Détection comportementale de malware P2P par analyse réseau

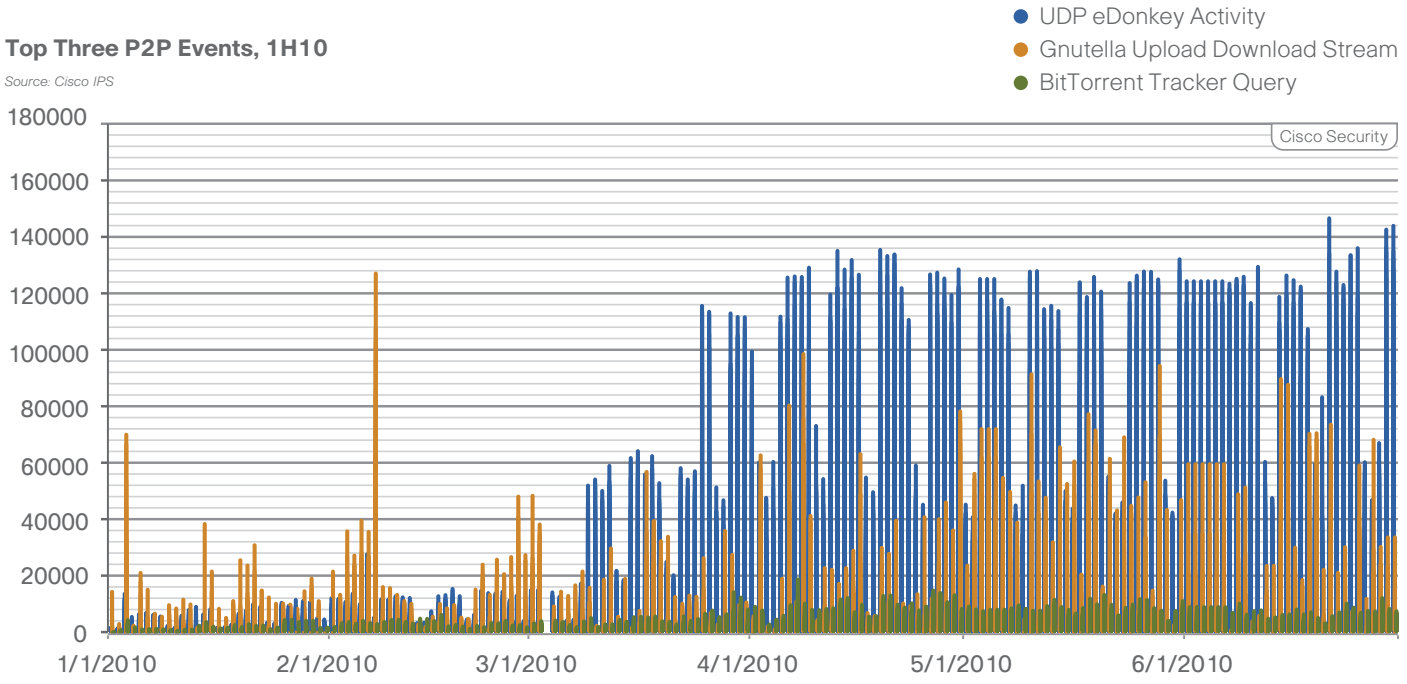
Nizar Kheir, Xiao Han

Orange labs

SSTIC 2013

orange™

Nombre croissant de malware P2P depuis 2010



Cisco 2Q10 Global Threat Report

Difficile de distinguer les flux P2P bénins et malicieux
(e.g. ZeroAcess vs kademlia, Storm vs overnet, etc.)

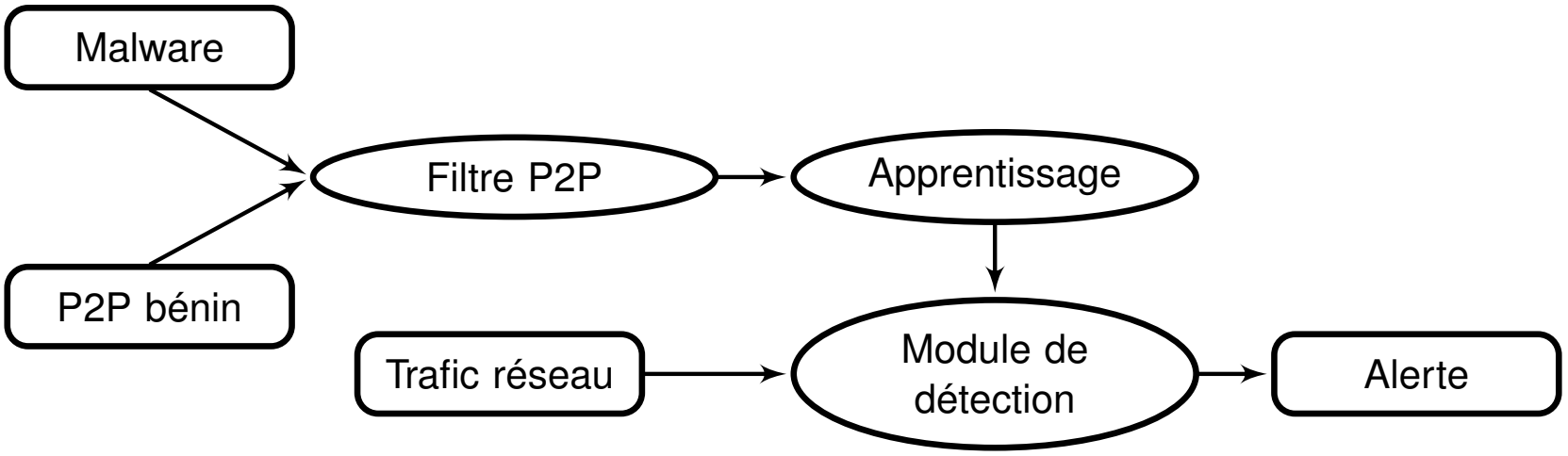
Approche purement comportementale

- Architecture décentralisée qui fonctionne hors DNS
  - Blacklist par nom de domaine impossible
- Communications souvent chiffrées
  - Détection par signature impossible

Notre approche

- Ensemble d'éléments comportementaux qui caractérisent le trafic P2P (footprint d'application)
- Méthode automatisée pour générer les footprints

Architecture de notre système



Filtrage/classification des flux réseau :

- Pre-cleaning : Nettoyage des flux non P2P
  - Flux précédés par des requêtes DNS résolues
  - Nombre insuffisant de tentatives de connexion échouée
- Classification comportementale par type d'application
- Elimination des applications non P2P

Validation du filtre P2P

Malware	Quantité
Win32.Sality et variants	481
Spy.ZBot et variants	9
Gen :Variant.Kazy variants	3
Gen :Trojan.Heur variants	5
Trojan.KillAV et variants	20
Win32.Nimnul et variants	9
Win32.Viking et variants	5
Autre	24

Input :

- 100,000 échantillons de malware de tout type (P2P et non P2P)

Résultat :

- 556 malwares P2P détectés, avec 0,014% FP

Module de détection

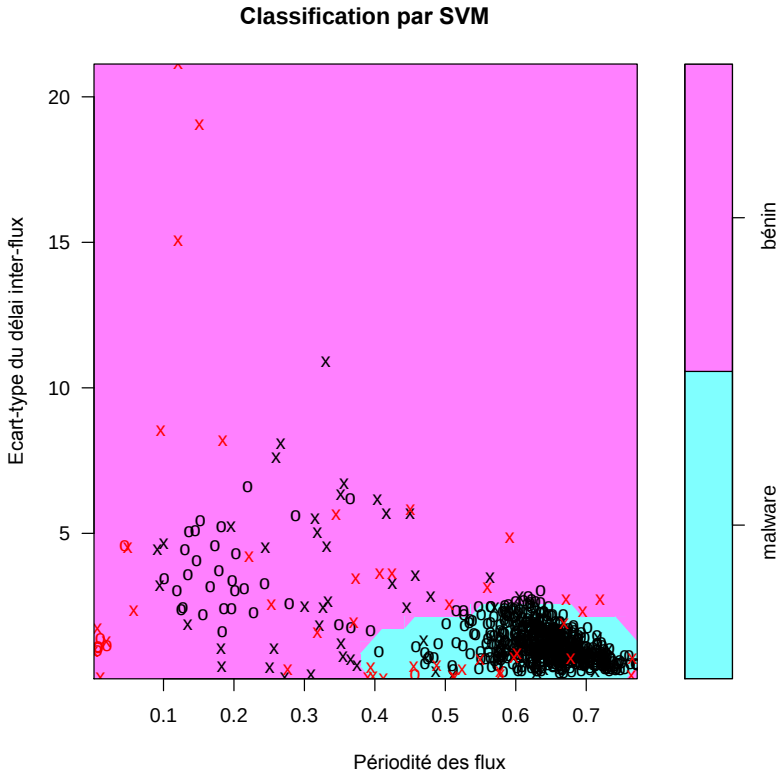
Apprentissage automatique

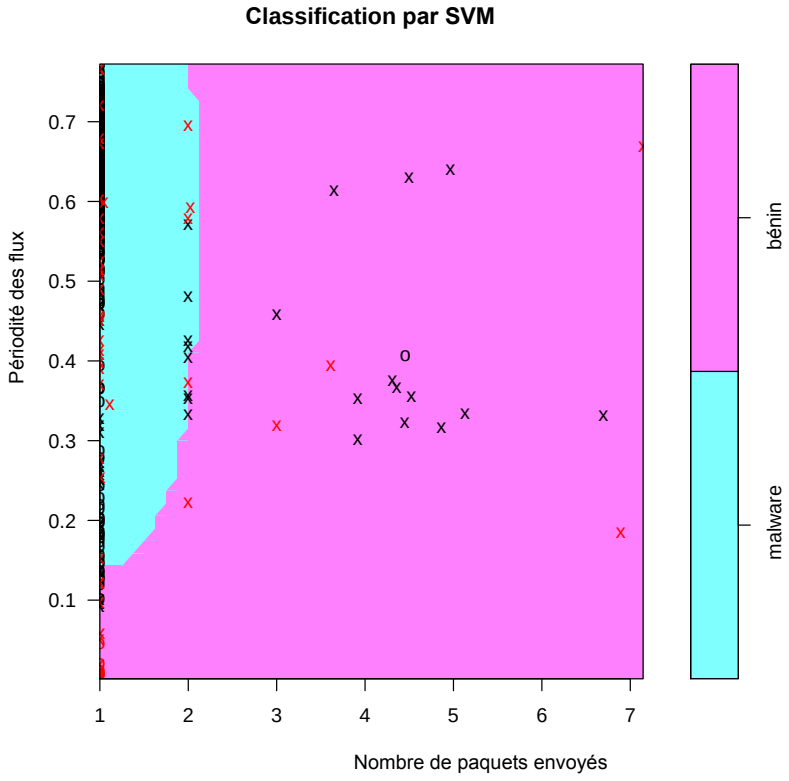
Classification par apprentissage supervisé

- Algorithme : Support Vector Machine(SVM)
  - Résoudre des problèmes de discrimination ou de régression
  - Transformation de l'espace de représentation des données d'entrées en un espace de plus grande dimension
- 667 footprints de malware et 52 footprints P2P bénins

Module de détection

Exemple de classification par SVM





- Validation croisée : 97,2% de précision

Résumé

- Conclusion :
  - Ensemble d'éléments qui décrivent le comportement du P2P
  - Module de filtrage P2P efficace
  - Module de détection par apprentissage supervisé
    - Même si un seul nœud est infecté
    - Même si aucune attaque n'est observée