BonWare, un botnet qui vous veut du bien

AlgoSecure

Smarter security for future technologies

INTERVENANTS

Hicham Ben-Hassine, Directeur, AlgoSecure

Architecte infrastructure et sécurité

Sommaire

- Contexte
- Nos motivations
- BonWare
- Limites et roadmap
- Recommandations

Contexte

- Menace botnet de plus en plus présente et critique
- Diversité des botnets

Botnet	Création	Action
Vawtrak	2013	Fraude bancaire (infection par pièce jointe docx, xlsx)
Dridex	2015	Fraude bancaire (envoi de pièce-jointe avec macro malveillante)
Zeus	2010	Fraude bancaire (infection par visite d'un site malveillant ou par email)
Mirai	2016	DDoS (contrôle à distance de caméras connectées)

Motivations

- Sensibiliser les utilisateurs du SI
- Démontrer la limite des protections « périmétriques » actuelles

  (FW, sandbox, IPS, AV, Antispam, Gateway messagerie)
- Avoir une approche SSI pragmatique
- Éduquer les utilisateurs aux bonnes pratiques SSI

BonWare – Quelques définitions

- Bot

  Ordinateur compromis par un logiciel malveillant

- Serveur de commande et de contrôle (C&C)

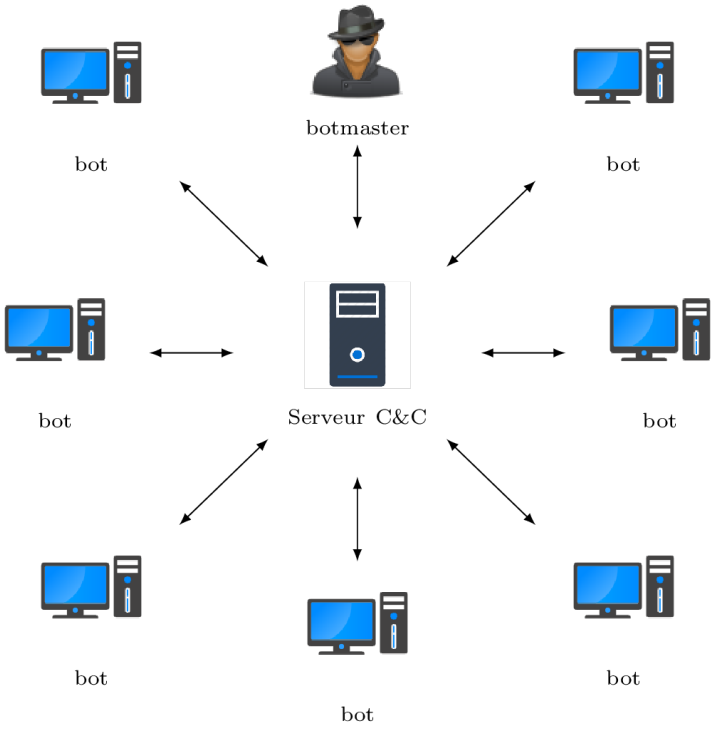
  Plateforme pour communiquer avec les bots

- Botnet

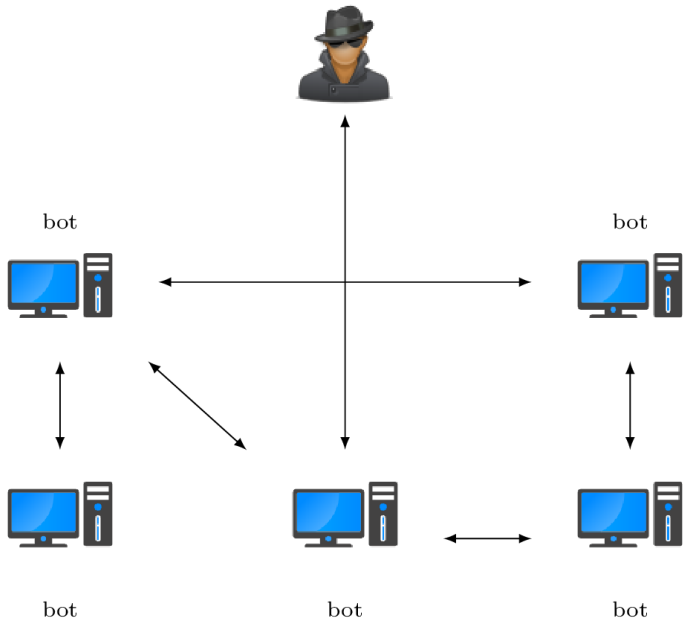
  Plusieurs bots connectés et administrés par un serveur C&C

BonWare – Topologies

- Centralisée



- P2P



BonWare – Topologies

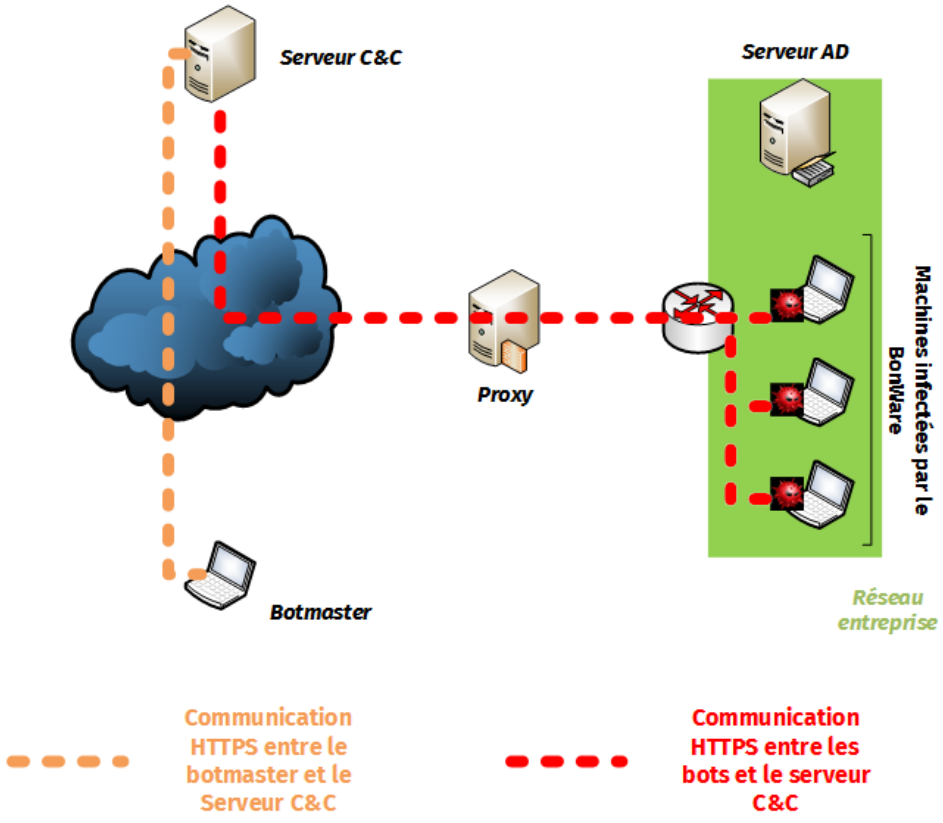
Infrastructure	Conception	Détection	Latence	Survie
Centralisée	Facile	Moyenne	Faible	Faible
P2P	Difficile	Faible	Moyenne	Moyenne
Non structurée	Facile	Haute	Haute	Haute

BonWare – Protocoles de communication

Protocole	Utilisation	Détection	Avantages	Inconvénients
IRC	Facile	Haute	Simple à utiliser	Protocole bloqué
DNS	Difficile	Faible	Encore peu connu	Trop de requêtes
HTTP(S)	Facile	Moyenne	Très utilisé	Parfois filtré

BonWare – Le projet

- Principe

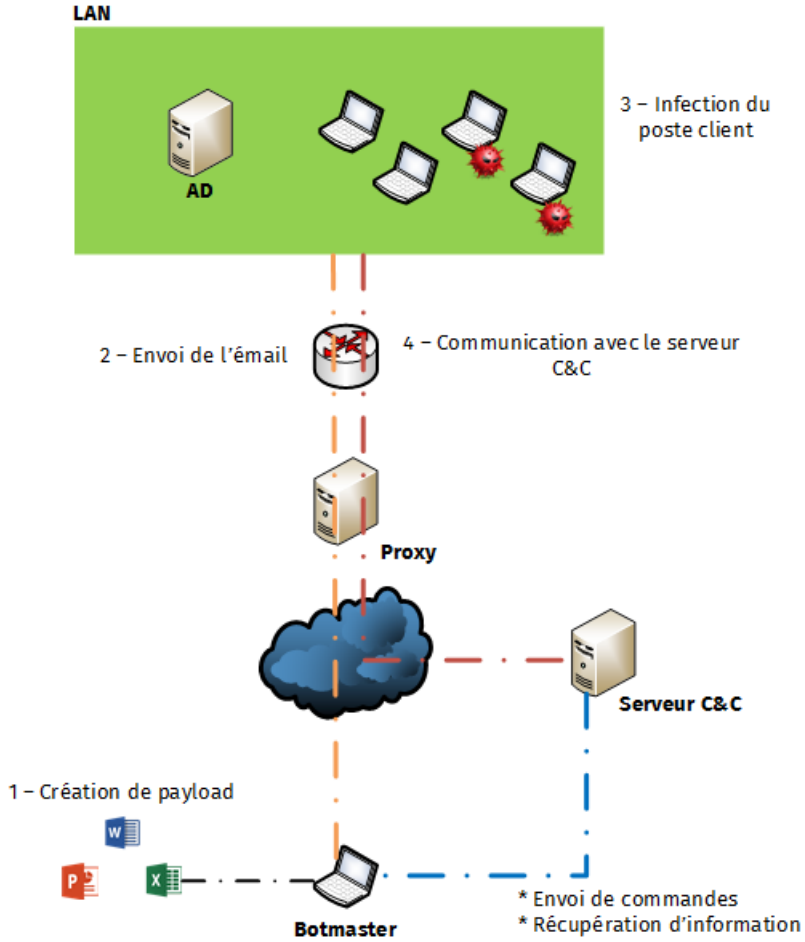


- Écosystème en 3 parties :
  - Le programme bot
  - Le serveur C&C
  - Une interface d'administration

BonWare – Fonctionnalités

- Capture d'écran
- Remote Shell
- Upload de fichiers
- Download de fichiers
- Auto suppression

BonWare – Scénario d'attaque



- Génération d'un payload (document office contenant la macro)
- Envoi de ce document au travers d'une campagne de phishing
- Infection du poste dès l'ouverture du document et activation de la macro
- Exécution de commandes à distance depuis le serveur C&C

BonWare – Retour d'expérience

- Le bonWare a été testé dans différents environnements

Environnements	Remarques
Laboratoire AlgoSecure	Test avec différentes solutions antivirales, aucune détection
PME	Détection de la macro lors du téléchargement dans le mail, mais pas de l'exécutable
Grand groupe	Aucune détection

Limites et roadmap

- Obfuscation de la macro
- Usage du BonWare à double tranchant

- Version 1.1 (réécriture avec des librairies Windows natives)
- Avoir notre propre obfuscateur
- Incorporer des outils SSI au sein du BonWare

Démo

Recommandations

- Vérifier la provenance d'un email avant d'ouvrir la pièce-jointe
- Ne pas activer les macros par défaut
- Éduquer les utilisateurs aux bonnes pratiques de sécurité
- Veiller à garder un socle à jour (OS, AV)
- Évaluer les équipements périmétriques

Principales références

- Éric Freyssinet, *Lutte contre les botnets : analyse et stratégie*, PhD thesis, Université Pierre et Marie CURIE, 2015
- Gunter Ollmann, *Botnet communication topologies : Understanding the intricacies of botnet command-and-control, Damballa*, 2009
- OpenDNS, *The role of DNS in botnet command & control*

Merci