Sécurité du réseau fixe d'un opérateur : focus sur les dénis de service

David Roy et Pascal Nourry
david.roy@orange.com
pascal.nourry@orange.com

Orange S.A.

Résumé. La sécurité du réseau fixe des opérateurs gagne régulièrement en maturité au regard de l'évolution des menaces, de la disponibilité des mesures techniques, du contexte géopolitique et du contexte réglementaire. Après avoir rappelé ce contexte et donné quelques éléments d'architecture sur le réseau fixe d'un opérateur de communications électroniques, le présent article se focalise sur le cas particulier des attaques de dénis de service. Il aborde notamment l'évolution des attaques, les techniques de détection mises en œuvre et il donne une vue sur l'outillage à la main de l'exploitant pour faire face à ces attaques. L'article fera un focus sur la mise en œuvre de BGP Flowspec. Puis il s'attardera sur la détection des attaques dans un L2VPN en analysant les remontés IPFIX (template L2-IP) et sur le déploiement des contre-mesures via Netconf.

1 Introduction

La première partie de l'article donne quelques éléments de contexte sur les menaces qui pèsent sur les opérateurs réseaux, sur la réglementation en matière de sécurité des réseaux, sur l'architecture du réseau d'Orange France et sur la politique de sécurité mise en œuvre. La deuxième partie décrit l'évolution des attaques de dénis de service (Denial of Service - DoS ou Distributed Denial of Service - DDoS) depuis 20 ans. Elle s'attarde notamment sur les contre-mesures mises en œuvre pour lutter contre les attaques DDoS par amplification et réflexion dans la sous-section 3.3 page 10. Elle se focalise ensuite sur les contre-mesures dynamiques basées sur BGP Flowspec récemment mises en œuvre devant la montée en puissance des attaques mixtes dans la sous-section 3.4 page 15. Elle se termine par le traitement atypique des attaques dans des L2VPN grâce aux informations collectées auprès des routeurs en IPFIX en utilisant le template L2-IP et en modifiant dynamiquement la configuration des routeurs via Netconf dans la sous-section 3.5 page 18.

2 Quelques éléments de contexte

2.1 Contexte Géopolitique

Historiquement, un nombre limité d'acteurs travaillaient « en confiance » sur les prémices du réseau qui allait devenir quelques années plus tard Internet. La résilience des réseaux était une priorité, mais pas leur sécurité. Des protocoles non sécurisés comme BGP (Border Gateway Protocol) ont été spécifiés et déployés il y a plus de trente ans [26]. Les serveurs connectés au réseau Internet étaient considérés comme sûr. Les acteurs historique de l'Internet ne pensaient pas qu'un serveur pouvait être piraté et attaqué par un tiers. Envoyer des paquets IP en usurpant l'adresse IP d'un tiers était inconcevable, entre ingénieurs de bonne composition. Puis le nombre d'acteurs a grandi de façon exponentielle pour atteindre la dimension qu'Internet a aujourd'hui. Depuis une vingtaine d'années, alternant incidents involontaires [1] et attaques intentionnelles de la part d'individus isolés [2] ou d'agences étatiques, [3] la sécurité est désormais prise en compte dans les réseaux des opérateurs qui constituent Internet. Elle évolue sans cesse au gré des menaces comme les attaques de dénis de service.

2.2 Contexte réglementaire français

Le contexte réglementaire a évolué depuis une dizaine d'années en France en matière de sécurité des opérateurs de communications électroniques [25]. Sans vouloir être exhaustif, il est possible de mentionner :

— Les obligations des opérateurs prévues dans le code des postes et des communications électroniques en matière de sécurité des réseaux, à l'image des articles D98-4 (disponibilité des réseaux) et D98-5 (I-secret des correspondances ; III- sécurité et intégrité des réseaux et des services).

1. L'incident mondial qui a touché le service Youtube en 2008 est un cas d'école souvent cité pour illustrer la faiblesse du protocole BGP (voir [2, 9, 21, 30] pour plus de détails) dans le contexte d'un incident qui peut être considéré comme involontaire dans sa dimension mondiale.

2. Les mouvements sociaux comme les *Gilets Jaunes* transpirent également sur Internet en prenant la forme d'attaques DoS ciblées observables sur le réseau d'Orange. Un autre exemple concerne le domaine des jeux en ligne ou des joueurs peu scrupuleux n'hésitent pas à lancer une attaque DoS contre leurs adversaires pour gagner une partie.

3. En matière de sécurité des réseaux et bien avant les révélations de Snowden en 2012, il est difficile de ne pas citer comme exemple la compromission du réseau mobile de Vodafone Greece en 2004-2005. Pour plus de détails voir [6] ou [29].

— La loi de programmation militaire 2014-2019 a introduit dans le code de la défense des contraintes particulières pour les OIV (Opérateurs d'Importance Vitale) des SAIV (Secteurs d'Activité d'Importance Vitale - dont le secteur « Communications électroniques, audiovisuel et information »). Il permet à l'ANSSI d'imposer des règles aux SIIV (Systèmes d'Information d'Importance Vitale). Un arrêté [28] fixe ainsi les règles applicables aux opérateurs de communications électroniques.
— Le code pénal intègre un dispositif atypique, en l'occurrence l'article 226-3, dans le contexte du secret des correspondances. Il soumet à autorisation de l'ANSSI la plupart des équipements réseaux utilisés par les opérateurs de communications électroniques. Tous les routeurs de coeur de réseau sont ainsi soumis à autorisation en raison. Ce dispositif a récemment évolué dans le contexte de la loi 5G [1] en élargissant les contraintes pour les opérateurs concernés.

Au delà de cette réponse réglementaire, il est également possible de mentionner le travail pédagogique appréciable de l'ANSSI. Il prend la forme de publications pédagogiques comme le guide sur la configuration de BGP [4] ou le guide sur la compréhension et l'anticipation des attaques DDoS [5].

2.3 Cas d'un réseau fixe en France

Genèse Il faut remonter aux années 1990 pour voir les prémices du réseau IP d'Orange sous la forme d'un réseau ATM. Le RBCI (Réseau Backbone et Collecte Internet), au sens de l'AS3215, est né en 1999 (voir figure 1).

Il n'a eu de cesse d'évoluer depuis. Au niveau capacitaire, le coeur a suivi l'évolution des performances des routeurs et des liens de transmissions :

— 1999 : liens STM POS à 155Mb/s,
— 2000 : liens POS à 2,5Gb/s,
— 2002 : liens POS à 10Gb/s,
— 2006 : liens 10GE à 10 Gb/s,
— 2014 : liens 100GE à 100 Gb/s.

Le Térabit par seconde de trafic observé aux bornes du RBCI a été passé en 2011 et les 10 Tb/s ont été franchis en 2018. Au niveau fonctionnel, d'un simple réseau offrant l'accès à Internet IPv4, le RBCI s'est mué en réseau complexe offrant des services VoIP, multicast, MPLS (L2VPN ou L3VPN) et IPv6 tant pour les besoins des offres Orange que pour les clients Wholesale.Les offres Orange Wholesale sont des offres de gros proposées aux opérateurs français afin de leur permettre de connecter, à

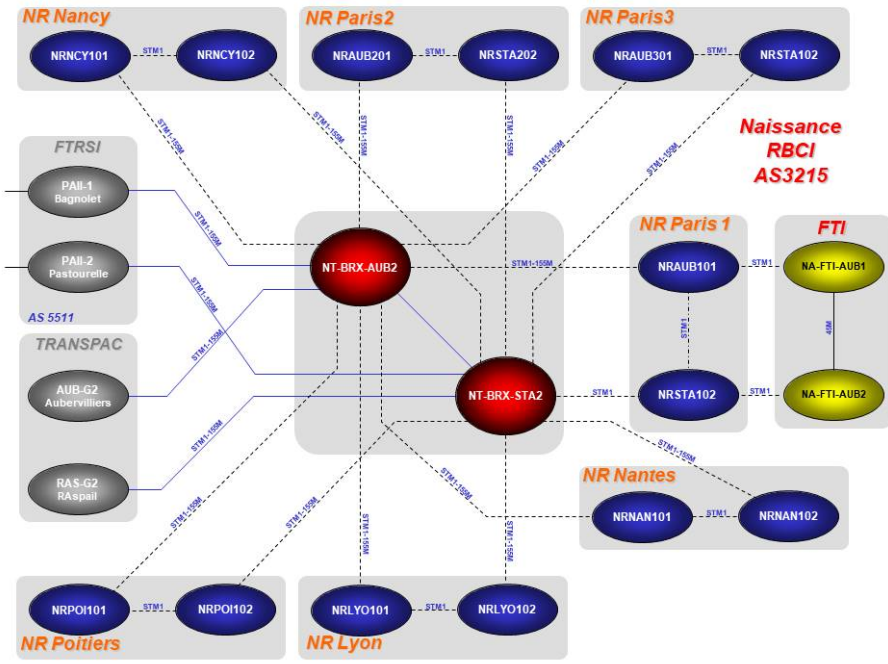

Fig. 1. Naissance du réseau d'Orange, l'AS3215 - RBCI, en 1999

travers le réseau fixe d'Orange, des clients qu'ils ne peuvent pas raccorder directement. L'architecture même du réseau a évolué au gré des usages afin d'optimiser dans les années 2000 le trafic très décentralisé là où aujourd'hui, un nombre limité d'acteurs concentre une part significative du trafic à l'image de Google/Youtube, Netflix ou Facebook.

Architecture réseau Le trafic usuel vient des points d'échanges nationaux et internationaux. Il transite par le coeur du RBCI, les réseaux de collecte et le réseau d'accès avant d'atteindre sa destination finale, un client Orange.

Les routeurs du RBCI qui raccordent les réseaux nationaux (respectivement internationaux) sont appelés routeurs de peering nationaux (resp. internationaux) ou points d'échanges nationaux (resp. internationaux). Le terme d'ASBR (Autonomous System Border Router) est également utilisé dans la suite du document pour identifier ces routeurs en bordure des autres réseaux. Dans le contexte des offres Wholesale reposant sur des tunnels MPLS de type L2VPN, le terme de PE (Provider Edge) désigne les routeurs de bordure.

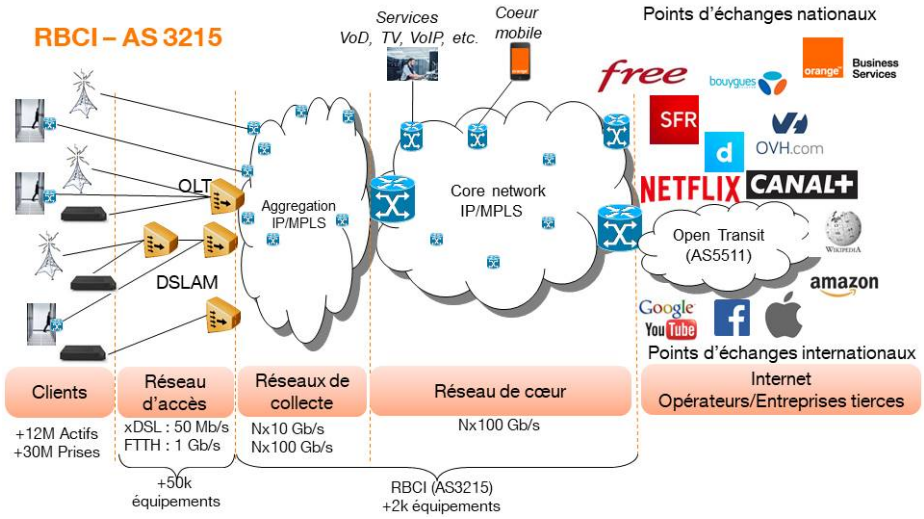

Fig. 2. Vue simplifiée du réseau IP d'Orange, l'AS3215 - RBCI

2.4 Politique de sécurité

Genèse La première politique de sécurité du réseau IP d'Orange date de 2004 dans un contexte déjà mouvementé entre la propagation rapide et massive des premiers virus *réseau* comme Blaster et sur fond de lutte contre le SPAM. Elle a ensuite évolué structurellement en 2008 puis en 2012-2013 pour prendre sa forme actuelle. La politique de sécurité du réseau IP est désormais composée :

- d'un document chapeau inspiré de la méthode EBIOS [3] identifiant les principes de sécurité mis en œuvre,
- de documents d'ingénierie et d'exploitation qui déclinent les principes de sécurité en explicitant la mise en œuvre opérationnelle et les procédures idoines,
- d'une automatisation permettant le déploiement de configuration et la vérification de la conformité des configurations avec une cible.

L'ensemble de ces documents vit grâce à une collaboration étroite entre l'exploitation et l'ingénierie du RBCI comme illustré figure 3.

Principes La politique de sécurité du RBCI se base sur quelques principes élémentaires :

- Les équipements en périphérie du RBCI doivent protéger le RBCI des agressions extérieures
  - fiabilisation des en-têtes IP (anti-spoofing, marquage QoS, etc.),

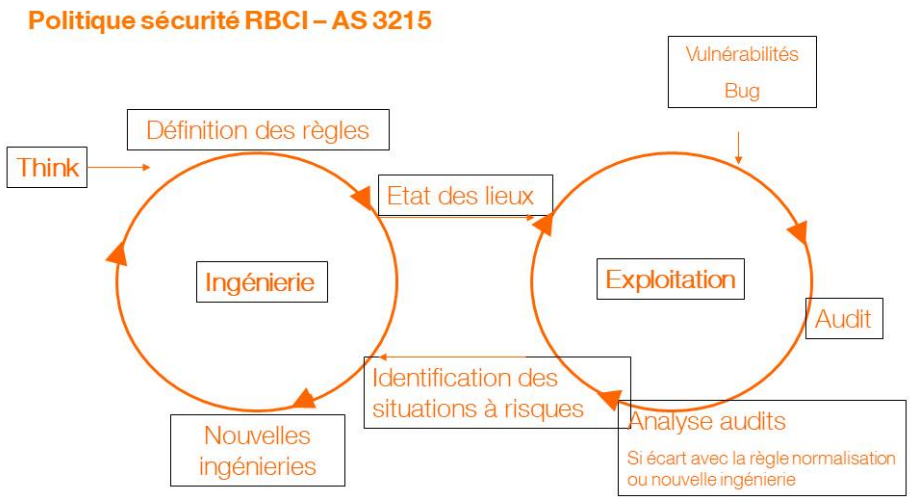

Fig. 3. Principe de mise en œuvre de la politique de sécurité

  - destruction du trafic non légitime (adresse IP source privée, mécanismes anti-DoS, etc.),
  - limitation de la visibilité du RBCI vis-à-vis de l'extérieur,
  - fiabilisation du plan de contrôle en mettant en œuvre notamment les bonnes pratiques BGP,
- Chaque équipement du RBCI doit se protéger en contrôlant toute information à destination de son plan de contrôle ou de son plan de management
  - mise en place de filtres sur la base de l'en-tête IP avec dans certains cas des limitations en débit,
  - exploitation des équipements en utilisant des protocoles sécurisés (par exemple SSHv2 avec une vigilance particulière sur les suites cryptographiques utilisées) et permettant un contrôle fin des accès,
  - mise en œuvre de la QoS afin de privilégier par exemple le plan de management et le plan de contrôle aux dépens du plan de données,
- Le RBCI doit être intégralement redondé pour être résilient dans tous les cas de panne simple, y compris en cas de *coup de pelleteuse* sur un axe de transmission.

Cette politique de sécurité prend tout son sens dès lors qu'il s'agit de mettre en œuvre des mécanismes de détection des incidents de dénis

de service et des mesures défensives pour protéger le réseau et les clients d'Orange de ces incidents. La section suivante va détailler la posture prise sur le RBCI au gré de l'évolution de la menace.

3 Attaques DoS

Les attaques DoS ne sont pas une nouveauté. Elles ont d'ailleurs déjà fait l'objet de présentations au SSTIC en 2005 [7] et en 2017 [24]. L'ANSSI a par ailleurs publié un guide en la matière en 2015 [5]. Cette section se focalise sur l'évolution des mesures prises par Orange au grè de l'apparition de nouvelles attaques. Elle s'attarde notamment sur les contre-mesures mises en œuvre pour lutter contre les attaques DDoS par amplification et réflexion dans la sous-section 3.3 page 10. Elle se focalise ensuite sur les contre-mesures dynamiques basées sur BGP Flowspec récemment mises en œuvre devant la montée en puissance des attaques mixtes dans la sous-section 3.4 page 15. Elle se termine par le traitement atypique des attaques dans des L2VPN grâce aux informations collectées auprès des routeurs en IPFIX en utilisant le motif L2-IP et en modifiant dynamiquement la configuration des routeurs via Netconf dans la sous-section 3.5 page 18.

3.1 Phase 1 : exploitation d'anomalies (1992-2004)

Les premières attaques Il est difficile de remonter l'historique des attaques de dénis de service et de donner la date de la première attaque. Dans les années 1990, la plupart des attaques de dénis de service exploitait des failles dans les logiciels.

Ainsi, en 1992, un faille dans l'implémentation d'ICMP sur SunOS 4.1x permettait à distance de fermer toutes les connexions réseaux d'un système vulnérable [10].

Les premiers cas d'usurpation d'adresse IP semblent mentionnés par le CERT-CC en janvier 1995 [11]. Plusieurs attaques de dénis de service sont ensuite documentés en 1996 par le CERT-CC. Il s'agit à vrai dire d'un festival puisque les principaux protocoles alors utilisés sont concernés, et cela sur toutes les plate-formes :

— En janvier 1996, une attaque DoS touchant UDP [12],
— En septembre 1996, les premiers cas de TCP Syn Flood [13],
— En décembre 1996, l'attaque *Ping to death* fait son apparition [8,14].

De nouvelles attaques apparaîtront les années suivantes, des routeurs étant eux même vulnérables à certaines d'entre-elles comme l'attaque *Land* [15] ou une vulnérabilité dans SNMP [17]. D'autres impactent le fonctionnement des réseaux comme l'attaque *Smurf* [16].

Les premières contre-mesures mises en œuvre sur le RBCI Il s'agissait alors principalement d'activer l'anti-spoofing sur les points de raccordement des clients Orange (Wanadoo) et de mettre en place des filtres de protection sur les accès aux équipements réseaux afin que seules les adresses IP sources autorisées puissent se connecter aux routeurs en administration.

3.2 Phase 2 : Premiers botnet (2002-2011)

Virus et Botnet Les années 2000 ont été marquées par l'exploitation de plusieurs failles depuis Internet afin de compromettre des PC/serveurs et d'exécuter des tâches à l'insu de leurs propriétaires : envoi massif de mails ou attaques de dénis de service.

Un exemple connu est le virus Blaster qui, en 2003, exploitait une faille dans l'interface RPC (Remote Procedure Call, principalement le port TCP 135) sur les systèmes Microsoft [18]. L'une des nuisances était de lancer une attaque DDoS sur le domaine `windowsupdate.com` [31].

Détection des attaques transitant par le RBCI Les premiers outils de détection ont été mis en œuvre sur le transitaire international du RBCI en 2007-2008 ce qui a permis d'avoir une idée de l'ampleur des attaques de dénis de service. Le RBCI s'est doté d'une capacité de détection limitée fin 2010 en se basant principalement sur les données netflow [20] des routeurs de peering nationaux/internationaux.

Quelques attaques étaient observées par mois avec des débits de l'ordre de 1 Gb/s provenant principalement de botnet internationaux et ciblant des clients d'Orange Pro/Entreprise ou des institutions. Elles dépassaient rarement 10 Gb/s, duraient généralement moins de 30 min et provenaient principalement des points de peering internationaux.

	1T09	2T09	3T09	4T09
Attaques entre 1 et 2 Gb/s	0	1	1	0
Attaques entre 2 et 4 Gb/s	0	0	0	0
Débit indicatif RBCI en Tb/s	0,6	0,6	0,7	0,7

Tableau 1. Nombre d'attaques DoS identifiées sur le RBCI par trimestre en 2009 (aucune attaque au-delà de 4 Gb/s)

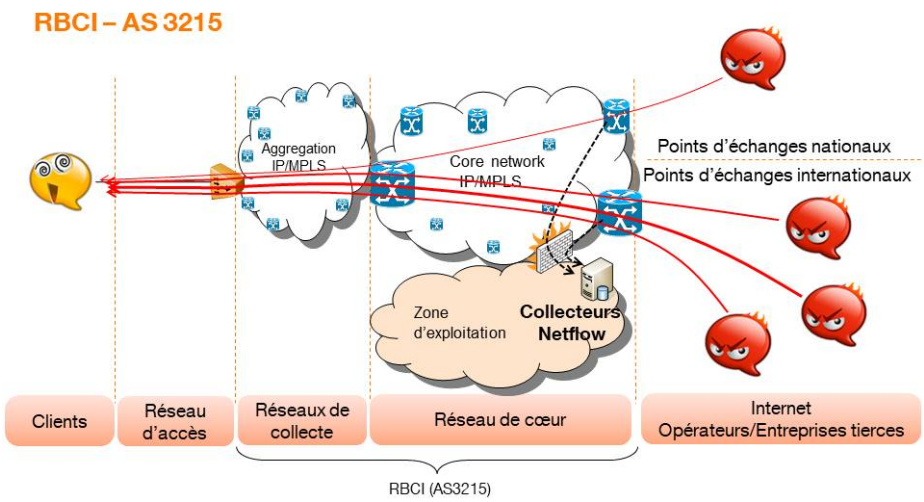

Fig. 4. Détection des attaques DoS sur le RBCI en 2011

Les contre-mesures mises en œuvre sur le RBCI En cas d'incident impactant un axe du RBCI, les exploitants avaient à leur disposition deux outils artisanaux :

— D'une part ils avaient la possibilité de déployer manuellement un filtre sur les points de peering nationaux et/ou internationaux, au plus près des sources de l'attaque si elles étaient identifiées. Un filtre s'entend ici par la capacité des routeurs à détruire du trafic sur une interface du routeur sur la base de l'adresse IP source/destination, du protocole ou du port source/destination. Les filtres sont implémentés en hardware et ils n'impactent usuellement pas les performances des routeurs.

— D'autre part, ils pouvaient activer un blackhole sur l'adresse IP destination cible de l'attaque s'il s'agissait de la seule information disponible, toujours au niveau des points de peering nationaux et/ou internationaux. Un blackhole consiste à introduire une route pour une adresse IP donnée vers l'interface *poubelle* du routeur à savoir null0. Cette mesure est radicale dans le sens où, si elle préserve le RBCI de toute saturation, elle détruit tout le trafic à destination de la cible de l'attaque sur le routeur concerné. Quelque part, elle permet donc à l'attaquant de nuire quand même à sa victime.

Cette boite a outil manuelle a été relativement peu utilisée pour plusieurs raisons :

— Le principal soucis de l'opérateur et de ne pas saturer les liens entre les routeurs. Sinon, plusieurs dizaines (voir centaines) de milliers de clients peuvent être impactés par une seule attaque. Les liens du RBCI pouvant alors absorber Nx10 Gb/s de trafic additionnel au trafic de pointe légitime, les attaques ne saturaient pas ces liens.

— Les délais de détection conjugués aux délais d'intervention faisaient que l'attaque était généralement terminée lorsque les exploitants étaient prêt à activer le filtre.

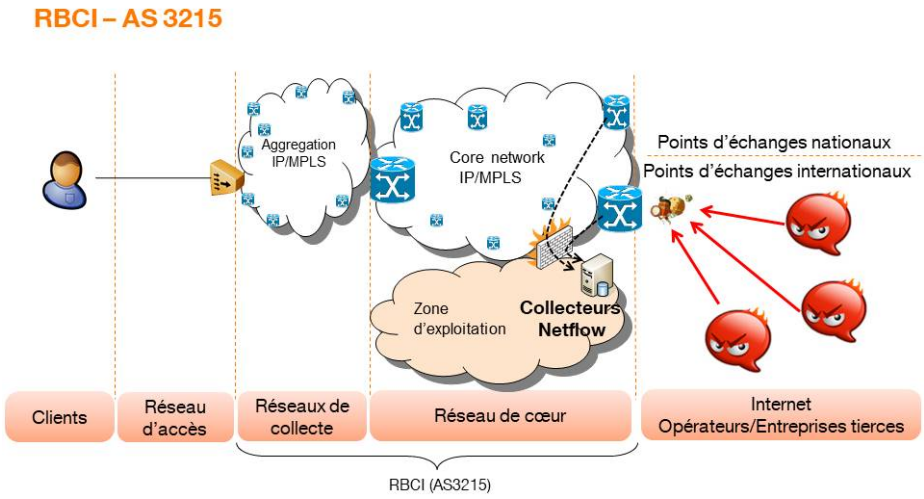

Fig. 5. Mise en œuvre d'un blackhole sur les routeurs de peering internationaux

3.3 Phase 3 : amplification et réflexion (2011-2015)

Click & DoS Les attaques par amplification/réflexion ont gagné en intérêt en 2011 notamment avec l'explosion des services Cloud. Ce type d'attaque s'appuie sur deux propriétés :

— d'une part sur des vulnérabilités (bug, faille comportementale) de certains services ouverts sur l'Internet (DNS, NTP, SNMP, SSDP, etc.),

— et d'autre part sur la capacité de ces services à générer une disparité d'utilisation de la bande passante entre une requête et une réponse.

> On parle ici de facteur d'amplification. Par exemple si une requête utilise un paquet de 128 octets et que la réponse en retour fait 1280 octets on parle d'un facteur d'amplification de 10.

Plusieurs sources recensent les vecteurs d'amplification les plus connus et leur signature à l'image du CERT-US [19]. Comme explicité dans ce document, ces attaques s'appuient toutes sur le protocole non connecté UDP à opposer au protocole connecté TCP. Il est donc possible d'usurper l'adresse IP source d'une victime afin d'adresser une requête vers un service Internet et la victime recevra la réponse.

Sur les réseaux d'opérateurs comme Orange, ces attaques sont généralement massivement distribuées en termes d'adresses IP sources (= adresses IP des rebonds utilisés pour l'amplification) mais visent la plupart du temps une IP destination unique. Les conséquences pour l'opérateur sont indirectes (la conséquence directe étant l'indisponibilité du site ou client visé). En effet, ces attaques, par leur caractère amplifié, sont très consommatrices de bande passante (plusieurs dizaines, voire centaines de Gbps) et ont pour conséquence la saturation de certains axes réseau de l'opérateur, perturbant ainsi indirectement l'ensemble du trafic de l'axe.

Observation sur le RBCI Ces attaques ont fait leur apparition sur le RBCI début 2012 avec d'emblée des débits plus élevés que les débits jusque là observés pour les attaques DoS de type *Botnet*. De quelques Gb/s, les attaques sont passées à quelques dizaines de Gb/s en quelques semaines avec un débit standard entre 30 et 40 Gb/s durant l'été 2012. Autre évolution substantielle, la fréquence des attaques supérieures à 1 Gb/s a été multipliée par 100 entre fin 2011 et fin 2012. Pendant la même période, le débit global du RBCI a augmenté de 30% environ. Des outils DoS sur étagère simples d'emploi et partiellement gratuits ont fait leur apparition en 2012. Les enjeux pour les attaquants ont aussi changé. Les attaques visent des clients grand public derrière une Livebox (profil souvent visé : les Gamers) ou plus rarement et habituellement en fonction de l'actualité (ex. G7, COP, Mouvement de grève) un site/service sensible pour lequel Orange est transitaire (service des Impôts, site gouvernemental, établissements scolaires...).

Orange a développé des outils dédiés à la supervision des ports UDP utilisés comme vecteurs d'attaque par réflexion et amplification. Dans un premier temps, ils se basaient sur le relevé de compteurs en SNMP. Ils ont désormais évolué vers de la Télémétrie.

Débit attaques En Gb/s	1T 2011	2T 2011	3T 2011	4T 2011	1T 2012	2T 2012	3T 2012	4T 2012	1T 2013	2T 2013	3T 2013	4T 2013
Entre 2 et 4	1	3	7	12	16	?	?	63	485	1124	919	1375
Entre 4 et 8	0	0	2	4	11	6	15	27	72	333	301	366
Entre 8 et 16	0	1	0	1	2	11	3	3	11	89	75	52
Entre 16 et 32	0	0	0	0	0	2	5	4	1	6	10	2
Entre 32 et 64	0	0	0	0	0	0	6	0	2	1	1	3
Entre 64 et 128	0	0	0	0	0	0	0	0	0	0	1	0
RBCI en Tb/s	0,8	0,8	0,9	1	1,1	1,1	1,1	1,3	1,4	1,4	1,5	1,6

Tableau 2. Nombre d'attaques DoS identifiées sur le RBCI par trimestre en 2011, 2012 et 2013 (aucune attaque au-delà de 128 Gb/s)

Industrialisation des contre-mesures mises en œuvre sur le RBCI La fréquence des attaques et le volume des attaques ont obligé Orange à réagir en industrialisant les contre-mesures :

— Une réflexion sur la gestion différenciée de la QoS (Quality of Service) a été initiée en 2008 sur le RBCI sous la forme d'une classification/priorisation/gestion différenciée des trafics dits sensibles de ceux dits *Best Effort*. Un trafic voix ou le trafic d'administration des routeurs par exemple ne seront pas traités de la même façon que du trafic Internet au sein des routeurs. En cas de congestion provoquée par une attaque venant d'Internet ("Best Effort") – le trafic sensible sera préservé (voix, administration des routeurs, protocole de routage). Le déploiement opérationnel a été réalisé en 2009-2010.

— La mise en place de filtres « statiques » de limitation de bande passante sur les signatures d'amplification les plus connus, notamment celles décrites par [19], à la périphérie du réseau d'Orange. Les outils précédents de supervision permettent un suivi fin de l'évolution des débits et d'adapter les seuils de déclenchement.

— L'ingénierie et les procédures de mise en œuvre des blackholes (ou puits de trafic) ont été revues afin de permettre un usage plus rapide et plus précis.

Quelques précisions techniques :

— Les filtres statiques sont positionnés en sortie sur les axes ASBR (Autonomous System Border Router = routeurs de peering) vers les routeurs de cœur afin d'améliorer la finesse des filtres et de limiter les zones arrières concernées.

— La bande passante autorisée par port source UDP est allouée globalement à l'axe ASBR vers le routeur de cœur indépendamment

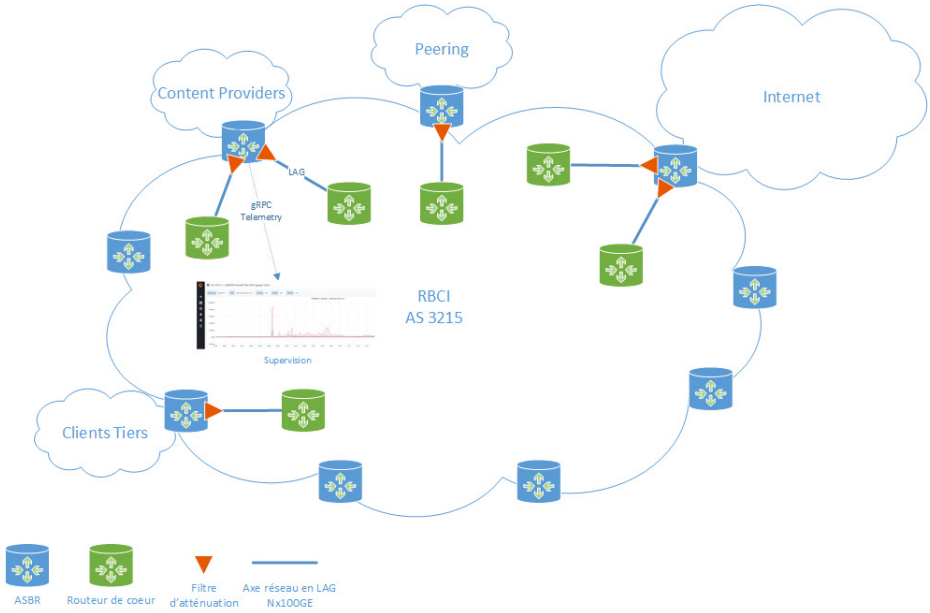

Fig. 6. Traitement des attaques DDoS par réflexion et amplification sur le RBCI

du nombre de liens présents dans le *Bundle* de liens 100GE (LAG Nx100GE). Cette valeur est distribuée et ajustée dynamiquement en fonction du nombre N de liens actifs dans le bundle. Ce point est important car il évite de modifier les valeurs de la bande passante autorisée lors des mises à jour capacitaires ou encore lors d'incidents mettant hors service certains liens physiques du bundle. Il s'appuie sur une fonction aujourd'hui uniquement disponible sur les routeurs Juniper nommée : `shared-bandwidth-policer` [23]

— Un suivi du trafic nominal, des attaques et atténuations résultantes est effectué via un canal de Telemetry gRPC.

Un exemple de configuration d'un routeur Juniper pour l'atténuation des attaques NTP par amplification est fourni ci-après :

```
term NTP {
    from {
        protocol udp;
        source-port ntp;
    }
    then {
        policer DOS-NTP;
        count DOS-NTP;
        accept;
    }
}
```

```
[...]
policer DOS-NTP {
    shared-bandwidth-policer;
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 625000;
    }
}
[...]
```

Listing 1. Filtre appliqué sur les routeurs

Échanges entre les opérateurs et avec les autorités françaises Durant cette période 2011-2015, plusieurs initiatives nationales ont vu le jour afin de partager les expériences respectives. La partie immergée de l'iceberg a été la publication du guide *Comprendre et anticiper les attaques DDoS* [5] par l'ANSSI avec la participation de plusieurs opérateurs dont Orange. Il est aussi possible de citer un effort particulier des opérateurs pour réduire la participation de nos clients aux attaques de dénis de service par amplification et par réflexion :

— Les opérateurs ont corrigés ou échangés des box qui comportaient des bug (ex : service DNS récursif ouvert sur l'interface WAN) utilisés par les personnes malveillantes pour lancer des attaques par amplification et par réflexion.
— Certains clients, notamment professionnels (ex : chaînes de magasin), ont choisi d'installer leur propre modem/routeur alternatifs mais ils l'ont mal configurés, laissant ouvert de nombreux ports ensuite utilisés par des personnes malveillantes pour lancer des attaques par amplification et par réflexion. Les cellules Abuse ont du intervenir, suite à des plaintes de tiers, pour inviter ces clients à mieux configurer leur modem/routeur.

Au niveau européen, l'ETNO (European Telecommunications Network Operators) a permis de partager l'évolution des menaces, les incidents et les bonnes pratiques. Au niveau international, les échanges avec les fournisseurs ont permis de faire évoluer les équipements réseaux (par exemple à travers l'identification de bugs dans l'implémentation de BGPFlowspec), les outils de détection et les outils dédiés au filtrage de trafic.

Les offres dédiées aux clients entreprises ont vu le jour pendant cette période. Il s'agit ici d'informer le client des attaques qu'il subit et, en fonction du choix du client, de lui proposer des contre-mesures adaptées.

3.4 Phase 4 : combinaison (2015 à aujourd'hui)

Détection d'attaques plus complexes Depuis 2015, les outils d'analyse détectent de plus en plus de dynamicité dans les signatures des attaques DDOS. La combinaison d'une attaque par amplification classique avec une attaque utilisant des ports dits dynamiques (autres que des services connus) est devenue une chose très courante sur les réseaux opérateurs. Les cibles visées étant encore, la plupart du temps, des destinations uniques. Ces attaques dynamiques ne peuvent pas être atténuées (rate-limit) ou supprimées (Blackhole) avec de simples filtres statiques.

Contre-mesures développées par Orange Orange France s'est appuyé sur deux mécanismes pour contrecarrer ces types d'attaques :

— Une détection des attaques avec une solution sur étagère.
— Des contre-mesures dynamiques s'appuyant sur un développement maison et le protocole BGP Flowspec.

En effet, aujourd'hui Orange utilise une solution sur étagère (Netscout/Arbor Peakflow SP) pour collecter les données de trafic échantillonnées (par le protocole Netflow/IPFIX) notamment en périphérie de l'AS3215. Ces données de trafic servent tout particulièrement à détecter des anomalies de trafic (comme les attaques DDOS). Cette solution fournit alors, lorsque cela est possible, une signature réseau du type d'attaque : (protocole utilisé UDP/TCP/RAW IP – Adresses IP source/destination en jeu – Ports source/destination en jeu etc...). Cette solution procède de façon progressive lors de la détection de la signature d'une attaque :

— Phase 1 : L'heuristique sur la première minute consiste à détecter/-pondérer les attaques par le débit afin de détecter rapidement les attaques les plus importantes en débit. Une alerte se déclenche sur détection d'un volume de trafic atypique vers une destination. A cet instant la solution fournit une signature macroscopique, à savoir uniquement les informations de types IP (adresses IP impliquées et protocole utilisé).
— Phase 2 : Entre 1 et 2 min après le début de la détection, la solution continue son apprentissage sur l'observation suspecte et fournit une version plus détaillée de l'attaque notamment avec les informations des couches TCP/UDP.
— Phase 3 : au-delà de 2 min, la solution effectue une mise à jour périodique de la signature de l'attaque jusqu'à ce que celle-ci s'arrête.

Ces différentes phases de détections sont disponibles au travers de notifications / API. C'est sur cette base qu'Orange France a développé

sa solution de contre-mesure des attaques dites dynamiques. La solution a été développée en Python. Elle porte le nom de code BAAM pour « Backbone Automatic Attack Mitigation ». Elle s'interface d'une part avec la solution sur étagère et d'autre part avec des Route Reflector Juniper dédiés au protocole BGP FlowSpec (FS).

Le protocole BGP Flowspec décrit, entre autres, par la RFC 5575 [27] permet de distribuer via BGP une signature réseau (adresse IP, protocole, ports etc...) et une action associée : discard, rate-limit, remarquage QoS, redirection... BGP Flowspec peut être assimilé à une solution de distribution d'ACL/de filtre via le protocole BGP. Les Route Reflector FlowSpec de l'AS3215 possèdent notamment une session iBGP FS avec tous les ASBR de l'AS3215.

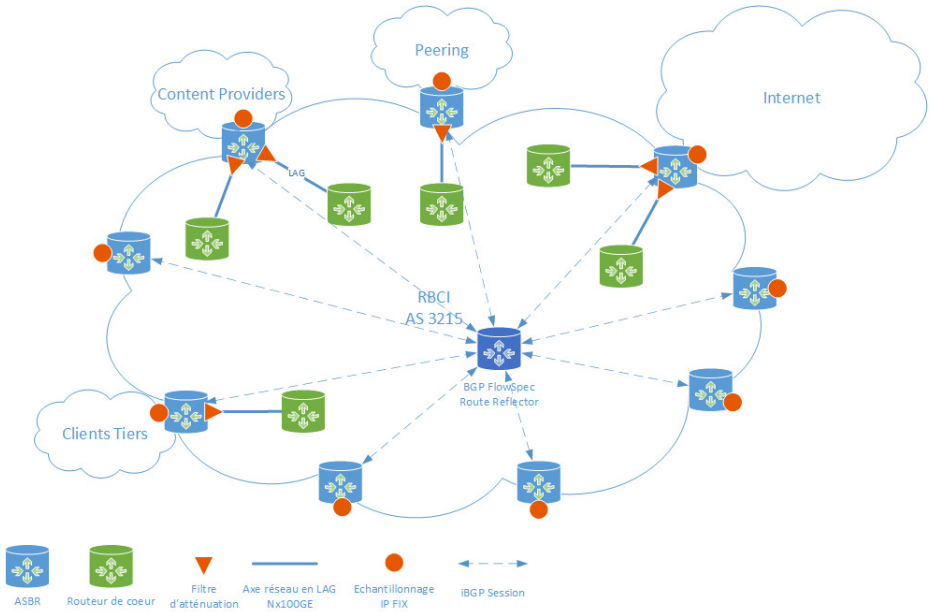

Fig. 7. Diffusion des règles de filtrage via BGP Flowspec aux ASBR

La solution propriétaire d'Orange est notifiée des attaques (lors de la Phase 1) par la solution sur étagère au travers d'un trap SNMP. Sur détection d'une attaque, l'outil propriétaire va venir poser une Route FlowSpec statique via le protocole Netconf sur les Route Reflector du RBCI. La route FlowSpec possède alors une signature macroscopique avec une action « discard » (Blackhole) basée en général sur l'adresse IP destination attaquée. Cette route FlowSpec statique est alors reflétée/distribuée, par

les Route Reflector, à l'ensemble des ASBR du réseau via BGP. En parallèle l'outil commence à interroger de façon périodique l'outil de détection en REST API pour obtenir plus de détail sur la signature. Dès que la signature détaillée est disponible, l'outil met à jour en temps réel via Netconf la définition de la route FlowSpec statique qui est à nouveau distribuée par BGP. Ceci permet d'être beaucoup plus sélectif sur le trafic à supprimer : seuls les ports participant à l'attaque visant la destination sont supprimés. Tant que l'outil n'est pas notifié par les sondes de détection que l'attaque est terminée, l'outil continue de surveiller l'évolution de la signature de l'attaque et met à jour, si nécessaire, celle-ci sur les Route Reflector.

N.B. : L'outil intègre aussi des conditions spécifiques, liées à la politique de sécurité interne à Orange, qui peuvent influer sur la pose ou non des routes FlowSpec statiques.

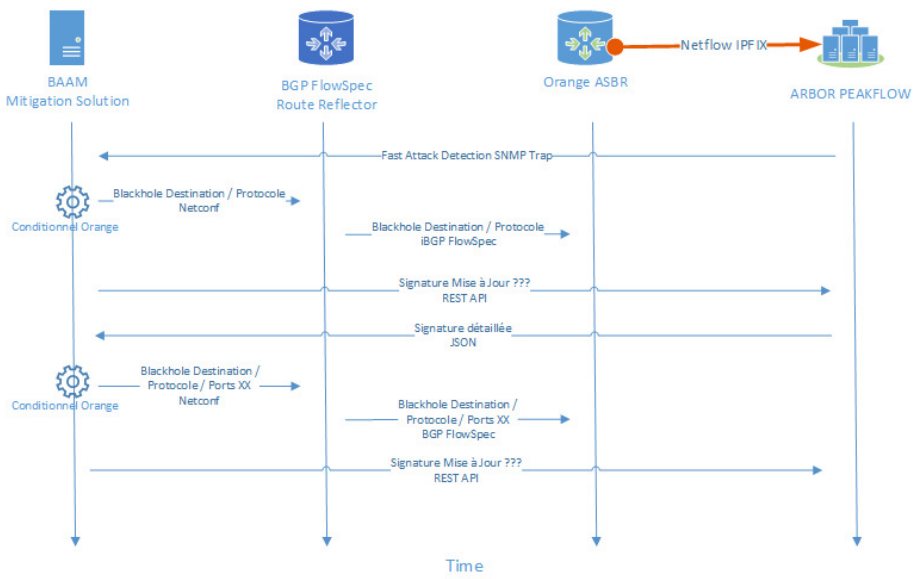

Fig. 8. Cinématique BGP Flowspec

Effet Gilets Jaunes Après avoir atteint un pic en 2015-2016, l'intensité des attaques a eu tendance à diminuer en 2017 et 2018. Le mouvement de contestation des *Gilets Jaunes* a manifestement trouvé un écho sur Internet pendant quelques mois.

Débit attaques En Gb/s	1T 2015	2T 2015	3T 2015	4T 2015	1T 2018	2T 2018	3T 2018	4T 2018	1T 2019	2T 2019	3T 2019	4T 2019
Entre 2 et 4	1702	2486	2668	4252	1169	1089	1089	2873	3990	2491	2645	1875
Entre 4 et 8	1111	1558	1768	2873	1283	917	731	2896	2590	1560	1662	1112
Entre 8 et 16	585	404	725	1143	298	653	295	1356	1400	1131	1011	1070
Entre 16 et 32	77	46	179	128	29	259	103	293	467	523	271	527
Entre 32 et 64	10	4	61	22	10	17	6	24	39	148	97	75
Entre 64 et 128	5	0	3	0	0	0	2	4	2	5	10	1
Entre 128 et 256	0	0	0	0	0	0	0	0	1	0	2	0

Tableau 3. Nombre d'attaques DoS identifiées sur le RBCI par trimestre en 2015, 2018 et 2019 (aucune attaque au-delà de 256 Gb/s)

3.5 Cas particulier des offres Wholesale : traitement des attaques DDoS affectant les L2VPN du réseau fixe

Le réseau d'Orange France AS3215 supporte de nombreuses « offres de gros », notamment des offres dites de niveau 2 (ou L2) qui consistent à collecter et livrer des trames Ethernet (Vlan ou non inclus) d'opérateurs ou clients tiers. Ces offres sont vendues par Orange Wholesale. Ces offres s'appuient sur le réseau de collecte et le cœur de réseau d'Orange France. Les ressources réseaux d'Orange sont donc mutualisées entre le trafic des clients d'Orange et ces offres de collecte L2. Orange n'a ainsi pas besoin d'interpréter la couche IP du trafic véhiculé sur ces offres de gros. Orange utilise la technologie MPLS pour faire transiter ce trafic entre des points de collecte et des points de livraison. On parle ici de technologie L2VPN et de tunnels L2VPN. Ces offres de gros permettent d'étendre le réseau de certains opérateurs / clients tiers au travers du réseau d'Orange afin que ces derniers augmentent leur capillarité afin de joindre leurs clients finaux.

Orange a subi récemment et à plusieurs reprises des attaques DDOS indirectes à l'intérieur de ces tunnels. Les attaques ne visaient pas directement des clients finaux Orange mais ceux des opérateurs / clients tiers qui étaient joignables au travers du réseau d'Orange. Orange subit dans ce cas de figure des dommages collatéraux. En effet, l'attaque DDOS véhiculée au travers du tunnel MPLS (L2VPN) peut congestionner certains axes mutualisés au sein du réseau d'Orange, généralement au niveau du réseau d'accès (de collecte) et par conséquent impacter les propres clients d'Orange mais aussi ceux d'autres opérateurs / clients tiers présents dans la zone touchée par l'attaque DDOS. La figure 9 illustre le principe.

Pour pallier ce type d'attaques, Orange s'est inspiré de la solution mise en place pour contrecarrer les attaques dynamiques. Il fallut dans un premier temps mettre en place de l'échantillonnage réseaux au niveau des

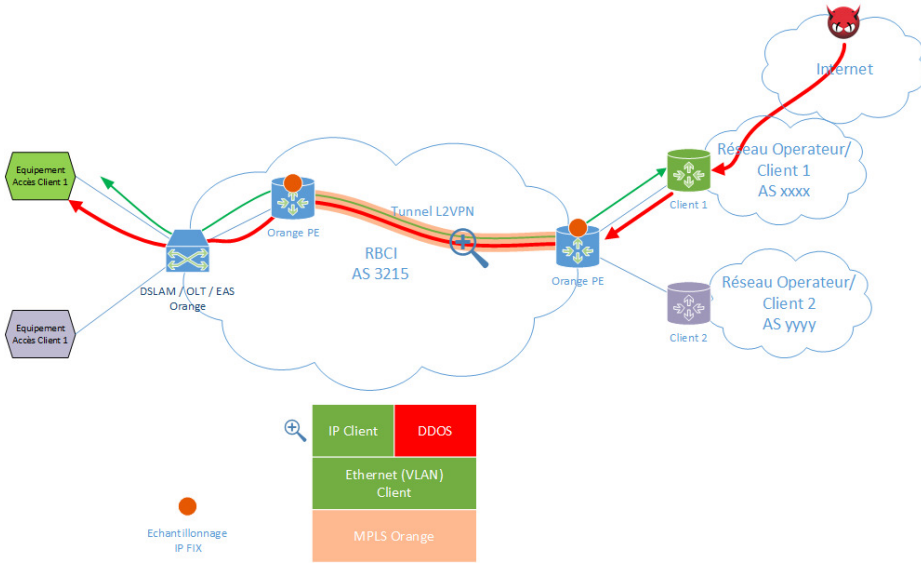

Fig. 9. Attaque DDoS sur une offre de collecte Orange Wholesale

PE Orange de collecte et de livraison. Cet échantillonnage est particulier car il s'agit de trafic L2VPN (Template IPFIX L2-IP sur routeurs Nokia). Cet échantillonnage permet d'avoir des statistiques sur les profils de trafic niveau 2 en entrée / sortie du réseau d'Orange. Qui plus est, les données échantillonnées fournissent des informations comme : les ports d'entrée/sortie des trafics, les VLANs, les adresses MACs etc... Le tableau ci-dessous liste l'ensemble des informations fournies par le template IPFIX L2-IP.

MAC Src Addr	IPv4 Src Addr	TCP control Bits (Flags)
MAC Dest Addr	IPv4 Dest Addr	Protocol
Ingress Physical Interface	IPv6 Src Addr	IPv6 Option Header
Egress Physical Interface IPv6	Dest Addr	IPv6 Next Header
Dot1q VLAN ID	Packet Count	IPv6 Flow Label
Dot1q Customer VLAN ID	Byte Count	TOS
Post Dot1q VLAN ID	Flow Start Milliseconds	IP Version
Post Dot1q Customer VLAN ID	Flow End Milliseconds	
Dest Port	Src Port	

Tableau 4. Template IPFIX L2-IP sur routeurs Nokia

Ce template, bien que supporté par les constructeurs de routeurs, n'était pas décodé par les principales solutions de collecteur IPFIX disponibles sur le marché et notamment la solution PeakFlow d'Arbor. Orange a donc travaillé avec Arbor afin que leurs sondes supportent ce nouveau template. Suite à cette implémentation, la solution PeakFlow a donc été en mesure de fournir des signatures sur le profil des attaques, il restait à mettre en place les contre-mesures d'atténuation. Malheureusement, les spécifications BGP Flowspec pour le trafic L2VPN sont encore à l'état de Draft [22] à l'IETF et non implémentées par les constructeurs de routeurs. Orange a donc développé une contre-mesure « maison » pour limiter les attaques DDOS au sein des tunnels L2VPN.

Construite sur le même principe que l'atténuation des attaques dynamiques, la solution de détection sur étagère fournit la signature des attaques DDOS L2VPN. Une solution logicielle développée par Orange, sur la base de la signature Arbor, permet ensuite d'identifier le service L2VPN, l'opérateur/client tiers, les points de collecte et livraison impliqués dans cette attaque et d'aller configurer automatiquement en CLI ou NETCONF les contre-mesures suivantes (dépendant du type d'offre/client/attaque) :

— Shutdown du port de livraison ou shutdown du port de collecte
— Shutdown du VLAN de livraison ou shutdown du VLAN de collecte
— Application d'un filtre de suppression de trafic Ethernet basé sur les adresses MAC src/dst sur le port de collecte ou de livraison.

La figure 10 résume la solution implémentée.

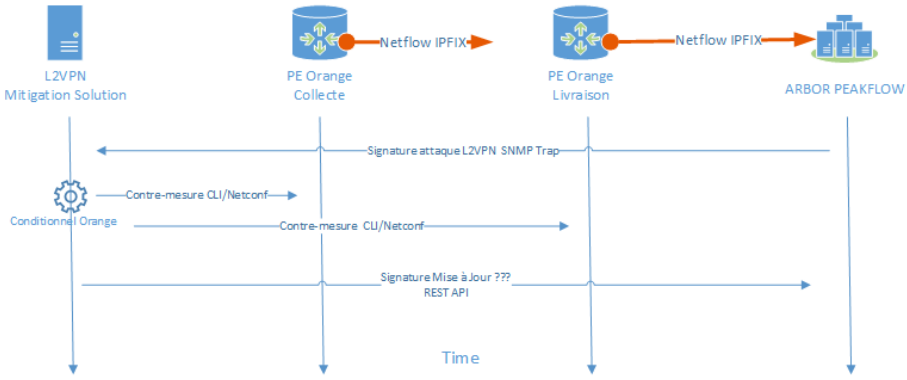

Fig. 10. Cinématique de détection et de mise en œuvre des contre-mesures dans le cas des attaques DDoS L2VPN

4 Conclusion

Depuis maintenant plus de 15 ans, Orange France a une attention particulière concernant la sécurité de son réseau fixe, le RBCI. Dans le contexte de la politique de sécurité de ce réseau, des outils de supervision des attaques de dénis de service sont mis en œuvre et régulièrement ajustés afin de tenir compte de l'évolution des attaques DoS. Il en va de même pour les contre-mesures mises en œuvre par les exploitants qui disposent aujourd'hui de contre-mesures automatisées que ce soit via BGP Flowspec ou via Netconf.

Si après un effet *Gilets Jaunes* marqué fin 2018-début 2019, la tendance est à la décrue, plusieurs évolutions doivent attirer l'attention. D'un côté, une montée notable en débit des accès clients, que ce soit côté fixe (passage du xDSL au FTTH), côté mobile (passage de la 4G à la 5G) ou chez les hébergeurs, ouvre des perspectives de montée en débit également des attaques de dénis de service, notamment en cas de botnet infectant les équipements des clients. D'un autre côté, le nombre d'objets connectés, quelques fois très mal sécurisés, a vocation à croître significativement dans les prochaines années, ouvrant la porte à des botnets de type MIRAI plus puissants.

Plus que jamais, il convient d'être vigilant, en amont, afin de détecter au plus tôt les signaux faibles qui préfigurent des attaques à venir. Outre une veille active, il est nécessaire de prendre régulièrement du recul sur les informations collectées au niveau des routeurs (IPFIX, SNMP ou Télémétrie). Il convient ensuite de déployer dès que possible des contre-mesures adaptées afin de réduire l'impact pour les clients. En se sens, le développement d'outils automatisés, basés notamment sur BGP Flowspec, Netconf ou des scripts Python, ouvre de perspectives pertinentes.

Références

1. LOI n°2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (NOR : ECOX1907688L). `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038864094&fastPos=1&fastReqId=1372147956&categorieLien=id&oldAction=rechTexte`, 2019.
2. Valentin Allaire, Sarah Nataf, and Pascal Nourry. Le routage, talon d'achille des réseaux. *C&ESAR*, 2015.
3. ANSSI. EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité. `https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/`, 2010.

4. ANSSI. Le guide des bonnes pratiques de configuration de BGP. https://www.ssi.gouv.fr/guide/le-guide-des-bonnes-pratiques-de-configuration-de-bgp/, 2013.
5. ANSSI. Comprendre et anticiper les attaques DDoS. https://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/, 2015.
6. James Bamford. A Death in Athens. https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/, 2015.
7. Renaud Bidou. Lutte contre les DoS réseau. *SSTIC*, 2005.
8. Mike Bremford. Ping of death. https://insecure.org/sploits/ping-o-death.html.
9. Martin Brown. Pakistan hijacks YouTube. http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/, 2008.
10. CERT Coordination Center, SEI, CMU. CA-1992-15 : Multiple SunOS Vulnerabilities Patched - ICMP redirects patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, all architectures. *1992 CERT Advisories*, 1992.
11. CERT Coordination Center, SEI, CMU. CA-1995-01 : IP Spoofing Attacks and Hijacked Terminal Connections. *1995 CERT Advisories*, 1995.
12. CERT Coordination Center, SEI, CMU. CA-1996-01 : UDP Port Denial-of-Service Attack . *1996 CERT Advisories*, 1996.
13. CERT Coordination Center, SEI, CMU. CA-1996-21 : TCP SYN Flooding and IP Spoofing Attacks. *1996 CERT Advisories*, 1996.
14. CERT Coordination Center, SEI, CMU. CA-1996-26 : Denial-of-Service Attack via ping. *1996 CERT Advisories*, 1996.
15. CERT Coordination Center, SEI, CMU. CA-1997-28 : IP Denial-of-Service Attacks. *1997 CERT Advisories*, 1997.
16. CERT Coordination Center, SEI, CMU. CA-1998-01 : Smurf IP Denial-of-Service Attacks. *1998 CERT Advisories*, 1998.
17. CERT Coordination Center, SEI, CMU. CA-2002-03 : Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP). *2002 CERT Advisories*, 2002.
18. CERT Coordination Center, SEI, CMU. CA-2003-20 : W32/Blaster worm. *2003 CERT Advisories*, 2003.
19. CERT-US. Alert (TA14-017A), UDP-Based Amplification Attacks (Original release date : January 17, 2014 ; Last revised : December 18, 2019. https://www.us-cert.gov/ncas/alerts/TA14-017A.
20. B. Claise. Cisco Systems NetFlow Services Export Version 9. RFC 3954, RFC Editor, October 2004.
21. François Contat, Sarah Nataf, and Guillaume Valadon. Influence des bonnes pratiques sur les incidents BGP. *SSTIC*, 2012.
22. W. Hoa, D. Eastlake, J. Uttaro, S. Litkowski, and S. Zhuang. BGP Dissemination of L2 Flow Specification Rules. INTERNET-DRAFT draft-ietf-idr-flowspec-l2vpn-13, INTERNET-DRAFT, December 2019.
23. Juniper. JunOS Tech Library, class of service user guide, shared-bandwidth-policer (Configuring). https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/shared-bandwidth-policer-edit-firewall-cs.html.

24. Octave Klaba. Conférence d'ouverture. *SSTIC*, 2017.
25. Franck Laurent and Pascal Nourry. Contexte réglementaire pour les opérateurs 5G. *C&ESAR*, 2019.
26. Kirk Lougheed and Yakov Rekhter. A Border Gateway Protocol (BGP). RFC 1105, RFC Editor, June 1989.
27. P. Marques, N. Sheth, R. Raszuk, B. Greene, J. Mauch, and D. McPherson. Dissemination of flow specification rules. RFC 5575, RFC Editor, August 2009.
28. Pour le Premier ministre et par délégation, le secrétaire général de la défense et de la sécurité nationale L. Gautier. Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous- secteur d'activités d'importance vitale «Communications électroniques et Internet» et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense (NOR : PRMD1630591A). `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033521327&fastPos=1&fastReqId=166301648&categorieLien=id&oldAction=rechTexte`, 2016.
29. Vassilis Prevelakis and Diomidis Spinellis. The Athens Affair. `https://spectrum.ieee.org/telecom/security/the-athens-affair`, 2007.
30. RIPE. YouTube Hijacking : A RIPE NCC RIS case study. `https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study`, 2008.
31. Symantec. W32.Blaster.Worm. `https://www.symantec.com/fr/ca/security-center/writeup/2003-081113-0229-99`, 2003.