informatiques en nuage «obscurs», appelés botnets, peuvent exécuter des millions d'ordinateurs infectés, appelés bots, lesquels répandent des logiciels malveillants. S'ils ne sont pas détectés, les botnets peuvent s'approprier suffisamment de puissance de calcul pour pénaliser votre réseau et vos activités.

Il est indispensable de procéder à une surveillance continue, à l'affût de cette menace insidieuse. En raison de son architecture unique, un botnet peut continuer à s'exécuter de manière endémique, et ce même si la plupart de ses bots sont détruits. Sans une détection préventive sur votre réseau, vous êtes constamment exposé à ce risque d'infection.

Des cibles tentantes

La puissance des ordinateurs et la rapidité de l'Internet d'aujourd'hui ont rendu possibles les activités de «cybercriminalité». Les cybercriminels et les botnets qu'ils contrôlent explorent les vulnérabilités de sécurité de votre ordinateur afin de capturer ces ressources abondantes à leur propre profit. Les botnets fonctionnent furtivement pour infecter votre ordinateur via un virus, mais sans dommage immédiat ou détectable. Cette attaque silencieuse transforme votre ordinateur en «bot» ou en «esclave zombie», qui reçoit ses commandes d'un «maître» central inconnu.

Une fois votre ordinateur corrompu, le virus informatique cherche à infecter discrètement et à se copier sur d'autre machines, afin d'augmenter augmenter la portée et la puissance du botnet.

La supériorité numérique

Les centres de données d'informatique dans le cloud modernes permettent de maximiser les performances tout en réduisant au minimum les pannes. À l'inverse, un botnet fonctionne à grande échelle et avec une force brute. Un botnet contrôle des millions de processeurs informatiques, d'innombrables gigaoctets de stockage et de mémoire, et suffisamment de bande passante combinée pour submerger les connexions Internet commerciales les plus larges, même de plusieurs gigabits. Les botnets ont un sérieux avantage face aux nuages commerciaux légitimes : ils peuvent croître à une vitesse incroyable, et ne connaissent aucune panne.

Propagation des botnets

Les botnets n'ont pas de cibles bien spécifiques à infecter. En fait, il se propagent en exploitant systématiquement une liste d'adresses IP ou en analysant de manière dynamique les machines et l'espace réseau qui les entoure, à la recherche de vulnérabilités spécifiques.

Par exemple, un programme bot peut détecter un ordinateur d'entreprise qu'il peut infecter via une vulnérabilité Windows pour laquelle aucun correctif n'a été appliqué. Il poursuit ensuite son objectif, en passant l'ensemble du réseau au crible afin de découvrir des vulnérabilités sur d'autres machines. Parallèlement, les machines qui viennent d'être infectées deviennent des bots fonctionnels. Le bot peut infecter d'autres ordinateurs du réseau, lesquels peuvent toucher d'autres entreprises ou d'autres clients. Et le cycle se poursuit.

Dans cet exemple, aucune des entreprises touchées n'était spécifiquement visée par un individu. Le botnet se propage partout où il détecte une vulnérabilité. Procéder à des analyses étendues afin d'identifier les individus impliqués dans la « faille » s'avérerait une perte inutile de temps et d'argent.

À qui profitent les botnets ?

Les botnets se propagent dans le but d'offrir à leurs propriétaires une incroyable puissance informatique via des nuages « noirs », qu'ils pourront exploiter à des fins cybercriminelles hautement lucratives.

Les propriétaires de botnets peuvent également les louer à des entreprises criminelles. Par exemple, une opération de spam pourrait utiliser un botnet pour envoyer des millions de messages de spam. Des entreprises peu scrupuleuses pourraient utiliser un botnet pour anéantir le site Web d'un concurrent via une attaque de déni de service paralysante. Les botnets peuvent également craquer des informations chiffrées, en testant des milliards de clés pour « déchiffrer brutalement » le chiffrement d'un travail dérobé qui serait protégé ou d'une base de données chiffrée.

Non seulement les activités de ce type sont hautement lucratives, mais elles favorisent et encouragent le développement de botnets encore plus efficaces. Par ailleurs, les concepteurs de botnets rendent les programmes de plus en plus sophistiqués en analysant les réponses du secteur de la sécurité face à leurs précédentes attaques.

Une nouvelle menace Web est détectée toutes les 4,5 secondes.

Sophos Labs, publié dans le rapport des menaces de sécurité du premier semestre 2011

Conséquences

L'infection des botnets peut avoir des conséquences immédiates et à long terme. La panne réseau est la pire des conséquences potentielles. Cela a un impact considérable sur les opérations informatiques, les ventes, la gestion des comptes client, la productivité des employés, et bien plus encore. Aujourd'hui, les pannes réseau ont un impact négatif sur tous les services et tous les canaux qui sont source de revenus. Le coût associé aux pertes commerciales peut monter en flèche. Mais le fardeau le plus lourd repose probablement sur les épaules des services informatiques. Responsables du bon fonctionnement de leur réseau d'entreprise et de leurs utilisateurs 24h/24, 7j/7, les administrateurs informatiques doivent trop souvent mettre de côté toutes les priorités stratégiques afin de rétablir les performances réseau et lutter contre des infections de botnet bien souvent récurrentes.

Mais certaines des conséquences à long terme plus insidieuses peuvent ternir la réputation d'une entreprise, et avoir un impact sur sa compétitivité ou même sa viabilité. Toute société dont les ordinateurs sont infectés dans le sillage destructeur d'un botnet court le risque d'endosser des responsabilités légales. Il peut s'ensuivre des coûts légaux, des procédures judiciaires, de mauvaises relations publiques, et bien plus encore, et ce même si la société touchée assure ne pas avoir été « au courant ». En outre, les clients, les partenaires et d'autres parties prenantes clés risquent d'être eux aussi d'être infectés à cause de leur partenaire commercial, en qui ils avaient confiance.

S'il s'avère qu'une société est à l'origine de failles de sécurité, sa responsabilité peut se trouver engager si ses ordinateurs ont été utilisés par un botnet pour pénétrer des sites Web, entraver des communications via des attaques de déni de service, partager des fichiers piratés ou attaquer des machines à l'aide de scripts de pirates informatiques.

La meilleure défense

Comme indiqué précédemment, les botnets représentent une sérieuse menace pour les entreprises ; ils attaquent les ordinateurs ou nœuds vulnérables de manière aléatoire et il est impossible de les relier à un opérateur.

Mais vous pouvez vous protéger contre ces attaques en utilisant les solutions adéquates et en appliquant quelques bonnes pratiques simples.

La cybercriminalité coûte 338 milliards de dollars à l'économie mondiale ; elle est encore plus lucrative que le trafic de drogue.

ZDNet

Pour protéger votre entreprise contre la menace des botnets, nous vous recommandons de procéder comme suit :

- Assurez-vous que vos systèmes d'exploitation et leurs programmes sont à jour et disposent des derniers correctifs.
- Utilisez une solution de défense de passerelle efficace afin d'éviter que les bots n'infectent vos ordinateurs.
- Testez les périmètres de vos stations de travail et de vos serveurs.
- En cas d'infection, évitez de dépenser de l'argent à rechercher des coupables que vous ne trouverez probablement jamais : coupables ; préférez investir dans une meilleure sécurisation de vos ressources afin de vous protéger contre la prochaine série d'attaques.

Vous pouvez éviter les intrusions des bots à l'aide de la protection adéquate, aisément et à moindre frais. Les passerelles Astaro Security Gateway sont dotées de systèmes de détection des intrusions capables de détecter et de bloquer les programmes de bot. Il vous suffit de dresser une liste des ordinateurs et des ressources que vous utilisez. Cette solution vous protège contre les attaques en temps réel. En outre, elle identifie les infections existantes afin qu'elles puissent être nettoyées et éradiquées. Nous pouvons créer un bouclier pour votre réseau, le protégeant ainsi des diverses menaces et attaques, afin que vous puissiez mener vos activités en toute confiance.

Pour en savoir plus

www.sophos.fr/network

Sophos Sarl, France:
Tél: +33 1 34 34 80 00
Courriel: sales@sophos.fr

Boston, Etats-Unis | Oxford, Royaume-Uni

Sophos Whitepaper 12.11v1.dFR

SOPHOS