Bitdefender®

# Les 11 questions les plus fréquentes sur les Botnets – et leurs réponses !

Ou pourquoi l'utilisation de listes noires de serveurs de commande et de contrôle (C&C) ne vous protègera pas.

# Sommaire



Auteur :
**George Yunaev**
Ingénieur Software Senior chez Bitdefender

# 1. Qu'est ce qu'un bot ?

Un bot est un type de malware qui, quand il contamine une machine, exerce un certain contrôle sur celle-ci. Cependant, à la différence d'un type ordinaire de malware, qui est autonome et qui n'a plus besoin d'intervention de son créateur une fois en circulation, le bot reçoit des instructions d'un maître (le bot master) et agit selon ses ordres. Ce sont sa capacité et sa nécessité à communiquer avec un serveur de contrôle à distance qui font du malware un "bot".

# 2. Quels types d'actions peut effectuer un bot ?

Un bot peut effectuer n'importe quelle action possible sur une machine, de la navigation Web au minage de Bitcoins. Cependant, il est typiquement utilisé pour certaines classes d'actions, telles que :

- Le vol d'informations (identifiants, documents, historiques des sites Web visités, communications) ;
- L'espionnage et le tracking (captures à partir d'une webcam, keylogging) ;
- Le hijacking (par exemple l'accès aux fichiers d'une entreprise en dupliquant les actions d'un utilisateur)
- Des activités malveillantes sur Internet (envoi de spam, fonctionnement en tant que proxys : contamination d'autres machines, hébergement de serveurs de commande, etc.).

Il y a, cependant, 2 types d'actions que le bot n'exécute pas :

- Les actions qui révèlent les infections. La capacité du bot à s'exécuter sur la machine serait réduite si les utilisateurs prenaient conscience que leur machine est infectée. Par conséquent, le bot s'efforce d'être discret et ne réalise aucune action qui aiderait l'utilisateur à se rendre compte d'une infection sur sa machine. Donc des actions telles que la modification des paramètres du navigateur ou l'apparition de fenêtres de dialogue ne sont pas typiques d'un bot ;
- Les actions qui menacent la "santé" de la machine. Le bot a besoin d'un environnement en bon état de marche pour fonctionner correctement : si l'environnement est compromis, la machine est réinitialisée et supprime donc le bot. Par conséquent, les bots n'ont pas l'habitude de perpétuer des actions destructrices qui peuvent entraver leur capacité à contrôler une machine.

Si ces actions ne sont pas réalisées, c'est parce qu'elles n'ont pas grand sens d'un point de vue business et non pas parce le bot n'en est pas capable. Au contraire, les bots peuvent tout à fait réaliser de telles actions et certains bots ont parfois été utilisés dans ce sens par le passé.

# 3. Qu'est ce qu'un botnet ?

Un botnet est un terme utilisé pour décrire un réseau de plusieurs ordinateurs infectés par un même malware, tous contrôlés par le même opérateur. Pour les besoins de la définition du botnet, la façon dont ces ordinateurs sont contrôlés importe peu, tant que le contrôle est opéré par le même opérateur/groupe. Le nombre d'ordinateurs infectés varie et peut aller de dizaines à des centaines de milliers d'ordinateurs infectés, voire même plus.

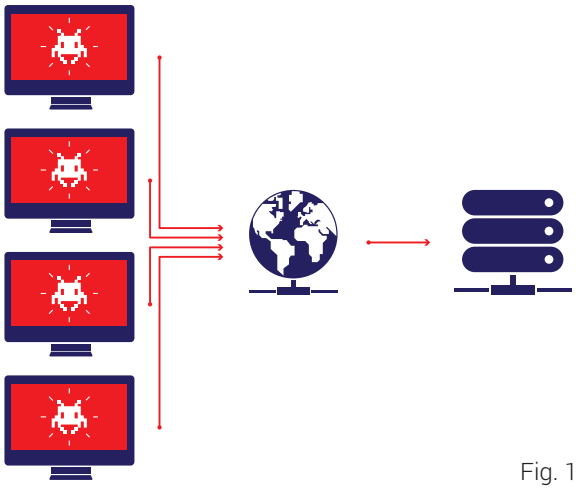

Fig. 1

Il n'est pas nécessaire pour ces ordinateurs de diffuser exactement le même modèle de malware, ou même d'utiliser les mêmes canaux ou serveurs de communication. Tant que ces bots sont contrôlés par un seul opérateur (qui peut être un groupe ou une personne) et peuvent agir ensemble, ils sont considérés comme un seul botnet.

Au contraire, d'un réseau d'entreprise par exemple, la composition d'un botnet n'est pas stable, mais fluide. Les nouveaux ordinateurs s'infectent et "se joignent" au botnet, tandis que d'autres ordinateurs "quittent" le botnet de façon permanente une fois que le malware est détecté et supprimé.

# 4. Comment un botnet apparaît-il ?

Tout d'abord, l'auteur du malware créé un programme spécial, qui servira de point de communication pour les bots. Ce programme fonctionne sur des machines dédiées et n'est typiquement jamais livré aux utilisateurs ; il est utilisé uniquement pour contrôler les bots.

Ensuite, le même ou un autre auteur de malware créé la partie du bot faite pour communiquer avec le programme décrit plus haut. Ce code est ensuite fusionné avec différentes charges utiles, selon le scénario de distribution. Par exemple, si le bot est distribué en tant qu'application légitime, la charge utile malveillante peut être ajoutée à des packages d'installation d'applications légitimes.

Puis, une fois que le malware est prêt, il est mis en circulation via des campagnes de spams, de phishing, des exploits ou des téléchargements via des sites Web infectés. Dès que la machine de l'utilisateur est infectée, l'instance du bot démarre, se connecte au point de communication et la machine devient partie intégrante du botnet.

Il est important de noter qu'un grand nombre de bots distribués n'arrivent pas jusqu'aux utilisateurs finaux ou n'infectent pas de machine. Certains utilisateurs n'ouvriront pas les pièces jointes malveillantes ou ne cliqueront pas sur le lien malveillant. D'autres utilisateurs ont une bonne solution de sécurité dont la protection proactive va bloquer la majorité des nouveaux malwares. Même les produits antivirus non proactifs mais seulement réactifs sont normalement assez rapidement à même de les détecter, une fois qu'ils sont rendus publics. Par conséquent, un auteur de malware devra modifier ses bots constamment afin qu'ils puissent avoir une chance de passer au moins à travers le premier niveau de détection des solutions sécurité. Ces changements impliquent naturellement plus de travail sur la création et la distribution de leurs botnets.

Pour résumer, les auteurs de malwares font beaucoup d'efforts dans la création de botnets et ils ne veulent pas que cela soit en vain. Cela affecte les choix de communication qui sont décrits ci-après.

# 5. Pourquoi un botnet apparaît-il ?

Comme évoqué plus haut, le développement, le déploiement et la gestion d'un botnet demande beaucoup d'efforts. Alors pourquoi les auteurs de malwares sont-ils prêts à sacrifier autant de temps pour la création de ces derniers ?

Leur but principal est de gagner de l'argent. Une fois le botnet mis en place et sous contrôle, les cyber-criminels ont plusieurs façons de capitaliser sur leur botnet. En général, ils vont louer le botnet à d'autres criminels pour un certain montant, et ces derniers l'utilisent alors à des fins malveillantes telles que :

- Des attaques coordonnées par déni de service (DDoS), durant lesquelles les machines infectées tentent d'inonder un serveur Web cible avec un nombre important de requêtes pour le mettre hors service. Ainsi, les utilisateurs légitimes du service attaqué ne peuvent pas accéder au serveur. Ces attaques peuvent avoir des motifs politiques (par exemple pour étouffer certains discours qui dérangent), ou encore être développées dans le but d'obtenir une rançon et dans ce cas les criminels exigent d'être payés pour "restaurer" l'utilisation normale du serveur cible ;
- Se cacher derrière l'utilisateur infecté pour exécuter une activité criminelle. Une fois la machine de l'utilisateur utilisée en tant que proxy, le criminel peut réaliser des crimes en ligne sans être visible. Dans ce cas, les actions peuvent être :
    - Des commandes frauduleuses en ligne (à l'aide de cartes bancaires volées par exemple) ;
    - Du hacking ou des tentatives d'effraction sur d'autres ordinateurs ;
    - Le téléchargement ou la distribution de contenu illégal ;
    - Du harcèlement, chantage ou envoi de menaces de mort.

Ces actions peuvent également sérieusement affecter l'utilisateur lui-même, car la loi peut considérer qu'il est à l'initiative de ces actions. Il risque alors d'être arrêté ou d'être l'objet de poursuites judiciaires[1]. Dans ces cas précis, le botnet est utilisé pour passer à travers une chaîne d'ordinateurs, souvent étalés sur plusieurs pays, pour diminuer les risques pour les pirates de se faire démasquer, en :

- infectant d'autres machines. Par exemple, un botnet peut être utilisé avec un autre malware basé sur un nouvel exploit, dans le but d'infecter d'autres machines. Dans ce cas, utiliser un botnet amplifie l'impact, permettant aux criminels de tenter d'infecter simultanément d'autres machines, par rapport à s'ils utilisaient des canaux de distribution classiques.
- envoyant des messages de spam. Tout comme pour infecter d'autres machines, l'utilisation d'un grand nombre d'ordinateurs contrôlés permet au cybercriminel d'envoyer plus de spams plus rapidement et de sources différentes, augmentant ainsi ses chances de ne pas être détecté.

En lui-même, le potentiel d'un botnet pour gagner de l'argent est considérable. À tel point que cela créé souvent une certaine rivalité entre différents auteurs de malwares. Des cas ont été relevés où ces derniers avaient inclus du code spécial dans leurs bots pour détecter et supprimer les malwares des "concurrents" et avaient même réparé la vulnérabilité exploitée par le malware du concurrent pour avoir accès à la machine eux-mêmes !

---

[1]Par exemple, une des publicités de DarkWeb, qui offre des services de hacking déclare : "Je peux télécharger, stocker et distribuer de la pornographie infantile en utilisant l'ordinateur de votre cible, de façon à ce qu'ils soient repérés facilement par les autorités. Je peux même en acheter en ligne à l'aide de leur carte de crédit. Plusieurs de mes clients ont fait arrêter leurs cibles et ont ainsi ruiné leur vie pour de bon."

# 6. Comment contrôle-t-on un botnet ?

Le botnet est contrôlé via un ordinateur dédié ou un groupe d'ordinateurs qui exécute une commande et contrôle le serveur (souvent abrégé en serveur C&C). Les bots communiquent et reçoivent des instructions de ce serveur dans un format compris par le bot. Le serveur exécute typiquement un certain nombre de fonctions, qui incluent :

• Donner des instructions aux bots pour exécuter ou programmer une certaine tâche ;

• Mettre à jour les bots eux-mêmes en les remplaçant par un nouveau type de malware ;

• Suivre le nombre de bots et la façon dont ils sont distribués (par région, pays ou encore fournisseur Internet).

Le serveur peut également proposer un panneau de contrôle accessible via une interface similaire à une interface Web pour un opérateur. Certains panneaux de contrôle sont très flexibles, permettant à l'opérateur de programmer une tâche uniquement pour les bots fonctionnant dans certaines zones géographiques ou sur des types d'utilisateurs différents (comme des réseaux entreprise). Certains vont même plus loin en offrant un accès à un tiers, permettant à d'autres hackers de louer l'utilisation du botnet à l'opérateur.

# 7. Existe-t-il une manière fiable de détecter les bots qui communiquent avec le serveur C&C ?

Chaque auteur de malware créé son propre protocole de façon indépendante. Il n'y a donc pas de langage, de protocole ou de façon de communiquer "standards". La raison est que le contenu de la communication avec les bots dépend fortement de la flexibilité du bot et des talents de programmation de son créateur. Cela peut varier de simples chaînes de texte exécutant les commandes, à des scripts plus complexes dans des langages tels que Python ou Lua.

La façon dont les bots communiquent peut aussi varier. Certains bots utilisent le protocole IRC, certains le protocole HTTP et d'autres encore un protocole personnalisé (par exemple certains bots utilisent le protocole ICMP pour communiquer). Certains utilisent un chiffrement fourni par le protocole (comme le HTTPS), d'autres implémentent le chiffrement eux-mêmes, tandis que certains n'utilisent aucun chiffrement. Les bots modernes sont hautement résistants à la surveillance du trafic, une détection fiable ne serait-ce que de la majorité des bots avec des "signatures de trafic" est impossible.

Ainsi, chaque bot doit être analysé séparément pour découvrir le protocole qu'il utilise, et dans le cas où le protocole est chiffré, il n'existe pas de manière simple et fiable pour détecter les communications.

# 8. Comment enquête-t-on sur les botnets ?

Lorsque les auteurs de malwares mettent leurs bots en circulation, tôt au tard ils font face à des experts en cybercriminalité. Les chercheurs en malwares capturent généralement la vague initiale de bots via différents canaux tels que des honeypots, des spams, des sites Web frauduleux ou des rapports de produits de sécurité.

Une fois que le bot est "capturé", il est analysé dans un environnement contrôlé. Généralement, les chercheurs veulent garder le bot "actif" pour recevoir les dernières mises à jour le concernant et ainsi accélérer le processus d'analyse. Parce que les mises à jour de bot ne sont pas fréquentes, recevoir des mises à jour directement dans un honeypot peut en simplifier l'analyse.

Le problème majeur ici est que les opérateurs de bots ne veulent pas que les chercheurs de malwares reçoivent ces mises à jour. Si l'opérateur de bot détecte que son bot est présent au sein d'un honeypot, il le sépare des autres bots et ne lui enverra plus de mises à jour. Les chercheurs doivent "convaincre" l'opérateur que la machine infectée est bien réelle et que celle-ci permet bien d'envoyer des spams ou d'infecter d'autres machines. Mais cette action pose des difficultés significatives pour l'activité des chercheurs puisque la machine en question reste infectée et continue à se comporter de façon illégale, ce qui peut engendrer de graves conséquences légales.

# 9. Peut-on bloquer les communications entre bots avec des solutions d'analyse de trafic ?

C'est une question typique basée sur les affirmations de certains vendeurs, qui assurent que leur solution peut détecter et bloquer les bots grâce à :

• Une liste d'adresses IP et de domaines C&C ;

• Une liste des schémas de trafic utilisés par les bots pour communiquer ;

• Une liste des noms de domaine auxquels les bots font des requêtes.

Malheureusement, toutes ces solutions ne peuvent détecter qu'une seule classe de bots. Aucune d'elles n'offre un ratio de détection de bots vraiment satisfaisant. Pour en comprendre la raison, voyons comment les bots communiquent entre eux.

## *Communication directe avec un serveur unique*

Les bots utilisant cette méthode communiquent directement avec un serveur unique ayant une adresse IP fixe. Ce mode est le plus facile à détecter et à bloquer, étant donné que tout ce que les chercheurs ont à faire est de capturer le bot et retracer la destination de ses communications - une tâche extrêmement aisée. Une fois que l'identité du serveur et sa localisation sont établis, les autorités coopèrent avec les Fournisseurs d'Accès à Internet (FAI) et ces derniers sont généralement très rapides pour le fermer. Et même si les FAI locaux ne coopèrent pas, le FAI principal en amont le fait généralement.

C'est la seule méthode qui peut être facilement mise en place avec les listes de blocage IP. Mais ce mode est rarement utilisé par les pirates de nos jours, car une fois que le serveur ne fonctionne plus, c'est tout le botnet qui est désactivé - et tous les efforts du créateur de malwares réduits à néant. Cela les force à choisir des moyens de communication plus performants.

## *Communication directe avec plusieurs serveurs*

Les bots utilisant cette méthode communiquent avec plusieurs serveurs C&C, dispersés géographiquement. Ce modèle de communication offre une certaine forme de résilience puisqu'il rend impossible la fermeture du réseau en ne prenant en compte qu'une seule instance de bot communiquant avec un seul serveur, ou prenant le contrôle de ce serveur. Les bots utilisant ce modèle se mettent automatiquement à jour de façon régulière pour ajouter de nouveaux serveurs à la liste et supprimer les serveurs qui ne sont plus actifs.

Mais encore une fois, quand la copie du bot est capturée et analysée par des chercheurs, toutes les informations du serveur codées en dur dans le bot sont découvertes et ce dernier est bloqué rapidement. Les créateurs de malwares contrent ce phénomène en utilisant des algorithmes appelés Domain Generation Algorithms (DGA). Désormais, les serveurs C&C ne sont plus codés en dur dans le bot, mais à la place la liste de serveurs C&C est générée grâce à un algorithme, basé sur certains paramètres tels que la date. Un tel algorithme peut générer des centaines de milliers de noms de domaines et le créateur de malwares n'a qu'à en enregistrer quelques-uns pour que le bot soit capable d'appréhender l'ensemble du réseau.

L'approche basée sur les DGA est difficile à contrer pour les solutions d'analyse de trafic qui dépendent des listes de domaine. Les listes de domaine possibles sont quasiment illimitées, étant donné le nombre de différents botnets existants. Cependant, le reverse-engineering du bot pour révéler l'algorithme utilisé est encore plus problématique. C'est un processus très chronophage (le malware est souvent "brouillé" et utilise d'autres techniques pour empêcher le reverse-engineering) et les bots sont trop fréquemment mis à jour. C'est pourquoi quand l'algorithme est finalement résolu, la plupart des bots utilisent déjà la dernière version avec un algorithme différent.

## *Communication directe via le réseau TOR*

C'est une méthode de communication relativement nouvelle (fin 2013), où les serveurs C&C sont dissimulés grâce au réseau anonyme TOR.

Ces serveurs sont très difficiles à pister et localiser avec des moyens traditionnels (ils sont largement utilisés par les criminels en ligne ayant des objectifs tels que la vente de drogues ou d'armes) et leur localisation nécessite typiquement une coopération avec les autorités.

Ils n'utilisent pas d'adresses IP traditionnelles et de noms de domaines, mais les adresses du "serveur caché" sous le domaine .onion. Seuls le malware et le dernier nœud de la chaîne savent avec quel serveur le malware essaye de communiquer. Cela signifie qu'aucune solution listée ci-dessus ne peut identifier ou bloquer une telle communication malware.

## *Communication via des nœuds intermédiaires*

Cette méthode de communication est relativement nouvelle car elle est plus complexe et nécessite plus de développement et de tests de la part des créateurs de bots. Avec cette méthode, les bots ne communiquent pas directement avec les serveurs mais avec les autres bots qui communiquent avec les serveurs :

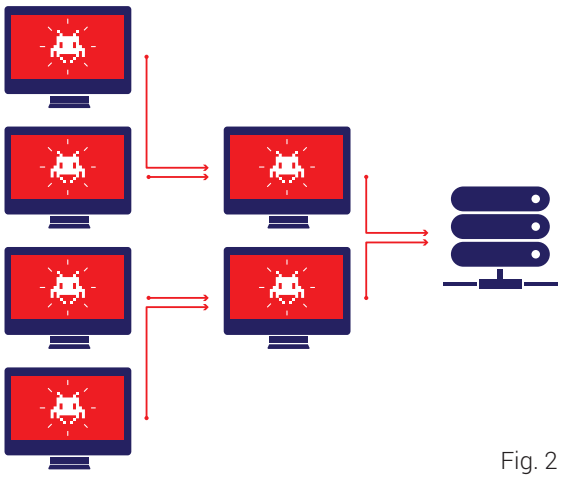

Fig. 2

Cette méthode de communication diminue la charge au niveau des serveurs et rend la détection des serveurs C&C plus difficile. Les chercheurs en malwares doivent passer plus de temps pour comprendre si le malware communique avec un serveur C&C ou avec une autre machine infectée. Il est évident que les listes d'IP du serveur C&C sont inutiles pour bloquer cette approche, comme la majorité des machines infectées communiquent avec d'autres machines infectées, et non avec les serveurs C&C.

### *Communication via des sites Web populaires*

Une méthode de communication très lucrative pour les auteurs de malwares est d'utiliser des sites Web populaires comme serveurs C&C. Un type de malware utilisait Gmail[2], Twitter[3] et Pastebin[4] pour les communications et les mises à jour. Cette approche permet de bénéficier d'avantages significatifs pour les créateurs de malwares. En voici quelques exemples :

- Les sites Web et les services populaires sont généralement disponibles à la plupart des utilisateurs, même dans les environnements les plus restrictifs ;
- Si on découvre que le service est utilisé en tant que serveur C&C, il ne sera pas fermé pour autant ; c'est plutôt le service lui-même qui devra gérer ce problème ;
- Ces services sont construits sur la base d'une architecture fiable, donc les créateurs de malwares n'ont pas à s'occuper des problèmes d'évolutivité et de fiabilité.

Alors que les versions plus anciennes de ces malwares étaient faciles à détecter car elles utilisaient des messages chiffrés, encodés en base64, ce qu'aucun utilisateur lambda n'utilise, il y a plusieurs façons pour les auteurs de malware d'éviter d'être détectés. Il est possible d'utiliser la sténographie, par exemple, pour dissimuler les instructions du serveur C&C - ou même des mises à jour du malware - dans le texte et les images. Clairement, n'importe quelle liste de serveurs C&C est inutile face à cette approche.

## 10. Peut-on analyser le trafic à la recherche "d'anomalies" pour détecter un bot ?

Cela dépend du mode de communication. Le principal problème de cette approche est qu'elle sera toujours réactive, étant donné que les bots ne cessent d'évoluer pour esquiver leur détection par les solutions de sécurité. Changer le protocole de chiffrement n'est donc pas un problème. De plus, il y a de nombreux moyens de se fondre dans des schémas de trafic existants (par exemple, utiliser l'authentification HTTP et les entêtes de cookies pour envoyer/recevoir des commandes - de tels champs peuvent contenir différentes valeurs qu'il est impossible de pister). Cette approche ne détectera donc que les bots les moins complexes.

## 11. Quelle est la meilleure façon pour détecter un bot ?

La façon la plus fiable de détecter un bot est de réaliser la détection dans la machine sur laquelle le malware est lui-même exécuté. Non seulement le malware ne pourra tout simplement pas infecter l'ordinateur, mais dans le cas où il passerait entre les mailles du filet, l'analyse comportementale pourra éventuellement détecter les actions malveillantes, même si le malware n'est pas connu du moteur antimalware. De plus, les routines de détection fonctionnent de la même façon si le malware ne communique pas du tout avec le serveur C&C. Et bien sûr, les mises à jour du moteur de détection détecteront le malware sur la machine plus tard, même si il parvient à passer inaperçu et que l'analyse comportementale ne le détecte pas au premier abord.

---

[2] "Les hackers utilisent des brouillons Gmail pour mettre à jour leurs malwares et subtiliser des données" : www.wired.com/2014/10/hackers-using- gmail-drafts-update-malware-steal-data ;

[3] "Un botnet utilise Twitter comme canal de commande" : www.arbornetworks.com/asert/2009/08/twitter-based-botnet-command- channel

[4] "Pastebin est un moyen pratique pour les cybercriminels d'héberger des malwares à distance" : www.securityintelligence.com/news/pastebin-convenient-way-cybercriminals-remotely-host-malware

Bitdefender propose des technologies de sécurité dans plus de 100 pays via un réseau de partenaires de premier plan, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Bitdefender associe ses technologies primées à des alliances et des partenariats commerciaux et renforce sa position sur le marché mondial via des alliances stratégiques avec des fournisseurs de technologies cloud et de virtualisation leaders dans le monde.



PROFIL TECHNOLOGY

Plus de **500 millions d'utilisateurs**
.sont protégés par les technologies Bitdefender

Bitdefender

Bitdefender est édité en France et dans les pays francophones par PROFIL TECHNOLOGY S.A., éditeur et distributeur de logiciels pour les particuliers et les entreprises.