

Les Réseaux BotNet

Mickaël BARROUX

Florent HACHE

Tony KHOSRAVI

Guillaume WRZYSZCZ

Mise en garde

Cette présentation est à exécuter dans un cadre strictement universitaire ou professionnel défini et expressément autorisé

- Article L323-1 du code pénal
 - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000€ d'amende
 - Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000€ d'amende
- Article L323-2 du code pénal
 - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000€ d'amende

Plan

1/ Présentation des Botnets

2/ Mise en place de Honeypots

3/ Le Botnet Waledac

4/ Démonstration

Introduction aux Botnets

- Botnet?
 - Réseau de bots
 - Bots IRC, calcul distribué, indexation web
- Réseau de machines zombies
 - > botnets malveillants (premières apparitions dans les 90's via IRC)

Les botnets malveillants – Usages et intérêts

- Différents usages à des fins malveillantes:
 - Attaque en dénis de service/chantage au déni de service, mise en place de logiciel espion, spam, phishing, DDoS, etc.
- Intérêts pour les pirates:
 - Motivation économique
 - Motivation idéologique
 - Motivation personnelle

Les botnets malveillants – Intérêts (suite)

“Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us. The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

You will also receive several bonuses.

- 1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about \$ 100 per night, for you it will cost only 70 \$ per day.*
- 2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.”*

Les botnets malveillants - Principe de fonctionnement



Les botnets malveillants - Chiffres

- Février 2010: 4000 à 5000 botnets actifs
- 2009: 5 millions de machines compromises dans un réseau de botnets destiné au spam (MessageLabs)
- 2007: $\frac{1}{4}$ machines faisant partie d'un botnet (Vint Cerf, co-inventeur de TCP/IP)

Risques Juridiques

- Ils sont différents en fonction de l'utilisation du botnet
- Jusqu'à 47 mois de prison pour du spam
- 10 ans de prison pour déni de service

Honeypots

- Nepenthes, pour émuler des failles windows
- Webtrap pour émuler des failles au niveau web
- Kojoney pour émuler un serveur SSH avec des comptes vulnérables au brute forcing

Résultat des Honeypots

La mise en place des honeypots décrite dans la section précédente a permis de récolter sur deux semaines :

- **10552** requêtes web malveillantes
- **431** sites hébergeant des fichiers malveillants
- **12627** attaques sur nepenthes
- **14** scripts PERL
- **20** scripts PHP
- **10** binaires Unix, win32

Analyse des scripts

```
##[ KONFIGURASI IRC ]##
my @servers = ("irc.byroe.net");
my %bot      = (
    nick      => "good[".int(rand(100))."]",
    ident     => "good".int(rand(100)),
    chan      => ["#Dragon_fly"],
    server    => $servers[rand(scalar(@servers))],
    port      => "6667"
);

my %boss = (
    Dragon_fly => {
    pass      => "kunci",
    status    => "admin",
    cryptz    => 0,
    login     => 0
    },

```

Analyse des binaires

Plus difficile mais résultat plus intéressant que les scripts

1^{ère} méthode :

- Désassembler le binaire
- Retracer l'exécution en exécutant les fichiers assembleurs

2^{ème} méthode :

- Exécuter le binaire dans un environnement restreint
- Utilisation du soft sandbox

Analyse des binaires

Outbound traffic (potentially malicious)

- **Attention!** There was a new connection established with a remote IRC Server. The

```
NICK n[USA|XP]0002913
USER 4625 "" "lol" :4625
JOIN #po#
NICK [USA|XP]9349820
USER 4548 "" "lol" :4548
```

Infiltration et analyse des botnets IRC

- Se connecter sur le salon de discussion du bot
- Passer par un réseau anonyme ou un proxy pour masquer son IP
- Se faire passer pour une machine vulnérable
- Attendre que les pirates envoient des commandes aux robots

Actions enregistrés sur les botnet étudiés

- La propagation
- Vol de numéro de carte bleue
- Envoi de spam
- Phising
- Brute force de comptes
- Stockage de warez

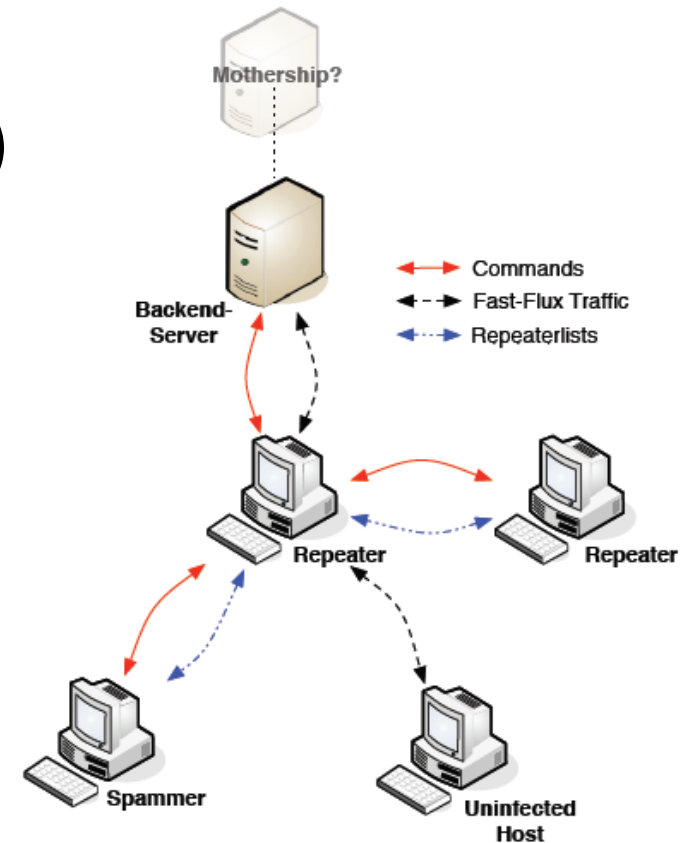
Cas d'étude : Waledac

- BotNet Waledac
 - Peer to Peer BotNet
 - L'un des plus gros BotNet aux Etats-Unis
 - Découvert par Microsoft

- Plan de l'étude
 - Structure de Waledac
 - Infiltration du BotNet Waledac
 - Résultat de l'infiltration

Waledac : Structure

- Spammer
 - IP privée (derrière un routeur NAT)
 - Exécute les commandes
 - Envoi les résultats
- Repeater
 - Point d'entrée pour les bots
 - IP public
 - Agent fast-flux
- Backend-Server
 - Transmet les requêtes au *Mothership*



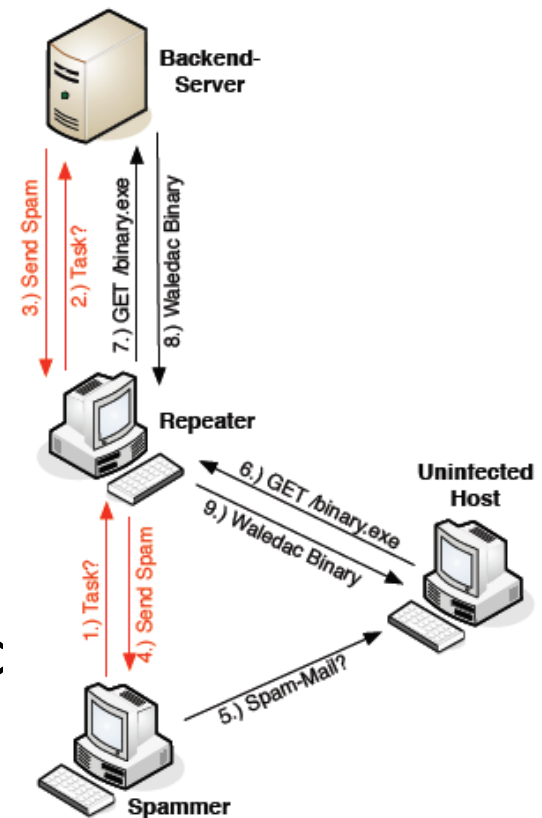
Waledac : Structure

- Communication entre Repeaters et Spammers
 - Echange de la liste des Repeaters actifs
 - URL : Nouvelle liste (Au bout de 10 tentative ratées)

- Peer to Peer uniquement pour le bas niveau

Waledac : Structure

- Mécanisme d'ajout d'un bot par mail
 - Le Spammer demande quoi faire
 - Envoi de la commande de spam par le Backend-Server
 - Spam par le Spammer
 - Récupération de l'exécutable par l'host non infecté
 - Infection par l'exécutable Waledac



Waledac : Infiltration et résultats

- Walowdac
 - Clone d'un repeater, répond directement au lieu de transférer la requête
 - Insertion d'IP de Walowdac dans le BotNet Waledac
- Données collectées
 - Information personnelle (FTP, HTTP, POP3)
 - ID + AS = unique pour chaque Bot
 - 403 685 bots recensés

Waledac : Mis KO par Microsoft

- BotNet stoppé par Microsoft
 - Blocage des noms de domaine majoritairement infectés par Waledac
 - Juste stoppé, les ordinateurs infectés le restent
- Prévention
 - Mise en place d'outils d'analyse pour détruire le BotNet
 - Eviter que Waledac soit relancé

Démonstration



Conclusion

- Les réseaux de botnets sont donc dangereux et assez difficiles à appréhender car on ne connaît pas l'étendue de ces réseaux et leur pouvoir
- Traçage faisable avec la mise en place de honeypots
- Questions ?

Bibliographie

- <https://pi1.informatik.uni-mannheim.de/filepool/publications/waledac-paper.pdf>
- <http://igm.univ-mlv.fr/~dr/XPOSE2009/botnets/analyse.html>
- <http://nonameblog.info/sur-la-piste-d-un-botnet/>
- <http://www.shadowserver.org/wiki/>
- <http://www.korben.info/location-dun-botnet-combien-ca-coute.html>
- <http://www.lemondeinformatique.fr/actualites/lire-des-chercheurs-montent-un-botnet-pour-comprendre-son-fonctionnement-32471.html>
- <http://fr.wikipedia.org/wiki/Botnet>
- <http://www.tech-faq.com/botnet.html>
- http://www.securite-informatique.gouv.fr/gp_article276.html
- http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1030284,00.html