Détection d'attaques DDoS dans les réseaux

Gilles Roudiere

Détection d'attaques DDoS dans les réseaux

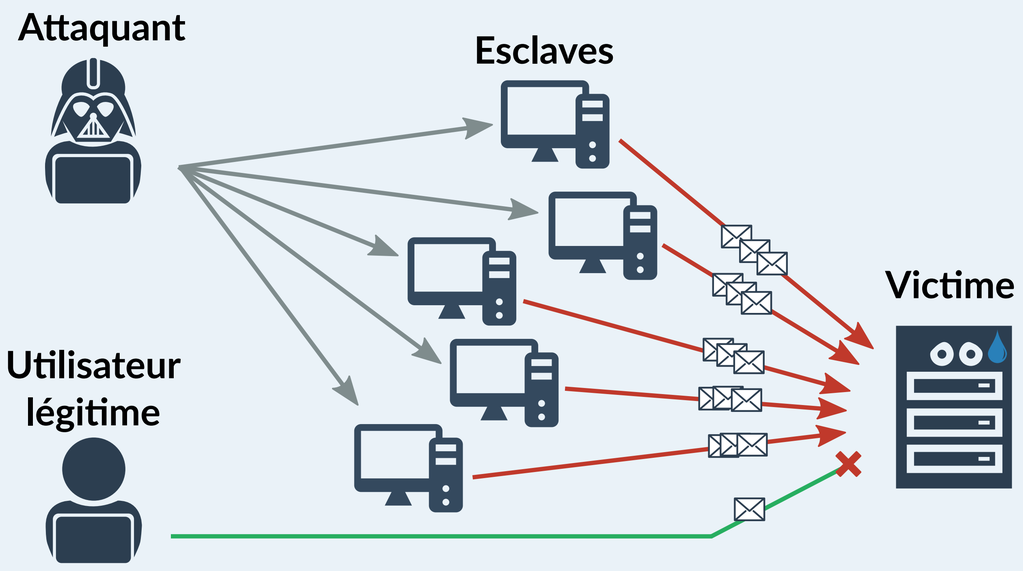
Gilles Roudière — *gilles.roudiere@laas.fr*
LAAS-CNRS — Université de Toulouse — INSA Toulouse

Contexte

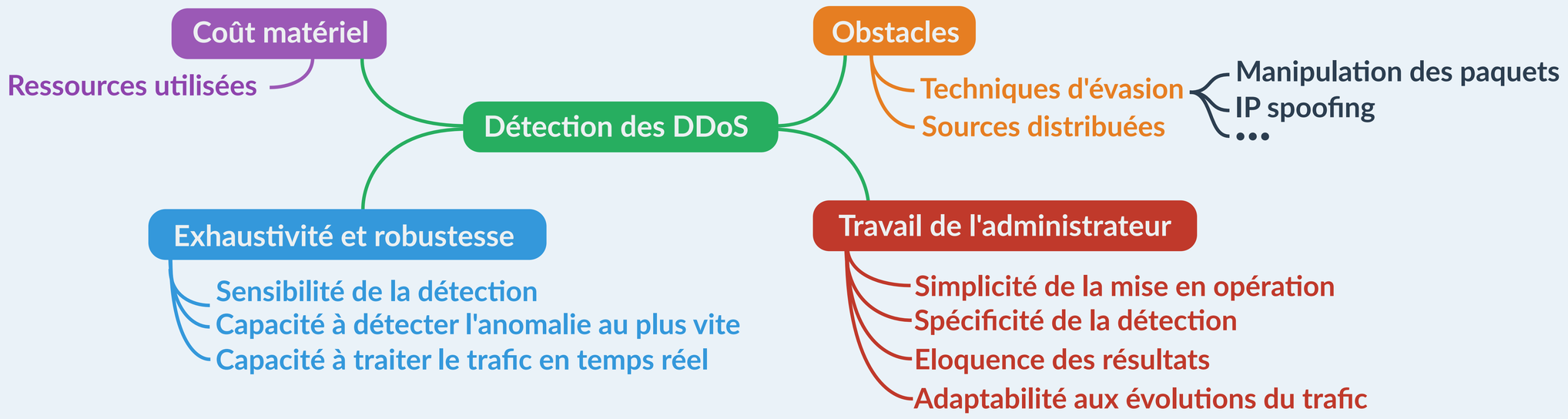
Attaques par Déni de Service Distribuées (DDoS)
= Un grand nombre de machines envoie des requêtes parasites à un système cible, l'empêchant de répondre aux requêtes légitimes.

Coûteuses **$2.5 millions** en moyenne par attaque,
63% des entreprises estime le coût de l'indisponibilité de leurs services à plus de **$100.000 par heure**.

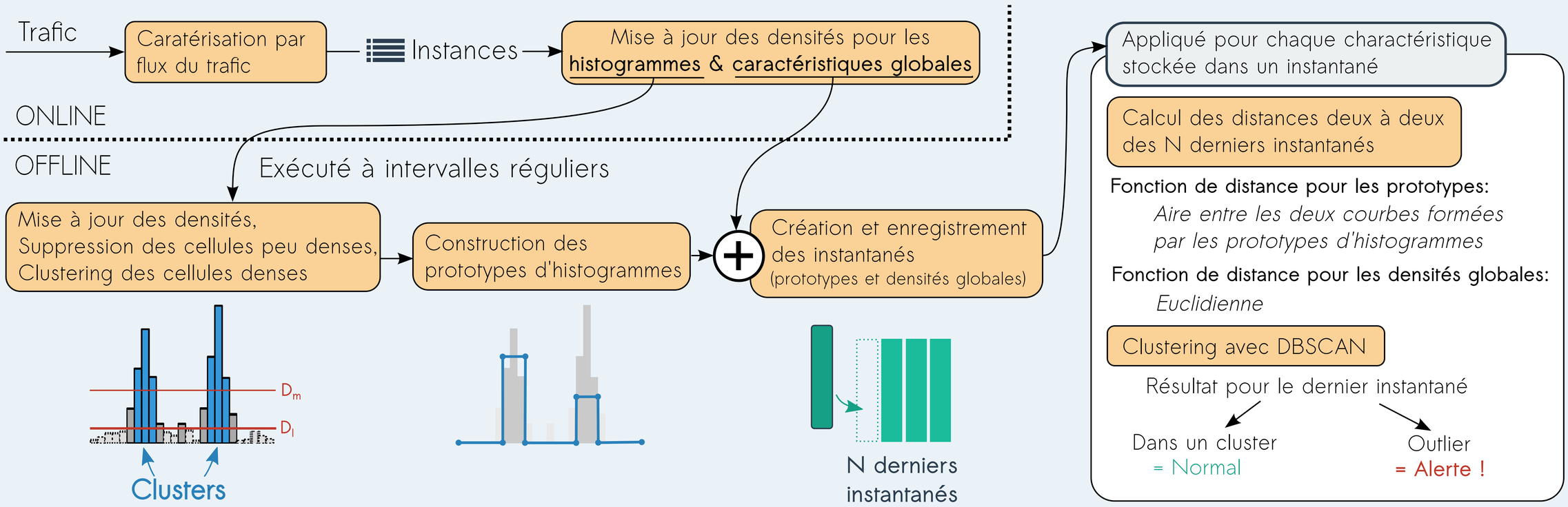
Nombreuses **84%** des entreprises en ont subi au moins une en 2016.
(Enquête réalisée auprès de 1010 organisations. Source : Neustar, 2017)



Problématique



AATAC (Autonomous Algorithm for Traffic Anomalies Characterization)



- Division du traitement en deux parties = détection **temps réel**, nécessitant peu de ressources de calcul,
- Des instantanés du trafic produits régulièrement :
  - Utilisant des histogrammes, qui sont graphiquement **simples à interpréter** (et plus parlants que l'entropie par exemple),
  - Formant une vue dynamique du trafic, **simplifiant la phase d'analyse**.

Expérimentations

SynthONTS : 13 anomalies générées dans un ensemble de traces réelles.
(Les travaux sur ce jeu de données continuent avec une extension en cours de la trace et du nombre d'anomalies synthétiques qu'il contient.)

Taux de vrais positifs : 0.83
Taux de faux positifs : 0.0013

Traces réelles : traces capturées à l'entrée d'un réseau d'entreprise (essentiellement du trafic web, contenant deux DDoS).

N	Online (Temps de calcul en s pour 1s de trafic)	Offline (Temps de calcul en ms)
100	0.20	0.029
1000	0.20	0.028
5000	0.21	0.030

Analyse des résultats : exemple avec un prototype d'histogramme