Représentation Graphique d'événements de sécurité

Renaud Bidou – Senior Security Specialist
renaudb@radware.com

radware

Introduction

Enoncé du problème

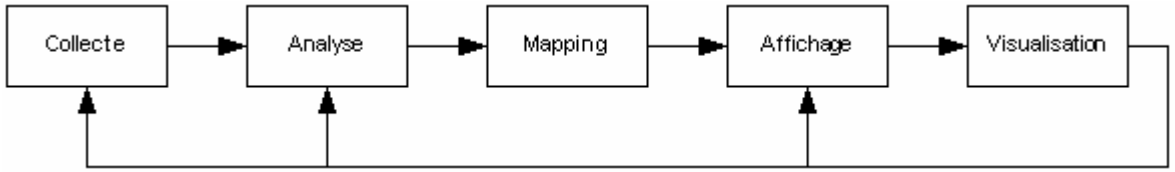
- Importante quantité de données
  - –Même après regroupement
  - –Information multidimensionnelle
- Exemples
  - –Bonet
    - Informations : plusieurs milliers de sources apparaissant comme légitimes
    - Dimensions : source / cible / URL / fréquence / user-agent / …
  - –Scans / Brute force
    - Informations : plusieurs milliers d’actions légitimes
    - Dimensions : source / cible / type de requête / résultat / …

Conséquence

- Limite des capacités d'analyse automatisées
  - Modèles limités à des scénarii communs
    - Comportement suspect d'une source
    - Analyse de schémas classiques: scan ⇨ intrusion
  - Niveau d'information insuffisant pour réagir
    - Caractéristiques d'un DoS (applicatif, réseau, ressource etc.)
- Limite de l'analyse « texte » par l'homme
  - Délais accrus
    - Réaction tardive
  - Risques d'erreurs
    - Réaction inappropriée

Objectif

- Fournir une nouvelle dimension à l'analyse
  - –Ajout de propriétés réentrantes
    - Étapes de collecte, d'analyse et d'affichage



- Intégrer l'être humain au processus
  - –Génération d'événements suite à une première analyse
  - –Intervention sur le processus d'analyse
  - –Modification de l'affichage
- Avantages de l'être humain
  - –Capacité de gestion de 150 Mbps de données[1]
  - –Performant dans la reconnaissance de modèles[2]
  - –Pas cher (si il est chinois)

1 Visual Display and Quantative Information - 2nd Edition - E. Tufte

2 Déjà vu, A user study : Using images for authentication - Racha Damija, Adrian Perring - Usenix Security 2000

Principes de la méthode

- Approche pragmatique
  - –Doit répondre à des besoins réels
    - Analyse à postériori d'événements indéterminés
      - Nombre important de données hétérogènes
      - Aucune indication particulière sur le ou les événements notables
    - Représentation exploitable des données
      - Conserver l'avantage de la représentation graphique
  - –Mise en oeuvre simple
    - Utilisation d'outil graphiques ouverts
    - Formats graphiques standards
    - Interface efficace
      - Pour permettre une analyse rapide

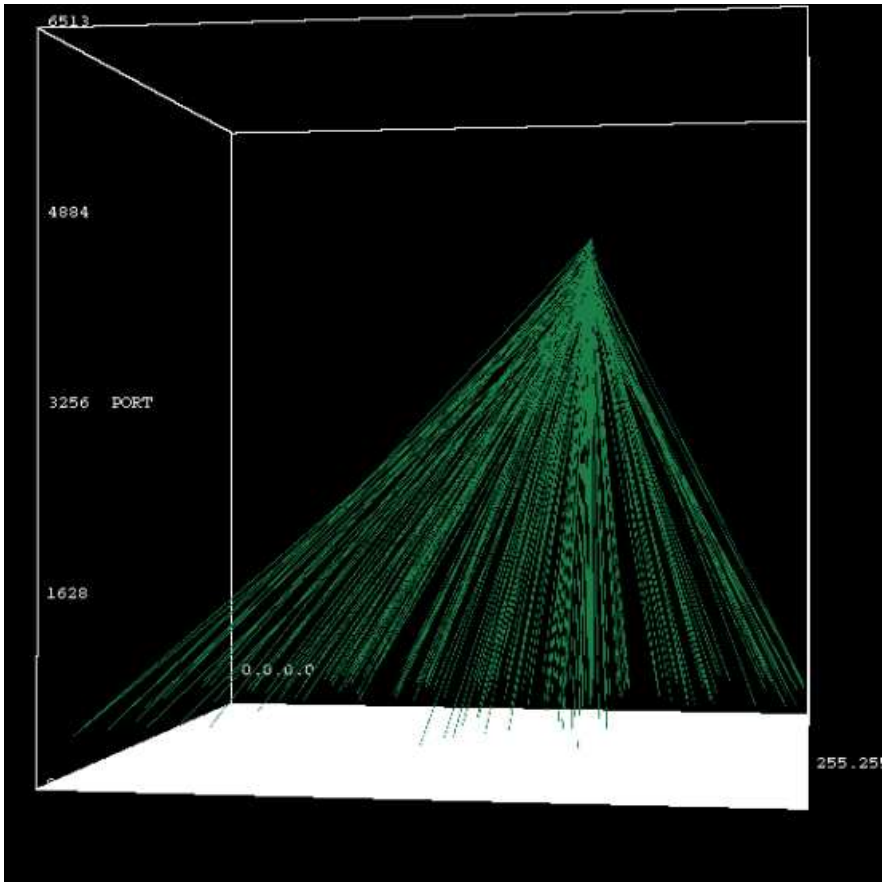
Existant

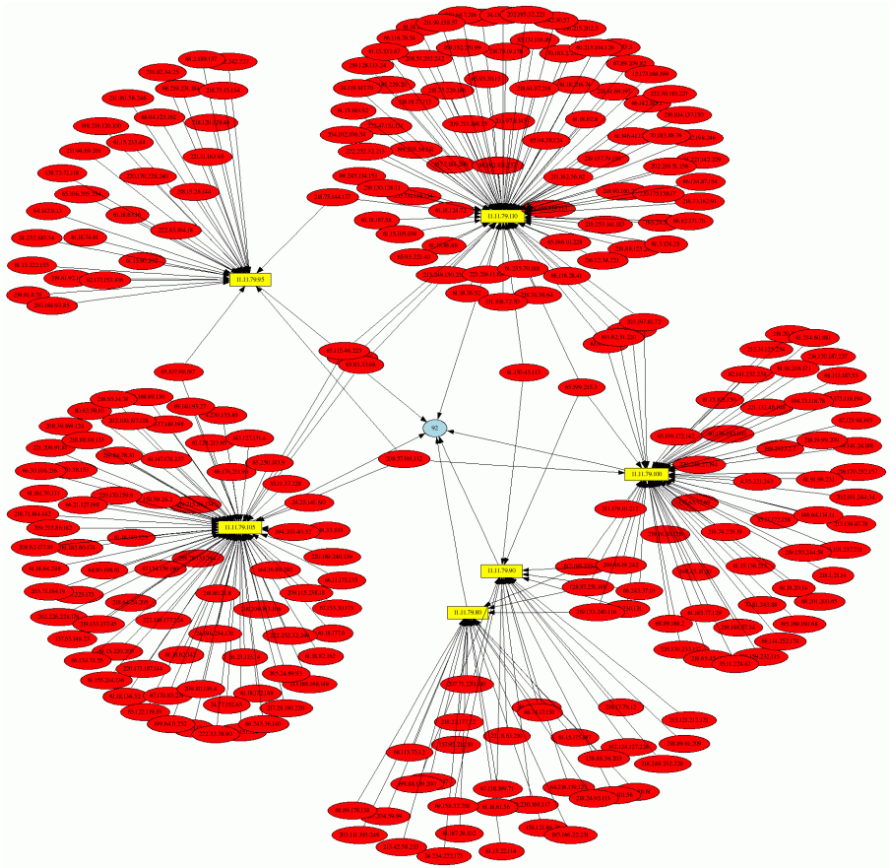
Existant

- Nombreuses théories de représentation
  - Souvent limitées à des cas spécifiques…
    - Propagation d'un ver particulier
    - Flood DNS
    - Brute force SSH
  - … ou inutiles
    - Scans de ports
- Peu de solutions exploitables
  - Dans un environnement réel
    - Besoin de flexibilité et d'exhaustivité
    - Interface simple et graphes explicites
  - En production
    - Solution industrialisable

Existant

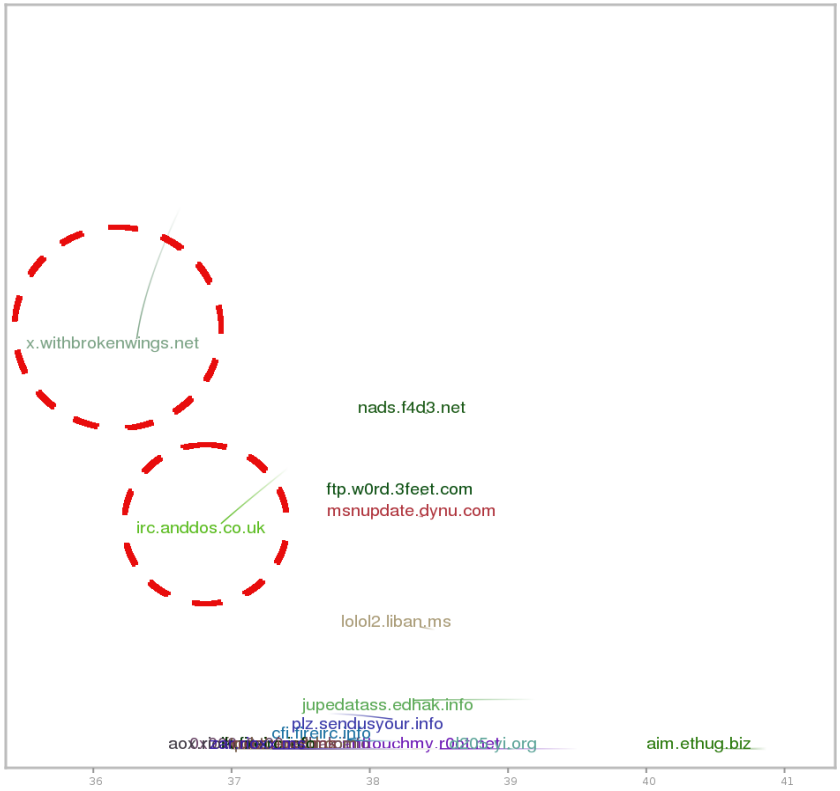
Propagation d’un ver

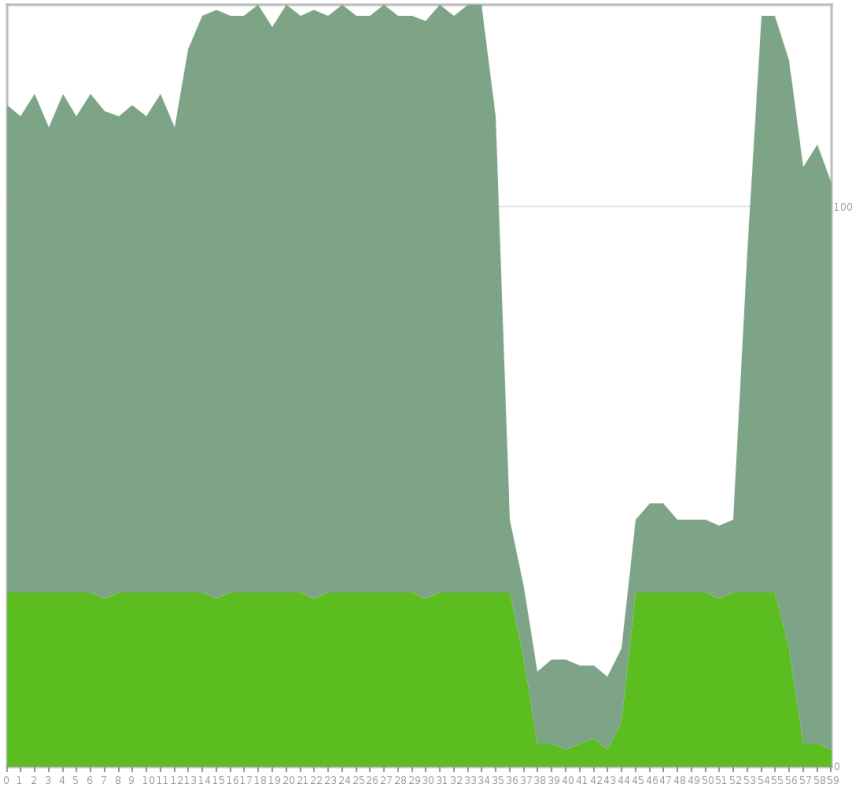




Existant

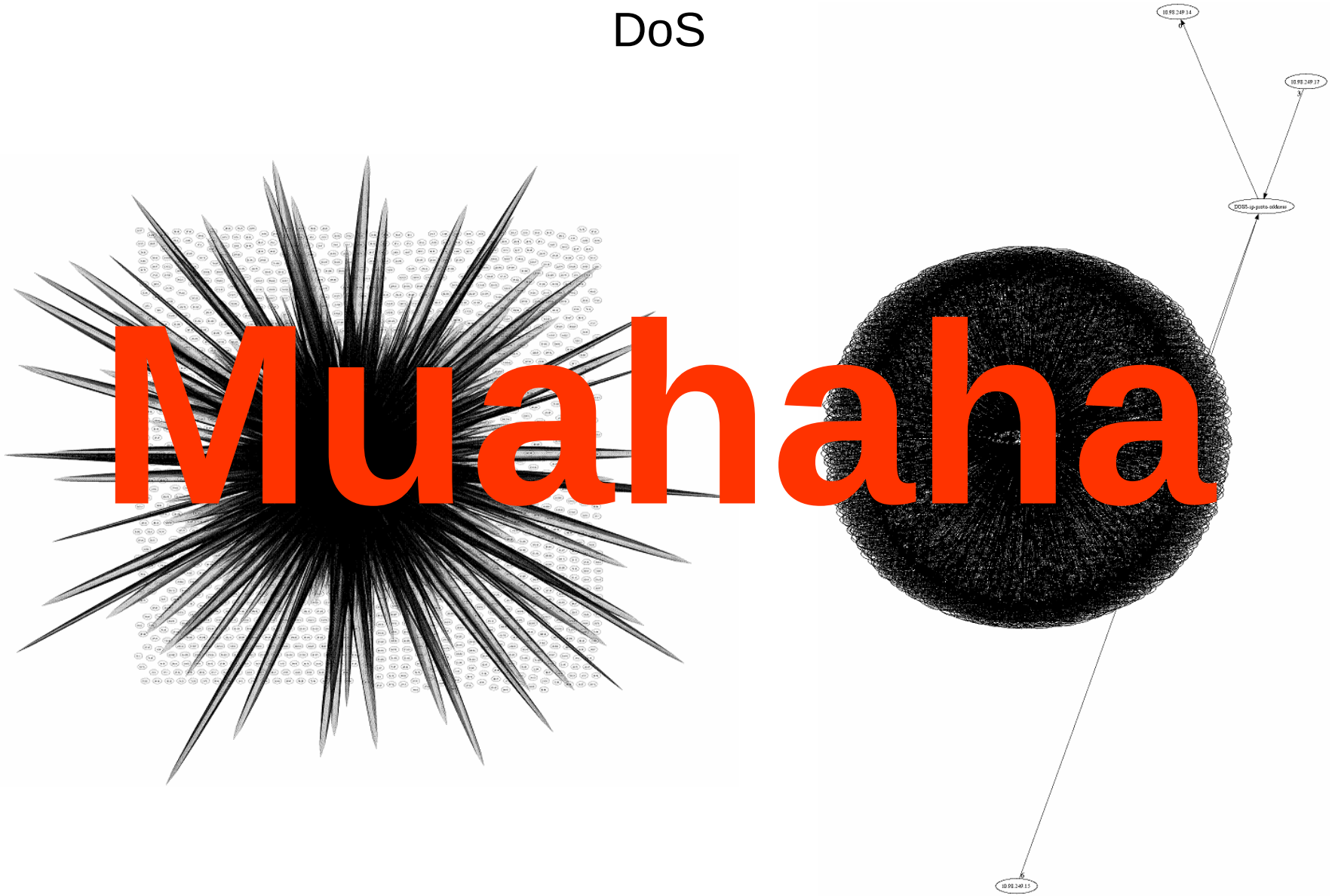
Botnet





Existant

DoS

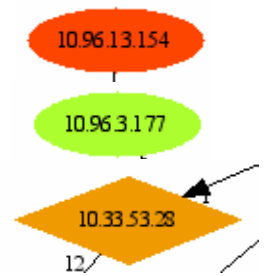


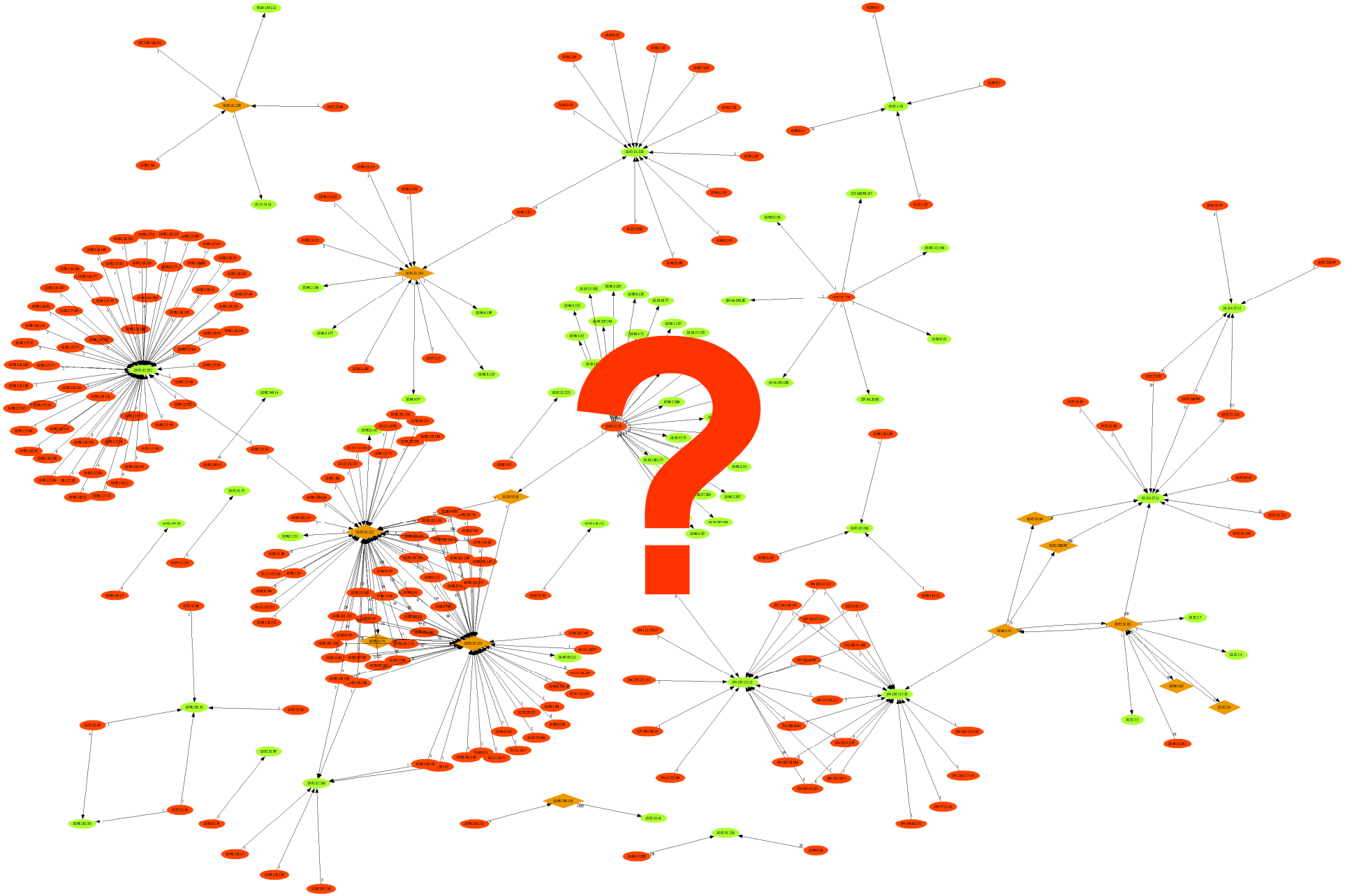
Approche simple
Source / Cible

Eléments de base

Source / Cible

- Eléments représentés
  - Systèmes source
  - Systèmes cible
  - Systèmes source et cible
  - Une représentation différente pour chaque type (forme, couleur etc.)
    - Source
    - Cibles
    - Rebond





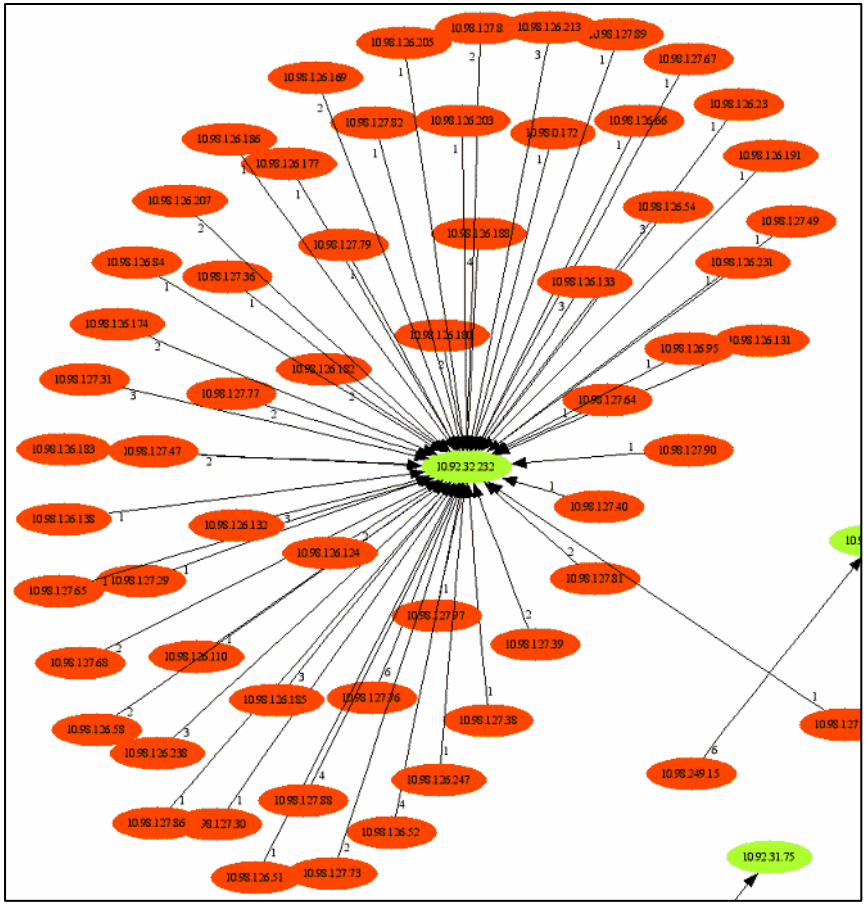
Eléments de base

Source / Cible

- Représentation pertinente de :
  - Opérations d’identification (scans)
  - Propagation
  - Dénis de service
  - Action isolée sur le réseau interne

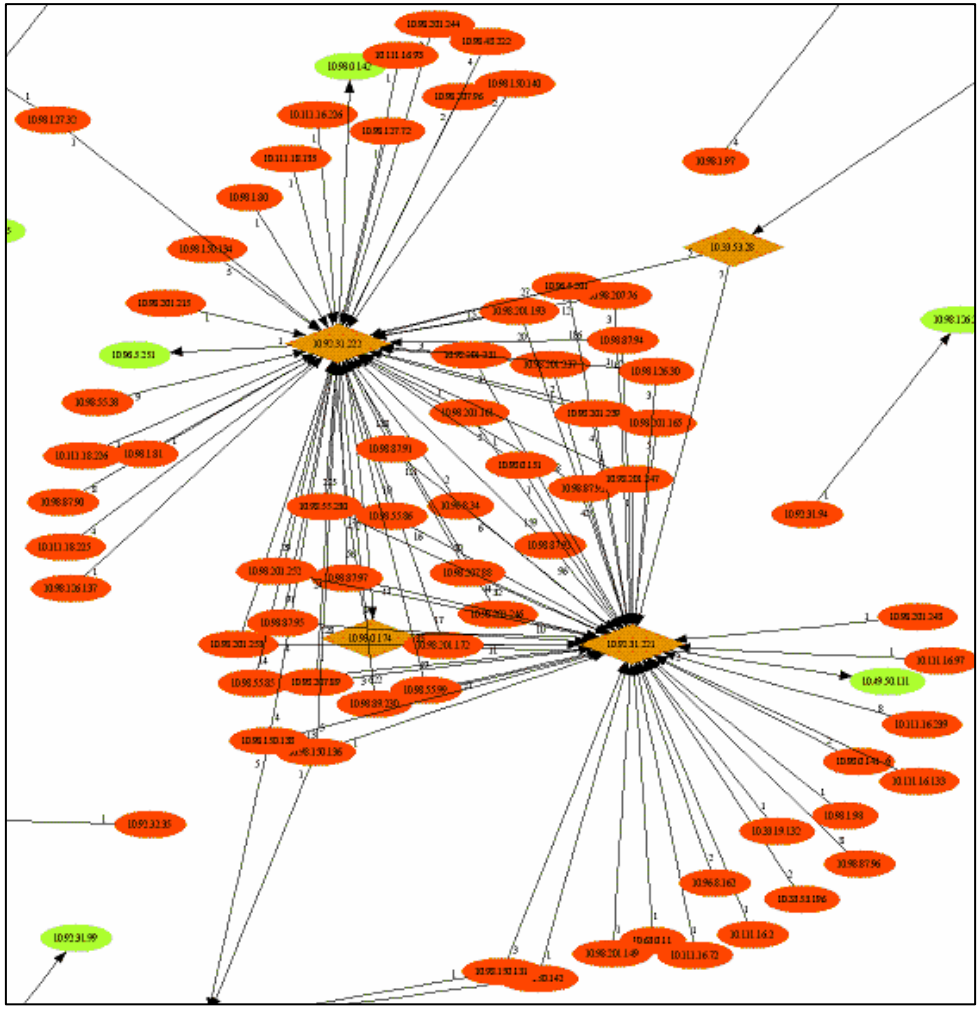
Source / Cible

Dénis de service ? Système exposé ?



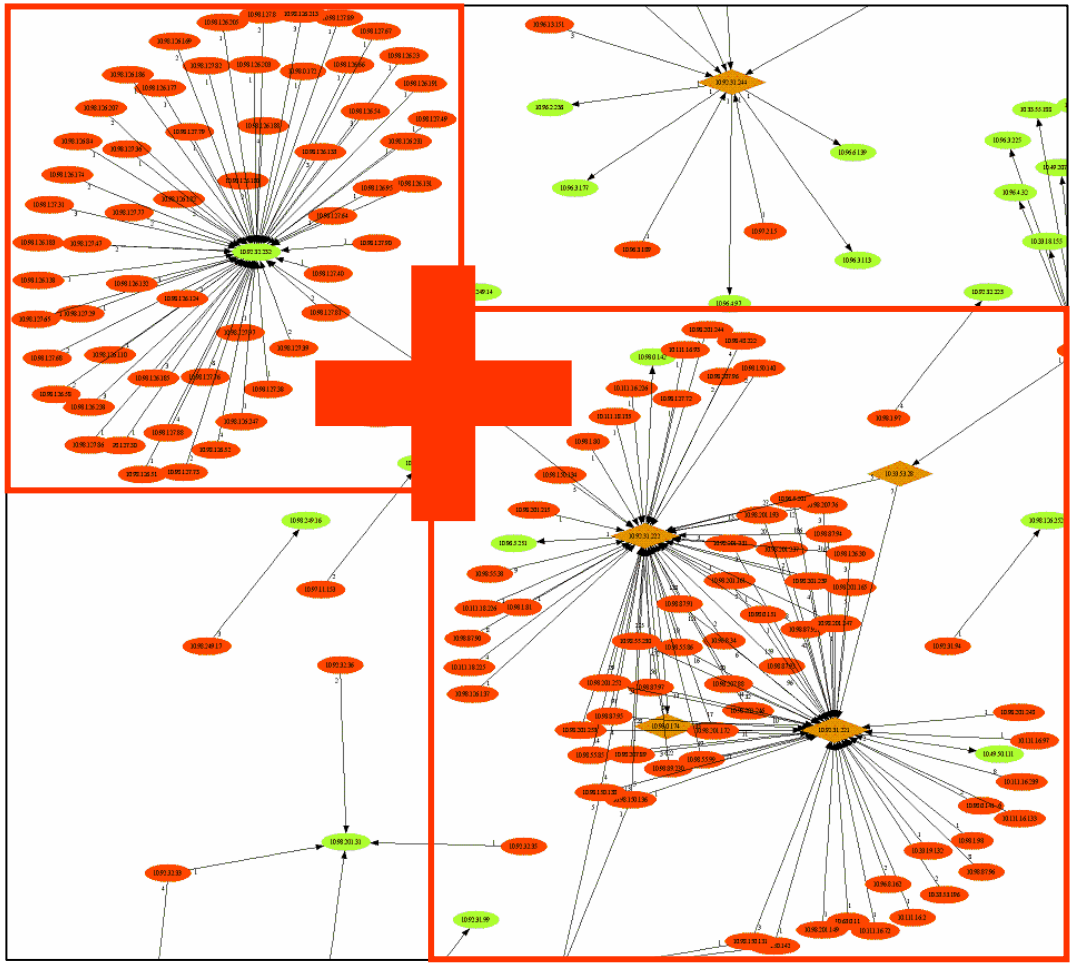
Source / Cible

Systèmes exposés et vulnérables ☺



Source / Cible

Dénis de service ? Système exposé ?

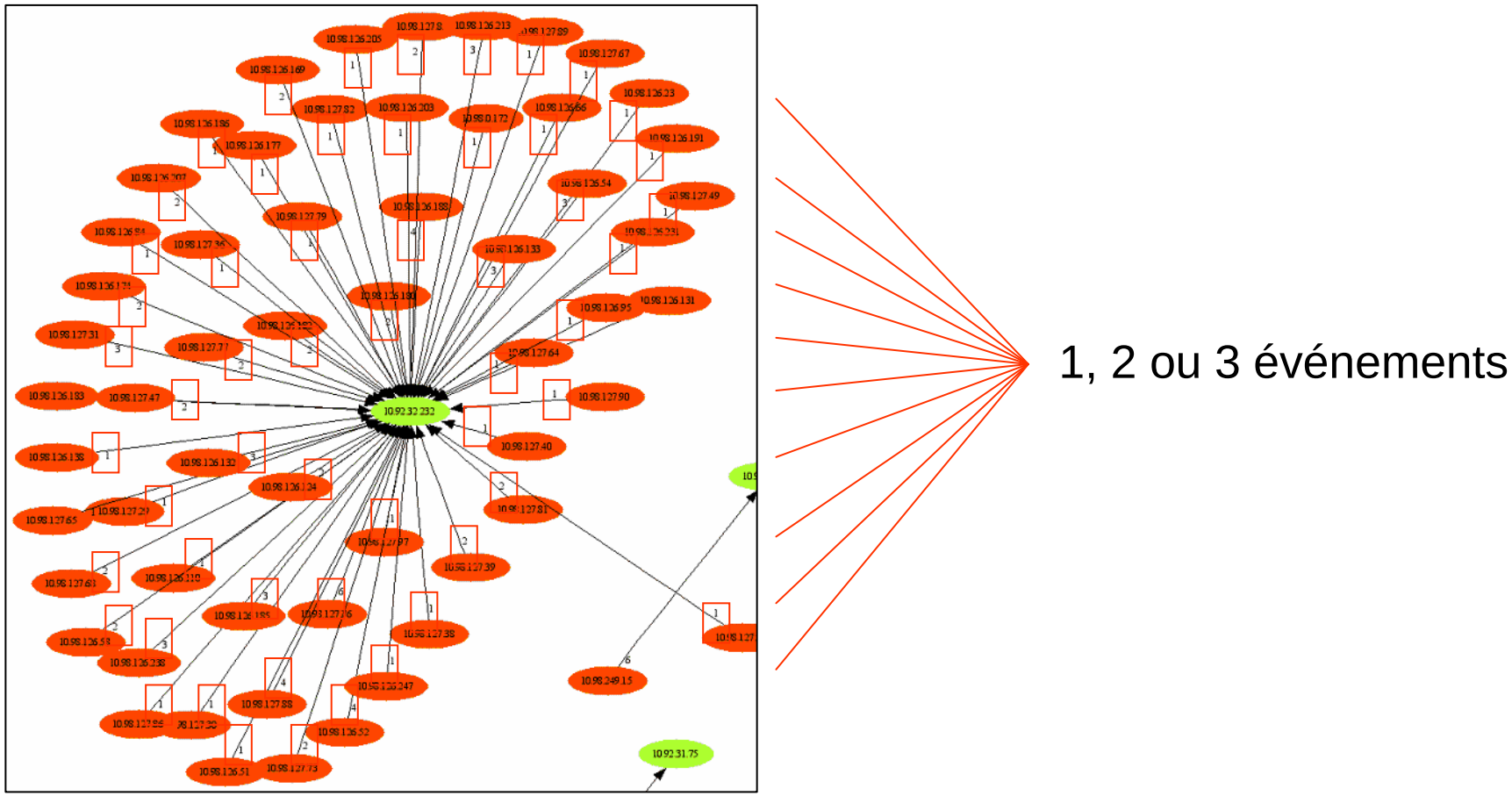


=DoS

Parceque sources différentes des sources attaquant les systèmes vulnérables

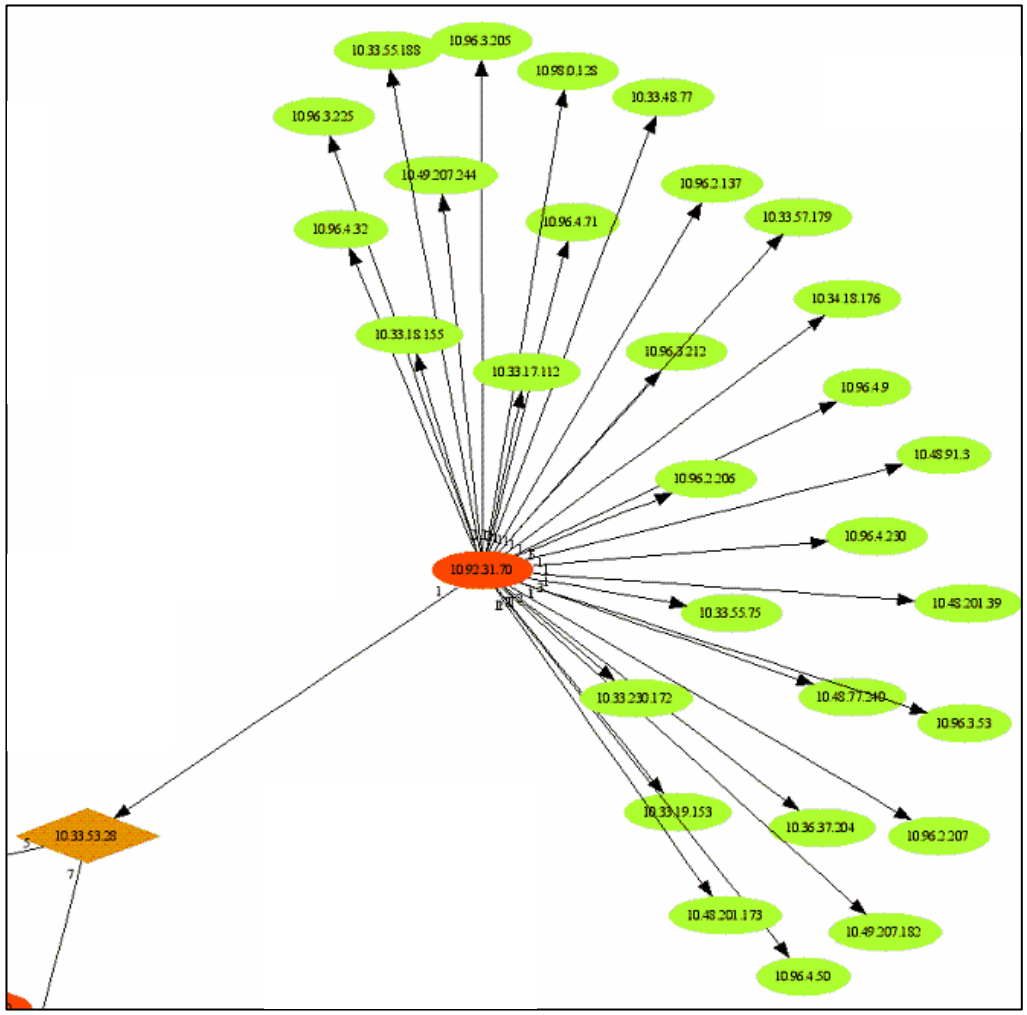
Source / Cible

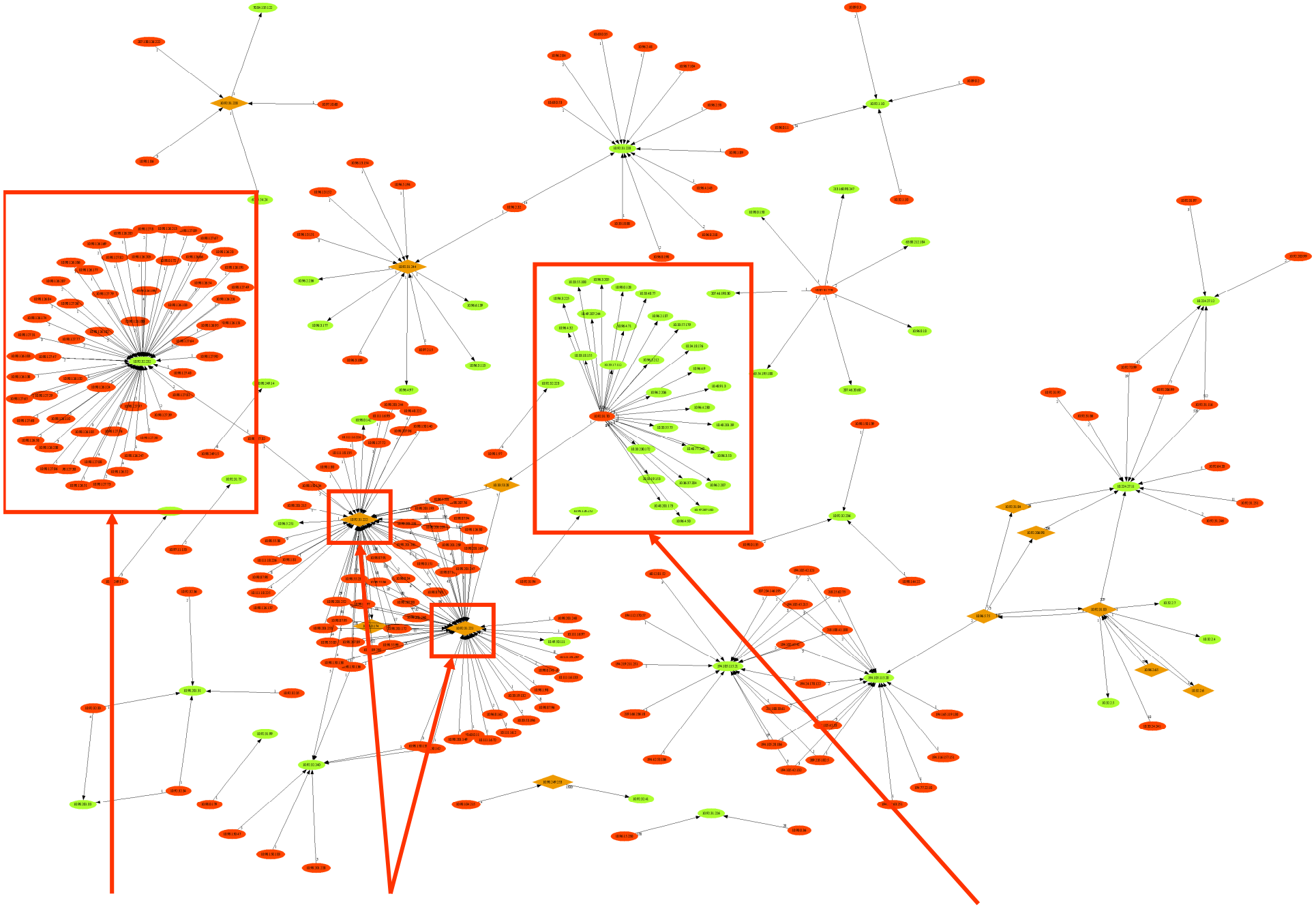
DoS Applicatif



Source / Cible

Ver ou scan de vulnérabilité horizontal

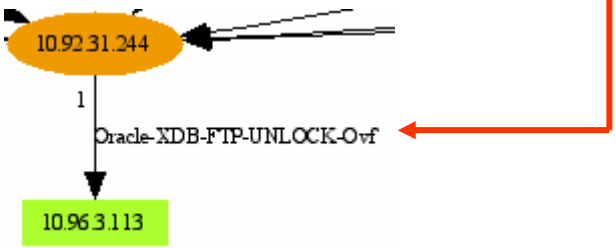



DDoS
Systèmes OpenBar
Identification + intrusion

Eléments de base

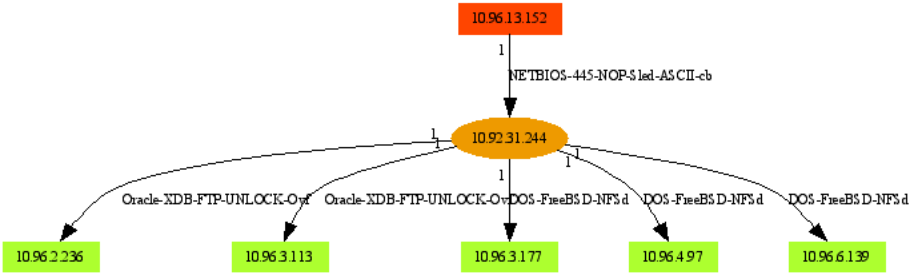
Source / Cible / Intrusion

- Eléments représentés
  - Systèmes source
  - Systèmes cible
  - Systèmes source et cible
  - Intrusion

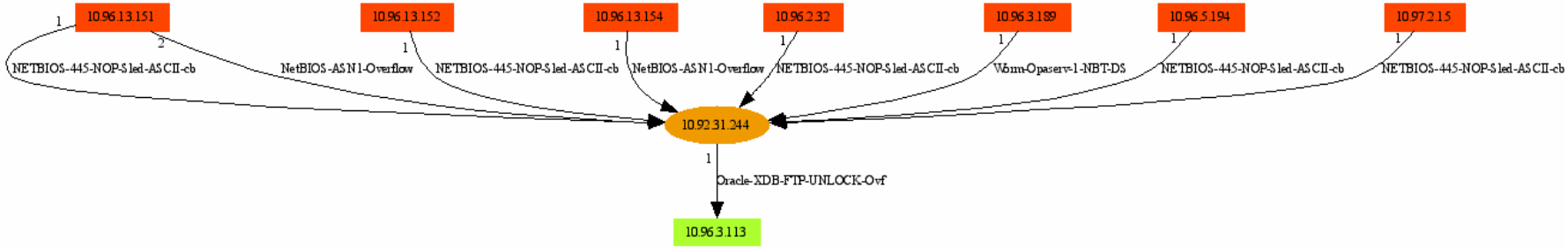


Source / Cible / Intrusion

- Intrusion sur le réseau interne



- Exploitation généralisée via killbill



Notion de regroupement

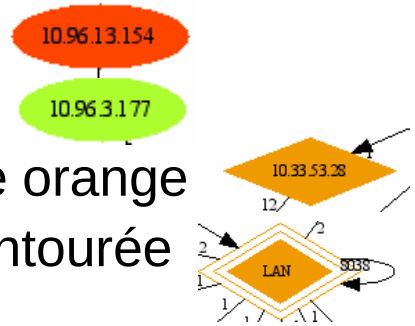
Principe

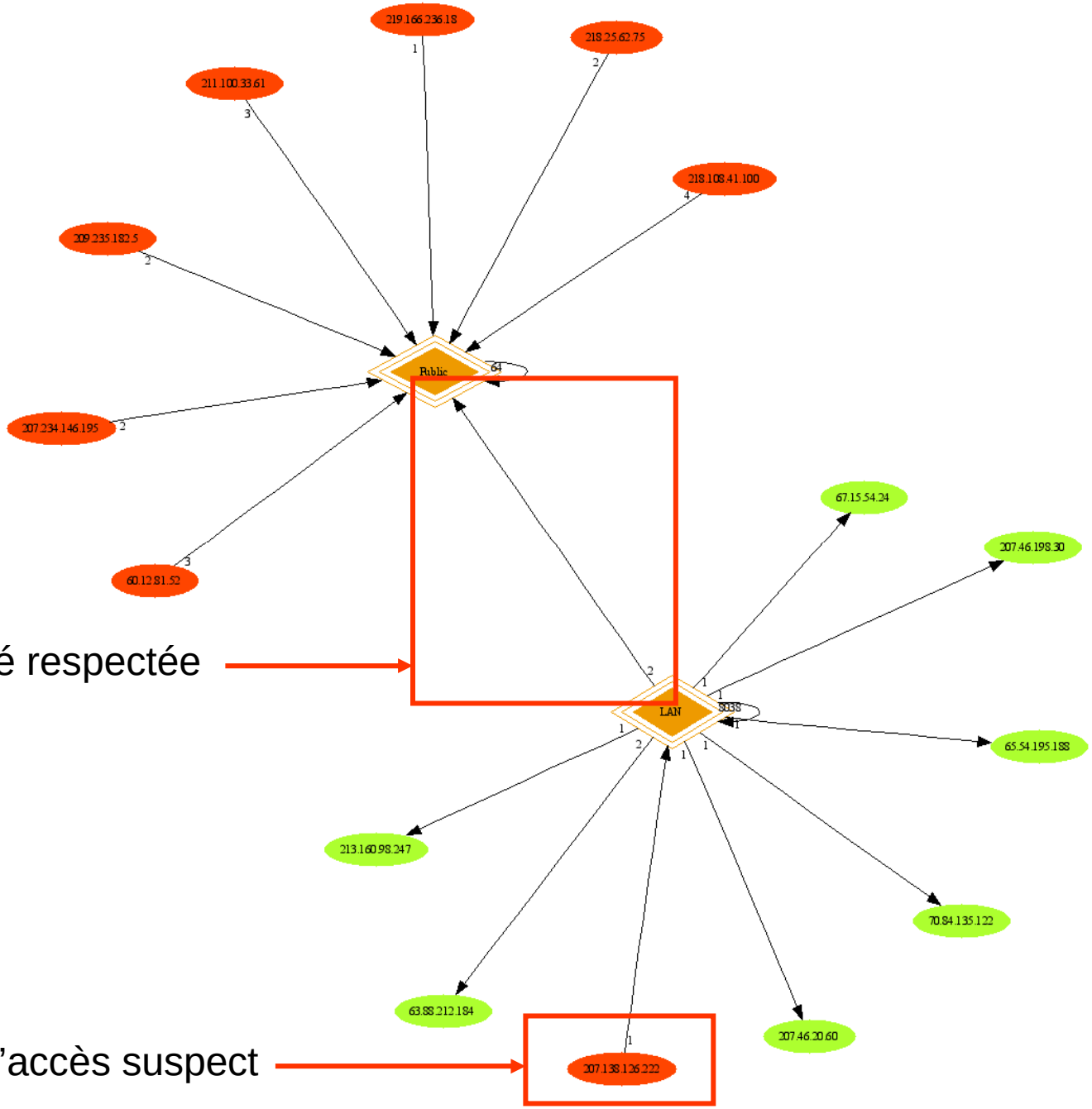
- Objectif
  - Fournir une vision plus stratégique
    - Outil d'aide à la décision
  - Regrouper les systèmes selon des critères
    - Logiques (zones de sécurité)
    - Physique (segments)
    - Géographique (sites)
    - Organisationels (services, hiérarchie)

- Représentation pertinente de :
  - Compromission de l'étanchéité des zones de sécurité
  - Usage de chemins d'accès aux ressources non référencés
  - Activité intersite

Eléments de base

- Eléments représentés
  - Systèmes source
  - Systèmes cible
  - Systèmes source et cible
  - Groupes de systèmes
  - Une représentation différente pour chaque type (forme, couleur etc.)
    - Source : rouge
    - Cibles : vert
    - Rebond : losange orange
    - Groupe : forme entourée





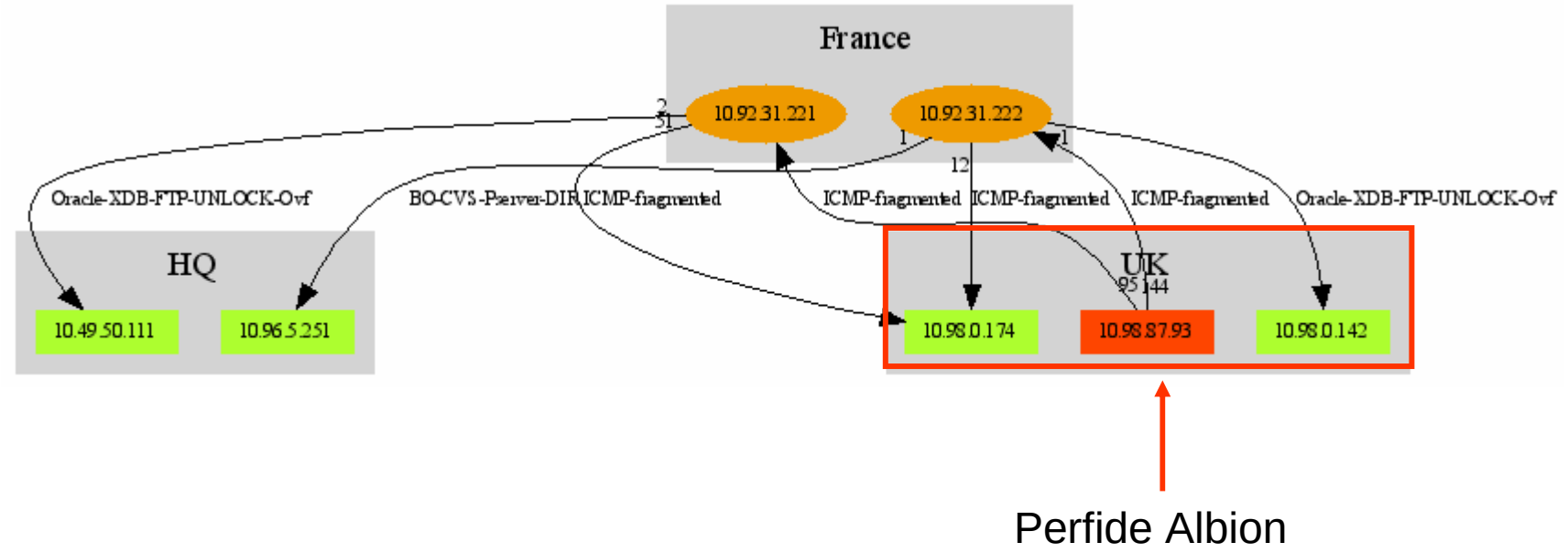
Etanchéité respectée

Chemin d'accès suspect

Eléments de base

- Eléments représentés
  - Systèmes source
  - Systèmes cible
  - Systèmes source et cible
  - Symbolique de groupes
  - Une représentation différente pour chaque type (forme, couleur etc.)
    - Source : rouge
    - Cibles : vert
    - Rebond : orange
    - Groupe : cadre

Intersites


France
10.92.31.221
10.92.31.222
HQ
10.49.50.111
10.96.5.251
UK
10.98.0.174
10.98.87.93
10.98.0.142
Oracle-XDB-FTP-UNLOCK-Ovf
BO-CVS-Pserver-DIR
ICMP-fragmented
ICMP-fragmented
ICMP-fragmented
ICMP-fragmented
Oracle-XDB-FTP-UNLOCK-Ovf
Perfide Albion

Outils utilisé

Outil

- DPViz
  - Analyse des logs de l'IPS Radware
  - Ecrit en PERL
  - Adaptation triviale à la plupart des IDS / IPS
  - Existe en mode texte ou PERL/Tk
  - bientôt sur http://www.iv2-technologies.com/~rbidou
- GraphViz
  - Bibliothèque de visualisation
  - Génération des graphes
  - Google sait où la trouver

DPViz

Lancement

```
=========[ DefensePro DataBase Vizualisation Tool ]=========
===========[ Renaud Bidou - renaudb@radware.com ]===========
==[ Connecting to database insite2 on 192.168.205.185
-> Done
==[ Getting generic statistics
-> 129278710 offending packets
->    200000 lines are stored in database
->     41248 sources
->       149 targets
==[ Preparing pre-filters
1 -> Filtering "Access List" with 993 sources and 143 targets
2 -> Filtering "DOSS-DNSRequests-Limit" with 40254 sources and 3 targets
==[ Welcome to the graph generator
>
```

Filtrage en amont

DPViz

```
> help
a|attack <filter>              Filters attack types (0 = All, 1 = only Intrusions, 2 = only DoS)
  c|cluster <action> <values> [!]       Perform <action> on network grouping
                                 a|add <net(CIDR format)>[:label] [!]
                                       [!] for negation : "all but" form
                                 d|del <net(CIDR format) | label>
                                 l|list
                                        example : cluster add 10.0.0.0/8:intranet box
                                        example : cluster del 10.0.0.0/8
                                        example : cluster del intranet
  d|destination <destination>   Sets the Source/destination of attacks (for type 3/4 graphs)
  g|generate <file name>        Generate graph to <filename> (default = random)
  h|help                        Print this help
  l|colors <color_set>          Sets the color style :
                                 std  : Standards (default) colors
                                 rdwr : Radware Corporate colors
                                 bw   : Black and White (because life is no fun)
  o|options                     Show option sets
  p|prefilter <command> <value> Work with pre-filters
                                 s|set <prefilter_id>
                                 u|unset <prefilter_id>
                                 l|list
  s|stats                       Prints current graph stats
  t|type <type>                 Set graph type :
                                 0 = source -> intrusion -> target
                                 1 = source -> target
                                 2 = source -> target + intrusion
                                 3 = * -> one target (set with d|destination command)
                                 4 = one source -> * (set with d|destination command)
  x|exit                        Exit
```

Une autre approche

Analyse et blocage d’un DoS

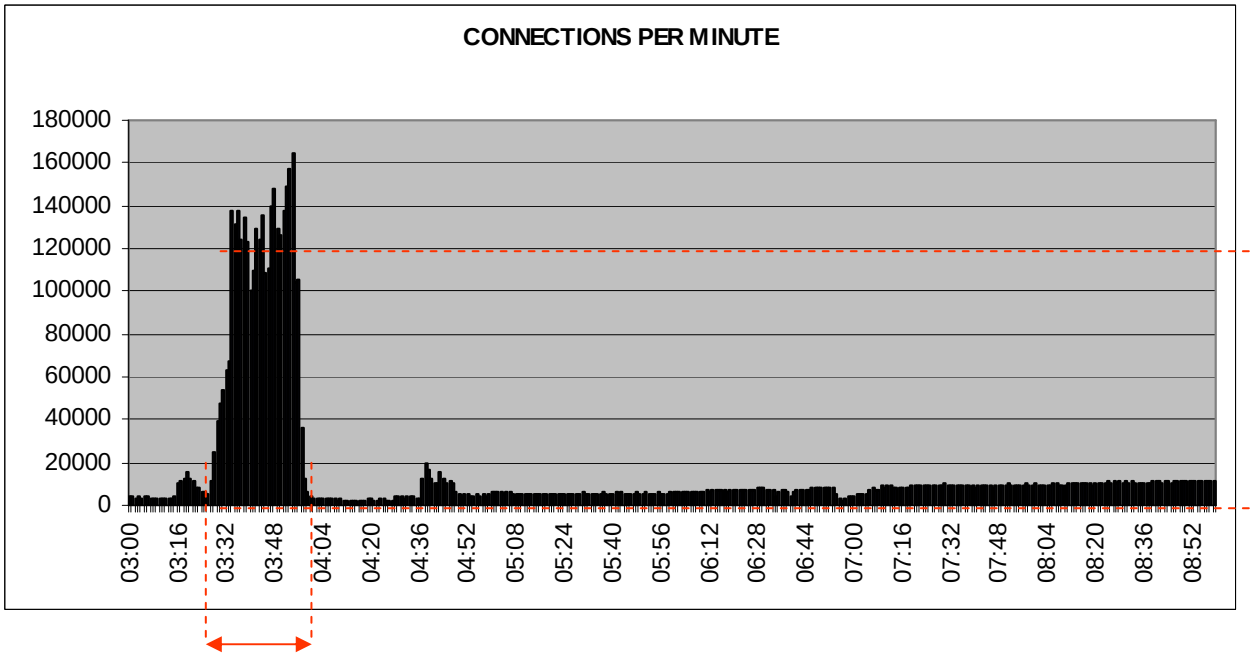
- Cas réel
  - Cible : Jeux en ligne et hébergement
  - Situé à Curaçao …
  - Protégé par un IPS
- Les événements
  - DoS sur les serveurs d’un client
  - Durée 20 minutes
  - Racket : 50.000 $ demandés
    - 1ère vague …
  - Les IPS n’ont rien vu

Nouvelle source de données

- Logs du serveur web
  - Information potentiellement pertinentes
    - connections, source et URL
    - user-agent, requête, code de réponse
    - Débit montant / descendant
  - sur 6 heures
- Volumes
  - 2,5 Go de texte
  - 5,5 Millions de lignes

Premiers résultats

- Type et moment de l’attaque

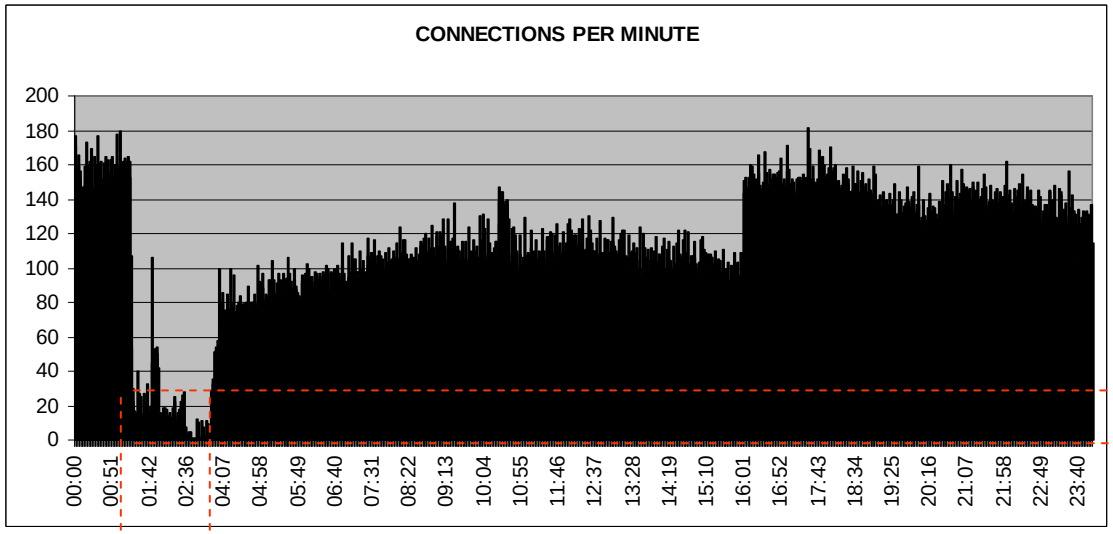


Type d’attaque:
Flood HTTP

Moment de l’attaque

Contre-exemple

- Type et moment de l’attaque

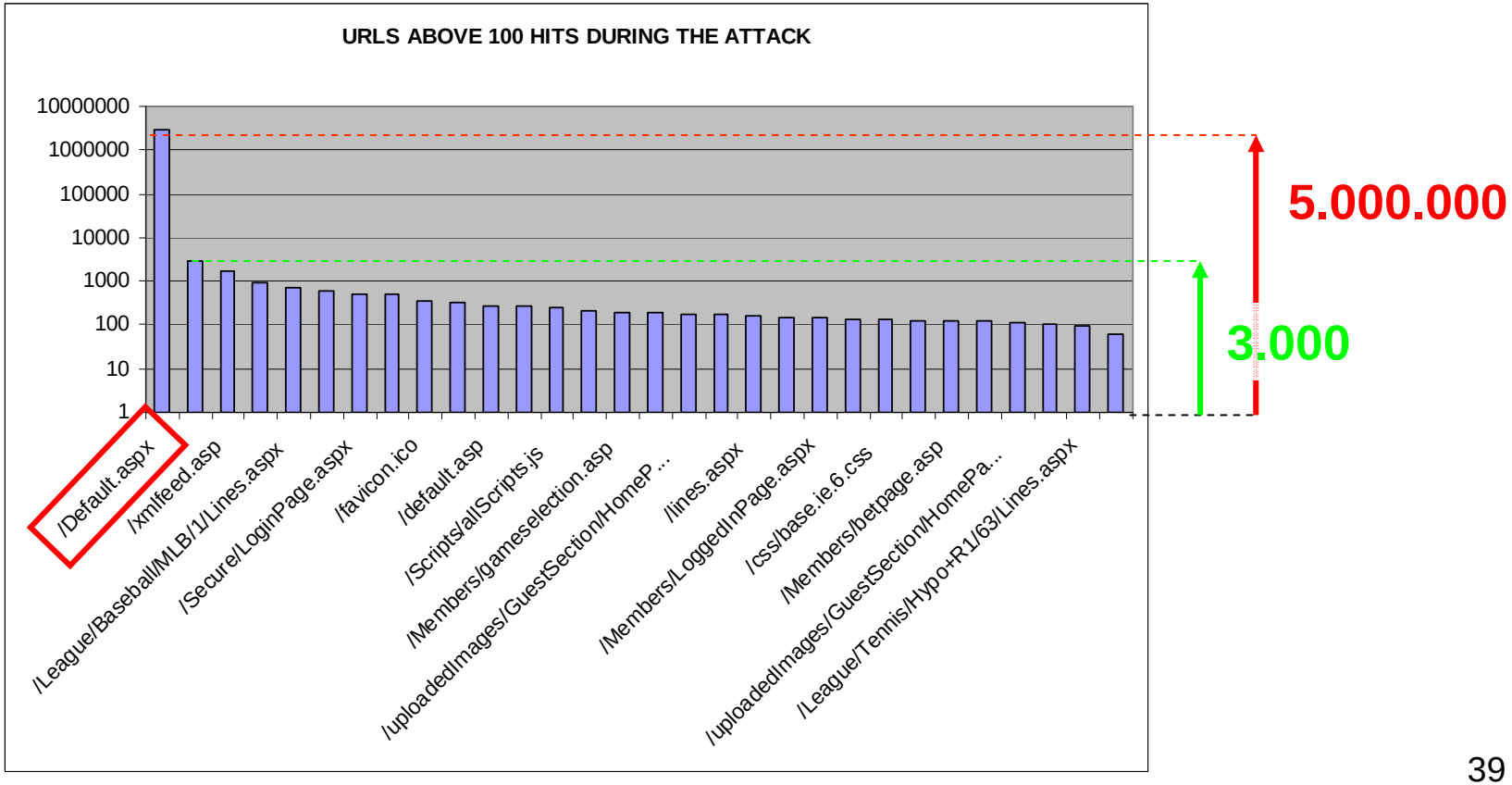


Type d’attaque:
Flood Réseau

Moment de l’attaque

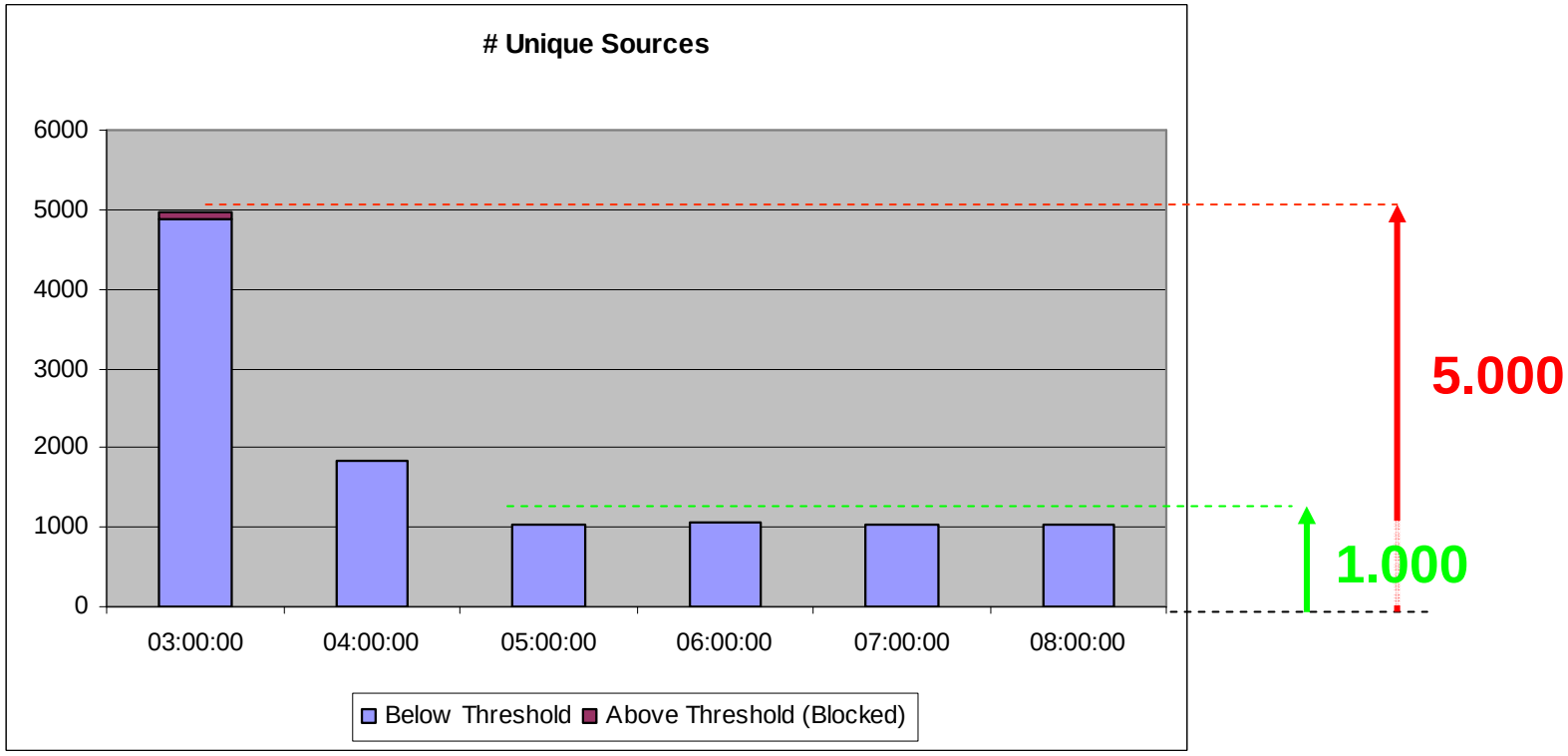
Cible

- Analyse par URL



Sources

- Taille du Botnet



Conclusion

Une approche complémentaire

- Facilite l’accès à l’information
  - Une droite est un ensemble infini de points alignés
- Simplifie l’analyse
  - Un bon dessin vaut mieux qu’une longue explication
- Accélère la compréhension d’un phénomène
  - Bon vous voyez ce que je veux dire
- Ajoute la composante humaine au processus
  - Ca saute aux yeux
- Enrichit la méthode d’analyse
  - Il faut voir çà sous un autre angle

Questions

radware