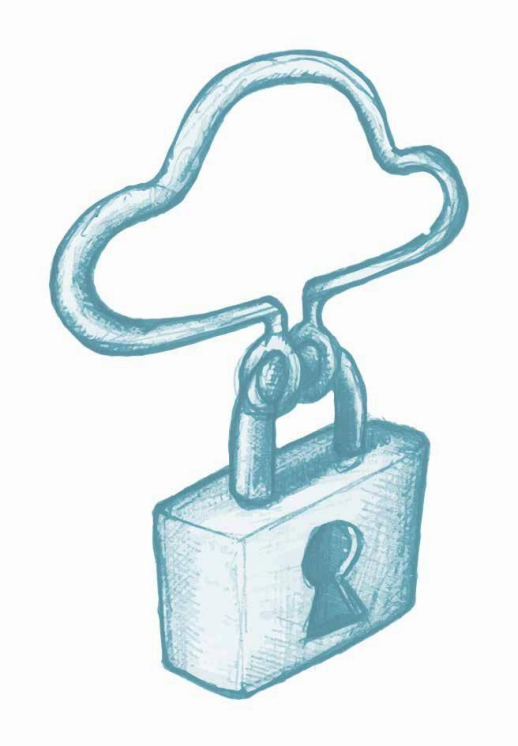
Bitdefender®

Analyse des menaces de sécurité affectant les entreprises Q4 2014



Aperçu général

L'anonymisation des botnets soulève de nouveaux problèmes de sécurité.

Bien que les botnets, de grands réseaux d'ordinateurs compromis gérés par des pirates à partir d'un serveur de commande et de contrôle (C&C) constituent un problème depuis de nombreuses années, ils continuent à évoluer. Alors que les entreprises de sécurité et les forces de l'ordre ont amélioré les techniques utilisées pour perturber ces systèmes de commande et de contrôle, les criminels continuent à améliorer leurs techniques pour les contourner. Les botnets et leur puissance sont une « ressource » que les criminels vendent pour envoyer du spam, réaliser des attaques par déni de service (DoS) et par déni de service distribué (DDoS) et jouent également un rôle dans l'augmentation des incidents liés à des ransomwares. **Ce document présente les menaces de sécurité affectant les entreprises** et s'intéresse à quelques techniques d'anonymisation des serveurs C&C utilisées actuellement.

Les botnets sont rentables

L'accélération du rythme auquel sont mis en circulation les malwares soulève des inquiétudes parmi les utilisateurs finaux et les entreprises. Les malwares, qui vont du plus simple au plus élaboré, constituent d'ailleurs un défi même pour des chercheurs en sécurité chevronnés. Ainsi la détection, la jugulation des épidémies et la suppression de ces attaques très sophistiquées peut s'avérer particulièrement ardue.

Alors que le nombre d'attaques par déni de service (DoS) et par déni de service distribué (DDoS) continue à augmenter, il existe d'autres utilisations malveillantes des botnets. Utilisés en tant que **plateformes commerciales de distribution de malwares**, les botnets peuvent être loués pour une courte période et permettent le déploiement immédiat de malwares (ransomwares en particulier) qui peuvent entraîner l'infection de plus nombreux systèmes.

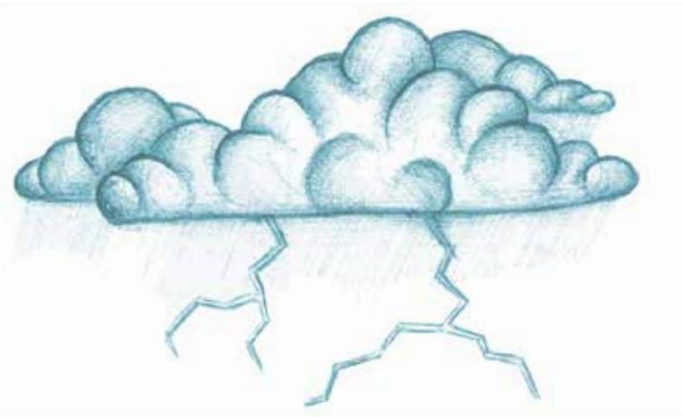
Le nombre d'attaques DoS et DDoS a augmenté, pour non pas pour des raisons idéologiques mais pour des raisons **financières**. De même, accéder aux données critiques d'une entreprise et **les vendre au plus offrant** (ou, dans le cas des ransomwares, les rendre à leur propriétaire contre une rançon) est en effet plus lucratif que d'autres activités cybercriminelles.

L'impact des botnets présents dans les entreprises va de ceux s'infiltrant dans les ordinateurs au hasard (en raison de l'absence de stratégie d'entreprise) aux attaques ciblant les entreprises et commanditées par des états. Les **botnets ciblant des entreprises** utilisent généralement des outils d'accès à distance (RAT) élaborés, avec différentes fonctions dont le camouflage, et sont capables d'utiliser les failles des réseaux traditionnels. Ils incluent généralement le support natif des serveurs proxy et peuvent utiliser les identifiants des utilisateurs pour sortir du réseau et accéder à un serveur de commande et de contrôle (Serveur C&C).

D'autres types de botnets dépendent de **composants malveillants « commerciaux »** (c'est-à-dire conçus à partir de **kits permettant de créer des malwares**). Cela signifie que le botmaster connaît bien l'entreprise et sait déjà où trouver des informations intéressantes.

Les **outils commandités par des états** et ciblant des secteurs et des technologies spécifiques varient à la fois en complexité et en fonctionnalités et ne présentent pas de caractéristiques perceptibles en matière de vecteurs d'infection et de charge utile.

Les botnets – le « dark cloud »



La multiplication des appareils connectés à Internet permet à un botmaster de s'emparer et de diriger des milliers, voire des centaines de milliers de machines « zombies ». Nos statistiques indiquent que la grande majorité des appareils faisant actuellement partie de botnets se trouve en Asie.

Comme pour tout réseau informatique, un certain niveau de contrôle doit être assuré. Les méthodes et infrastructures employées pour diriger un botnet ont beaucoup évolué. L'utilisation de **l'anonymisation de Tor** pour diriger un réseau entier de « zombies » avec des **serveurs proxy multiniveaux** est une nouvelle tendance qui suscite de nombreuses interrogations quant à la manière de démanteler ces grandes infrastructures.

Les botnets classiques fonctionnent en recontactant un serveur C&C statique, ce qui permet à une société de sécurité de lancer relativement facilement une procédure de démantèlement et de mettre en place un système de « trou noir ». Aujourd'hui, nous constatons qu'un grand nombre de botnets ont recours à des méthodes bien plus élaborées de serveurs C&C. Nous nous intéresserons par la suite à **deux célèbres botnets** et aux techniques qu'ils emploient.

CryptoLocker

Lorsque CryptoLocker accède à un ordinateur, il contacte son centre de commande et de contrôle qui, à son tour, génère une paire de clés RSA de 2048 bits. La clé publique est renvoyée à l'ordinateur et sera utilisée pour crypter les fichiers avec des extensions spécifiques. Pour vous donner une idée de la puissance de la clé, imaginez que si l'on avait commencé à cracker la clé sur un ordinateur standard juste après le Big Bang, le déchiffrement n'en serait qu'à 0,02%.

Notre recherche sur Cryptolocker a révélé que **le processus d'anonymisation est géré dans son ensemble par des serveurs proxy à plusieurs niveaux qui masquent la communication entre les bots et le botmaster**.

Le serveur proxy de niveau 1 transmet le trafic de la victime vers un serveur secondaire afin de le rendre anonyme et de masquer l'emplacement du serveur de clés. Ce proxy gère également la résolution des noms de domaine, permettant ainsi à ceux qui l'utilisent de modifier rapidement les noms de domaine afin d'éviter leur suspension.

Le serveur proxy de niveau 2 récupère les informations transmises par celui de niveau 1, les filtre et les transmet via des tunnels d'encapsulation GRE (Encapsulation Générique de Routage) à d'autres serveurs (probablement des serveurs proxy de niveau 3). Le serveur possède 10 adresses IP différentes. Lorsque des paquets de données atteignent la première interface, ils sont automatiquement transmis via un tunnel GRE spécifique et le trafic est traité par ordre de priorité. Lorsque des requêtes proviennent d'adresses IP appartenant aux forces de l'ordre, à des équipes d'intervention d'urgence en sécurité informatique (CERT) ou à des sociétés de sécurité, le serveur met en place un mécanisme afin de les ajouter à un « black hole », routant tous les paquets provenant de ces IP vers /dev/null.

Le serveur de niveau 2 comprend deux fonctionnalités principales : **il protège le trafic** en analysant sa provenance et en **bloquant les organismes d'application de la loi ou les sociétés de sécurité et envoie les données reçues des serveurs de premier niveau via des connexions fortement cryptées et redondantes**.

À noter : Les serveurs proxy de niveau 1 et 2 peuvent être personnalisés rapidement en déployant des outils spécialisés (appartenant aux personnes ayant développé le ransomware) mis à disposition par le propriétaire de l'infrastructure. Lorsque l'un des outils s'exécute, un serveur standard devient un proxy de niveau 1 ou 2 en quelques minutes, en fonction de la durée de la propagation du DNS.

Bien que Cryptolocker puisse disparaître grâce aux efforts conjoints de sociétés de sécurité et d'organismes chargés de l'application de la loi, le problème du réseau de distribution de contenu demeure. L'épine dorsale d'un botnet est l'infrastructure de communication et, dans ce cas, elle est conçue pour s'adapter à l'augmentation du nombre d'opérations et fournir un accès redondant à d'autres nœuds en cas de défaillance, mais également pour rendre le flux de données anonyme et empêcher les victimes, les organismes chargés de l'application de la loi et les entreprises de sécurité de retrouver le véritable centre d'opérations.

Les **botnets anonymes de nouvelle génération** sont conçus pour être **complètement extensibles, invisibles et extrêmement souples** lors de leur reprise d'activité suite à d'importants démantèlements, grâce à l'anonymisation des communications via Tor.

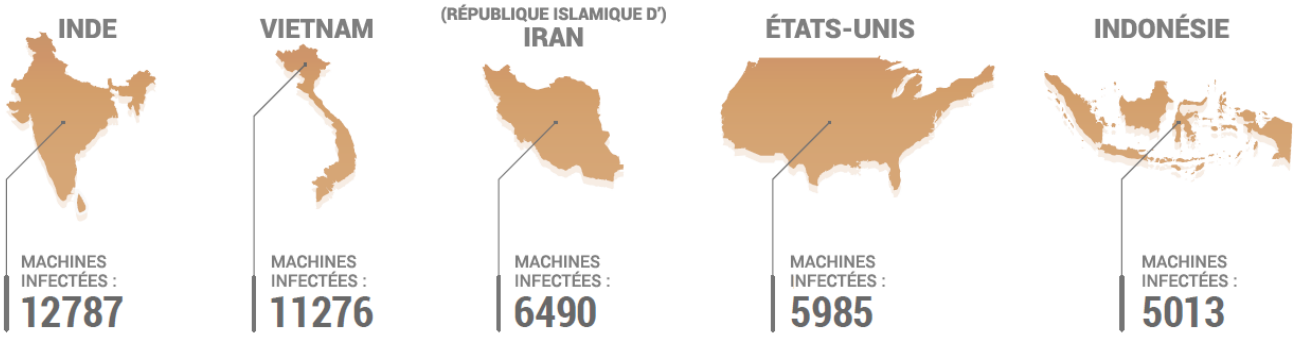
PushDo

Pushdo, cheval de Troie transmettant des messages de spam et des malwares, utilise également des **clés privées et publiques pour protéger la communication entre les bots et le serveur C&C**. Il sert principalement à envoyer du spam à partir de machines infectées mais peut également télécharger d'autres fichiers malveillants.

De **nouveaux fichiers binaires Pushdo** contiennent un **réseau overlay chiffré**, qui est un réseau alternatif de vérification. Si les conditions spécifiées dans le réseau overlay ne sont pas remplies, l'échantillon ne s'exécute pas correctement, cela afin d'éviter d'être détecté par les sandbox et rendre plus difficile le travail des analystes. De plus, une liste contenant environ 100 noms de domaine sains, masquant le nom de domaine codé en dur du C&C se trouve dans l'overlay et non dans le fichier binaire.

Il utilise également un **nouvel algorithme de génération de noms de domaine (DGA, Domain Generation Algorithm)** afin de générer des noms de domaine autres que ceux des échantillons analysés auparavant.

Après avoir étudié l'un d'entre eux, nous avons trouvé le nombre de machines infectées appelant leur serveur de contrôle et de commande et les avons classées par pays. Voici les quarante pays en comptant le plus :



Classement	Pays	Nombre de machines infectées	Classement	Pays	Nombre de machines infectées
1	Inde	12787	21	Pakistan	1119
2	Vietnam	11276	22	Afrique du Sud	1096
3	République islamique d'Iran	6490	23	Kazakhstan	1065
4	États-Unis	5985	24	Venezuela	1024
5	Indonésie	5013	25	Algérie	1022
6	Thaïlande	4678	26	Espagne	939
7	Turquie	4507	27	Chine	914
8	Pérou	4168	28	Royaume-Uni	910
9	Argentine	4132	29	Allemagne	870
10	Mexique	3433	30	Roumanie	865
11	Égypte	2442	31	Japon	858
12	Italie	2271	32	Maroc	755
13	Philippines	2257	33	Arabie saoudite	750
14	Brésil	1858	34	Chili	737
15	Taïwan	1833	35	Ukraine	724
16	Russie	1602	36	République de Corée	683
17	Malaisie	1586	37	Guatemala	666
18	Pologne	1336	38	Équateur	641
19	France	1214	39	Israël	597
20	Colombie	1213	40	Hong Kong	561

Nous recommandons vivement aux **utilisateurs finaux** de **prêter davantage attention aux ressources qu'ils consultent en ligne**, ainsi **qu'à ce qu'ils installent sur leurs ordinateurs**. **Les mises à jour logicielles de produits tiers** tels que Java, Adobe Reader et Flash devraient être **déployées dès qu'elles sont publiées**, de même que les mises à jour des systèmes d'exploitation. **L'utilisation de solutions antimalwares performantes sont, comme toujours, vivement recommandées**.

Les entreprises ont également besoin **d'appliquer des correctifs** et de **disposer d'antimalwares fiables sur tous les systèmes**. La base de toute protection est la gestion centralisée ainsi qu'une équipe spécialisée dédiée. Identifier un petit cluster de systèmes infectés, en détectant par exemple un malware « orphelin », peut ne rien signifier du tout – ou, au contraire, peut indiquer qu'il s'agit du maillon faible d'une chaîne d'attaque et que des investigations et une vigilance supplémentaires sont nécessaires afin d'éviter que d'autres éléments de l'attaque ne persistent.