Botnets,

les fantômes de l'internet

Iheb Khemissi - iheb.khemissi@gmail.com
Joris Brémond - joris.bremond@gmail.com

6 Novembre 2009

Définition d'un botnet

Botnet (ro**BOT NET**work)

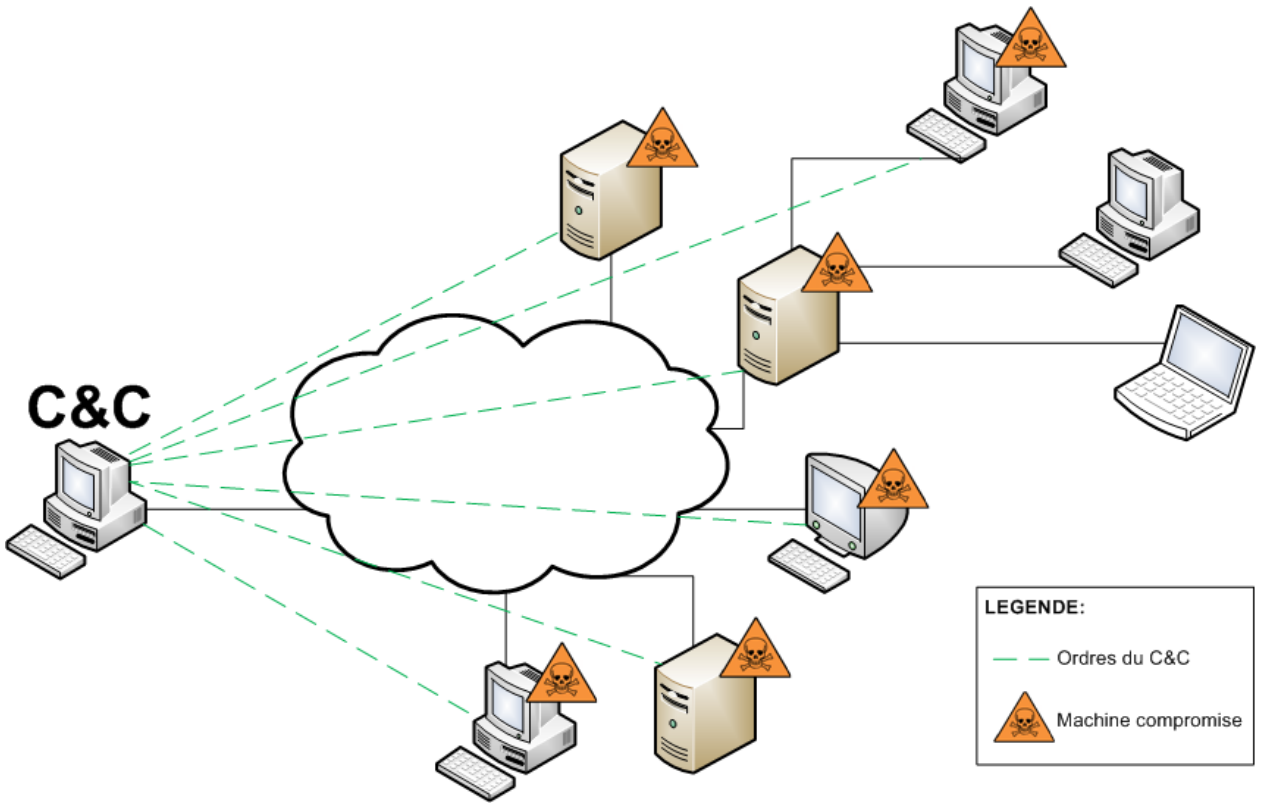
- première apparition : GTBot en 1998
- un réseau d'ordinateurs compromis (zombies)
- réseau géré par un Botmaster et/ou des Bots (programmes malveillants)
- OS concernés : Windows (mais aussi Linux et MacOS)

Définition d'un botnet

Vinton Cerf (le père d'Internet) :
Le problème des botnets serait désormais d'ordre pandémique : un quart de tous les ordinateurs connectés au réseau appartiendrait avant tout à un botnet et serait donc sous le contrôle de pirates.

Définition d'un botnet

Architecture centralisée :

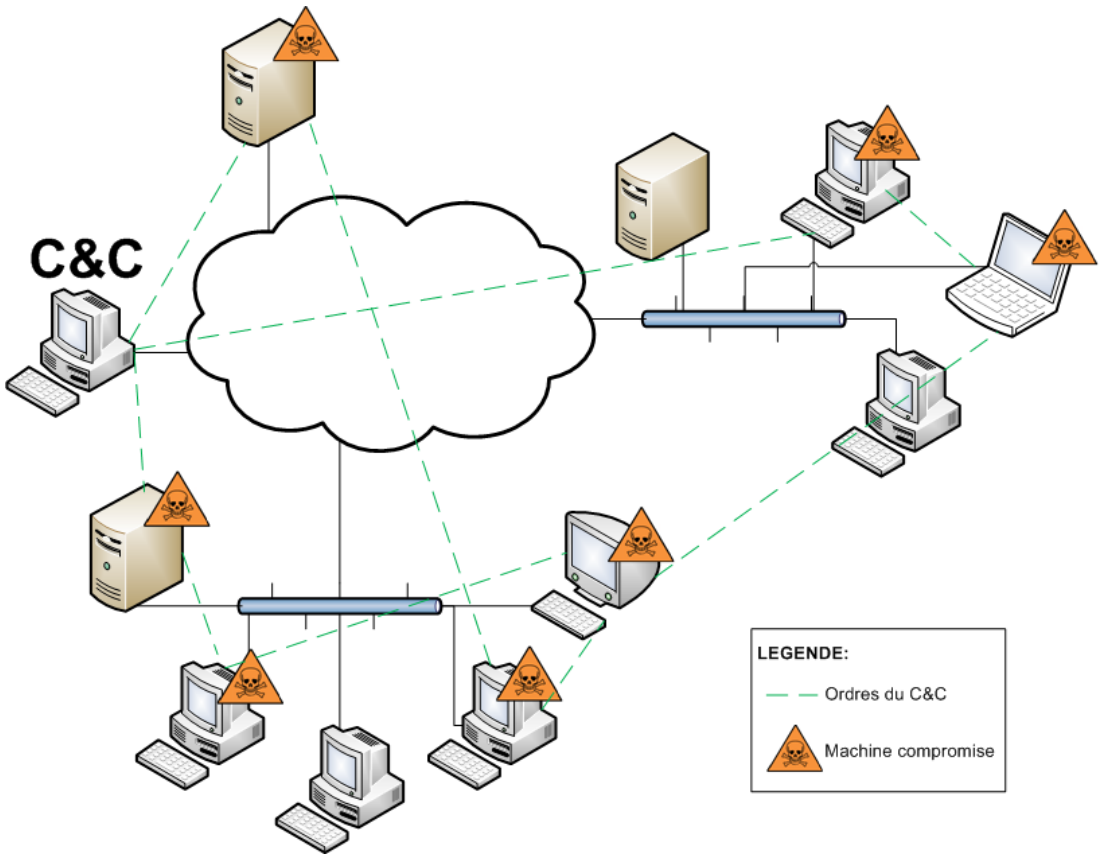


Exemples

Botnets IRC et HTTP

Définition d'un botnet

Architecture P2P :



Exemples

Botnets P2P (utilisation du réseau Gnutella par exemple)

Définition d'un botnet

Tailles des Botnets

De l'ordre de dizaines, voir de centaines de milliers de machines zombies

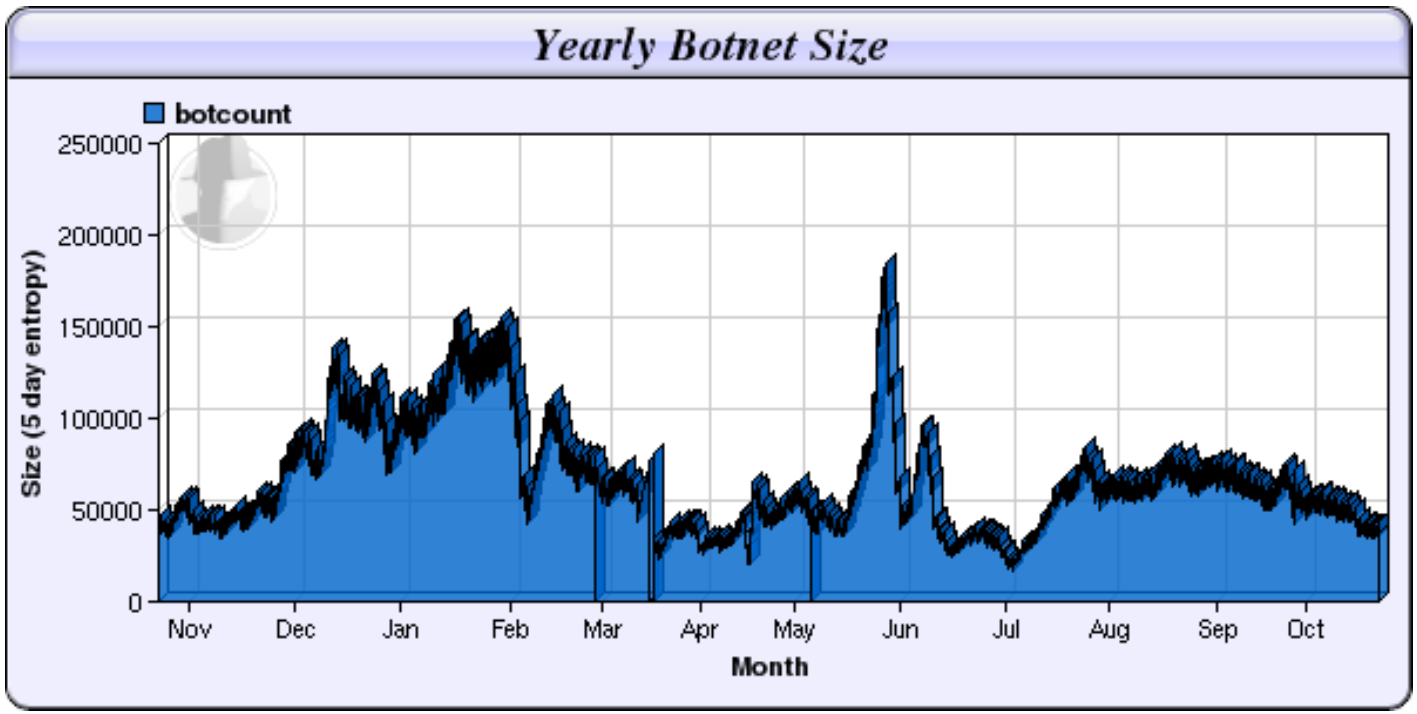
Les plus grands botnets ainsi que leurs nombre de machines

- Srizbi : 315 000
- Bobax : 185 000
- Rustock : 150 000
- Storm : 85 000
- NuCrypt : 20 000

Définition d'un botnet

Evolution du nombre de botnets

de Novembre 2008 jusqu'à Octobre 2009



Source : ShadowServer.org Octobre 2009

Motivations

Gain d'argent

- Spam : motivation numéro 1 (marché noir très actif)
- Chantage : pour éviter les DDoS
- Vente et location : de nouvelles ressources
- Vol d'informations : CB, Bourse, ...
- Clics frauduleux : Google AdSense, ...

Motivations

Patriotisme

- Attaque des sites estoniens et géorgiens par des pirates russes
- Déni de service contre les sites de radio américaine (Radio/Free Europe) à l'occasion de la commémoration des victimes de Tchernobyl
- Tentative d'attaque du site de CNN par des pirates chinois

Motivations

Auto-protection

- Utilisation de passerelles pour ne pas pouvoir remonter jusqu'à la source
- Utilisation des techniques fast-flux

Motivations

Contre-attaque

Moyen de pression/vengeance contre des mesures prises par le gouvernement ou les acteurs majeurs d'un domaine
Par exemple :

- Déni de service du site d'Hapodi
- Déni de service du site de Castlecops (organisation anti-spam)

Fonctionnement des botnets

IRC

- Architecture centralisée
- Simplicité de mise en oeuvre (mIRC, ...)
- Utilisation des canaux IRC (topics, messages) pour l'envoi des commandes vers les bots
- Performance (non gourmant en bande passante)

Points faibles

- Vulnérabilité du botnet (serveur central)
- Connexion en permanence
- Facile à détecter (filtrage du flux IRC)

Fonctionnement des botnets

HTTP

- Architecture centralisée
- Difficile à détecter (flux HTTP + SSL)
- Connexion vers des serveurs web pour récupérer les ordres

Points forts

- Connexions régulières entre les bots et le C&C (non permanente)
- Recherche des ordres dans des forums, avec des mots clés ou même dans des images (stéganographie)

Point faible

- Vulnérabilité du botnet (serveur central)

Fonctionnement des botnets

P2P :

- depuis 2004
- architecture décentralisée
- indépendant de l'architecture DNS
- pas de vision globale du réseau par un bot
- le botmaster donne les informations comme un bot faisant partie du réseau
- l'information transite de voisin en voisin

Points forts

- difficile à repérer
- très difficile à neutraliser

Fonctionnement des botnets

Méthodes d'infections

- code malveillant envoyé en pièce jointe d'un e-mail
- utilisation de failles liées aux navigateurs
- exploitation de failles de logiciels connus
- fichier d'apparence saine, mais contenant un cheval de Troie (jeux, logiciels, etc.)
- code malveillant camouflé dans des cracks téléchargés sur les réseaux P2P (Windows 7 RC)
- des machines infectées peuvent en contaminer d'autres (scan réseau, exploitation de failles)
- utilisation de rootkit permettant le camouflage du botnet

Fonctionnement des botnets

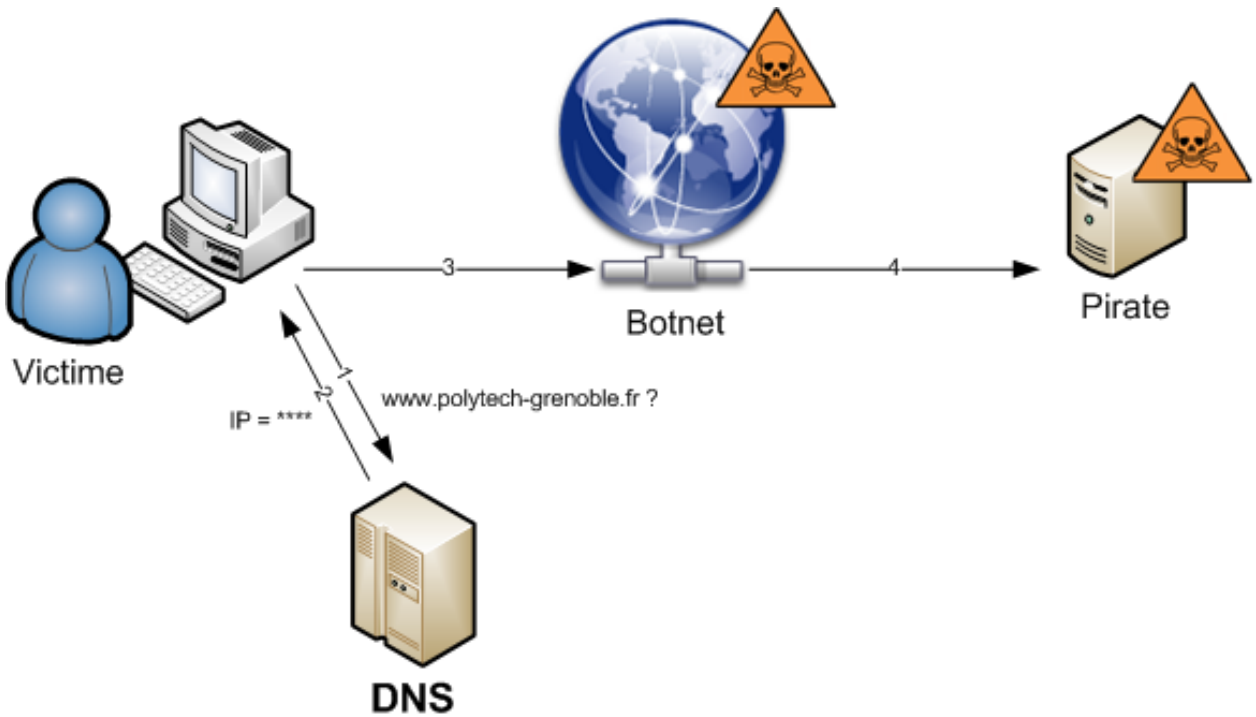
Fast-flux

- Utilisation de passerelles intermédiaires entre le pirate et ses victimes
- Camouflage de l'adresse du pirate

Plusieurs méthodes

- Fast-flux simple (Single-flux)
- Fast-flux double (Double-flux)
- Fast-flux double évolué

Fonctionnement des botnets



Illutration de la technique de fast-flux

Fonctionnement des botnets

Fast-flux simple

Fast-flux simple

- Utilisation d'un ou de plusieurs domaines
- Bot : choix de l'URL destination en fonction du type de requête
- Changement régulier des IP associés au nom du domaine (DNS)
- Utlisation de machines zombies en Reverse Proxy (transfert des requêtes de la victime vers le serveur réel)

Point fort

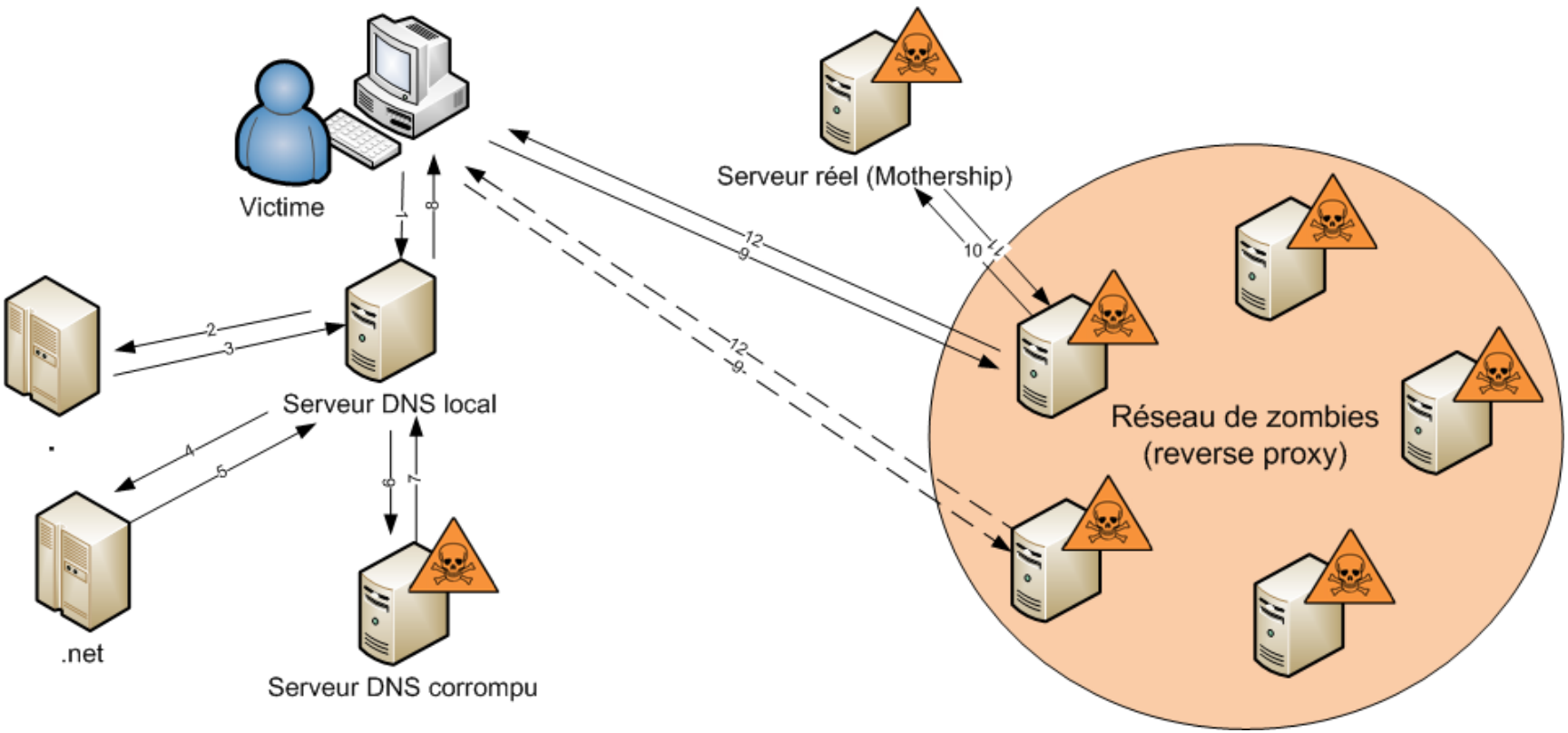
- Camouflage de l'IP du serveur réel

Point faible

- Adresse du serveur de noms compromis

Fonctionnement des botnets

Fast-flux simple



Exemple d'une requête en utilisant le fast-flux simple

Fonctionnement des botnets

Fast-flux double

Fast-flux double

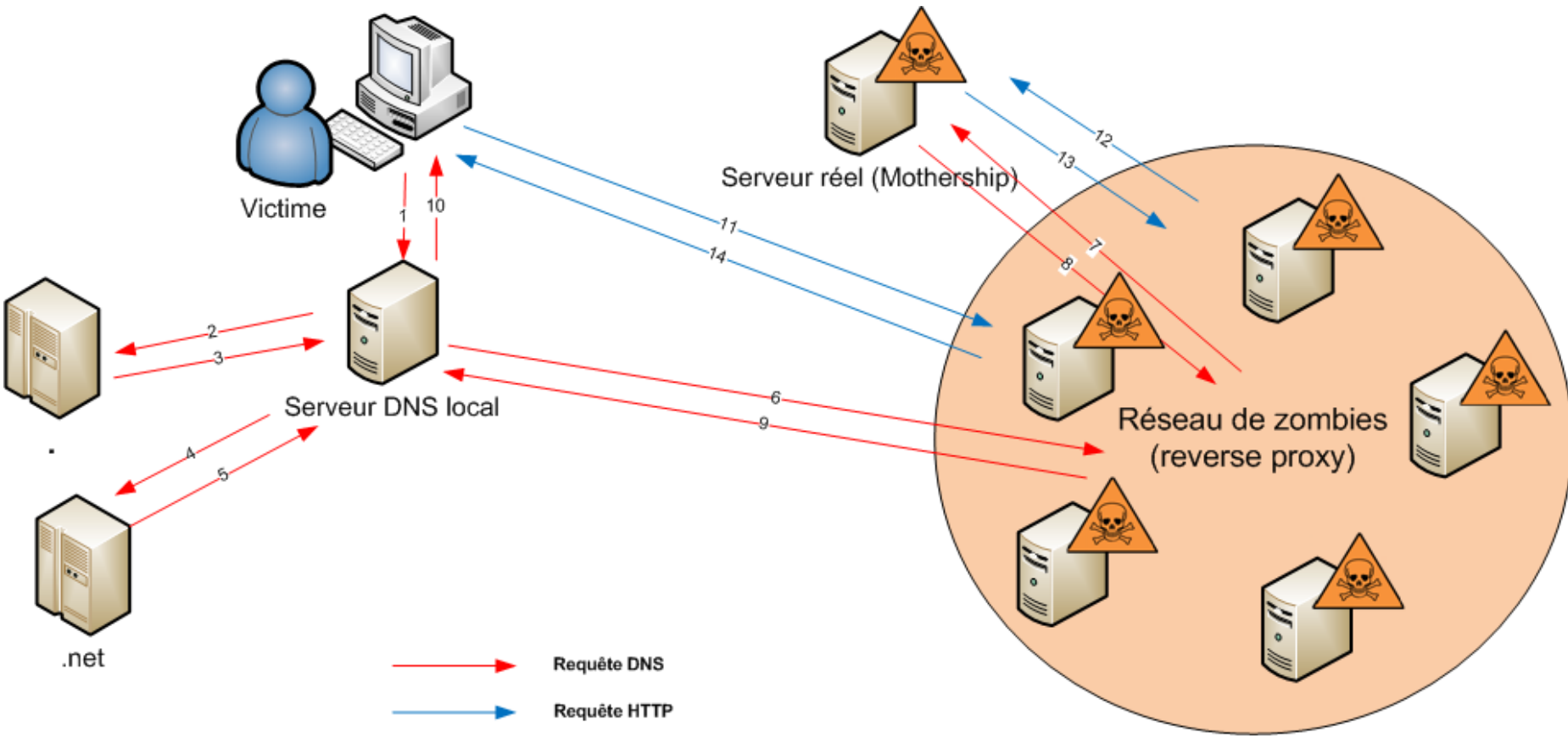
- Fast-flux simple +
- redirection des requêtes effectuées au serveur DNS ayant autorité sur la zone vers les machines compromises
- changement de l'association NS/IP régulier auprès du registrar
- choix judicieux du registrar (peu regardant sur les activités des clients)

Point fort

- disponibilité quasi optimale
- résiste à l'arrêt d'un serveur DNS

Fonctionnement des botnets

Fast-flux double



Fonctionnement des botnets

Fast-flux double évolué

Fast-flux double évolué

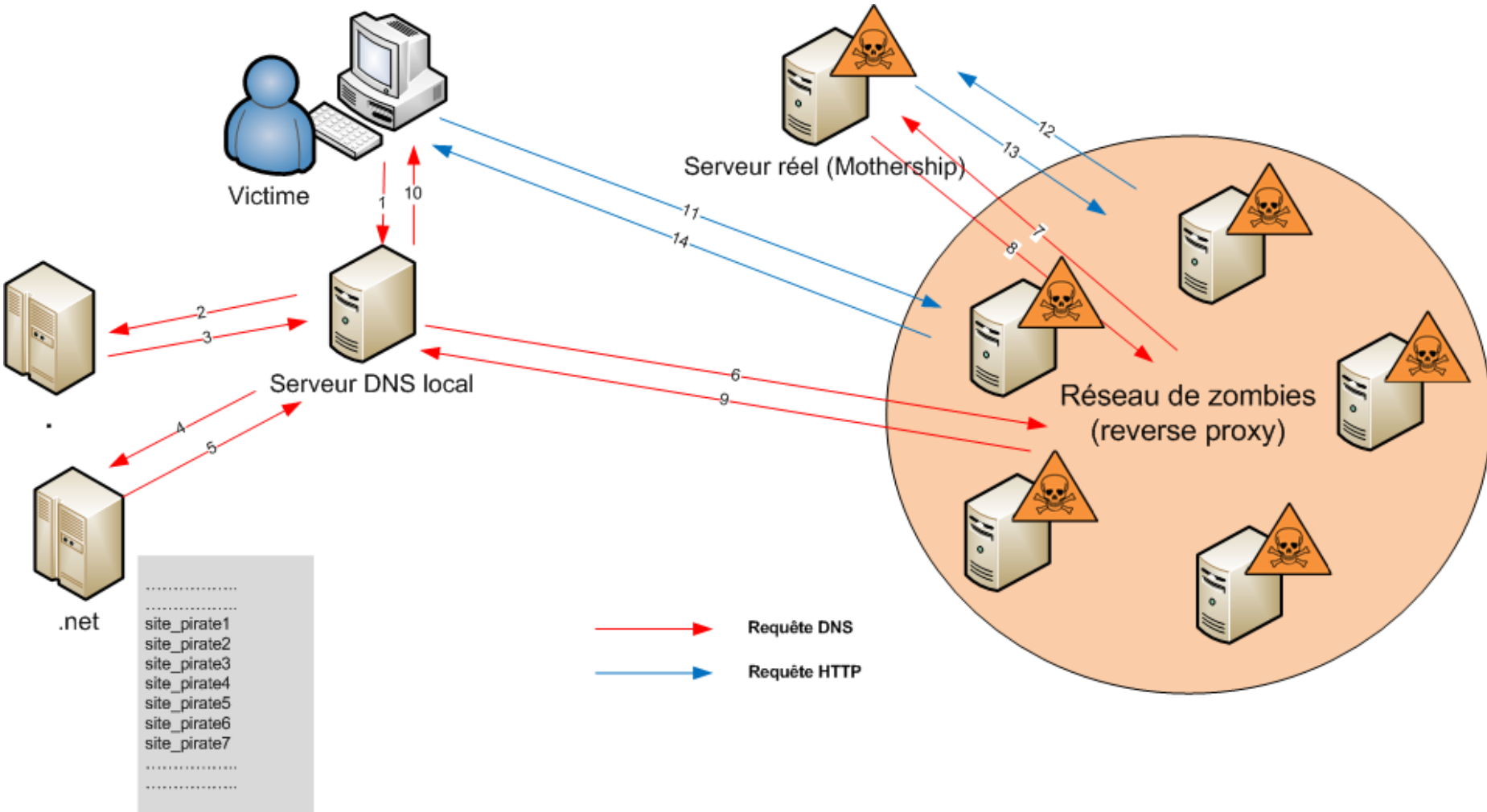
- Fast-flux double +
- plusieurs noms de domaine
- sur chaque nom de domaine, redirection vers l'architecture double-flux

Point fort

- disponibilité optimale
- résiste à la suppression d'un domaine dans le registrar

Fonctionnement des botnets

Fast-flux double évolué



Evolution

Utilisation des techniques des botnets modernes

- Cloud Computing
- Grid Computing (Super-calculateur virtuel)
- Montée à l'échelle (applications, web, ...)
- Tolérance aux fautes
- Test de charge

La recette (logiciels Open Source ou gratuits) :

- Couche matérielle : ordinateurs + réseau
- OS léger : Ubuntu Server Edition (JEOS)
- Logiciel de virtualisation : Enomalism
- Sécurité : Open VPN
- Communication : eXtensible Messaging and Presence Protocol

Prévention et détection

Deux points important doivent être pris en compte pour se protéger des botnets :

- sensibilisation des utilisateurs
- gestion du parc informatique adéquate

Attention :

La prévention diminue les risques mais ne permet pas de les éliminer complètement

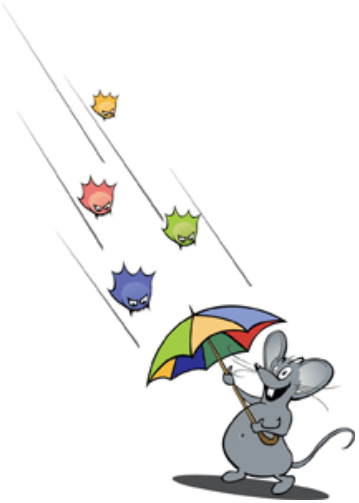


FIGURE: source : http ://blog.eun.org/

Prévention et détection

Côté utilisateur et poste client

Installation d'outils de détection :

- logiciel antivirus
- pare-feu personnel
- outil de détection de logiciels espions

Mise à jour régulière :

- système d'exploitation
- logiciel antivirus (et s'assurer de la validité de celle-ci : désactivation possible par le botnet)
- navigateur web (ne pas installer de plugins non signés)
- client de messagerie
- logiciel de messagerie instantané
- logiciels de bureautique

Prévention et détection

Côté utilisateur et poste client

Précautions :

- ne pas travailler en mode administrateur
- ne pas désactiver les mises à jour automatiques
- ne pas suivre les liens contenus dans les spam
- être vigilant sur les pièces jointes
- les correctifs logiciels ne sont jamais envoyés par mail
- droit de lecture sur les exécutables si possible et contrôle d'intégrité
- ne pas télécharger n'importe quoi (cracks, etc.) !

Prévention et détection

Côté administrateur

- existence de listes noires : RBLs (Real-time Black Lists) ⇒ génération de filtres
- surveillance du trafic réseau (protocole IRC, P2P) ⇒ NDIS (Network Intrusion Detection System)
- être vigilant avec les applications PHP sur serveur WEB (failles de sécurité)
- gestion stricte des mots de passe
- définition d'une politique pour la gestion des correctifs de sécurité
- ne pas laisser de coté les ordinateurs nomades
- droit restreint pour les utilisateurs
- analyse des journaux après infections (découverte nouvelles machines infectées, trouver le C&C)
- mise en place de pare-feu, proxy, filtrage SMTP, VLAN

Commerce de botnets

- Des propriétaires de botnets louent ou vendent une partie ou la totalité de leur infrastructure
- Ces botmasters peuvent aussi vendre leurs services : réalisation d'une attaque DDoS, envoi de SPAM, etc.

Commerce de botnets

Les tarifs :

- 2 à 25$: informations de carte de crédit
- 7$: compte PayPal
- 8$: compte World of Warcraft
- 15$: infection de 1000 systèmes
- 25 à 100$: par attaque DDoS, 10 premières minutes offertes, puis 20$ l'heure, 100$ la journée
- 495$: 20 millions de spams pendant 14 jours

(source : laboratoire de sécurité G DATA - 2007/2008)

Commerce de botnets

MPack : Outil pirate basé sur PHP - Vendu sur certains forums environ 700$

Fonctionnalités :

- exploite les vulnérabilités des navigateurs
- installe à distance des malwares grâce à ces vulnérabilités

Support :

- un an de support gratuit (Mise à jour, bug, etc.)
- possibilité de télécharger de nouveaux exploits, entre 50 et 150$

Commerce de botnets

Exemple BBC (14 Mars 2009)

- achat d'un botnet de 22000 ordinateurs, pour une émission sur les nouvelles technologies
- prix de la transaction : entre 5000 et 7000 euros
- test d'envoi massif de spams
- réalisation d'une DDoS sur le site Prevx (ayant donné son accord)

Polémique :

- la BBC a payé des cybers criminels pour l'achat du botnet !

Démonstration

Fast-flux

Derniers botnets fast-flux découverts par abuse.ch (02/11/2009)

Conclusion

Conclusion

- Technique de communication de plus en plus pointue et difficile à découvrir
- Des bots de plus en plus intelligents
- Les utilisateurs manquent de sensiblisation face aux menaces

Sources

- **CLUSIF (Club de la sécurité de l'information Français) - 2009 - Bots et botnets**
  https ://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2009-Bots-et-Botnets.pdf
- **Martin Overton, IBM Global Services**
  Bots and Botnets : Risks, Issues and Prevention
- **John Kristoff Presentation (2004)**
  http ://www.nanog.org/meetings/nanog32/
- **Botnet count**
  http ://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCounts
- **Build your own botnet with open source software**
  http ://howto.wired.com/wiki/Build_your_own_botnet_with_open_source_software
- **Mobile botnets**
  http ://www.daemon.be/maarten/mobbot.html
- **Botnet**
  http ://en.wikipedia.org/wiki/Botnet
- **MADYNES - INRIA Nancy Grand Est, CNRS, Nancy-Université : Jérôme François, Radu State,Olivier Festor**
  Les botnets et la supervision à large échelle
- **Attack of the Bots**
  http ://www.wired.com/wired/archive/14.11/botnet.html

Sources

- **Adrien GUINAULT, consultant sécurité Xmco Partners** Les Fast-Flux Networks, http ://www.xmcopartners.com/article-fast-flux.html
- **AuthSecu : le site de la sécurité réseau des entreprises** http ://www.authsecu.com/affichage-news/981-news-securite-spams-les-botnets-s-adaptent-en-changeant-de-strategie.htm
- **A botnet by any other name** http ://www.securityfocus.com/columnists/501
- **Global botnets : summary report** http ://atlas.arbor.net/summary/botnets
- **First linux botnet (12/09/2009)** http ://www.theregister.co.uk/2009/09/12/linux_zombies_push_malware/
- **Premier botnet de MacOS (iBotnet) (20/04/2009)** http ://www.itespresso.fr/le-premier-botnet-compose-de-mac-zombies-a-ete-repere-24852.html
- **Offrez vous un botnet pour noel** http ://www.itespresso.fr/securite-pour-noel-offrez-vous-un-reseau-dordinateurs-zombies-31331.html

Questions

Merci pour votre attention

Questions ?