Méthodologie pour la caractérisation des relais d'attaques par déni de service distribué

Camille Moriot, François Lesueur, Nicolas Stouls, Fabrice Valois, Marie-Pierre Escudié

camille.moriot@insa-lyon.fr

Journée thématique du GT SSLR 2021 sur la sécurité des réseaux

GDR Sécurité x GDR Réseaux et Systèmes Distribués

11 mai 2021

citi Lab — Inria — INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Les attaques DDoS en 2020

Les attaques DDoS volumétriques sont aujourd'hui toujours en pleine progression :

809 Mpps : la plus grande attaque en nombre de paquets par seconde limitée par Akamai

Akamai Blog

2.3 Tbps : la plus grande attaque enregistrée en volume

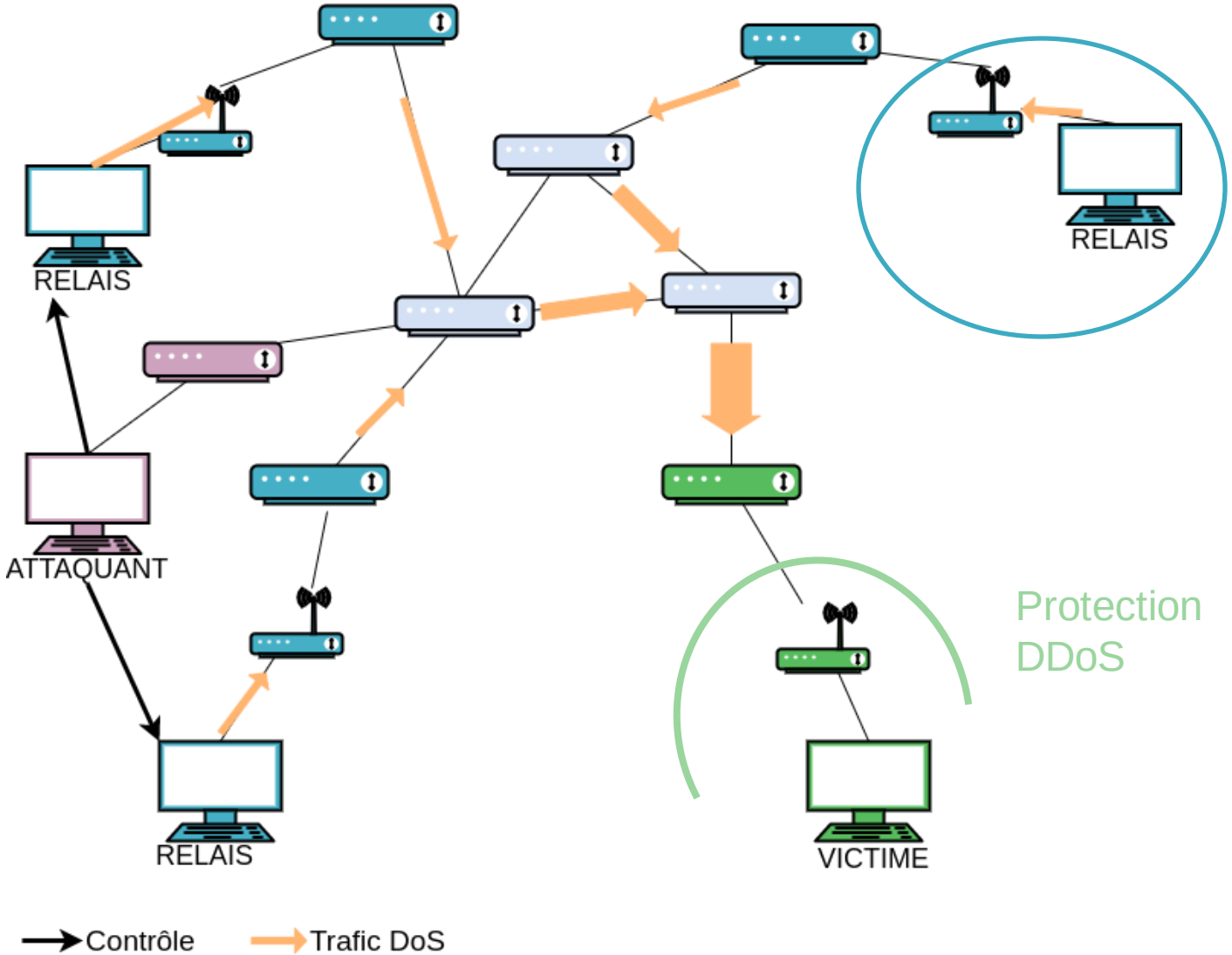
AWS Shield Threat Landscape Report – Q1 2020

4.83 Millions d'attaques DDoS durant la première moitié de 2020

Augmentation de **25%** des attaques DDoS pendant le confinement

Rapport Netscout s1 2020

Les attaques DDoS volumétriques



Notre objectif :
Étudier les relais d'attaques pour mieux les comprendre et attaquer le problème au niveau de la source.

Que sait-on sur les relais ?

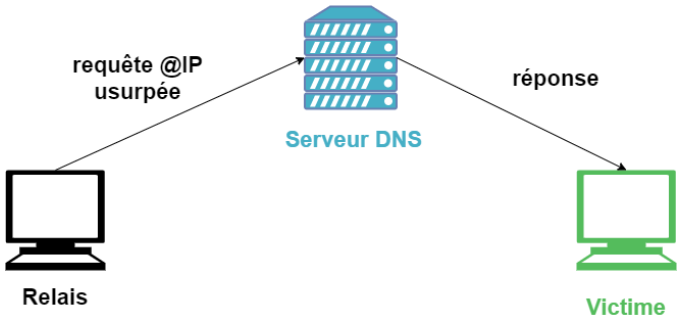
Qui sont-ils ? Où sont-ils ? Quels sont leurs réseaux ?

Systèmes infectés dans un botnet [1]

- Objets IoT
- Infection

Système servant d'amplificateur [2]

- DNS, SMTP, ICMP
- Usurpation d'identité



Serveur dans le Cloud [3]

- Bonne bande passante, bas coût, location à l'heure

Localiser les relais via les adresses IP [4]

[1] A. Wang, W. Chang, S. Chen, and A. Mohaisen, "Delving Into Internet DDoS Attacks by Botnets : Characterization and Analysis," IEEE/ACM Trans. Netw., vol. 26, no. 6, pp. 2843–2855, 2018.

[2] C. Rossow, "Amplification Hell : Revisiting Network Protocols for DDoS Abuse," in 21st Annual Network and Distributed System Security Symposium, NDSS,USA, 2014.

[3] Z. He, T. Zhang, and R. B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," in 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017, USA, 2017, pp. 114–120.

[4] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in IFIP/IEEE International Symposium on Integrated Network Management, IM 2015, Canada, 2015, pp. 243–251.

Problématique

Quelles structures socio-organisationnelles et techniques se trouvent derrière les relais d'attaques DDoS ?

Collecte et structuration des traces

1.

Qu'est-ce qu'on collecte ?

Capture d'attaque réelle récente enregistrée au plus près de la victime.

Sous quel format ?

pcap,
netflow,
IP/Ports.

Où ?

Sites de e-commerce,
Réseaux universitaires,
Compétitions de jeux vidéo.

Analyse qualitative des sources

2.

Comment est-ce qu'on analyse ?

On s'appuie sur des bases de données et des outils existants.

Sur quelles ressources s'appuie-t-on ?

RDAP,
Wikidata,
Liste NREN,
Censys/Shodan.

Quelles informations souhaite-t-on identifier ?

Socio-organisationnelle :
Nature/type,
Culture,
Nombre de personnes,

Socio-technique :
Services,
Géographie,
Répartition géographique,
Taille.

Synthèse et outils pour la visualisation

3.

Comment sont analysés les résultats ?

Les résultats sont analysés en fonction du volume de trafic généré par chaque source.

Comment sont synthétisées les données ?

Les traces sont exportées au format JSON sans mention des ips sources.

Comment sont visualisées les données ?

Un dashboard Kibana,
Un outil wireshark.

Conclusions et perspectives

Bilan :

- Proposition de méthodologie
- Implémentation avec liaisons Wikidata et RDAP
- Premières traces

Perspectives :

- Implémenter l'analyse des services
- Trouver plus de traces à analyser
- Analyser les résultats pour identifier les points stratégiques pour déployer des solutions

Merci pour votre attention !
Vous avez des questions ?

Méthodologie pour la caractérisation des relais d'attaques par déni de service distribué

Camille Moriot, François Lesueur, Nicolas Stouls, Fabrice Valois, Marie-Pierre Escudié

camille.moriot@insa-lyon.fr

Journée thématique du GT SSLR 2021 sur la sécurité des réseaux

GDR Sécurité x GDR Réseaux et Systèmes Distribués

11 mai 2021

citi Lab — Inria — INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON