Présentation général des botnets

Guillaume Pillot

Club de Hacking de l'Université Laval

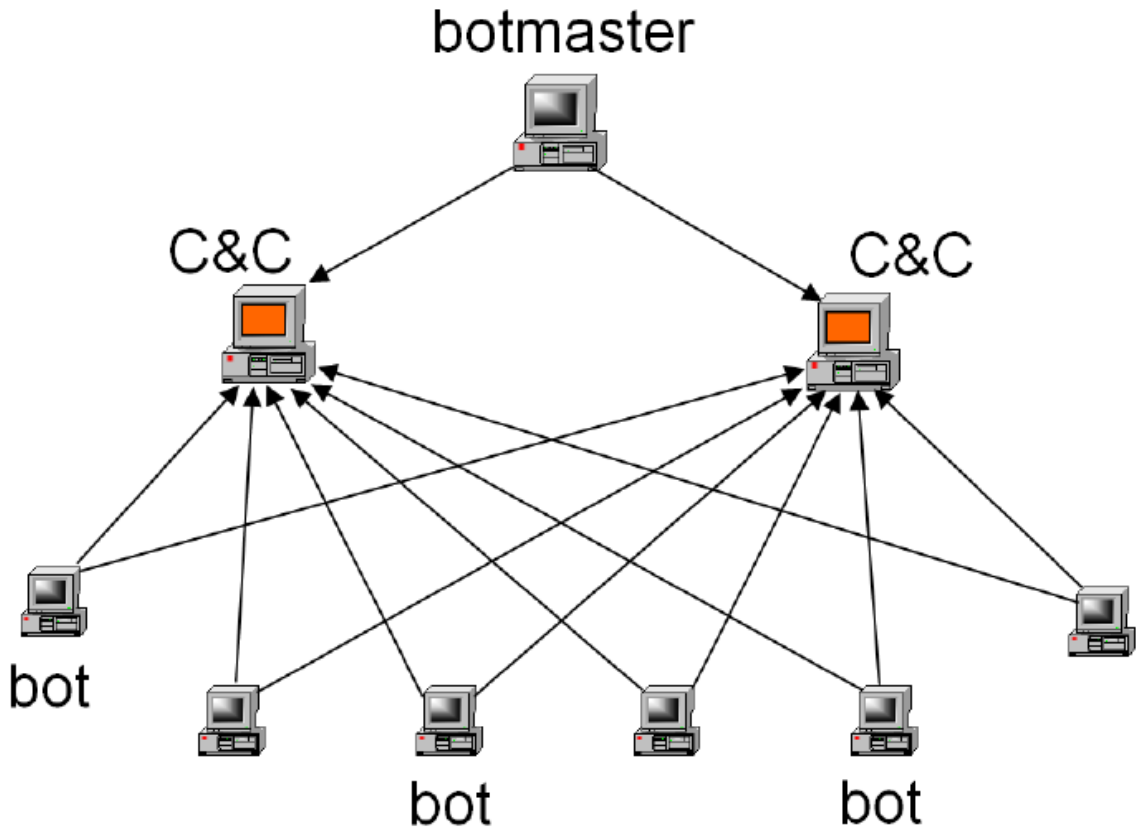
5 Mai 2015

Qu'est qu'un botnet ?

- Un botnet est un réseau de bots (nommé aussi zombies)
- Un bot est une machine compromise
- Les botnets permettent les attaques DDOS, l'envoi de spam et bien d'autres attaques
- Un botnet est habituellement composé de milliers de machines
- Les autorités ont du mal à lutter contre ces réseaux

Botnet centralisé

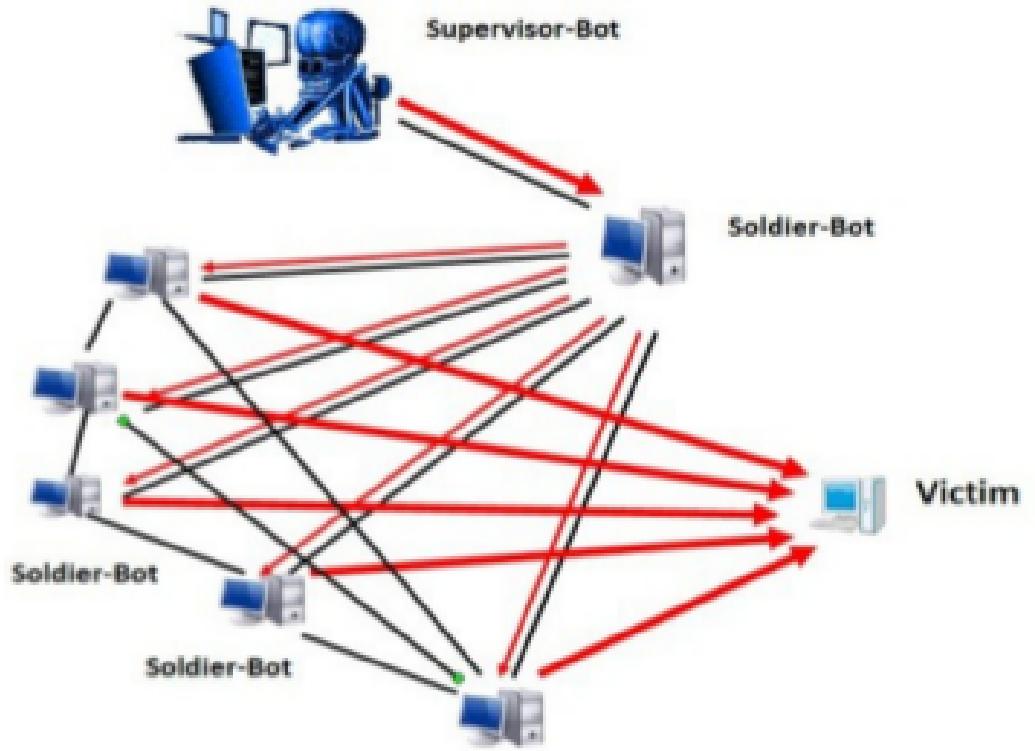
- Premier botnet
- Serveur de Command&Control (C&C) envoient les instructions aux bots
- Facile à gérer mais facile à détecter et neutraliser



Architecture classique d'un botnet centralisé

Botnet P2P

- Botnet actuel
- Plus difficile à détecter mais plus difficile à gérer



Architecture d'un botnet P2P

Techniques de détection

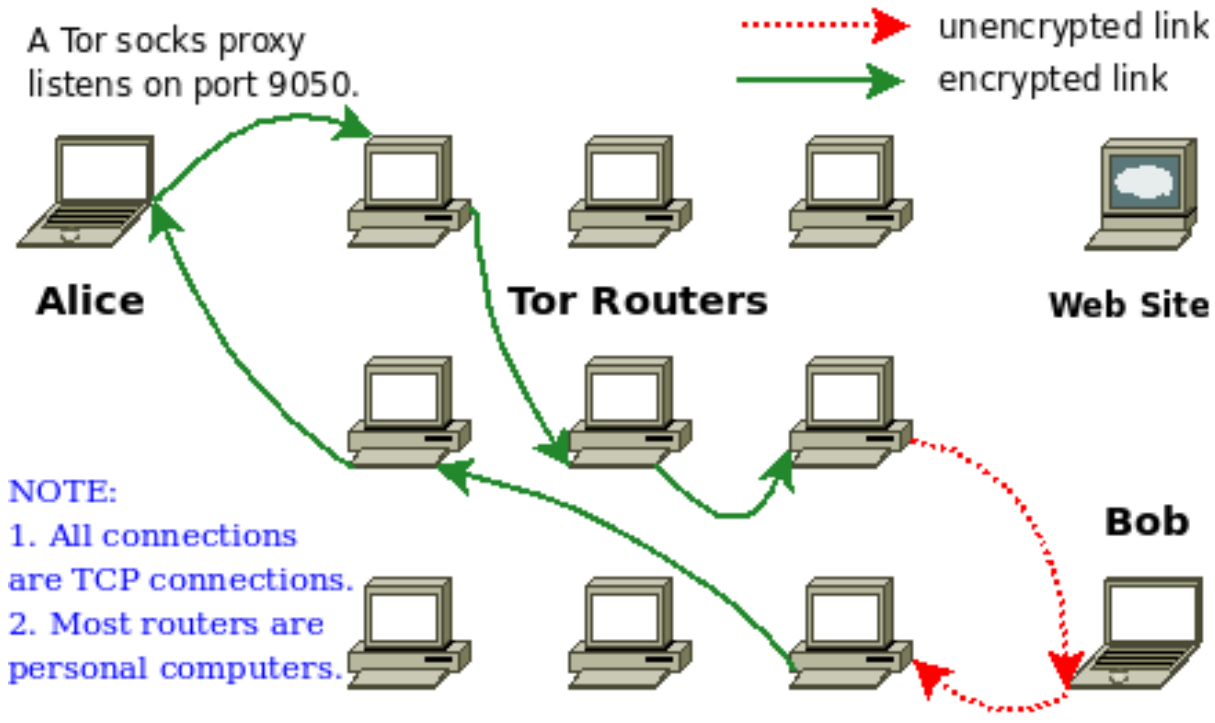
- Honeypot
- Adresses IP : ne peut fonctionner que si l'on connaît le botnet
- Analyse du trafic DNS
- Anomalie dans le réseau : engendre un fort taux de faux positif
- Data mining
- Sybil Attack (pourrir le réseau P2P)

OnionBot

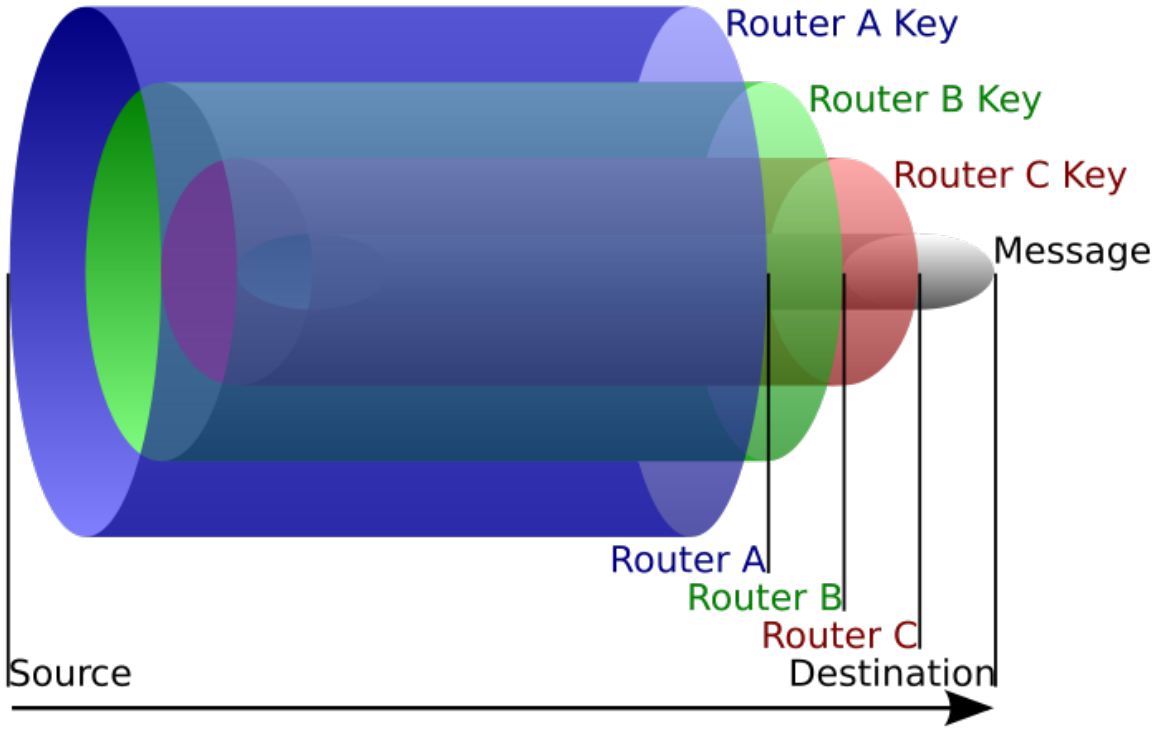
- Botnet de nouvelle génération
- Utilisation du réseau anonyme TOR

The Onion Router

- Réseau anonyme le plus populaire
- Communication par circuit de machines
- Identification par adresse .onion anonyme

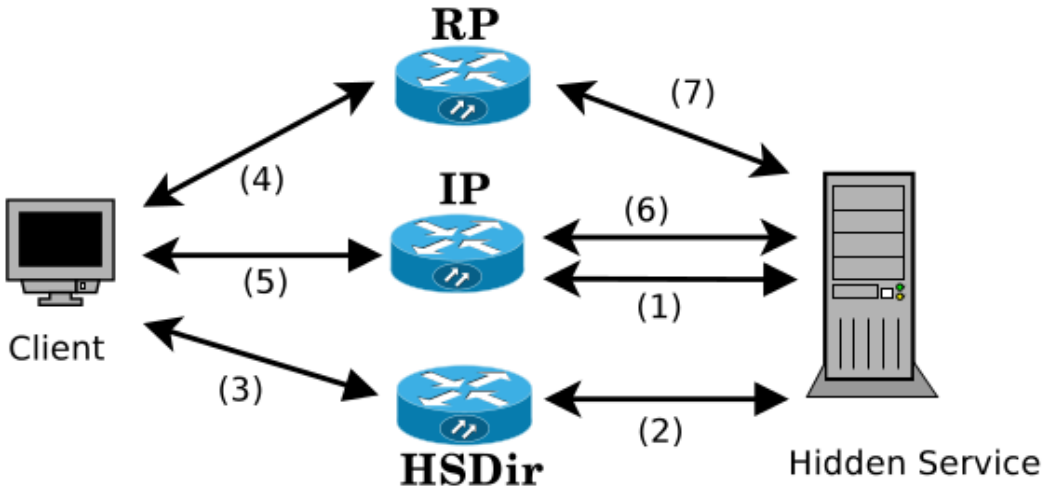


Circuit aller-retour dans le réseau TOR

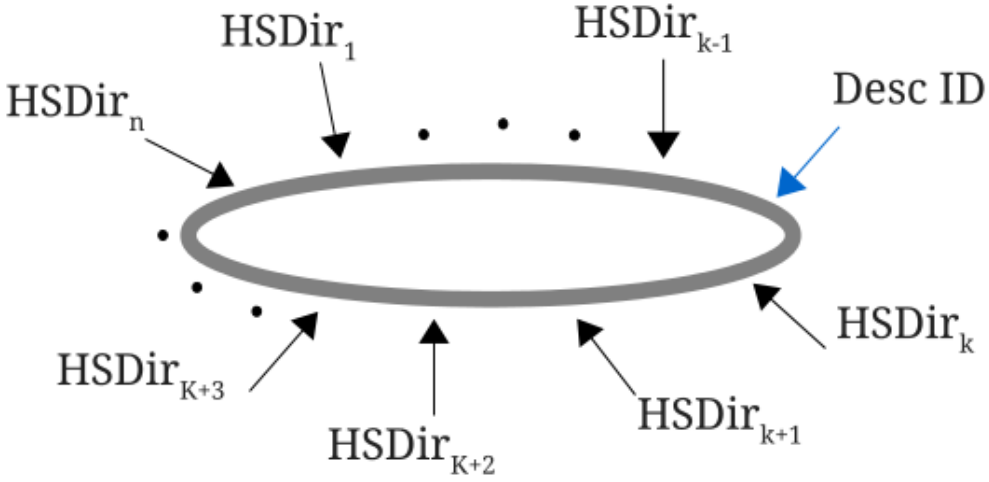


Couche d'encryption d'un message

Service caché



Étapes de connexion à un service caché



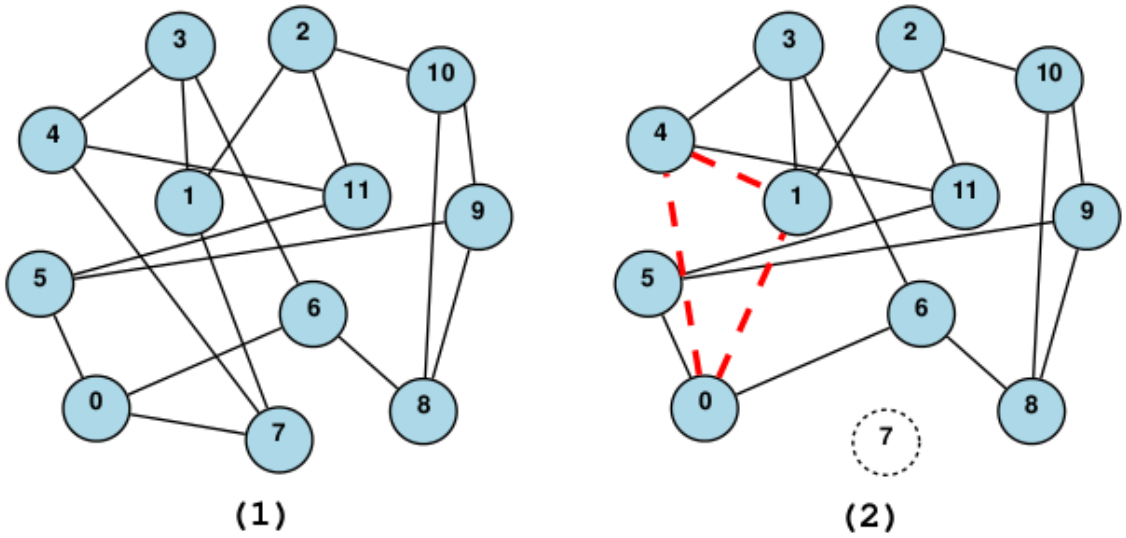
Anneau des relais HSDir

Fonctionnement d'OnionBot

- Infection
- Ralliement ou Bootstraping
- Attente
- Éxécution

Maintenance du graphe de communication d'OnionBot

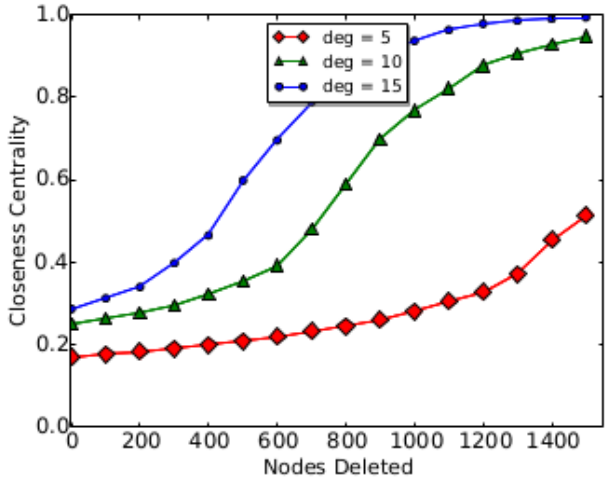
- Graphe du voisin du voisin
- Réparation
- Élagage (pruning)



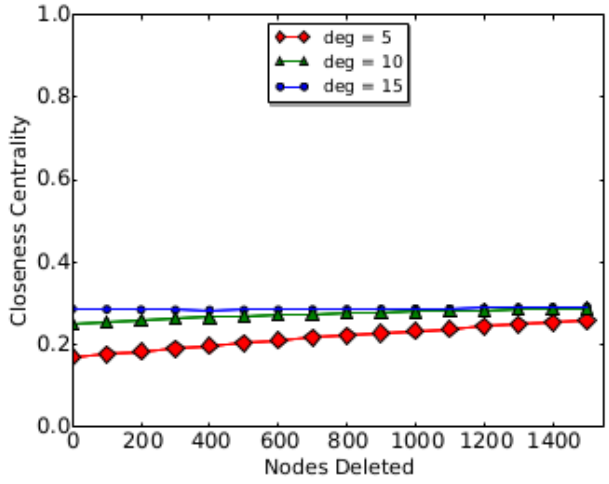
Effacement d'un noeud

Évaluation d'OnionBot

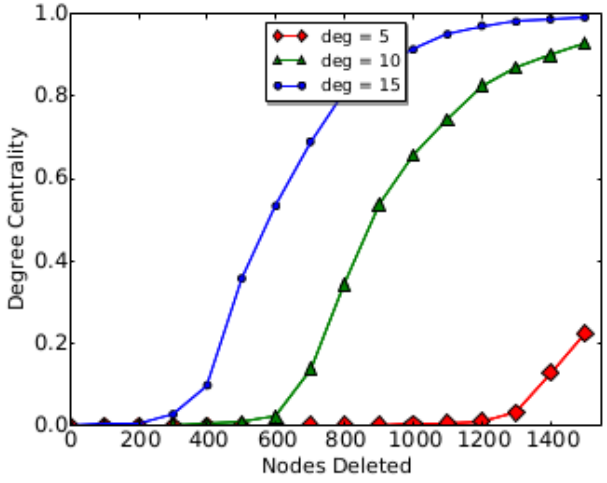
- Test de la robustesse du réseau avec la proximité de centralité et le degré de centralité



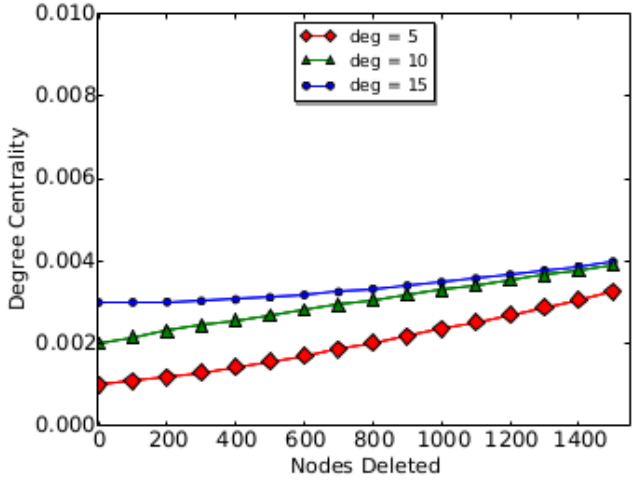
(a) without pruning



(b) with pruning



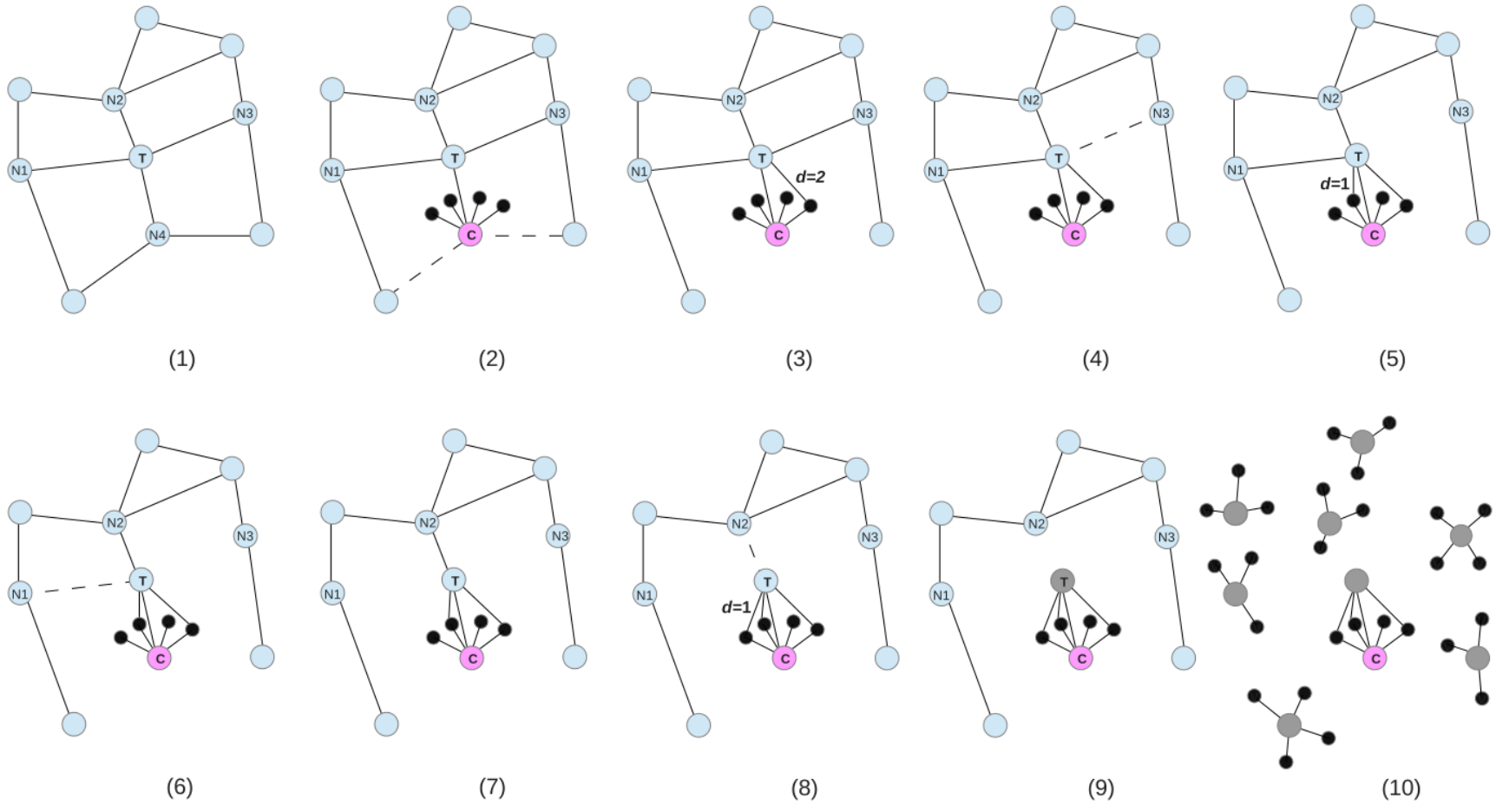
(c) without pruning



(d) with pruning

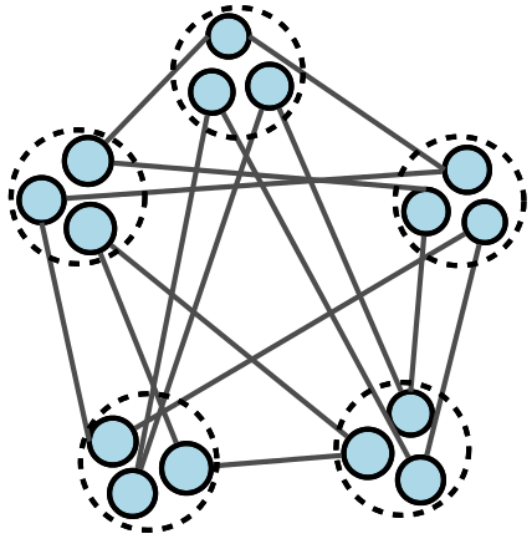
Atténuation d'OnionBot

- Devenir un relais HSDirs
- Sybil Onion Attack Protocol (SOAP)



Attaque SOAP

SuperOnionBot



SuperOnion avec n=5,m=3 et i=2

Autres

- Lien vers l'article : `http://arxiv.org/pdf/1501.03378v1.pdf`
- Organisation NorthSec
- ihack
- Questions sur un autre sujet ?