


| | | |
|---|--|--------------|
|  | Niveau de classification : Public | Version :1.0 |
| | Guide de protection contre les « botnets » | 21/11/2022 |

Guide de protection contre les « botnets »

❖ Définitions :

Botnet : Un botnet est un réseau d'ordinateurs ou d'appareils IoT connectés à Internet et infectés par des logiciels malveillants.

Bot : Chaque appareil individuel au sein du réseau de botnet est appelé un bot.

Bot master : Le bot master est la personne qui contrôle et exploite l'infrastructure du botnet et utilise les appareils compromis pour lancer des cyberattaques.

❖ Types d'attaques de botnets

Les créateurs de botnets ont toujours quelque chose à gagner, que ce soit de l'argent ou une satisfaction personnelle.

Un botnet peut être utilisé pour mener de nombreux types d'attaques, notamment :

- **Des attaques par déni de service distribué (DDoS)**, Lors d'une attaque par déni de service distribué, le botnet envoie un nombre excessif de demandes à un serveur ou à une application ciblée pour saturer la bande passante ou provoquer un épuisement des ressources pour causer une perte de la disponibilité du système informatique.
- **Le minage de cryptomonnaies**, qui utilise la puissance de traitement de la machine infectée pour effectuer des calculs complexes pour créer une cryptomonnaie et octroyer un gain financier pour le propriétaire de botnet.
- **L'installation de logiciels espions** pour surveiller les activités des utilisateurs et collecter leurs données sensibles.
- **Le spam/ Phishing**, qui consiste à utiliser les machines du botnet pour expédier en masse un grand volume d'e-mails non sollicités par les destinataires à des fins publicitaires ou malhonnêtes ou propager des logiciels malveillants dans le cadre d'une campagne d'hameçonnage.
- **Compromission d'accès** par les attaques par force brute.
- **Fraude aux clics** généré par du trafic Web fictif ou des publicités pour générer des revenus.

❖ Modèles de botnets

-**Modèle client/serveur** : basés sur l'architecture client-serveur, où un serveur de commande et de contrôle (C&C) gère l'ensemble du botnet. En raison de sa simplicité, l'inconvénient de l'utilisation d'un modèle centralisé est que le serveur de commande et de contrôle est facile à trouver et à désactiver. Les deux canaux de communication C&C les plus courants sont IRC et HTTP.

-**Peer-to-Peer** : La nouvelle génération de botnets est plus sophistiquée, ont une organisation aléatoire où les bots partagent des commandes entre eux et ne sont pas en contact direct avec le serveur de commande et de contrôle.

❖ Les bonnes pratiques pour la protection contre les botnets :

Voici quelques signes à surveiller au sein de votre réseau en cas d'attaques botnet:

- Activité inhabituelle : Connexion internet lente, mise à jour bloquée,...
- Utilisation inexplicite de la bande passante du réseau.
- Comportement inhabituel à l'arrêt ou au démarrage.
- Des fenêtres pop-up inattendues (résultant d'une activité de fraude au clic).

❖ Les bonnes pratiques pour la protection contre les botnets :

Pour s'en protéger, cela passe par l'adoption de plusieurs bonnes pratiques :

- Mettre à jour régulièrement votre système d'exploitation, vos navigateurs Web et aussi votre solution antivirus.
- Sauvegarder et crypter vos données critiques dans des disques externes et des serveurs de backup protégés et isolés d'Internet.
- Utilisez une configuration sécurisée et s'assurer que les accès à vos serveurs, vos équipements réseaux, vos ressources partagées et vos services en ligne (RDP, TELNET, SSH, FTP, SMB, NetBios, SMTP, POP3, etc. ...) sont limités, contrôlés et protégés avec des mots de passe robustes.
- Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de trafic réseau.
- Mettre en place des solutions de journalisation nécessaires pour contrôler les événements survenus sur vos serveurs critiques et vos équipements réseaux.
- Scanner les réseaux afin de déterminer les failles puis procéder à les corriger en installant les patches correctifs depuis les sources officielles.
- Désactiver les ports inutilisés.
- Blacklister les adresses IP uniques d'hôtes malveillants ou des sous-réseaux entiers présentant des activités suspectes.

- Sensibiliser vos employés sur les attaques de Phishing, Social Engineering et les ransomwares.
- Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail, par les applications de messagerie de Facebook / Twitter / Instagram etc... ou à travers vos réseaux sociaux et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.
- Implémenter les techniques :
 - « DNS Reverse Lookup <<https://manuals.gfi.com/en/kerio/connect/content/server-configuration/mail-delivery-and-dns-records/essential-dns-records-for-mail-delivery-and-spam-protection-1223.html>>»
 - SPF (Sender Policy Framework -RFC 4408) <<https://tools.ietf.org/html/rfc4408>>, DKIM ADSP (Author Domain Signing Practices -RFC 5617 <<https://tools.ietf.org/html/rfc5617>>)
 - DMARC (Domain-based Message Authentication, Reporting, and Conformance – RFC 7489 <<https://tools.ietf.org/html/rfc7489>>
- Changer le mot de passe par défaut par un autre plus robuste pour assurer une administration sécurisée de votre périphérique IoT.
- S'assurer que le micrologiciel / Firmware de votre périphérique IoT est à jour.
- Utiliser l'authentification à deux facteurs (2FA) ou multifactorielle.
- Auditer les comptes d'utilisateurs disposant de privilèges administratifs et configurer les contrôles d'accès selon le principe du moindre privilège.
- Évitez les téléchargements à partir de réseaux P2P et de partage de fichiers.
- Évitez d'acheter des appareils dont la sécurité est faible.