CYBER THREAT INTELLIGENCE - AN OVERVIEW AND PRACTICAL APPROACHES USING OPEN SOURCE SECURITY TOOLS

Sujet de recherche : les botnets, fonctionnement, cycle de vie, utilisation et expérimentations

en vue de l'obtention du Master 2 Informatique

Spécialité *Services, Sécurité des Systèmes et des Réseaux*

Parcours *Sécurité des Systèmes d'Information*

SOMMAIRE :

++ici mettre à jour avec les accents à la fin le sommaire

INTRODUCTION

Dans le cadre de l'UE « Cyber Threat Intelligence » avec Monsieur Alexandre Dulaunoy, nous devions réaliser un projet portant sur un sujet qui nous était propre. J'ai ici choisi de m'attacher aux botnets. Plus particulièrement de comprendre précisément leur fonctionnement, leurs buts et leur utilisation actuelle.

DEFINITION

Un botnet est un terme qui désigne un groupe d'ordinateurs infectés et contrôlés par un attaquant à distance (détournés à l'insu de leurs propriétaires).

Les ordinateurs faisant partie d'un botnet sont souvent appelés « bots » ou « zombies ».Il n'y a pas de taille requise pour pouvoir considérer un groupe d'ordinateurs comme un botnet (les petits botnets peuvent comprendre quelques centaines, voire quelques milliers de machines, alors que les botnets les plus grands peuvent comprendre jusqu'à des millions de machines).

FONCTIONNEMENT D'UN BOTNET

La première étape de la création d'un botnet est donc l'infection d'ordinateurs. C'est la première phase.

➔ Phase initiale

L'infection a lieu via des mécanismes classiques, qui vont aussi dépendre du type de périphériques visés :

- Malware en pièces jointe
- Cheval de Troie
- Faille de navigateur web
- « Drive-by » download

On remarque donc d'ores et déjà l'importance de cliquer seulement sur ce que l'on considère « fiable », d'avoir un système mis à jour, et correctement protégé par un anti-virus. Ces différentes actions combinées permettent de se prémunir de cette infection dans presque tous les cas.

Une fois installé, cet outil malveillant va déclarer la machine à un centre de contrôle (Command and Control serveur, que l'on abrègera par la suite par C&C), et elle sera donc considérée comme machine active. Celle-ci va donc pouvoir être contrôlée à distance. Nous reviendrons sur cette communication plus précisément à la fin de cette partie.

Avant d'être considérée comme totalement opérationnelle, plusieurs autres phases sont nécessaires :

➔ Phase de mise à jour

Ici on va s'occuper de mettre à jour notre botnet, donc nos machines infectées. Mise à jour des machines, ajouts de fonctionnalités, modification de signatures … (Cette modification de signature est cruciale, il va falloir modifier les « charges actives » pour continuer à passer sous le radar et ne pas être reconnu par les anti-virus …)

➔ Phase d'auto-protection

Le but va être ici de garder le contrôle sur la machine infectée, tout en étant dissimulé.

- Installation de rootkits (outil permettant de pérenniser un accès de la manière la plus furtive possible)
- Modification du système cible (firewall, anti-virus …)
- Suppression de logiciels qui pourraient nous nuire
- Exploitation de failles du système hôte (escalade de privilèges par exemple)

➔ Phase de propagation

Plus la taille d'un botnet est grande, plus celui-ci sera puissant et plus les attaques lancées seront critiques.

Le but va donc être à chaque fois d'étendre notre réseau de machines infectées :

- Campagne de spams : malware en pièces jointes, liens web malveillant …
- Exploitation de failles, de backdoors sur des serveurs
- Tentatives de bruteforce sur des serveurs …

➔ Phase opérationnelle

Celui-ci est fonctionnel, et les machines peuvent obéir aux ordres qu'on leur communique.

On peut utiliser notre botnet pour :

- Réaliser des campagnes de spam par mail
- Réaliser des opérations de phishing
- Comme on l'a déjà dit précédemment, on peut identifier et infecter d'autres machines
- Réaliser des attaques de déni de service (DDoS) de grandes ampleurs.
- Se « cacher » derrière un utilisateur infecté pour exécuter une action criminelle (hacking, commandes frauduleuses …)
- Fraude au clic
- Espionnage
- Vol d'informations sur les machines compromises
- Keylogger : vol de cartes de crédit …
- Miner des crypto monnaies (très lucratif avec l'explosion du prix du bitcoin ces dernières années)

- Exploitation de la puissance des calculs de toutes les machines infectées pour réaliser du calcul distribué : calcul de mot de passe

Le but principal d'un botnet est de gagner de l'argent. Un botnet va pouvoir être loué à d'autres attaquants pour leur permettre de réaliser leurs attaques.

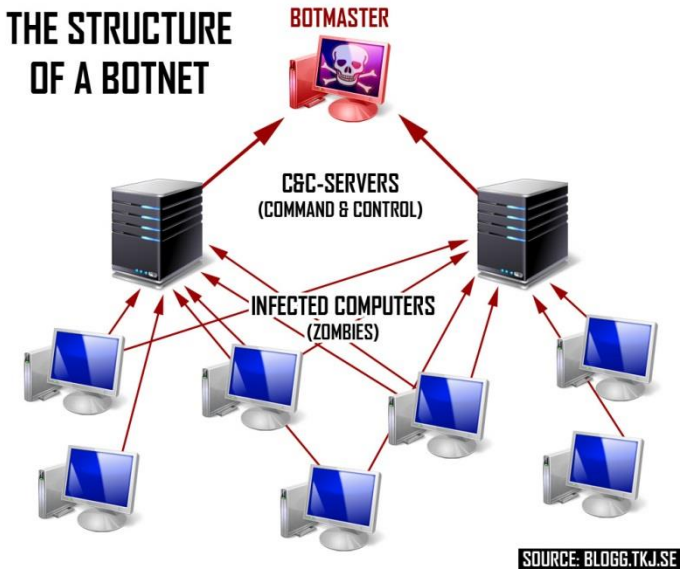
Les deux actions que les bots n'effectueront pas sont celles qui pourraient révéler leur présence (le but est de garder la machine infectée fonctionnelle le plus longtemps possible et on ne veut donc pas que les utilisateurs prennent conscience de l'infection de leur machine) et celles qui menaceraient la santé de la machine (pour la même raison que précédemment, le but est de garder l'environnement en bon état de marche).

Un point que nous n'avons pas abordé mais qui est néanmoins crucial est la communication avec notre botnet. Il existe différentes possibilités et modèles. On note que le contrôleur maitre du botnet est appelé botmaster.

Modèle client-serveur

On a tous nos différents bots qui communiquent avec un ou plusieurs centres de contrôle : C&Cs serveurs. Avoir plusieurs C&Cs serveurs permet d'avoir de la redondance et donc de s'assurer que si un tombe, on pourra toujours envoyer des instructions à nos zombies.

Mais cela ne rend absolument pas le botnet indestructible pour autant … Si les serveurs C&C sont découverts et rendus inopérables, alors entre guillemets, le botnet n'est plus.

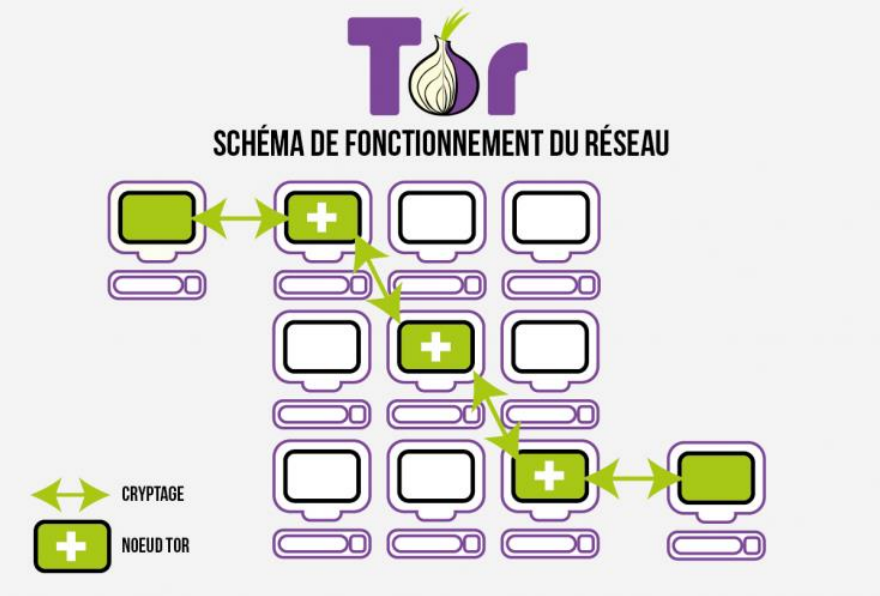


++Parler de DGA

Tor

Il est aussi à noter que certains botnets sont contrôlés au travers du réseau d'anonymisation Tor avec des serveurs C&C uniquement accessibles depuis ce réseau.

Le protocole de service caché « hidden service » a été conçu pour masquer l'adresse IP des clients du service et celle du service auprès des clients, ce qui rend presque impossible pour les parties concernées de déterminer l'emplacement physique ou la véritable identité de chacune des parties.

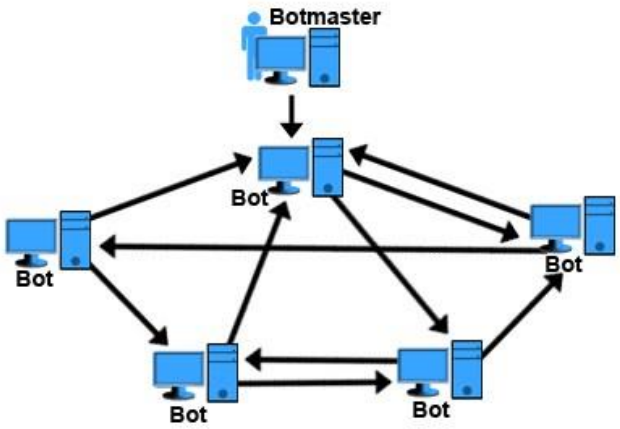


Modèle Peer-to-Peer (P2P)

Plutôt que se reposer sur un ou plusieurs serveurs C&C centralisés, les derniers botnets utilisent maintenant un modèle décentralisé « structure peer-to-peer ».

Chaque bot fonctionne autant en tant que client que serveur. Chacun à une liste de périphériques infectés et vont leur transférer différentes informations …

Cette structure va permettre de rendre le botnet beaucoup plus difficile à stopper par les forces de l'ordre puisque il n'y a rien de centralisé.

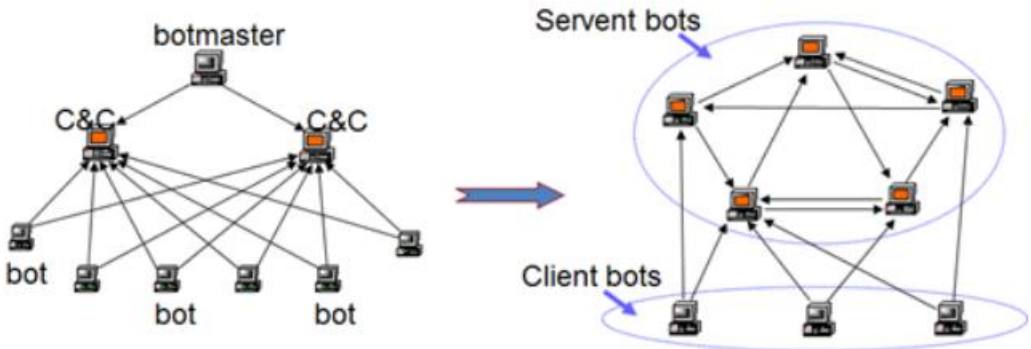


Voici une comparaison entre le modèle centralisé et le modèle peer-to-peer :

TABLE I. Comparison Between Centralized & P2P

S.No.	Parameters	Botnets	
		Centralized	*P2P*
1.	Tracking	Easier	Difficult
2.	Single Point of failure	Can destroy the whole Botnet	Will not affect much
3.	Cost incurred	Higher cost	Low
4.	Risk of Hijacking	Hijacking of Bot-controller can reveal the identity of Bot-master	Hijacking Bot peer cannot reveal the identity of Bot-master
5.	Command distribution speed	Faster	Slower
6.	Management	Easy	Difficult

Modèle Hybride :



From centralized botnet to hybrid peer-to-peer botnet

Récemment, les chercheurs en sécurité de chez Symantec ont découvert un nouveau type d'architecture hybride entre un modèle client-serveur et un modèle peer-to-peer. Le modèle peer-to-peer va prendre le relais au cas où les serveurs C&C ne sont plus accessibles.

C'est ici le modèle d'architecture le plus puissant et le plus inquiétant. En effet il possède tous les avantages : pas de « single point of failure », redondance des C&Cs et même si l'on arriverait à les faire tomber, le botnet se reposerait ensuite sur son architecture P2P.

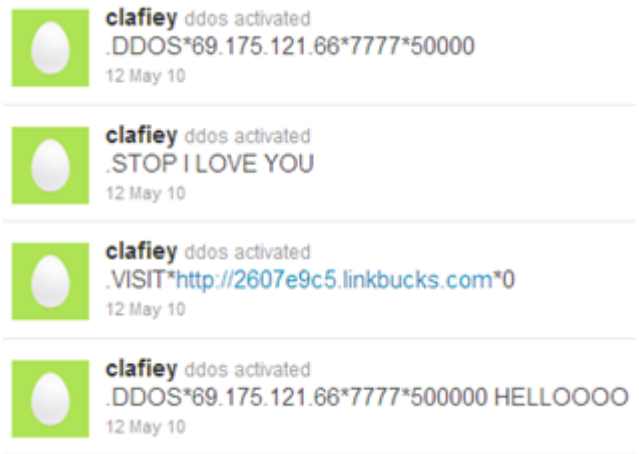
Les canaux de communication peuvent être très différents. Originellement et encore très utilisé maintenant est le canal IRC. D'autres botnets fonctionnent grâce à des protocoles réseaux classiques pour ne pas attirer l'attention tels que ICMP, TCP ou encore UDP. HTTP et HTTPS sont aussi grandement utilisés du fait qu'il n'est plus nécessaire d'avoir une connexion permanente comme pour le peer-to-peer ou irc, et que en plus on reste « sous le radar » en utilisant un des protocoles le plus commun et courant.

Exemple : chaque bot pourrait télécharger un fichier d'une adresse tel que http://exemple.com/commandebot et réaliser les actions indiquées.

Les méthodes de communication ont beaucoup évolués ces dernières années et se sont adaptées au Web 2.0 : simple recherche internet sur certains mots-clés pour identifier des ordres ou l'adresse de connexion de C&C ou encore l'utilisation de messagerie instantanée telle que MSN.

L'une des dernières tendances est l'utilisation de protocoles et d'applications connues tels que les réseaux sociaux.

➔ Fichier de commandes ou de mises à jours uploadés sur Evernote, Twitter, Pastebin

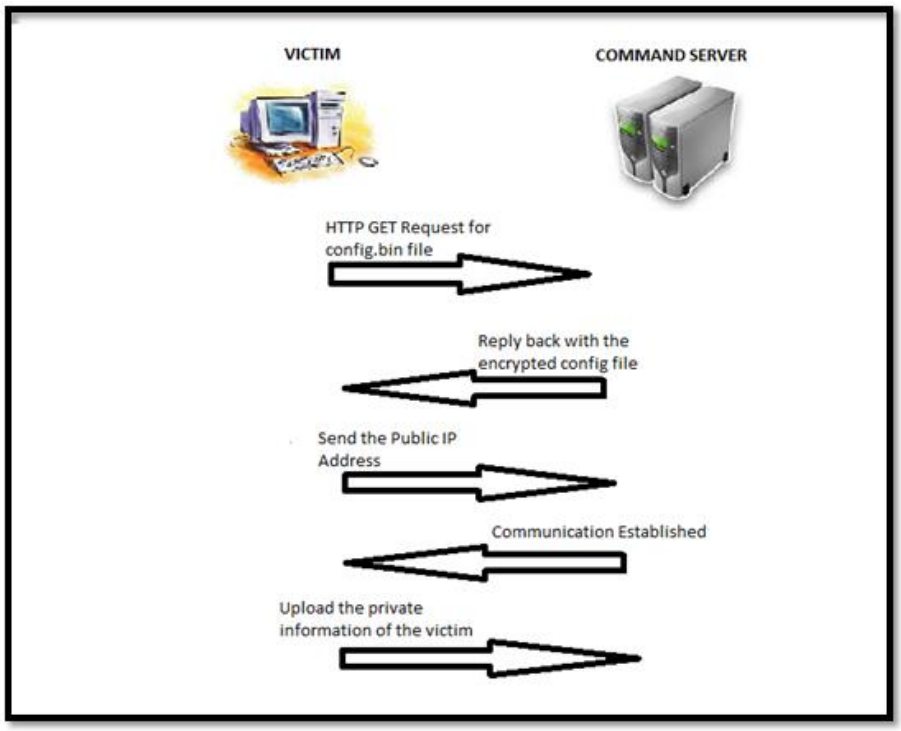


➔ Utilisation du « cloud », google drive …

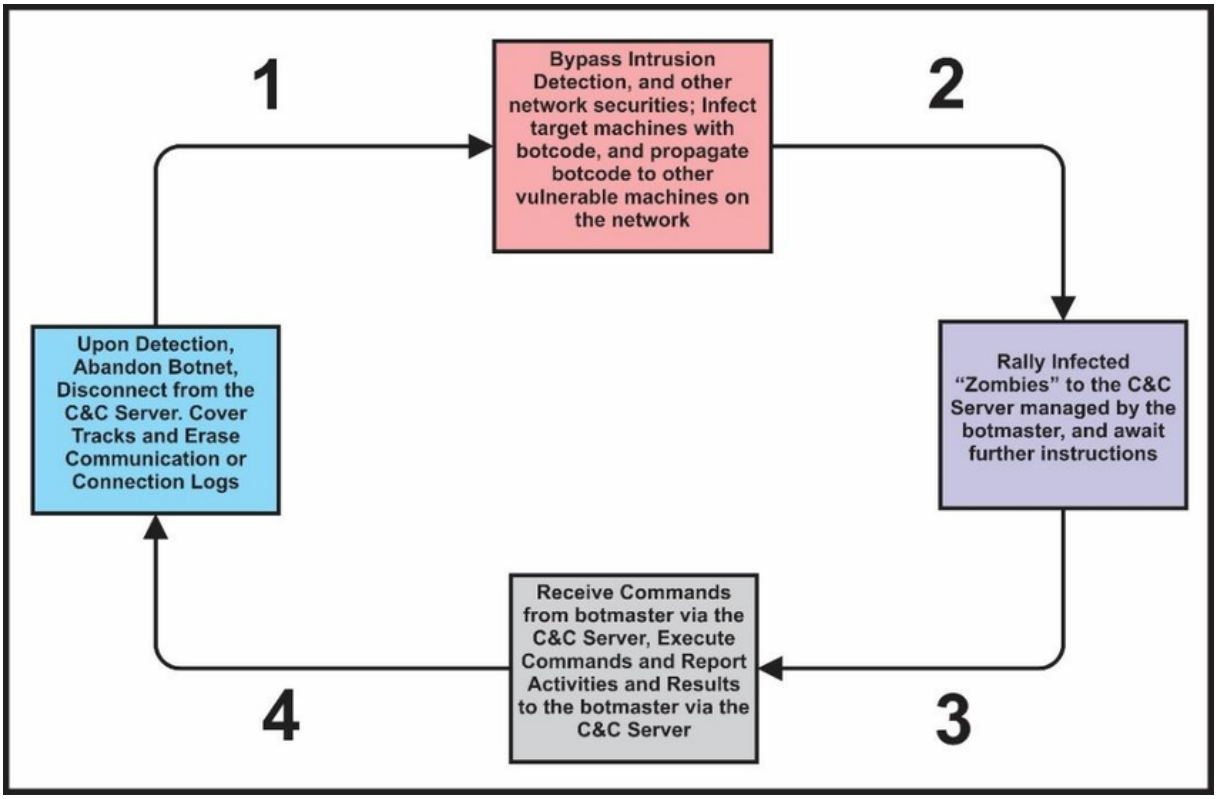
Cette méthode communication est aussi très lucrative, et permet aux auteurs de malware de bénéficier de nombreux avantages :

- Ces services sont généralement disponibles pour tout les utilisateurs et ne seront pas bloqués par des politiques d'entreprise restrictives par exemple
- Si il est découvert en tant que C&C, le site ne sera pas fermé … ce sera à lui de gérer le problème
- L'architecture meme de ces services populaires est fiable et performante, donc pas de problème de disponiblité, d'évolutivité …

Sur la page suivante, on peut voir un schéma détaillant la récupération par un bot des commandes qu'il doit effectuer via le protocole http et une requete de type GET sur son C&C.



Pour conclure, voici un schéma synthétique du cycle de vie et de fonctionnement d'un botnet :



LES BOTNETS « CELEBRES »

CLASSIFICATION

Il existe plusieurs classifications de botnets. Il est possible de les différencier selon leur architecture, selon le protocole réseau utilisé ou la cible visée.

Les catégoriser n'est pas chose aisée, cela va aussi dépendre grandement du but précis pour lequel ces architectures sont créées dans un premier lieu (cela va influencer des facteurs tel que le malware utilisé pour compromettre les victimes …).

Nous avons expliqué précédemment les différents modèles d'architecture, en voici une synthèse :

- Modèle client-serveur, basé sur la présence d'un ou plusieurs C&C
- Modèle peer-to-peer
- Modèle hybride

A cela s'ajoute l'utilisation ou non du réseau Tor.

Vient ensuite les différents moyens de communication et protocoles réseaux employés :

- Protocole IRC
- Protocoles classiques tels que TCP, ICMP, UDP
- Messagerie instantanée tels que MSN, ICQ
- http et https
- Utilisation des réseaux sociaux (Twitter, Facebook, Evernote)

Les botnets peuvent aussi se différencier par les cibles et les plateformes qu'ils visent, on distingue ici :

- PCs et laptops
- Mobiles
- IOT : internet of things

++continuer avec les images de taxonomie trouvées

QUELS MOYENS POUR LES STOPPER ?

Les bots modernes sont hautement résistants à la surveillance du trafic, on ne peut avoir une détection fiable de la majorité de ceux-ci … Les bots ne cessent d'évoluer pour esquiver leur détection par les différents antivirus et solutions de sécurité. De plus comme nous l'avons vus précédemment il y a de très nombreux moyens de passer à travers les mailles du filet (exemple : utiliser les entêtes de cookies http pour envoyer/recevoir des commandes …)

Certaines solutions existent néanmoins pour les détecter et les bloquer :

- Liste d'adresses IP et de domaines C&C
- Liste des schémas de trafic utilisés par les bots pour communiquer
- Liste de noms domaine auxquels les bots font des requêtes

Il n'y pas de standards pour la création de botnets. Il n'y a pas de langage, d'architecture ou de protocoles standards et définis. Tout est entre guillemets laissés à l'imagination de l'auteur de malware et de son inventivité et connaissances.

EXPERIMENTATION CONCRETE : CREATION ET CONTROLE D'UN BOTNET

Dans le cadre de notre projet de synthèse de cette année qui consistait à attaquer les serveurs de nos camarades et à nous défendre de leurs attaques, j'ai vu l'opportunité d'une attaque complexe me permettant de constituer un réseau de cibles infectées et auxquelles je pourrais envoyer des commandes : autrement dit un botnet.

Voici donc ici ma démarche, ainsi que la partie technique détaillée :

CONCLUSION

Les botnets sont des armes « redoutables » et continueront à être un enjeu et un outil majeur dans le domaine de la « sécurité informatique » .Leur capacité d'action et la difficulté à les stopper les rends particulièrement efficace. Posséder un botnet permet de rapporter beaucoup d'argent et de capitaliser très rapidement (un botnet est de près ou loin concerné dans presque chaque type d'attaque complexe).

Ce projet fut très instructif, c'est un sujet que je ne connaissais que très peu et qui m'a permis donc de renforcer grandement mes connaissances à leur sujet.

++Malware as a service, rent, big concern, + statistiques