Quand le ciel s'effondre

Atténuation à l'échelle du réseau des attaques DDoS à haut volume par réflexion/amplification

Roland Dobbins rdobbins@arbor.net
Ingénieur principal, ASERT

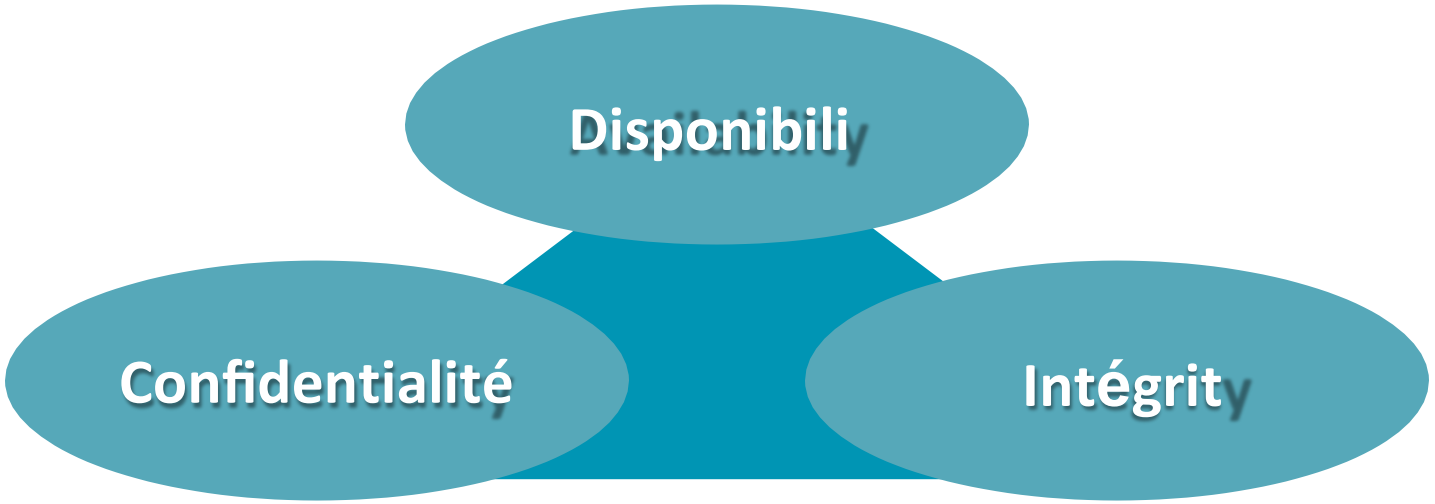
Introduction & Contexte

Contexte des DDoS

Qu'est-ce qu'une attaque par déni de service distribué (DDoS) ?

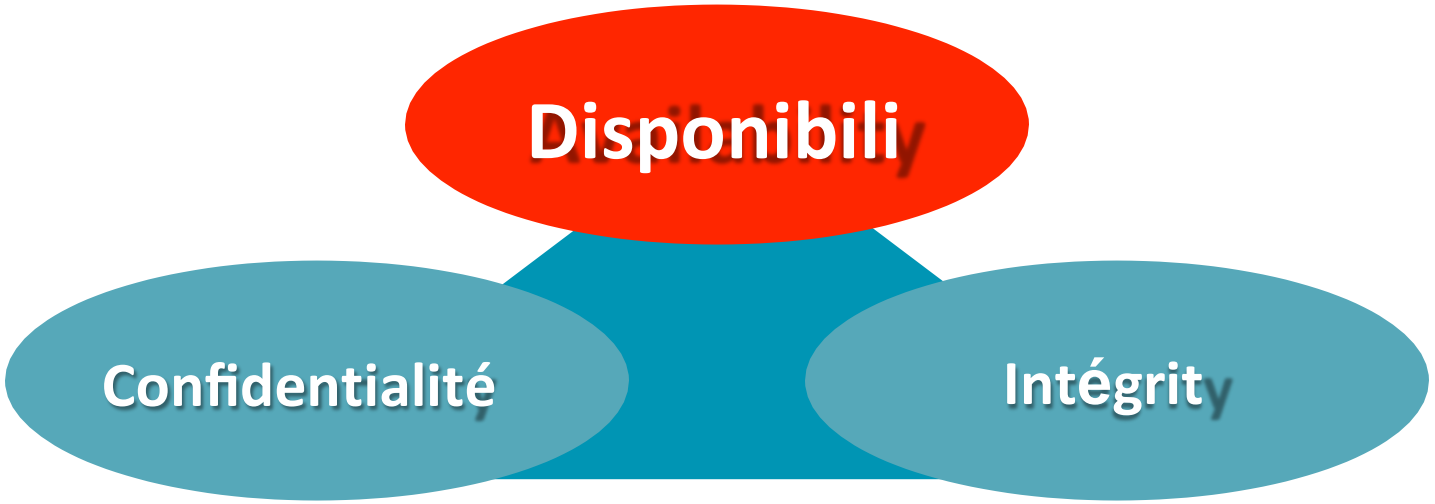
- Une tentative de **consommer des ressources** limitées, d'**exploiter les faiblesses** de la conception ou de la mise en œuvre du logiciel, ou d'**exploiter le manque de capacité de** l'infrastructure.
- Cible la **disponibilité** et l'**utilité** des ressources informatiques et du réseau.
- Les attaques sont presque toujours **distribuées** pour avoir un effet encore plus important (par exemple, DDoS).
- Les **dommages collatéraux** causés par une attaque peuvent être aussi graves, voire pires, que l'attaque elle-même.
- **Les attaques DDoS affectent la disponibilitéPas de** disponibilité, no applications/services/ data/Internet! pas de revenus !
- Les attaques DDoS sont des attaques **contre la capacité et/ou l'état** !

Trois caractéristiques de



- L'objectif de la sécurité est de maintenir ces trois caractéristiques

Trois caractéristiques de



- L'objectif principal de la défense contre les DDoS est de maintenir la disponibilité face aux attaques.

La quasi-totalité des dépenses et des efforts en matière de sécurité sont axés sur la confidentialité et l'intégrité.

- La confidentialité et l'intégrité sont des concepts relativement simples, faciles à comprendre pour les non-spécialistes.
- Dans la pratique, la confidentialité et l'intégrité équivalent à peu près au cryptage, ce qui est facile à comprendre pour les non-spécialistes.
- En réalité, ils ne se limitent pas au cryptage, mais il est facile de crier victoire : "Nous avons un antivirus, nous avons le cryptage des disques, nous sommes conformes aux normes PCI, woo- hoo ! ”
- Et pourtant, des centaines de millions d'hôtes infectés par des robots, des réseaux d'entreprises de toutes tailles et de tous secteurs ont été complètement pénétrés, la propriété intellectuelle a été volée, des secrets militaires ont été divulgués, etc.
- La disponibilité ne peut pas être modifiée - le serveur Web, le serveur DNS et le PBX VoIP sont soit en service, soit hors service. Il n'y a aucun moyen d'obscurcir, d'exagérer ou de tergiverser en ce qui concerne la posture de sécurité réelle, dans le monde réel.
- La disponibilité exige des praticiens de la sécurité opérationnelle (opsec) qui comprennent le TCP/IP et le routage/commutation ; qui comprennent les serveurs Web ; qui comprennent les serveurs DNS ; qui comprennent la sécurité ; qui comprennent la couche 7.
- Ces personnes sont rares et ne sont pas bon marché. La plupart des organisations ne connaissent même pas les compétences requises et l'étendue de l'expérience à rechercher afin d'identifier et d'engager les bonnes personnes.

La disponibilité est difficile !

- Le maintien de la disponibilité face à une attaque exige une combinaison de compétences, d'architecture, d'agilité opérationnelle, de capacités d'analyse et d'atténuation que la plupart des organisations ne possèdent tout simplement pas.
- En pratique, la plupart des organisations ne tiennent jamais compte de la disponibilité lorsqu'elles conçoivent/spécifient/construisent/déploient/testent des applications/services/propriétés en ligne.
- Dans la pratique, la plupart des organisations ne font jamais le lien logique entre le maintien de la disponibilité et la continuité des activités.
- Dans la pratique, la plupart des organisations ne soumettent jamais leurs piles d'applications/services à des tests de stress afin de déterminer les lacunes en matière d'évolutivité/résilience et de les corriger.
- En pratique, la plupart des organisations n'ont pas de plan d'atténuation des attaques DDoS - ou si elles ont un plan, elles ne le répètent jamais !

Reflection/Amplification des attaques DDoS

Évolution des attaques DDoS par réflexion/amplification

- De nombreuses variétés d'attaques DDoS par réflexion/amplification ont été observées "dans la nature" depuis **18 ans ou plus.**
- À partir d'octobre 2013, des attaques DDoS de réflexion/amplification NTP très médiatisées ont été lancées contre divers services de **jeux en ligne**.
- Avec des **dizaines de millions d'utilisateurs simultanés** touchés, ces attaques ont été rapportées dans la presse technologique grand public.
- Mais ces attaques ne sont pas nouvelles - les **plus grandes attaques DDoS observées** sont toutes des attaques par réflexion/amplification, et **ce depuis des années**.
- Les attaques par réflexion/amplification nécessitent de pouvoir **usurper l'adresse IP de la cible** visée.
- Dans la plupart des attaques DDoS volumétriques, le débit (pps) est plus important que bandwidth (bps). Dans la plupart des attaques DDoS par réflexion/amplification, **le bps est plus important que le pps** - il remplit les tuyaux !

Composants d'une attaque DDoS par réflexion/amplification

Amplification

- L'attaquant fait une demande relativement petite qui génère une réponse beaucoup plus grande. C'est le cas de la plupart des réponses du serveur (pas toutes).

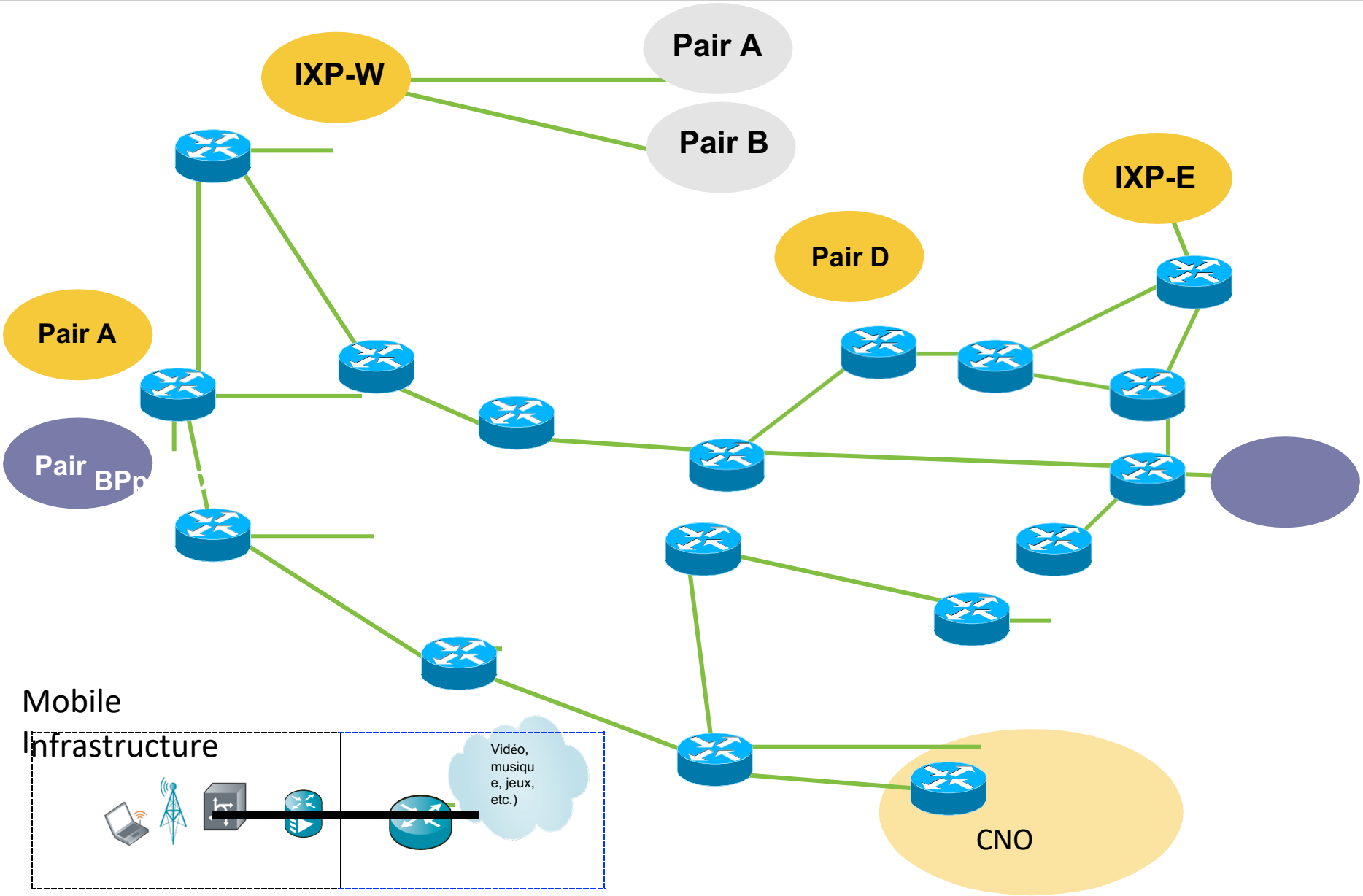
Réflexion

- L'attaquant envoie des requêtes usurpées à un grand nombre de dispositifs connectés à Internet, qui répondent aux requêtes. Grâce à l'usurpation d'adresse IP, l'adresse "source" est définie comme la cible réelle de l'attaque, où toutes les réponses sont envoyées. De nombreux services peuvent être exploités pour servir de réflecteurs.

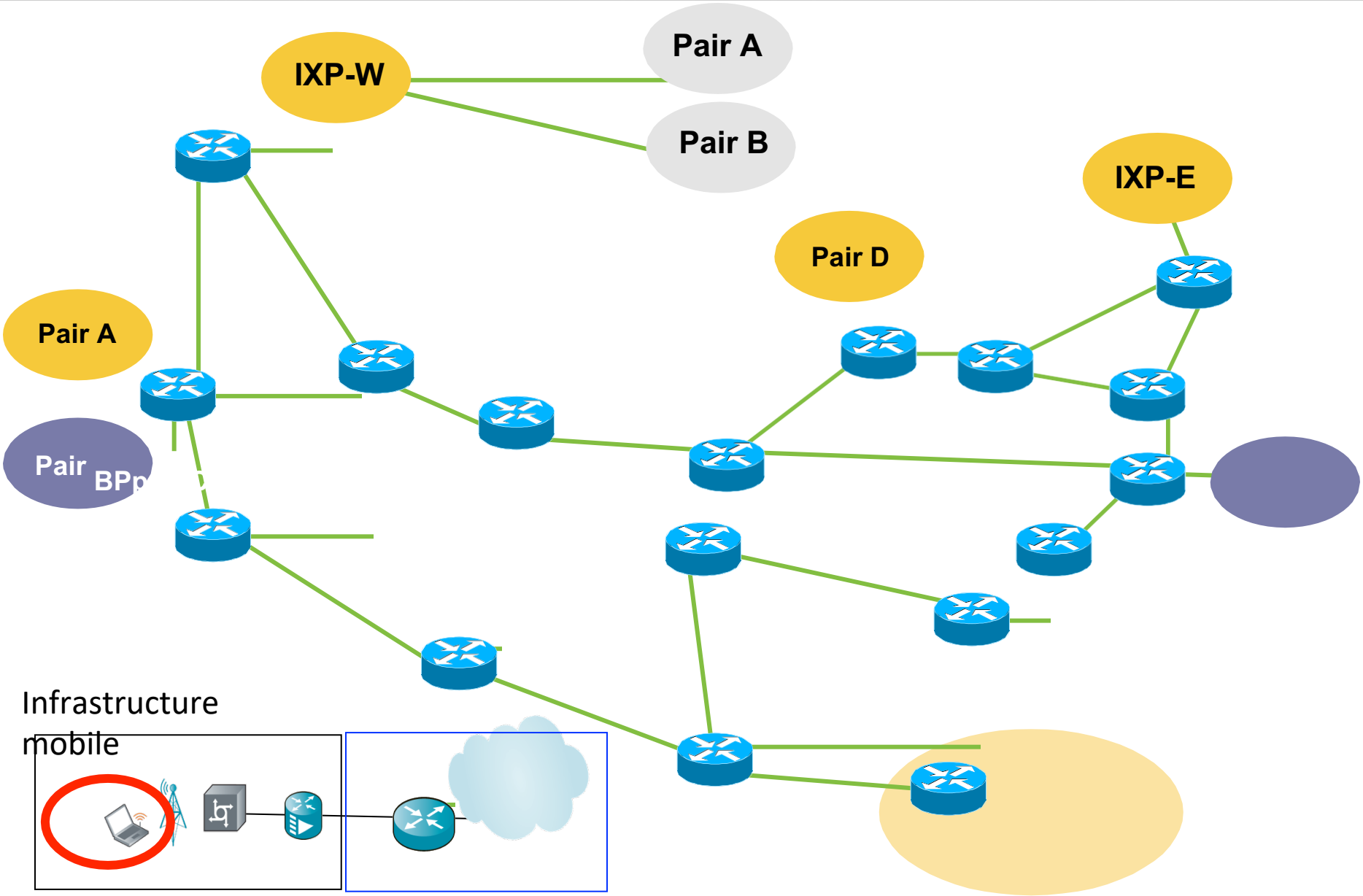
Impact des attaques DDoS par réflexion/amplification

- Les serveurs, les services, les applications, l'accès à l'Internet, etc. sur le réseau cible ***sont submergés et rendus indisponibles*** par le simple volume de trafic - des dizaines ou des centaines de gigaoctets par seconde fréquemment.
- ***Saturation complète*** des liens de peering/transit du réseau cible.
- ***Saturation totale ou quasi-totale*** des liaisons d'échange de trafic/liaisons de transit/liaisons principales des réseaux intermédiaires entre les réflecteurs/amplificateurs et le réseau cible - y compris les réseaux des pairs directs/fournisseurs de transit du réseau cible.
- ***Dommages collatéraux généralisés*** - perte de paquets, retards, forte latence pour le trafic Internet des parties non impliquées qui se trouvent simplement à traverser des réseaux saturés par ces attaques.
- ***Indisponibilité*** des serveurs/services/applications, accès à l'Internet pour les spectateurs topologiquement proches du réseau cible.

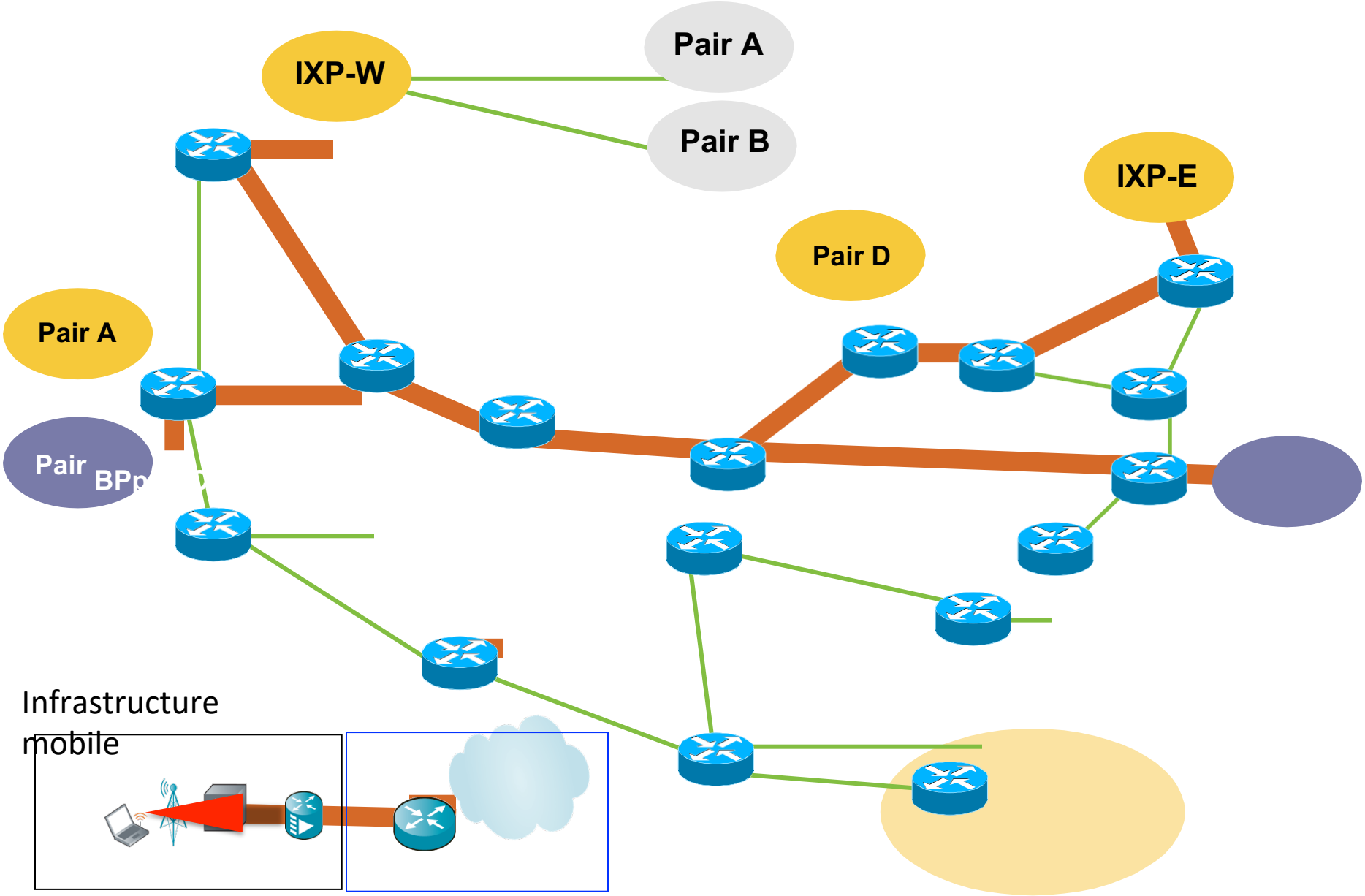
Effets d'une attaque DDoS de réflexion/amplification de 400 Go/s sur la capacité du réseau



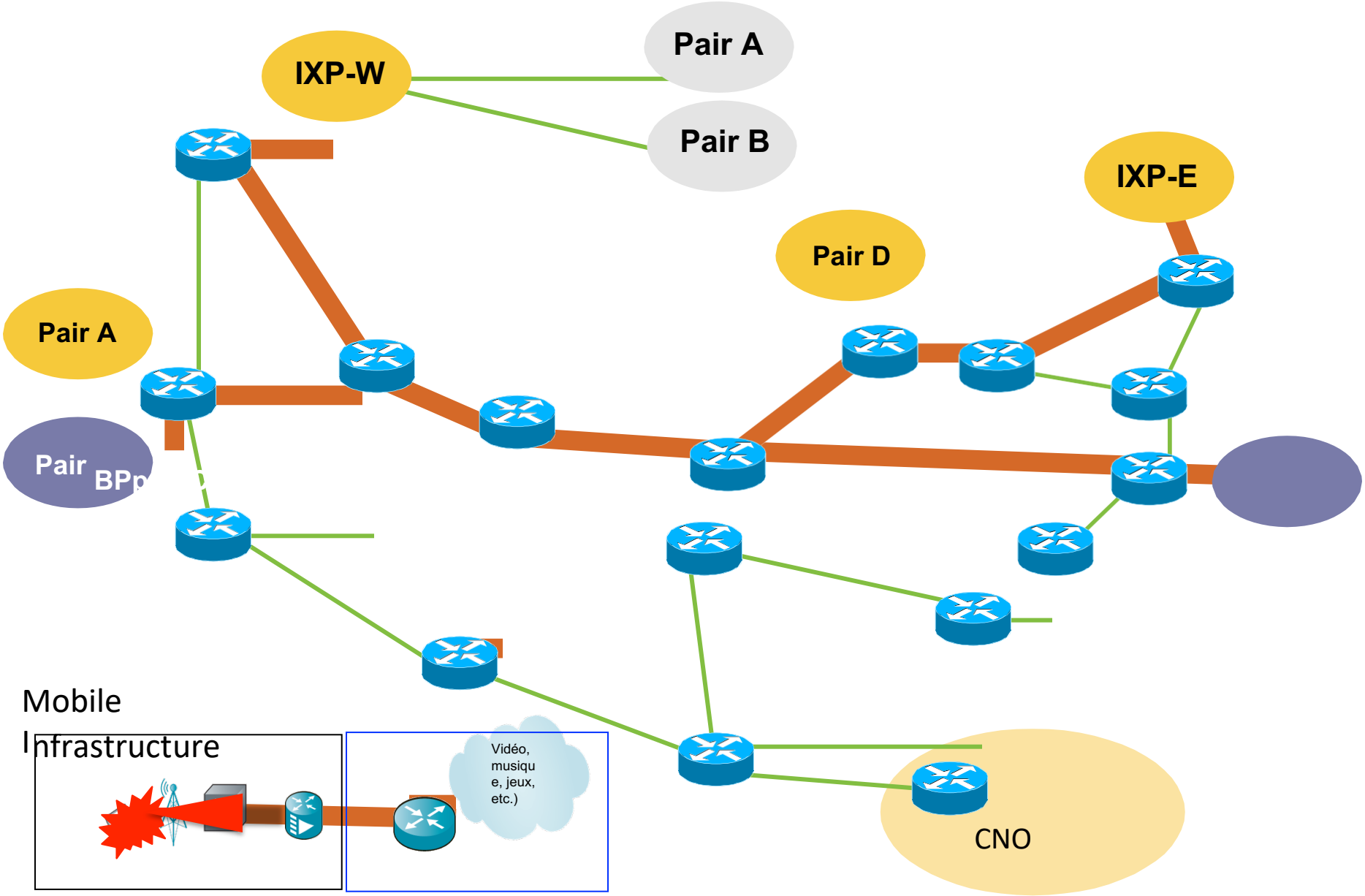
Effets d'une attaque DDoS de réflexion/amplification de 400 Go/s sur la capacité du réseau



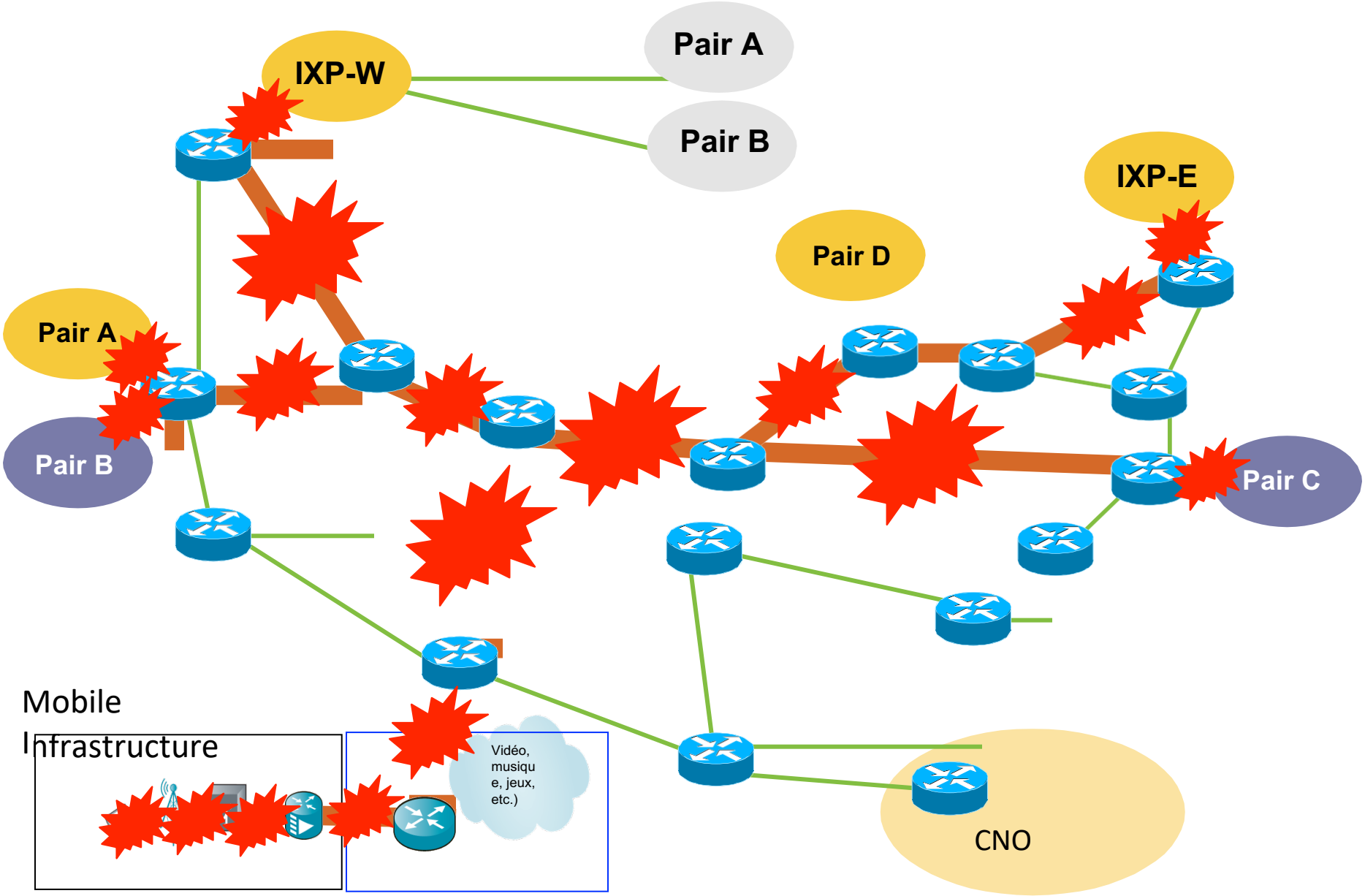
Effets d'une attaque DDoS de réflexion/amplification de 400 Go/s sur la capacité du réseau



Effets d'une attaque DDoS de réflexion/amplification de 400 Go/s sur la capacité du réseau



Effets d'une attaque DDoS de réflexion/amplification de 400 Go/s sur la capacité du réseau



Les deux principaux facteurs qui rendent ces attaques possibles

- Non-déploiement de ***mécanismes de validation de l'adresse source (par exemple, anti-spoofing)*** tels que Unicast Reverse-Path Forwarding (uRPF), ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, ACLs, etc. sur tous les bords des réseaux des ISP et des entreprises.

- ***Services mal configurés et abusifs*** fonctionnant sur des serveurs, des routeurs, des commutateurs, des dispositifs CPE domestiques, etc.

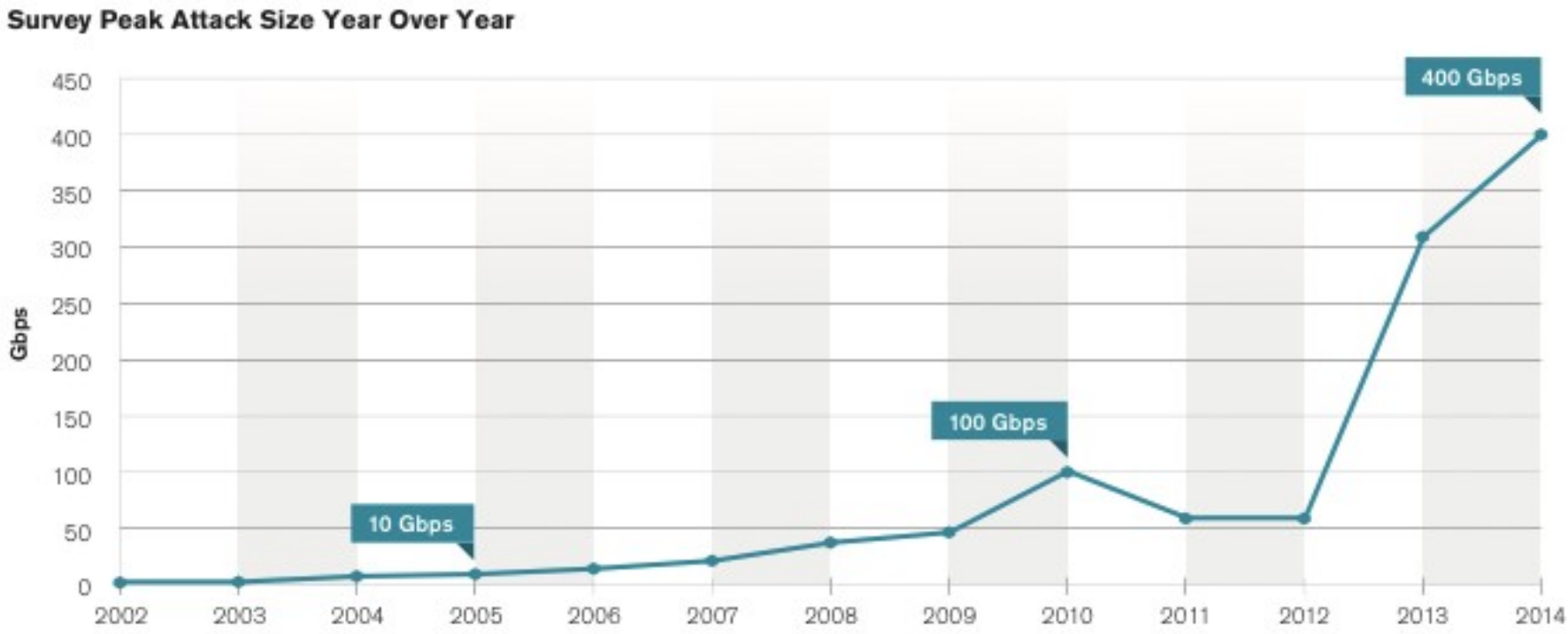
Les deux principaux facteurs qui rendent ces attaques possibles

- Non-déploiement de ***mécanismes de validation de l'adresse source (par exemple, anti-spoofing)*** tels que Unicast Reverse-Path Forwarding (uRPF), ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, ACLs, etc. sur tous les bords des réseaux des ISP et des entreprises.

- ***Services mal configurés et abusifs*** fonctionnant sur des serveurs, des routeurs, des commutateurs, des dispositifs CPE domestiques, etc.

Croissance des volumes d'attaques DDoS, 2002 - 2014

La *quasi-totalité de la* croissance du volume des attaques DDoS au cours des 12 dernières années est due à la montée en popularité des méthodologies de reflection/amplification des attaques DDoS.



La capacité à usurper le traffic est *nécessaire pour* lancer des attaques de reflection/amplification DDoS.

Facteurs contributifs supplémentaires

- Les opérateurs de réseau n'utilisent pas la collecte et l'analyse de ***la télémétrie des flux*** (par exemple, NetFlow, cflowd/jflow, etc.) pour la détection/classification/retour des attaques.
- Les fournisseurs d'accès à Internet et les entreprises ne parviennent pas à ***rechercher de manière proactive les services abusifs*** *sur leurs réseaux* ***et à y remédier, ni à*** rechercher et à alerter les clients/utilisateurs utilisant des services abusifs - en ***bloquant les services abusifs*** jusqu'à ce qu'ils soient corrigés, si nécessaire.
- L'incapacité à déployer et à utiliser efficacement des ***outils de réaction et d'atténuation des attaques DDoS***, tels que Source-Based Remotely-Triggered Blackholing (**S/RTBH)**, **flowspec** et Intelligent DDoS Mitigation Systems (**IDMS)**.
- L'incapacité à ***financer et à donner la priorité à la disponibilité au*** même titre que la confidentialité et l'intégrité dans la sphère de la sécurité.
- L'***incapacité de*** nombreuses entreprises/ASP à souscrire au programme ***"Clean Pipes"***.

  Services d'atténuation des attaques DDoS offerts par les ISP/MSSP.

Quels types d'appareils sont utilisés de manière abusive ?

- Dispositifs ***CPE (customer premise equipment) à large bande pour les consommateurs*** - par exemple, routeurs/modems à large bande domestiques avec des paramètres par défaut de facteurs non sécurisés (et parfois insécurisables !).
- ***Dispositifs d'équipement de fournisseur (PE) de qualité commerciale*** - par exemple, des ***routeurs et des commutateurs de couche 3*** plus grands et ***plus puissants*** utilisés par les FAI et les entreprises.
- ***Serveurs (réels ou virtuels)*** exécutant des démons de service mal configurés et abusifs - serveurs domestiques mis en place par les utilisateurs finaux, serveurs commerciaux mis en place par les FAI et les entreprises.
- Les ***appareils intégrés*** comme les imprimantes connectées au réseau (!), les enregistreurs numériques, etc.
- L'***internet des objets*** est en train de devenir rapidement le ***botnet des objets*** !

Réflexion/Amplification Attaque Terminologie

- ***Source de l'attaque*** - point d'origine des paquets d'attaque usurpés.
- ***Réflecteur*** - nœuds par lesquels les paquets d'attaque sont "réfléchis" vers la cible de l'attaque et/ou vers un nœud amplificateur séparé avant d'être réfléchis vers la cible.
- ***Amplificateur*** - nœuds qui reçoivent des paquets d'attaque non usurpés de la part des nœuds réflecteurs et génèrent ensuite des paquets de réponse beaucoup plus grands, qui sont renvoyés aux réflecteurs.
- ***Réflecteur/amplificateur*** - nœuds qui effectuent à la fois la réflexion et l'amplification des paquets d'attaque, puis transmettent les réponses non usurpées et amplifiées à la cible finale de l'attaque. De nombreuses attaques par réflexion/amplification (pas toutes) fonctionnent de cette manière.
- ***Trajet d'attaque*** - éléments distincts du chemin logique que le trafic d'attaque emprunte pour aller de la source de l'attaque aux réflecteurs/amplificateurs, et des réflecteurs/amplificateurs à la cible de l'attaque.

Trafic spolié et trafic non spolié

- Source de l'attaque - reflector/amplifier les adresses IP sources sont ***usurpées L'***. attaquant ***usurpe l'***adresse IP de la cible ultime de l'attaque.
- Si des réflecteurs et des amplificateurs distincts sont impliqués, le trafic du réflecteur vers l'amplificateur ***n'***est ***pas usurpé***, le trafic de l'amplificateur vers le réflecteur ***n'***est ***pas usurpé*** et le trafic du réflecteur vers la cible de l'attaque ***n'***est ***pas usurpé***.
- Si des réflecteurs/amplificateurs combinés sont impliqués, le trafic entre les réflecteurs/amplificateurs et la cible de l'attaque ***n'***est ***pas usurpé***.
- Cela signifie que la cible de l'attaque voit les ***véritables adresses IP*** du trafic d'attaque qui l'assaillent à l'étape ultime de l'attaque.
- Ce fait a des ***implications positives*** importantes ***pour les options d'atténuation*** disponibles pour la cible de l'attaque - mais ***le nombre même d'IP sources*** est souvent un facteur de complication.

Cinq vecteurs de réflexion/amplification courants

- **Chargen** – 30-year-old tool for testing network link integrity and performance.
  Rarement (jamais ?) utilisé de nos jours pour son objectif – 30-year-old tool for testing network link integrity and performance. initial. Mis en œuvre de manière absurde à l'ère moderne par des vendeurs de périphériques embarqués sans expérience.
- **DNS** - le système de nom de domaine résout les noms humains en adresses IP. Il fait partie du "plan de contrôle" de l'internet. Pas de DNS = pas d'Internet.
- **SNMP** - Simple Network Management (gestion de réseau simple) Protocol.
  Utilisé pour surveiller et éventuellement configurer les dispositifs, services, etc. Protocol. de l'infrastructure du réseau.
- **NTP** - Network Time Protocol fournit des services de synchronisation du temps pour votre routers/switches/laptops/tablets/phones/etc. service Internet le plus important dont routers/switches/laptops/tablets/phones/etc.
  vous n'avez jamais entendu parler.
- **SSDP** - Simple Services Discovery Protocol (protocole de découverte de services simples) agit comme un système d'énumération de services mal conçu et mal mis en œuvre pour le système d'information de l'entreprise.
  UPnP mal conçu et mis en œuvre.

La réflexion/amplification ne se limite pas à ces cinq vecteurs.

- De nombreux protocoles/services peuvent être exploités par les attaquants pour lancer des attaques DDoS par réflexion/amplification.
- Ces cinq éléments - DNS, chargen, SNMP, SSDP et NTP - sont des vecteurs de réflexion/amplification couramment observés.
- La plupart des attaques par réflexion/amplification (pas toutes) utilisent le protocole UDP.
- Les mêmes principes généraux que ceux évoqués à propos de ces cinq vecteurs s'appliquent également aux autres.
- Il existe des différences spécifiques aux protocoles et aux services qui s'appliquent également.
- Les attaquants étudient et utilisent aussi activement d'autres vecteurs de réflexion/amplification - soyez prêt !

Cinq vecteurs de réflexion/amplification courants

Abréviation	Protocole	Ports	Facteur d'amplification	# Serveurs abusifs
CHARGEN	Protocole de génération de caractères	UDP / 19	18x/1000x	Des dizaines de milliers (90K)
DNS	Système de nom de domaine	UDP / 53	160x	Millions (27M)
NTP	Protocole de temps réseau	UDP / 123	1000x	Plus de cent mille (119K)
SNMP	Protocole de gestion de réseau simple	UDP / 161	880x	Millions (5M)
SSDP	Protocole de découverte de service simple	UDP /1900	20x/83x	Millions (2M)

Reflection/Amplification du PNT

Facteur d'amplification - NTP

Abréviation	Protocole	Ports	Facteur d'amplification	# Serveurs abusifs
CHARGEN	Protocole de génération de caractères	UDP / 19	18x/1000x	Des dizaines de milliers (90K)
DNS	Système de nom de domaine	UDP / 53	160x	Millions (27M)
NTP	Protocole de temps réseau	UDP / 123	1000x	Plus de cent mille (119K)
SNMP	Protocole de gestion de réseau simple	UDP / 161	880x	Millions (5M)
SSDP	Protocole de découverte de service simple	UDP /1900	20x/83x	Millions (2M)

Caractéristiques d'une attaque par réflexion/amplification

- L'attaquant ***usurpe l'***adresse IP de la cible de l'attaque, envoie *monlist*, *showpeers* ou d'autres requêtes administratives NTP de niveau 6/-7 à plusieurs services NTP abusifs fonctionnant sur des serveurs, des routeurs, des dispositifs CPE domestiques, etc.
- L'attaquant choisit le port UDP qu'il souhaite cibler (généralement UDP/80 ou UDP/123, mais il peut s'agir de ***n'importe quel port de son choix***) et l'utilise comme source.
- Les services NTP "répondent" à la cible de l'attaque avec flux ***non falsifiés*** de paquets de ~468 octets ***provenant de UDP/123*** vers la cible ***; le port de destination est le port source choisi par l'attaquant*** pour générer les requêtes NTP *monlist/showpeers/etc.*

Caractéristiques d'une attaque par réflexion/amplification (suite)

- Lorsque ces multiples flux de réponses NTP ***non usurpées*** convergent, le volume de l'attaque peut être ***énorme*** - la plus grande attaque vérifiée de ce type à ce jour ***dépasse les 300 gigaoctets par seconde***. Les attaques de ***100gb/sec*** sont monnaie courante.
- En raison du volume des attaques, la ***bande passante de transit Internet*** de la cible, ainsi que la bande passante principale des pairs/amonts de la cible, de même que la bande passante principale des réseaux intermédiaires entre les divers services NTP utilisés abusivement et la cible, sont ***saturées*** par le trafic d'attaque ***non usurpé***.
- Dans la plupart des attaques, les attaquants exploitent entre ~4 000 et ~7 000 services NTP abusifs. ***Jusqu'à 50 000 services NTP*** ont été observés dans certaines attaques.

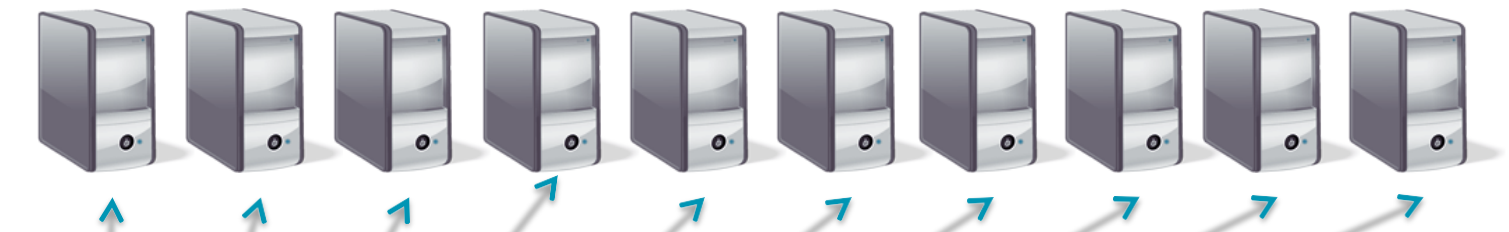
Méthodologie d'attaque par réflexion/amplification du NTP

NTP abusif Serveurs

Serveurs accessibles par Internet, routeurs, dispositifs CPE domestiques, etc.

172.19.234.6/32

Méthodologie d'attaque par réflexion/amplification du NTP

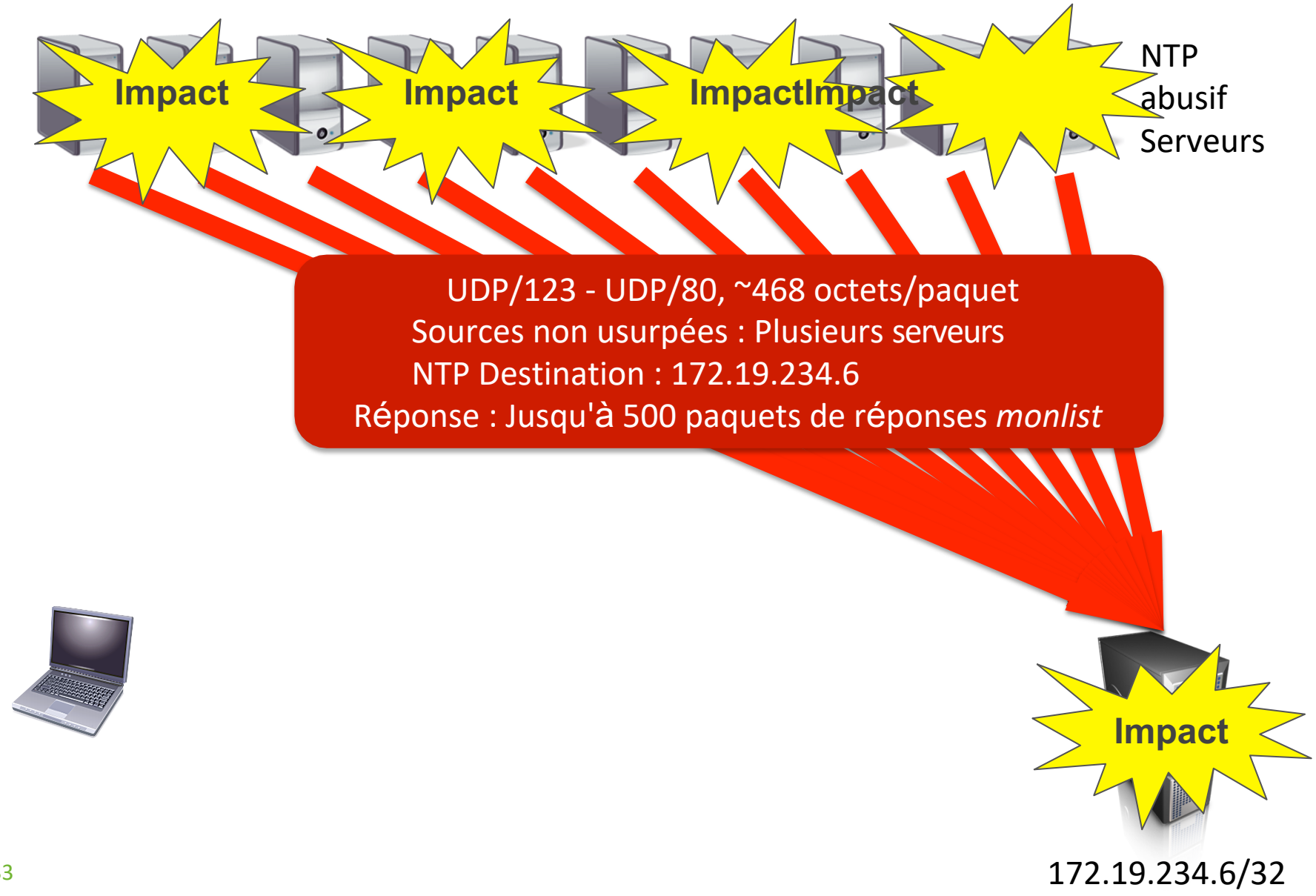


NTP abusif Serveurs

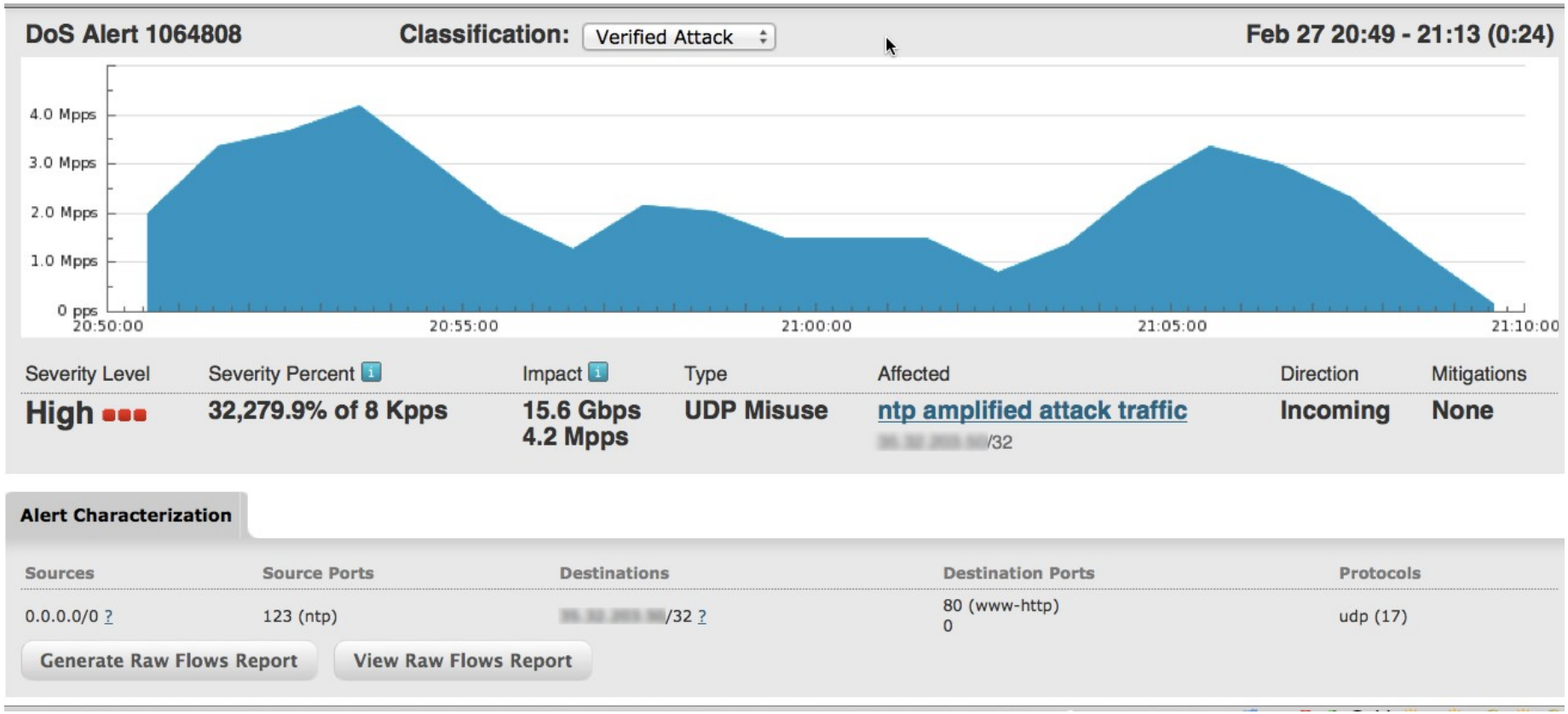
UDP/80 - UDP/123, ~50 octets/packet Spoofed Source : 172.19.234.6 Destinations : Plusieurs serveurs NTP Requête NTP : *monlist*

172.19.234.6/32

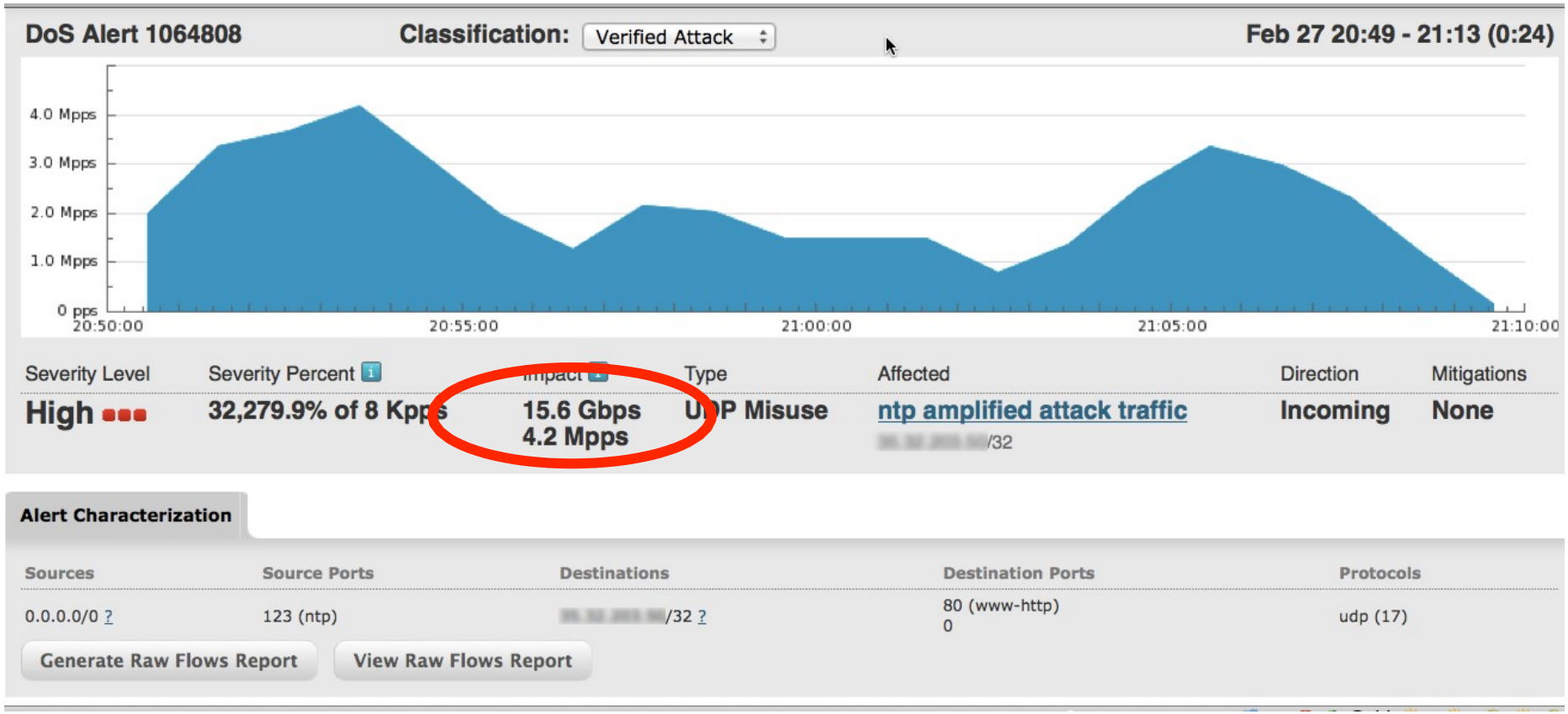
Méthodologie d'attaque par réflexion/amplification du NTP



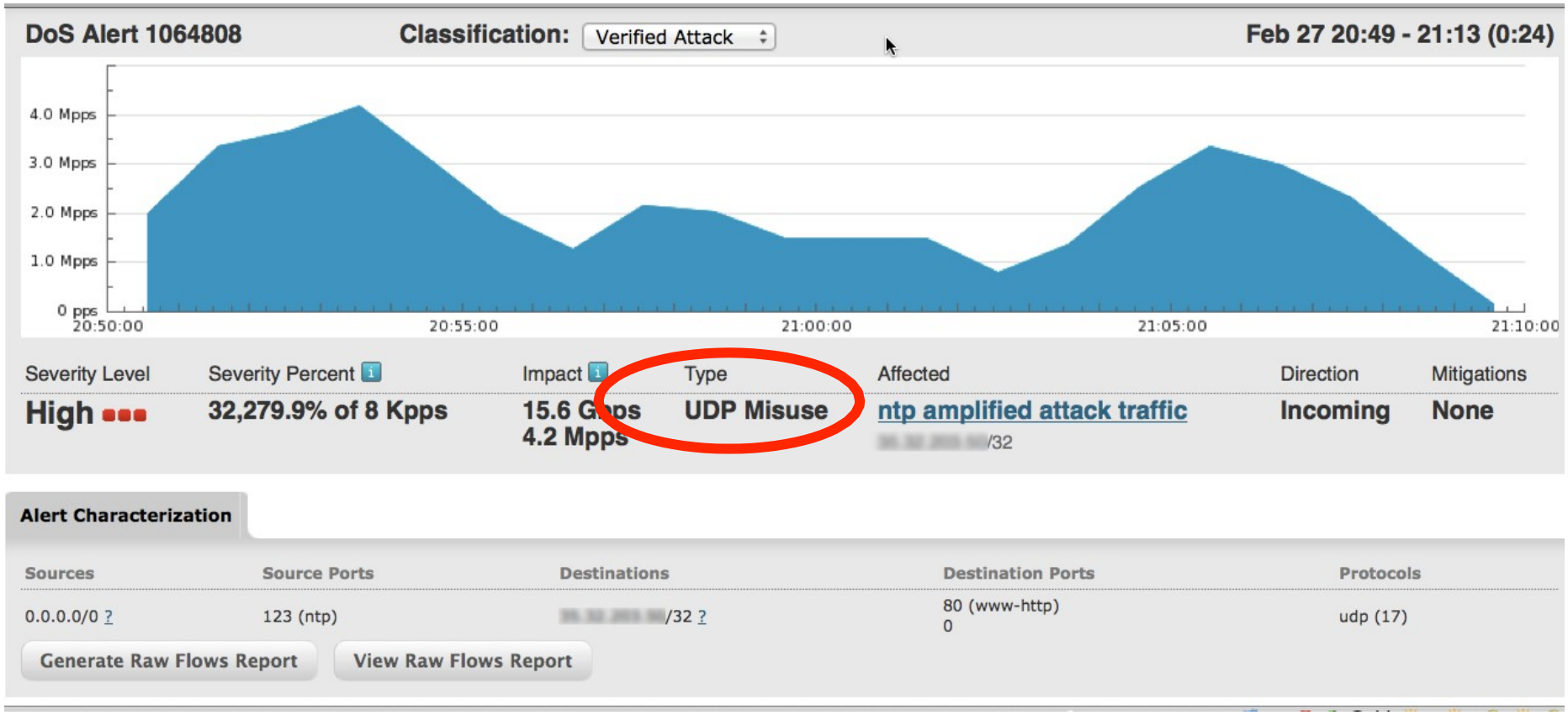
Attaque par réflexion/amplification du NTP



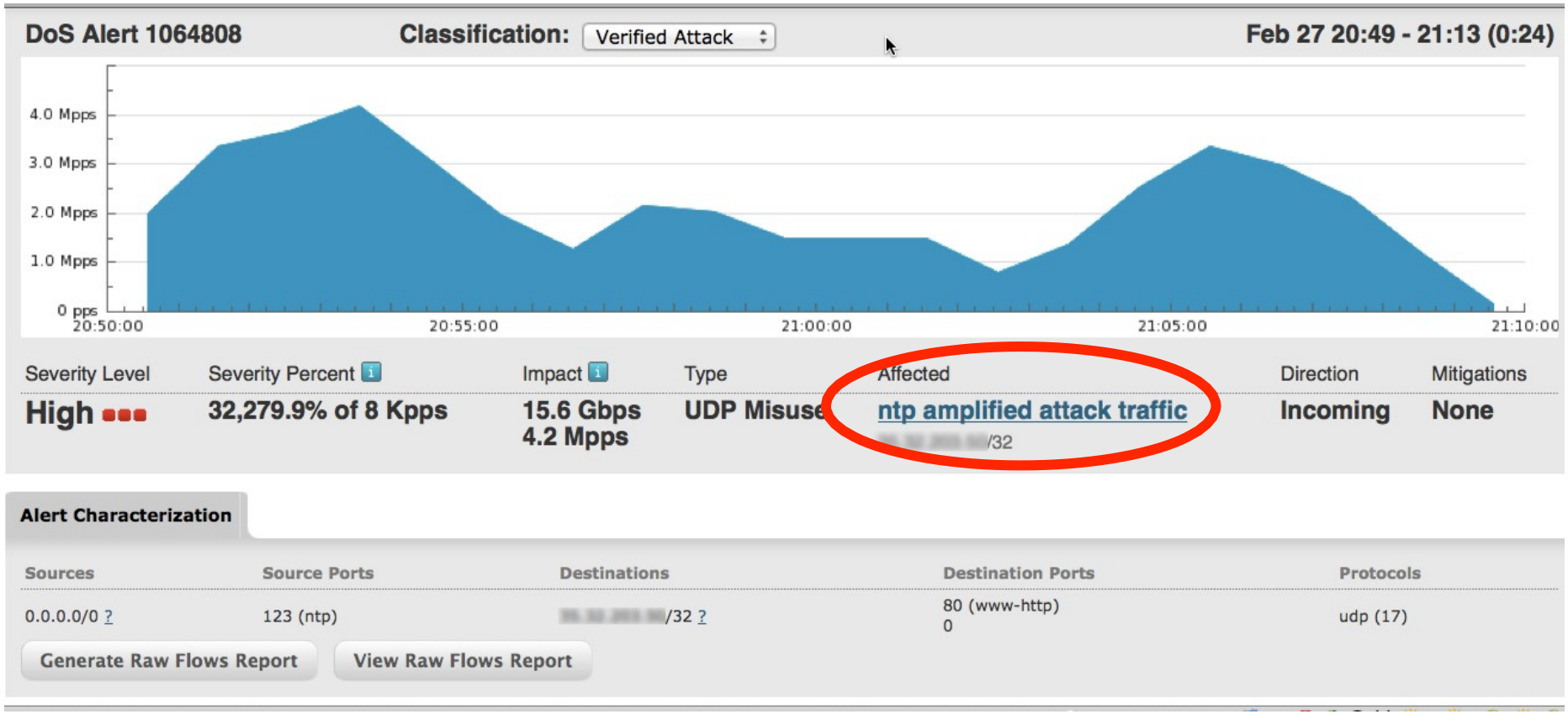
Attaque par réflexion/amplification du NTP



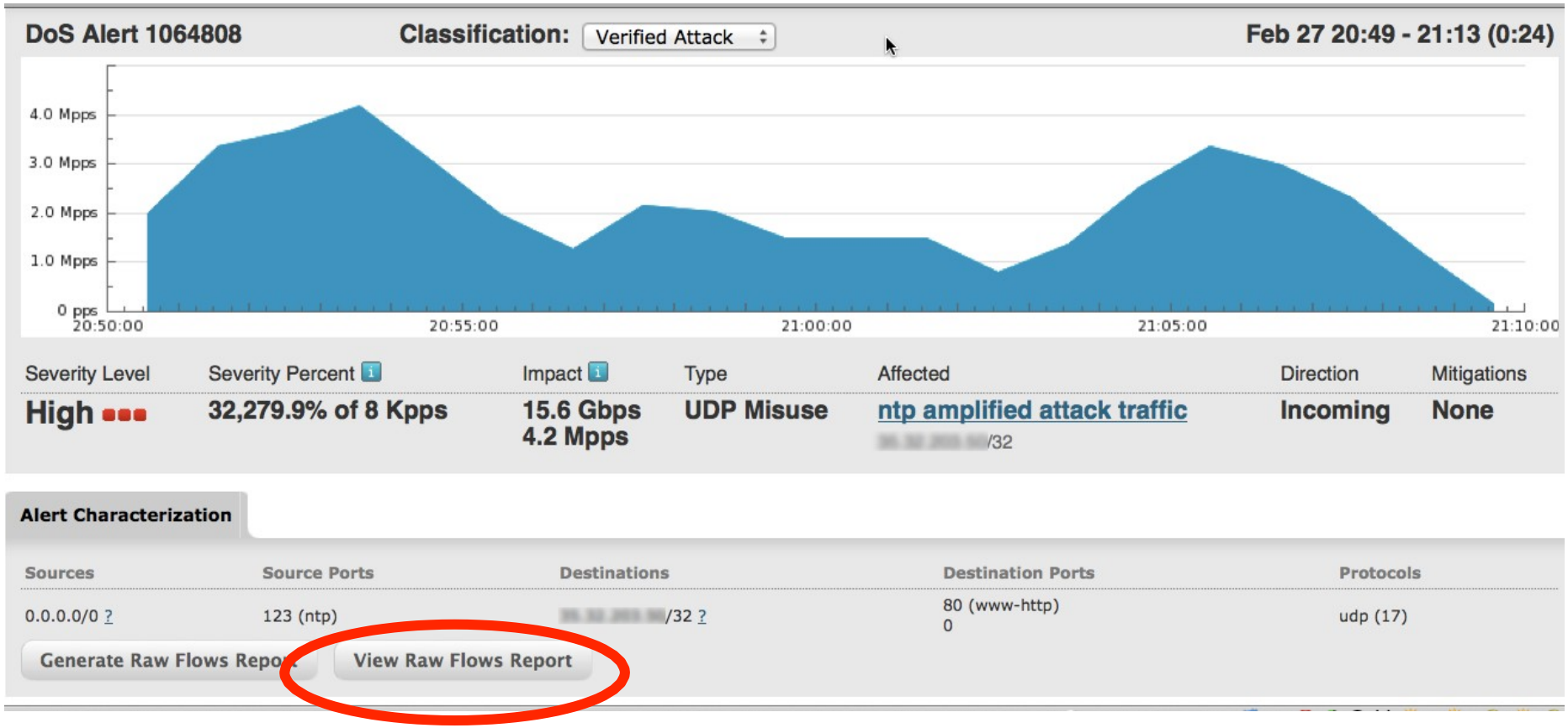
Attaque par réflexion/amplification du NTP



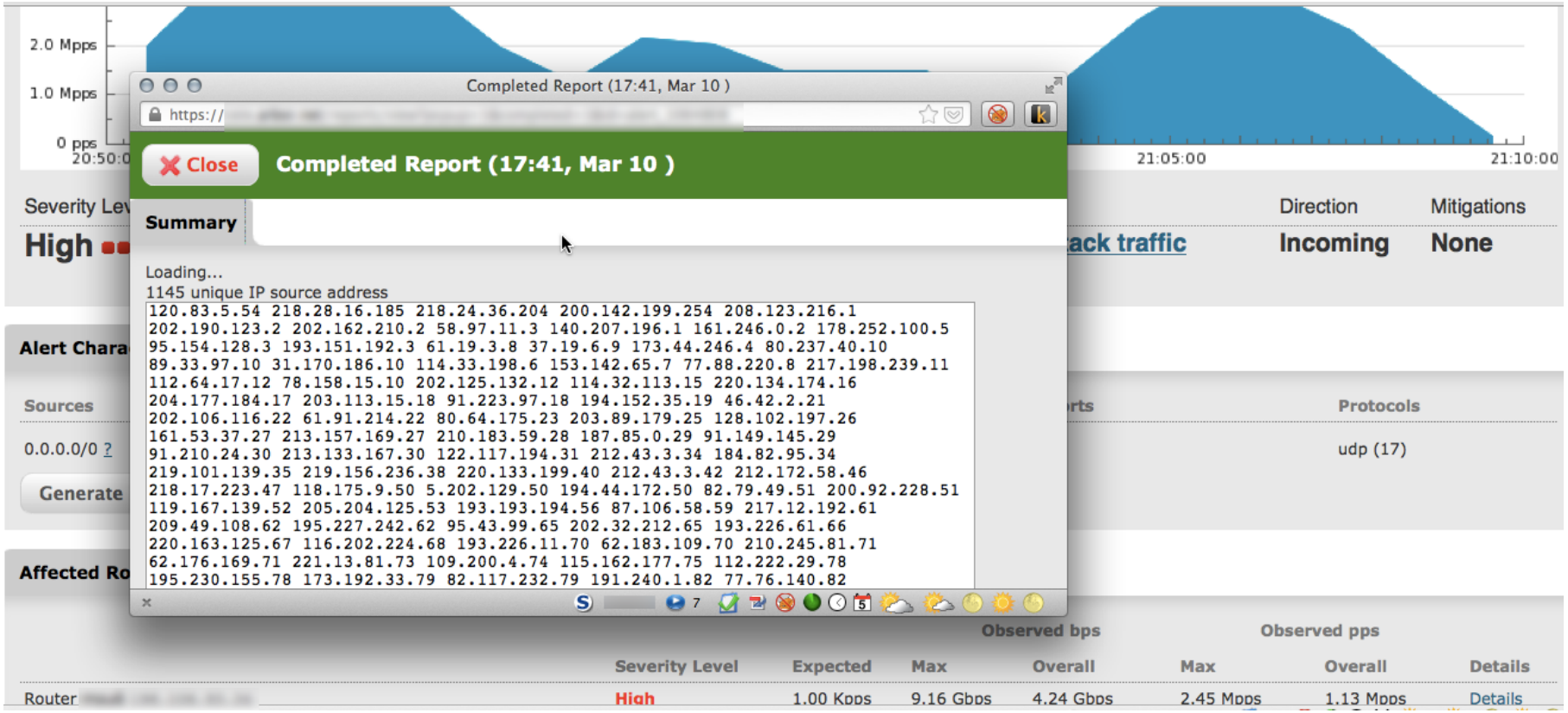
Attaque par réflexion/amplification du NTP



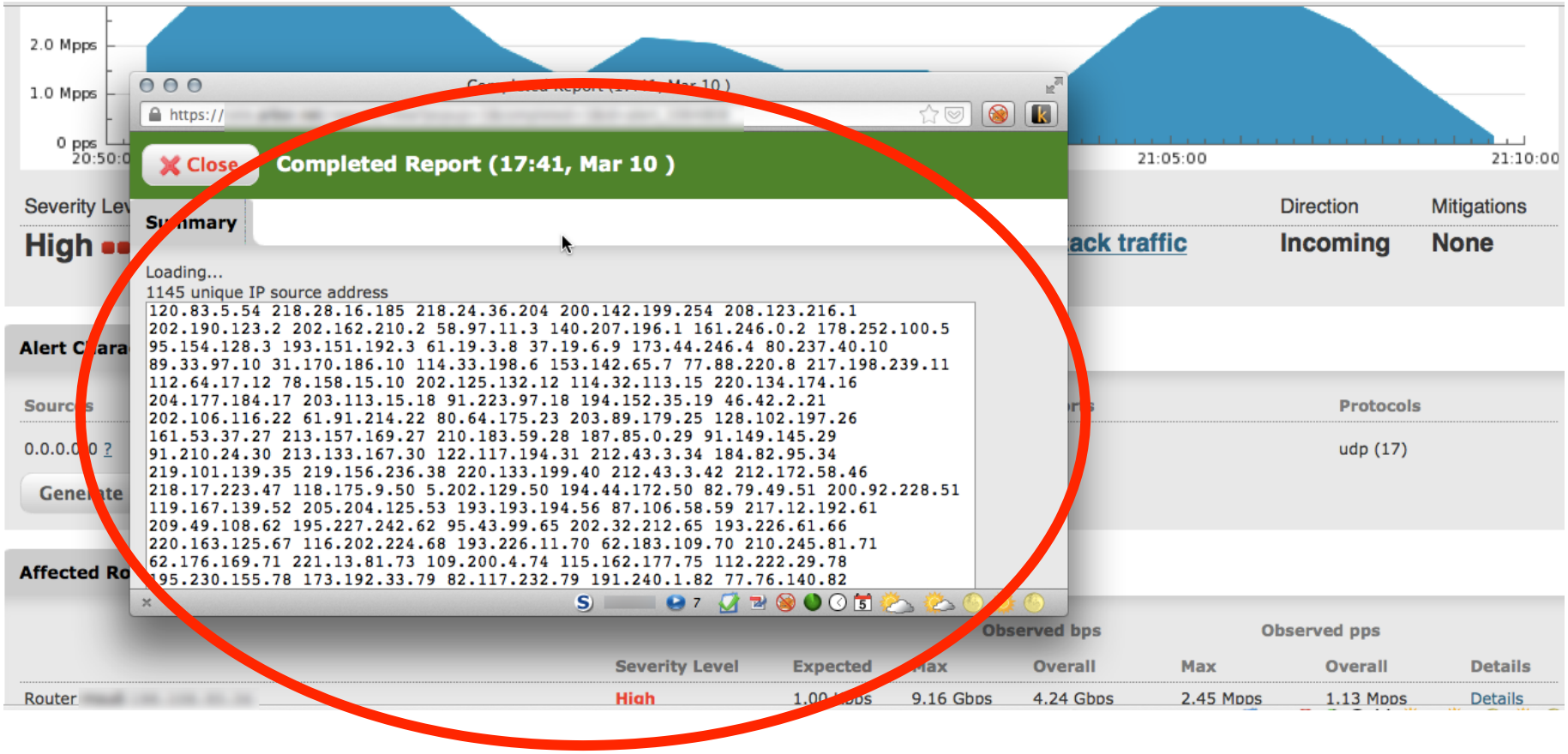
Attaque par réflexion/amplification du NTP



Attaque par réflexion/amplification du NTP



Attaque par réflexion/amplification du NTP



Attaque par réflexion/amplification du NTP

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router	High	1.00 Kpps	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Interface (SNMP 120) xe-0/0/0.22		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router	High	1.00 Kpps	5.52 Gbps	2.60 Gbps	1.48 Mpps	695.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	2.17 Gbps	1.12 Gbps	580.42 Kpps	298.98 Kpps	Details

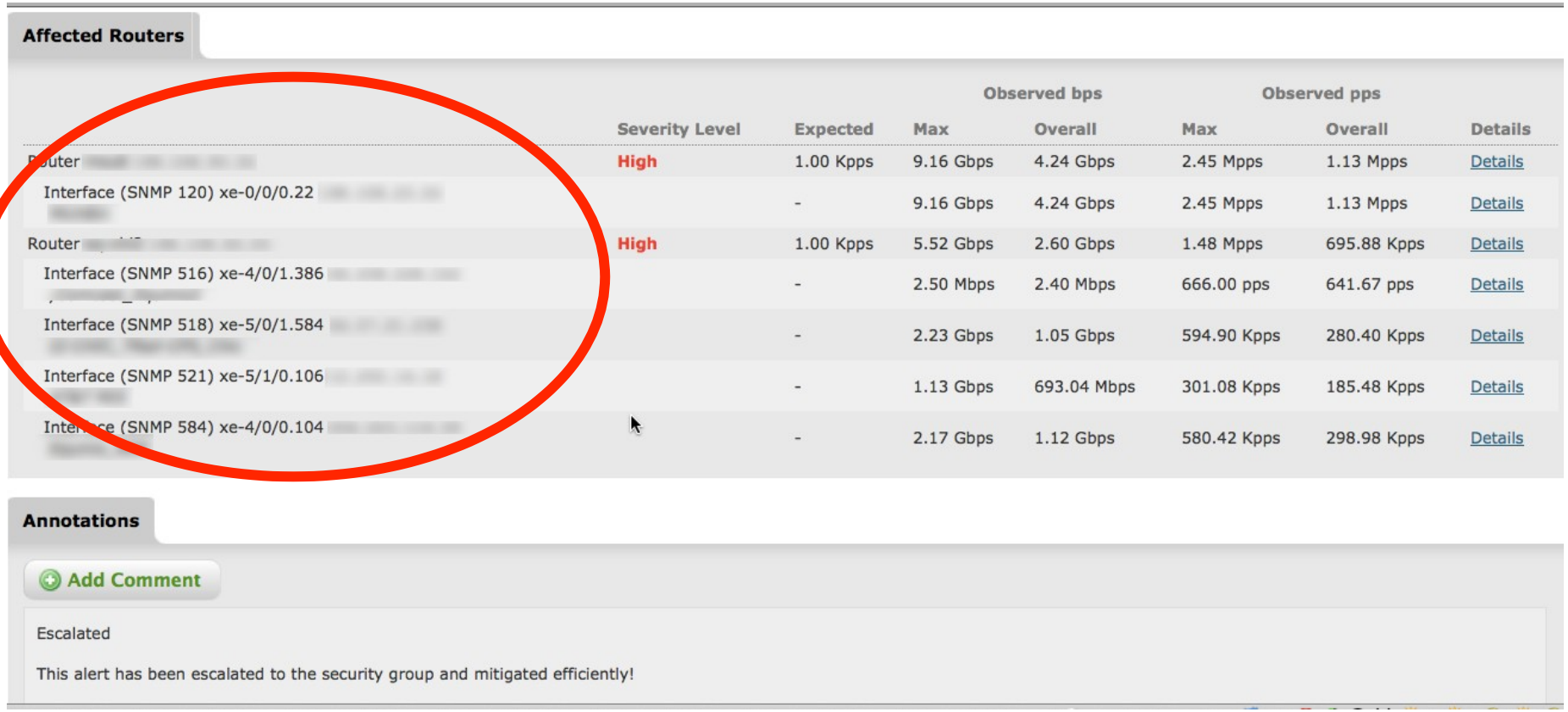
Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

Attaque par réflexion/amplification du NTP



Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	1.00 Kpps	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Interface (SNMP 120) xe-0/0/0.22		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router	High	1.00 Kpps	5.52 Gbps	2.60 Gbps	1.48 Mpps	695.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	2.17 Gbps	1.12 Gbps	580.42 Kpps	298.98 Kpps	Details

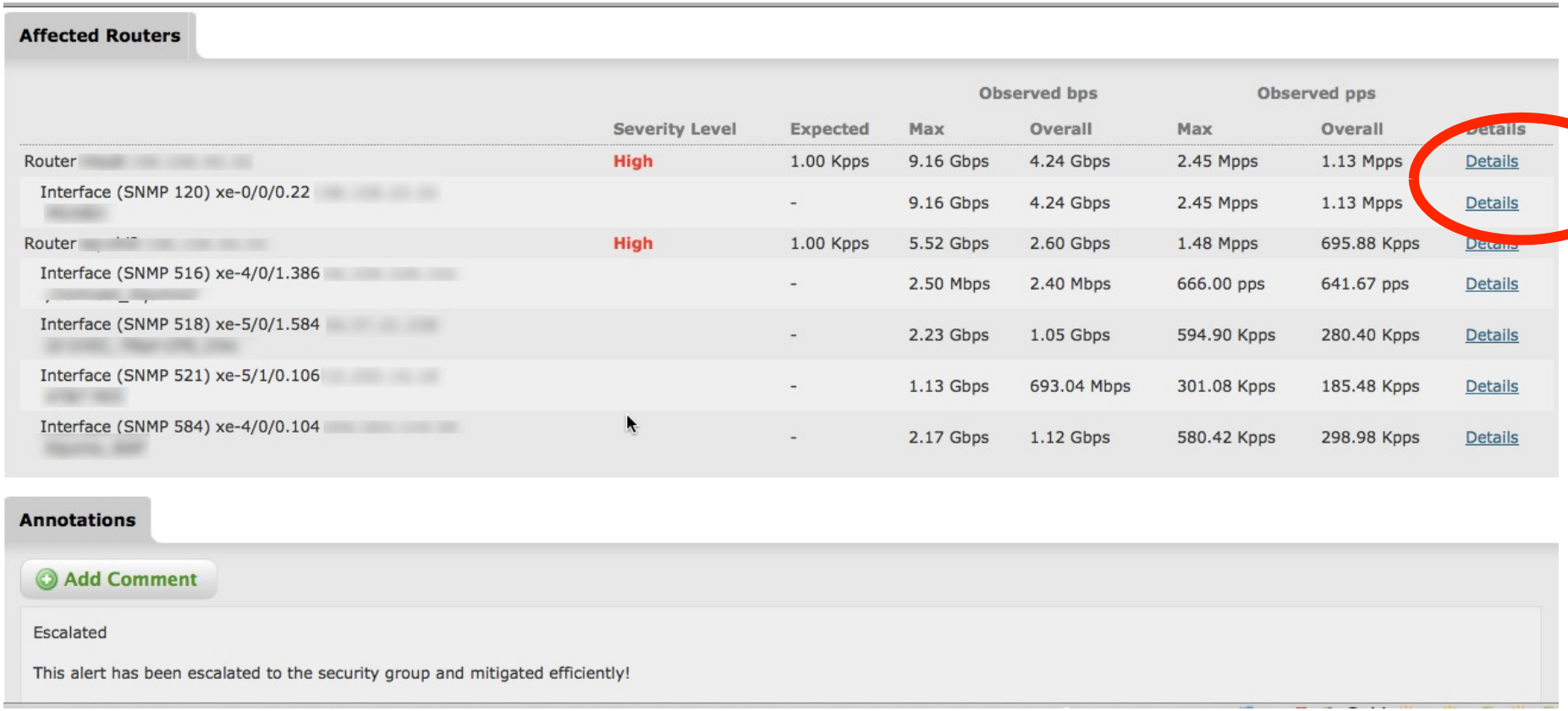
Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

Attaque par réflexion/amplification du NTP



Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	1.00 Kpps	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Interface (SNMP 120) xe-0/0/0.22		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router	High	1.00 Kpps	5.52 Gbps	2.60 Gbps	1.48 Mpps	695.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	2.17 Gbps	1.12 Gbps	580.42 Kpps	298.98 Kpps	Details

Annotations

Add Comment

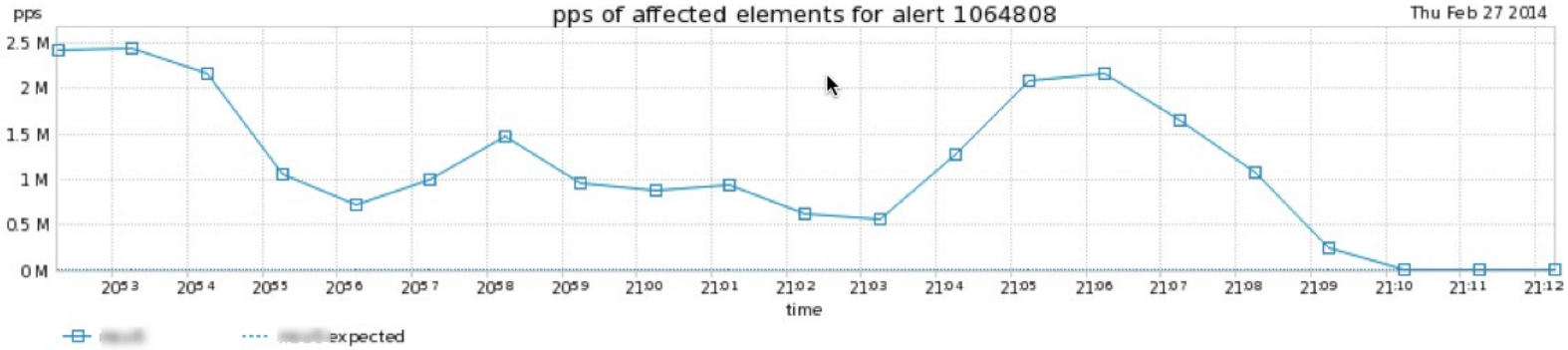
Escalated

This alert has been escalated to the security group and mitigated efficiently!

Attaque par réflexion/amplification du NTP

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1064808	High 32,279.9% Of 8.0 Kpps	15.61 Gbps 4.17 Mpps	0:24 (Ended)	Thu, Feb 27 2014, 20:49:34	Incoming	UDP (Misuse)	ntp amplified attack traffic [redacted]/32 ntp amplified attack traffic



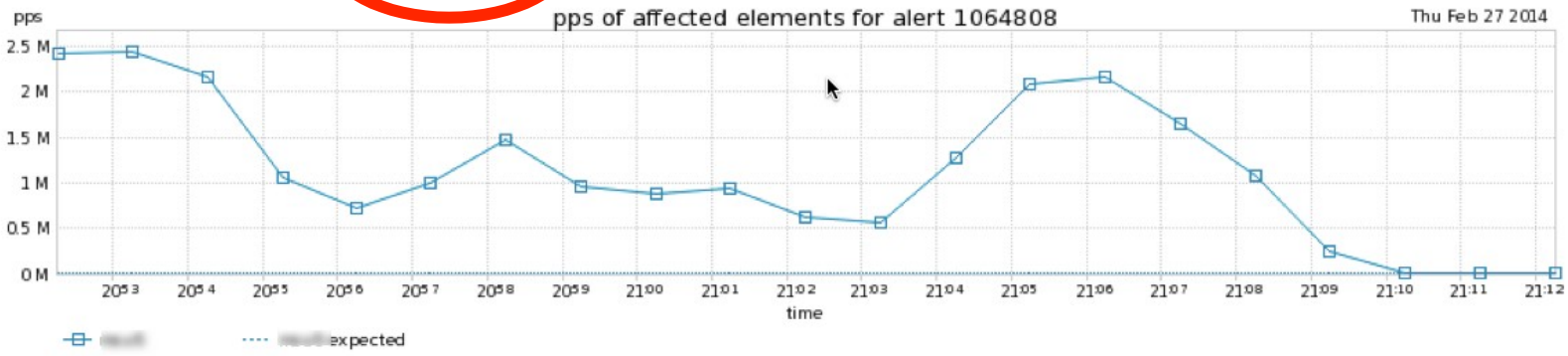
Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	1.00 kpps	9.16 G	4.24 G	2.45 M	1.13 M

Attaque par réflexion/amplification du NTP

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1064808	High 32,279.9% Of 8.0 Kpps	15.61 Gbps 4.17 Mpps	0:24 (Ended)	Thu, Feb 27 2014, 20:49:34	Incoming	UDP (Misuse)	ntp amplified attack traffic [redacted]/32 ntp amplified attack traffic



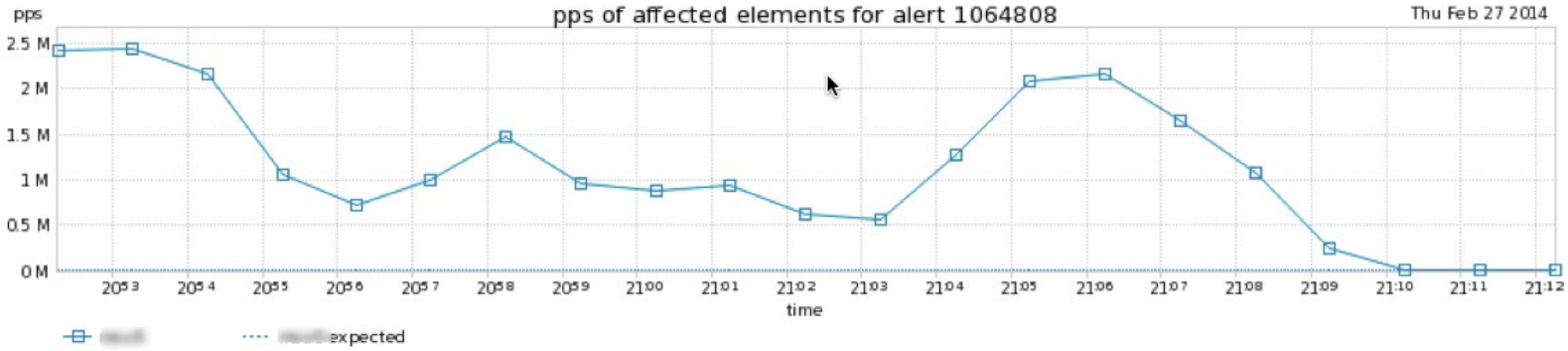
Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	1.00 kpps	9.16 G	4.24 G	2.45 M	1.13 M

Attaque par réflexion/amplification du NTP

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1064808	High 32,279.9% Of 8.0 Kpps	15.61 Gbps 4.17 Mpps	0:24 (Ended)	Thu, Feb 27 2014, 20:49:34	Incoming	UDP (Misuse)	ntp amplified attack traffic [redacted]/32 ntp amplified attack traffic



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	1.00 kpps	9.16 G	4.24 G	2.45 M	1.13 M

Attaque par réflexion/amplification du NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Attaque par réflexion/amplification du NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Attaque par réflexion/amplification du NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Attaque par réflexion/amplification du NTP

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
ntp (123)	udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Attaque par réflexion/amplification du NTP

http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.22 [redacted]	120	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.32 [redacted]	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20 [redacted]	157	113.86 G	243.38 M	467.82	723.49 M	193.31 k	17.06	☑

For assistance with this product, please contact support@arbornetworks.com. About

Attaque par réflexion/amplification du NTP

http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.22	120	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.32	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20	157	113.86 G	243.38 M	467.82	723.49 M	193.31 k	17.06	☑

For assistance with this product, please contact support@arbornetworks.com. About

Attaque par réflexion/amplification du NTP

http (80)	udp (17)	619.52 G	1.32 G	467.87	3.94 G	1.05 M	92.80	☑
0 - 127	udp (17)	1.40 M	3.00 k	468.00	8.92 k	2.38	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.22 [redacted]	120	667.44 G	1.43 G	467.77	4.24 G	1.13 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-0/0/0.32 [redacted]	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20 [redacted]	157	113.86 G	243.38 M	467.82	723.49 M	193.31 k	17.06	☑

For assistance with this product, please contact support@arbornetworks.com. About

Reflection/Amplification des DNS

Facteur d'amplification - DNS

Abréviation	Protocole	Ports	Facteur d'amplification	# Serveurs abusifs
CHARGEN	Protocole de génération de caractères	UDP / 19	18x/1000x	Des dizaines de milliers (90K)
DNS	Système de nom de domaine	UDP / 53	160x	Millions (27M)
NTP	Protocole de temps réseau	UDP / 123	1000x	Plus de cent mille (119K)
SNMP	Protocole de gestion de réseau simple	UDP / 161	880x	Millions (5M)
SSDP	Protocole de découverte de service simple	UDP /1900	20x/83x	Millions (2M)

Caractéristiques d'une attaque par réflexion/amplification

- L'attaquant usurpe l'adresse IP de la cible de l'attaque, en envoyant des requêtes DNS pour de grands enregistrements DNS pré-identifiés (enregistrements ANY, grands enregistrements TXT, etc.) soit à des serveurs DNS récursifs ouverts abusifs, soit directement à des serveurs DNS faisant autorité.
- L'attaquant choisit le port UDP qu'il souhaite cibler - avec le DNS, il est généralement limité à UDP/53 ou UDP/1024-65535. Le port de destination est UDP/53.
- Les serveurs "répondent" soit directement à la cible de l'attaque, soit au serveur DNS récursif ouvert intermédiaire, avec des réponses DNS volumineuses. La cible de l'attaque verra des flux de réponses DNS non sollicitées décomposées en fragments initiaux et non initiaux.
- La taille de la réponse est généralement comprise entre 4096 et 8192 octets (elle peut être plus petite ou plus grande) et est divisée en plusieurs fragments.
- La taille des paquets reçus par la cible de l'attaque est généralement de ~1500 octets en raison des MTU Ethernet courantes - et il y en a beaucoup.

Caractéristiques d'une attaque par réflexion/amplification (suite)

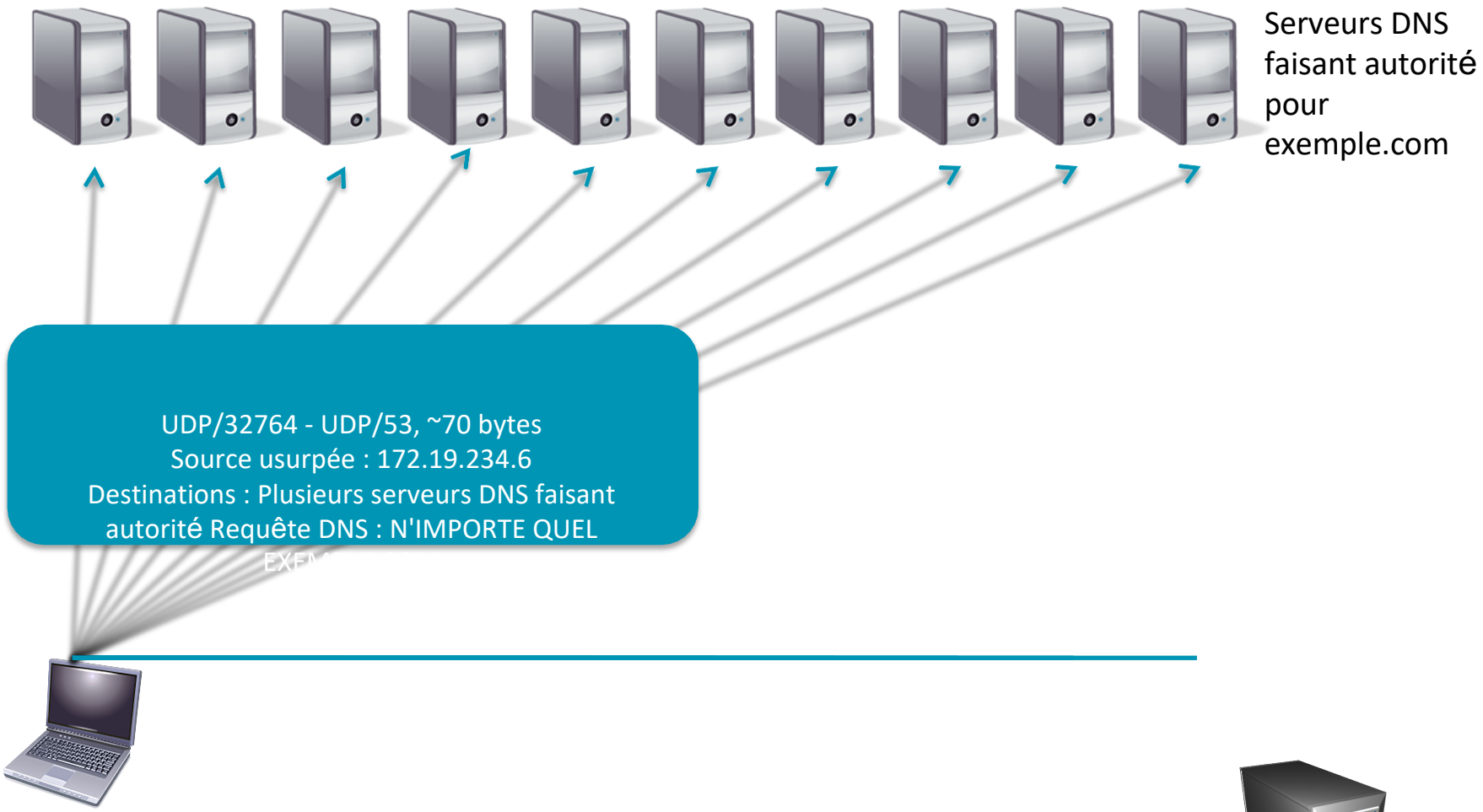
- Lorsque ces multiples flux de réponses DNS fragmentées convergent, le volume d'attaque peut être énorme - la plus grande attaque vérifiée de ce type à ce jour est de ~200gb/sec. 100 gigaoctets/seconde ; les attaques sont monnaie courante.
- La bande passante de transit Internet de la cible, ainsi que la bande passante principale des pairs/upstreams de la cible, ainsi que la bande passante principale des réseaux intermédiaires entre les différents services DNS utilisés de manière abusive et la cible, sont saturées.
- Dans la plupart des attaques impliquant des serveurs DNS récursifs ouverts intermédiaires sont des réflecteurs, entre ~20 000 et 30 000 DNS récursifs abusifs sont exploités par les attaquants. Jusqu'à 50 000 serveurs DNS récursifs ouverts abusifs ont été observés dans certaines attaques.
- Dans les attaques exploitant directement les serveurs DNS faisant autorité, des centaines ou des milliers de ces serveurs sont utilisés par les attaquants.
- De nombreux serveurs DNS faisant autorité et bien connus sont anycasted, avec de multiples instances déployées sur Internet.

Méthodologie d'attaque par réflexion/amplification

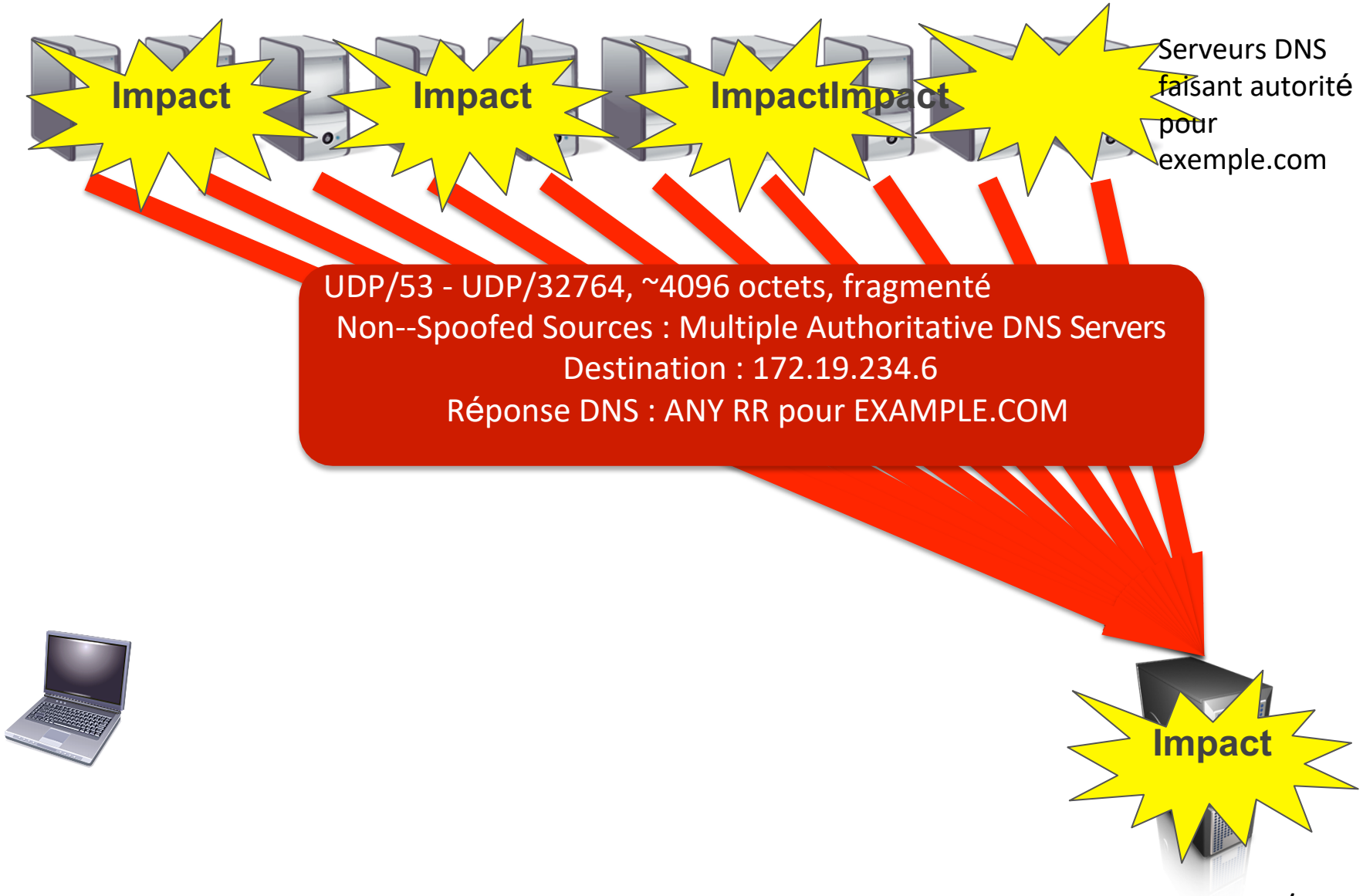
Serveurs DNS faisant autorité pour exemple.com

172.19.234.6/32

Méthodologie d'attaque par réflexion/amplification



Méthodologie d'attaque par réflexion/amplification



Méthode d'attaque par réflexion/amplification du DNS #2

Serveurs DNS faisant autorité pour exemple.com

DNS récursif abusif Serveurs

Serveurs accessibles par Internet, routeurs, dispositifs CPE domestiques, etc.

172.19.234.6/32

Méthode d'attaque par réflexion/amplification du DNS #2

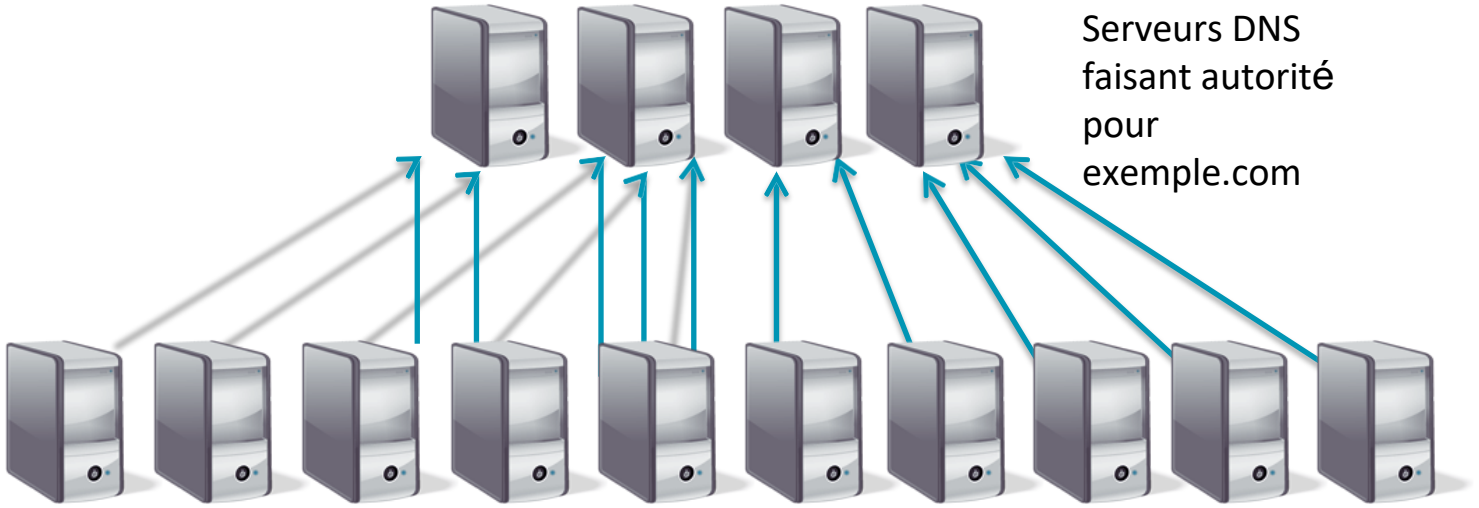
Serveurs DNS faisant autorité pour exemple.com

DNS récursif abusif Serveurs

UDP/1988 - UDP/53, ~70 bytes
Source usurpée : 172.19.234.6
Destinations : Plusieurs serveurs DNS faisant autorité Requête DNS : TXT PGP.EXEMPLE.COM

172.19.234.6/32

Méthode d'attaque par réflexion/amplification du DNS #2



Serveurs DNS faisant autorité pour exemple.com

DNS récursif abusif Serveurs

UDP/variable- UDP/53, ~70 octets
Sources non usurpées : Plusieurs serveurs DNS récursifs
Destinations : Plusieurs serveurs DNS faisant autorité
Requête DNS : TXT PGP.EXEMPLE.COM

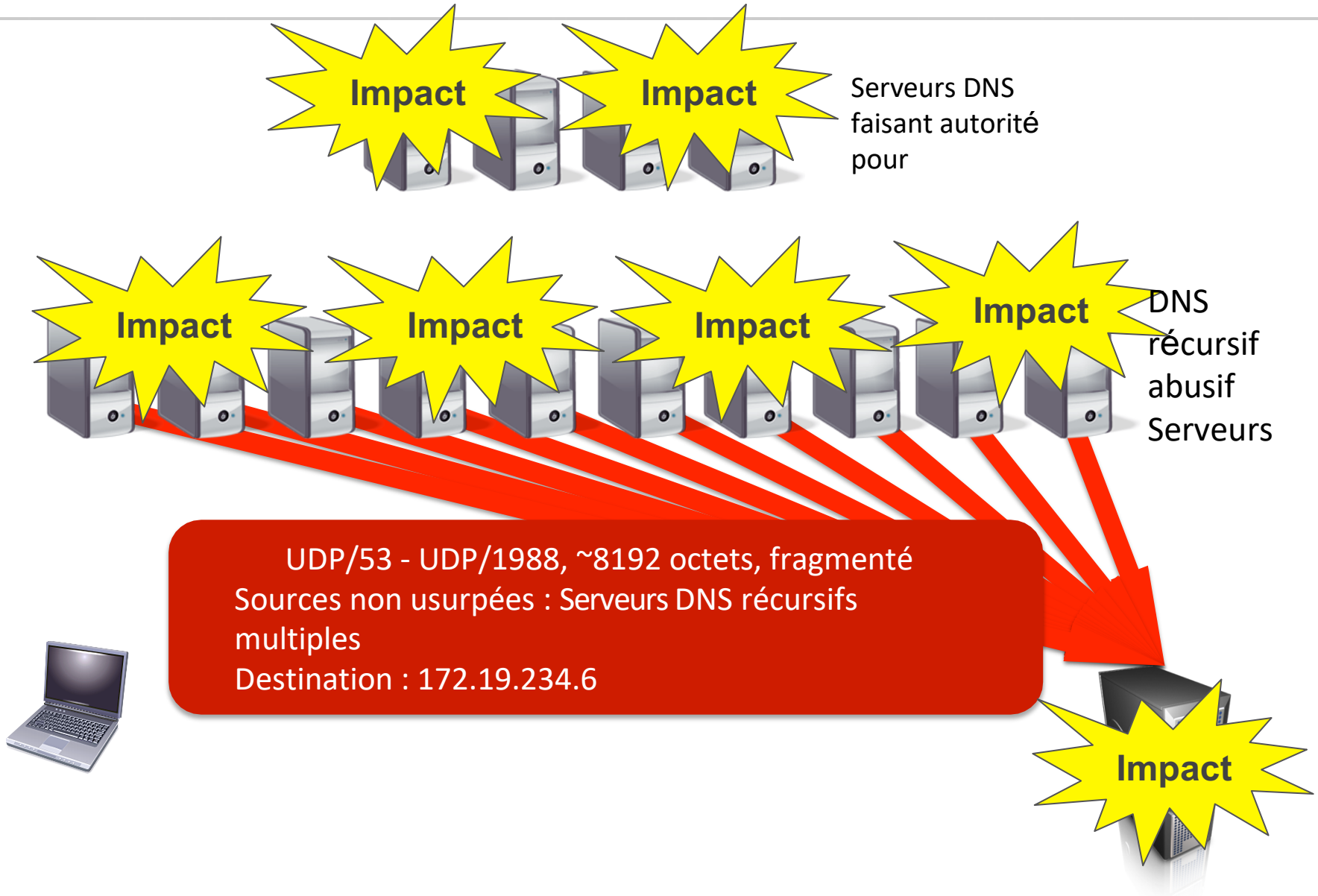
172.19.234.6/32

Méthode d'attaque par réflexion/amplification du DNS #2

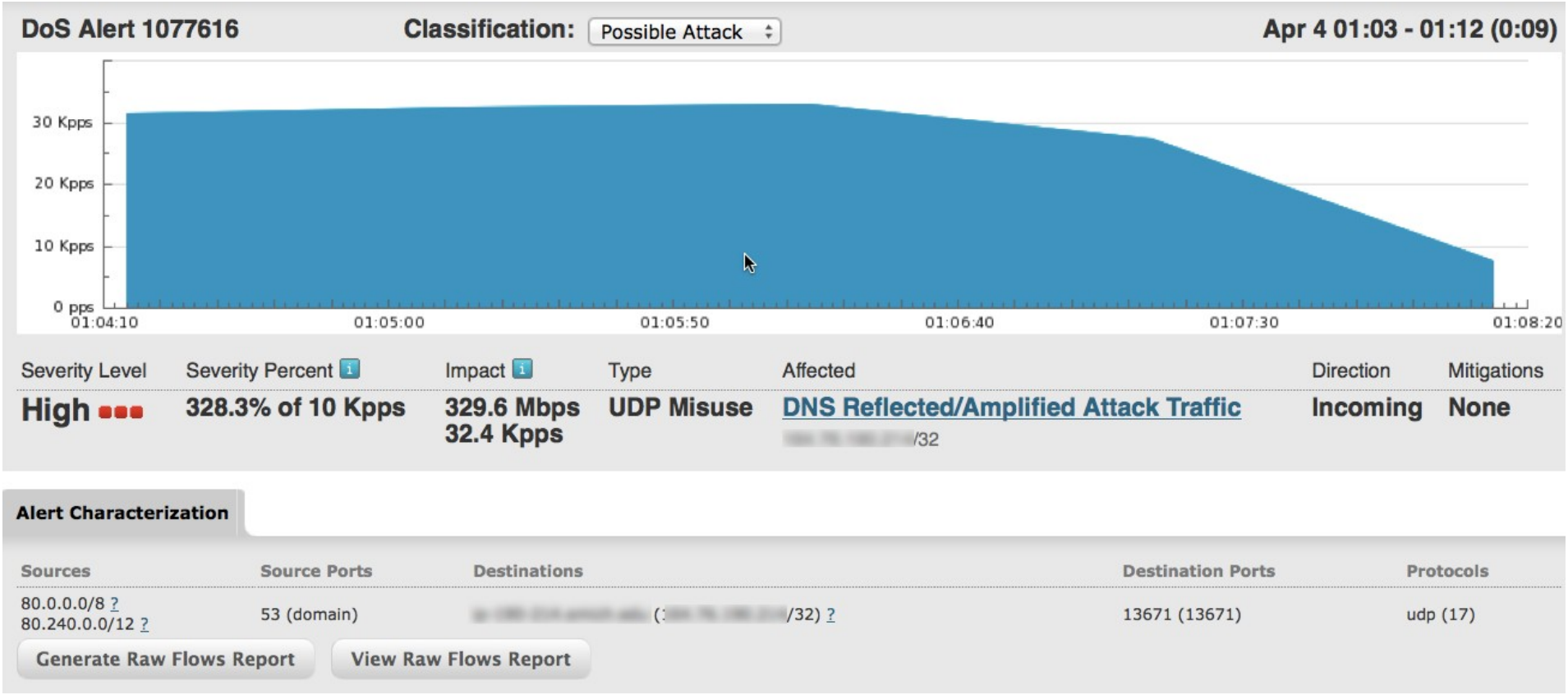
UDP/53 - UDP/variable, ~8192 octets, fragmenté
Sources non usurpées : Plusieurs serveurs DNS faisant autorité Destination : Serveurs DNS récursifs multiples
Réponse DNS : TXT RR pour PGP.EXAMPLE.COM

172.19.234.6/32

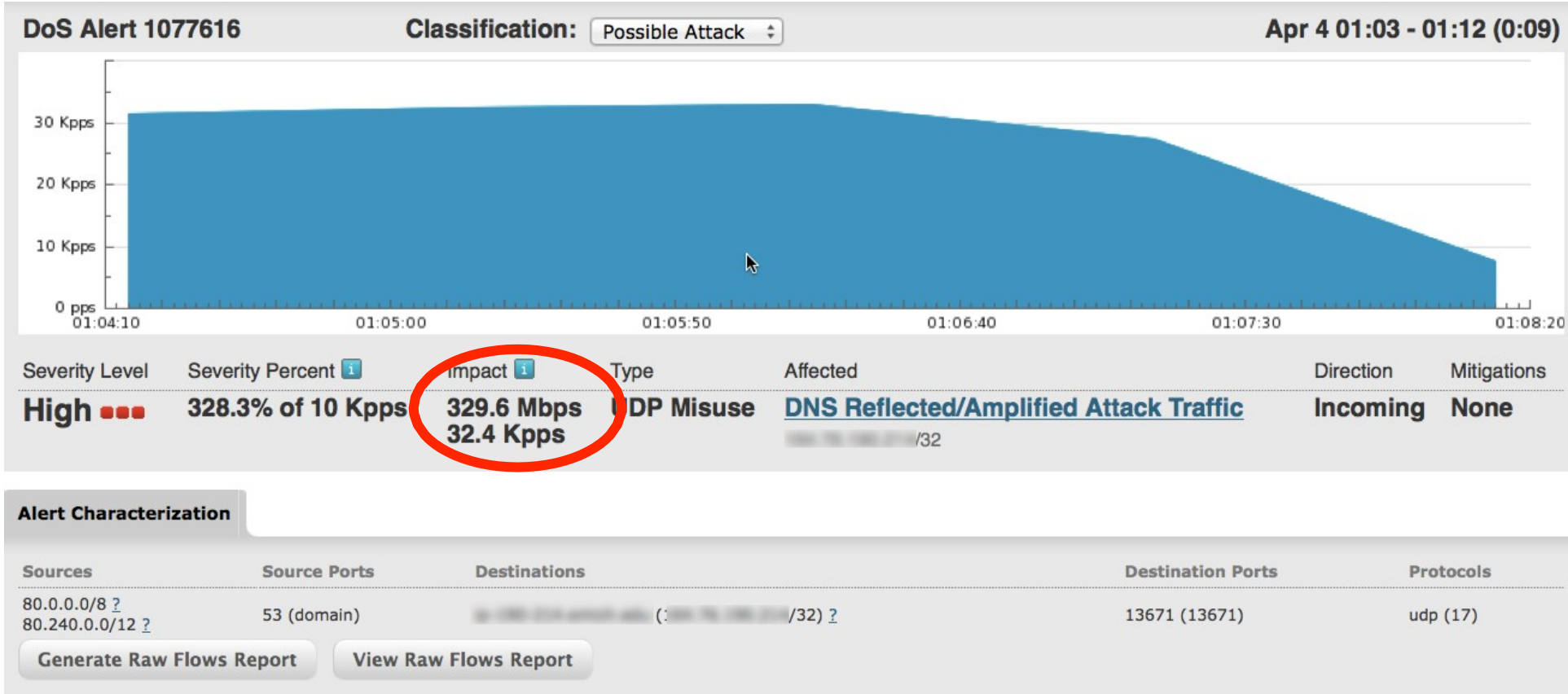
Méthode d'attaque par réflexion/amplification du



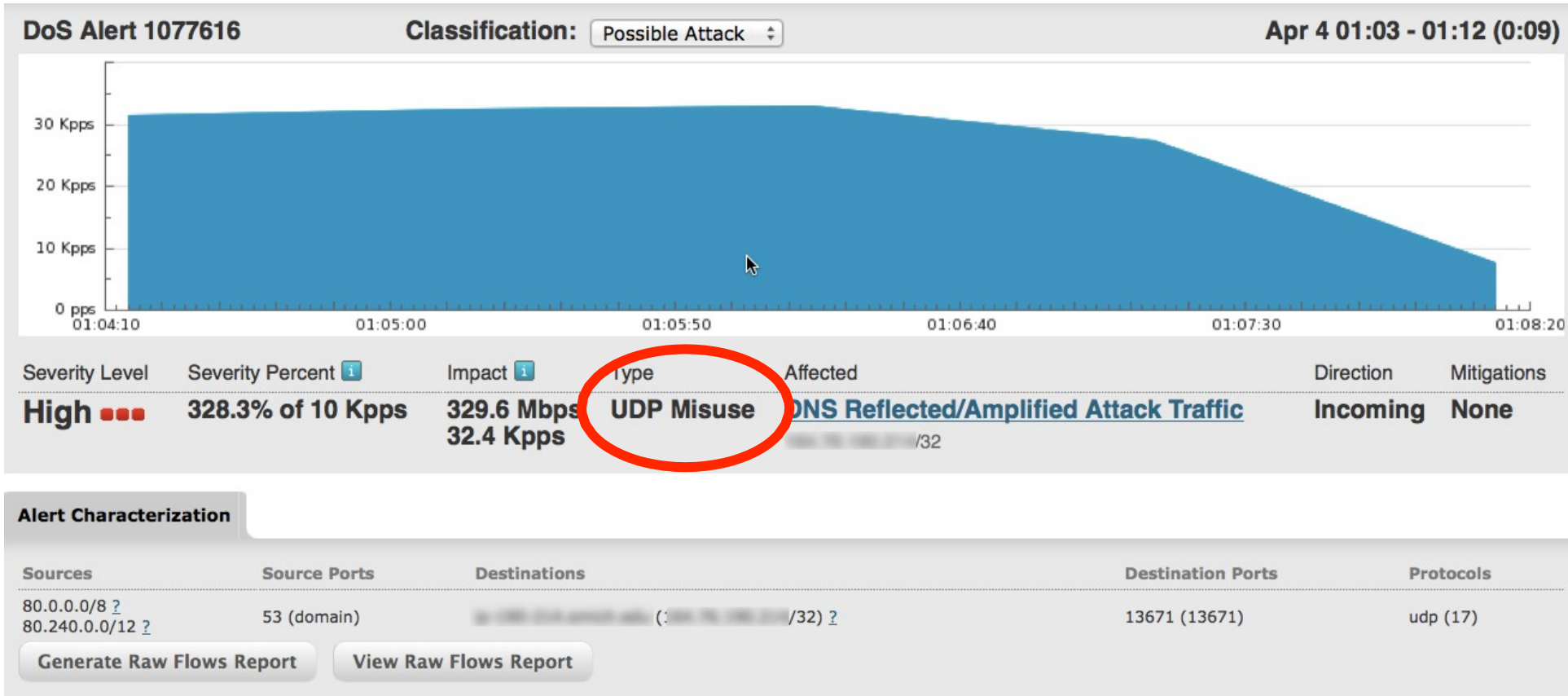
Attaque par réflexion/amplification du DNS - UDP/53



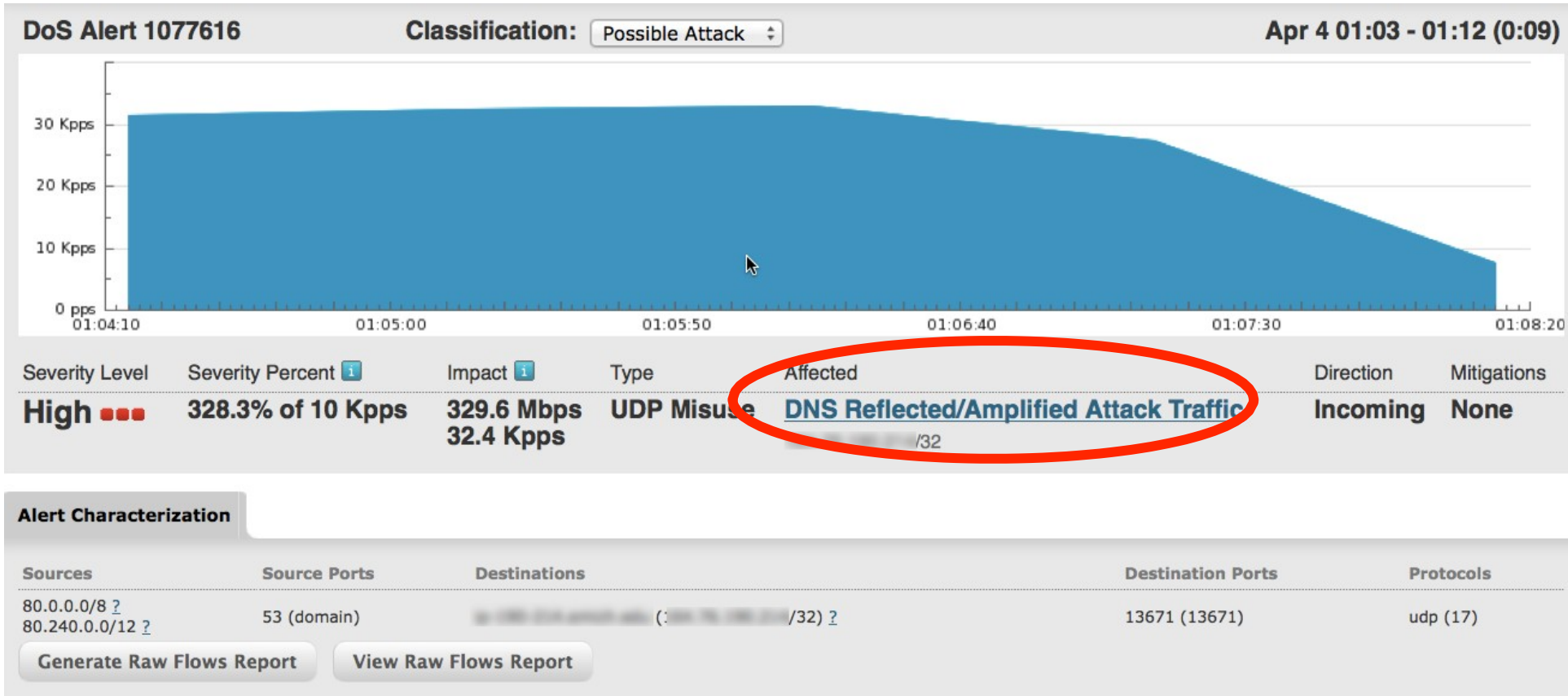
Attaque par réflexion/amplification du DNS - UDP/53



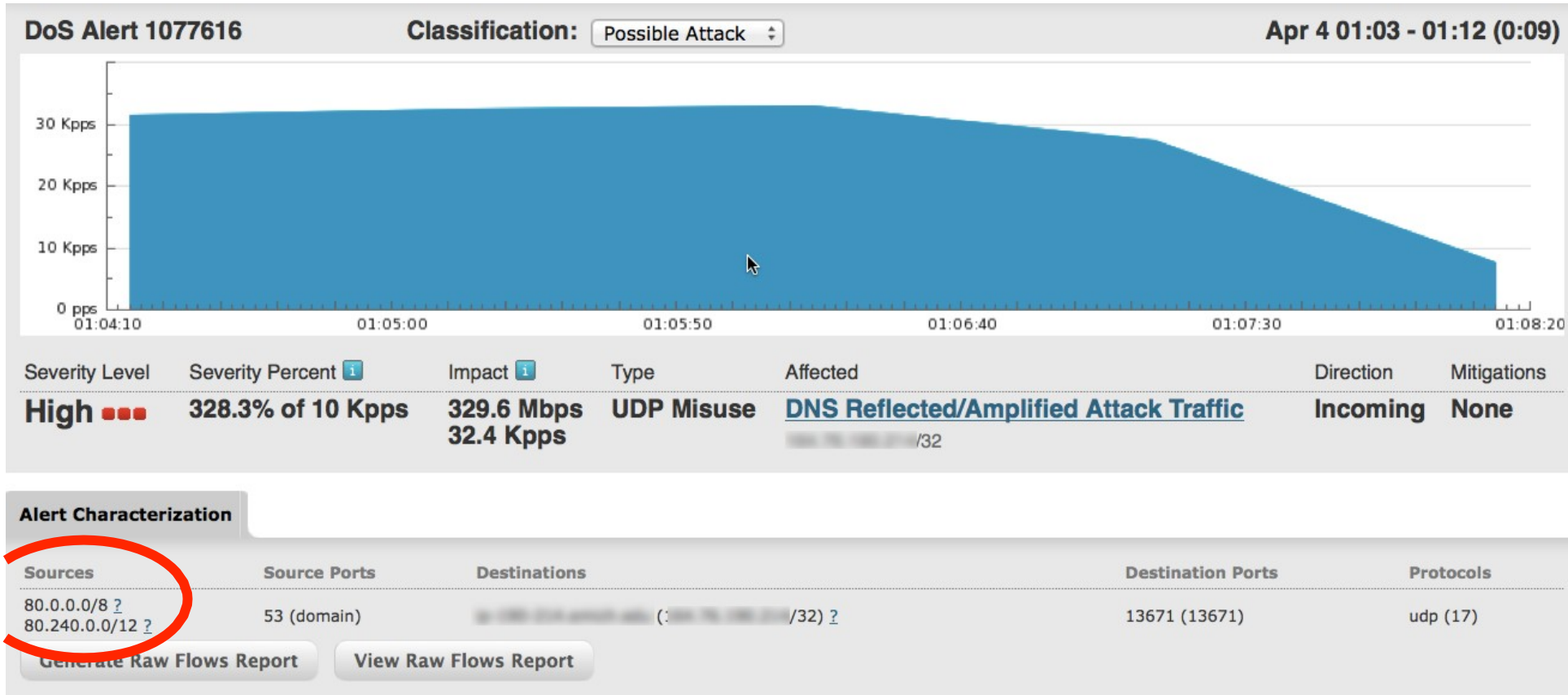
Attaque par réflexion/amplification du DNS - UDP/53



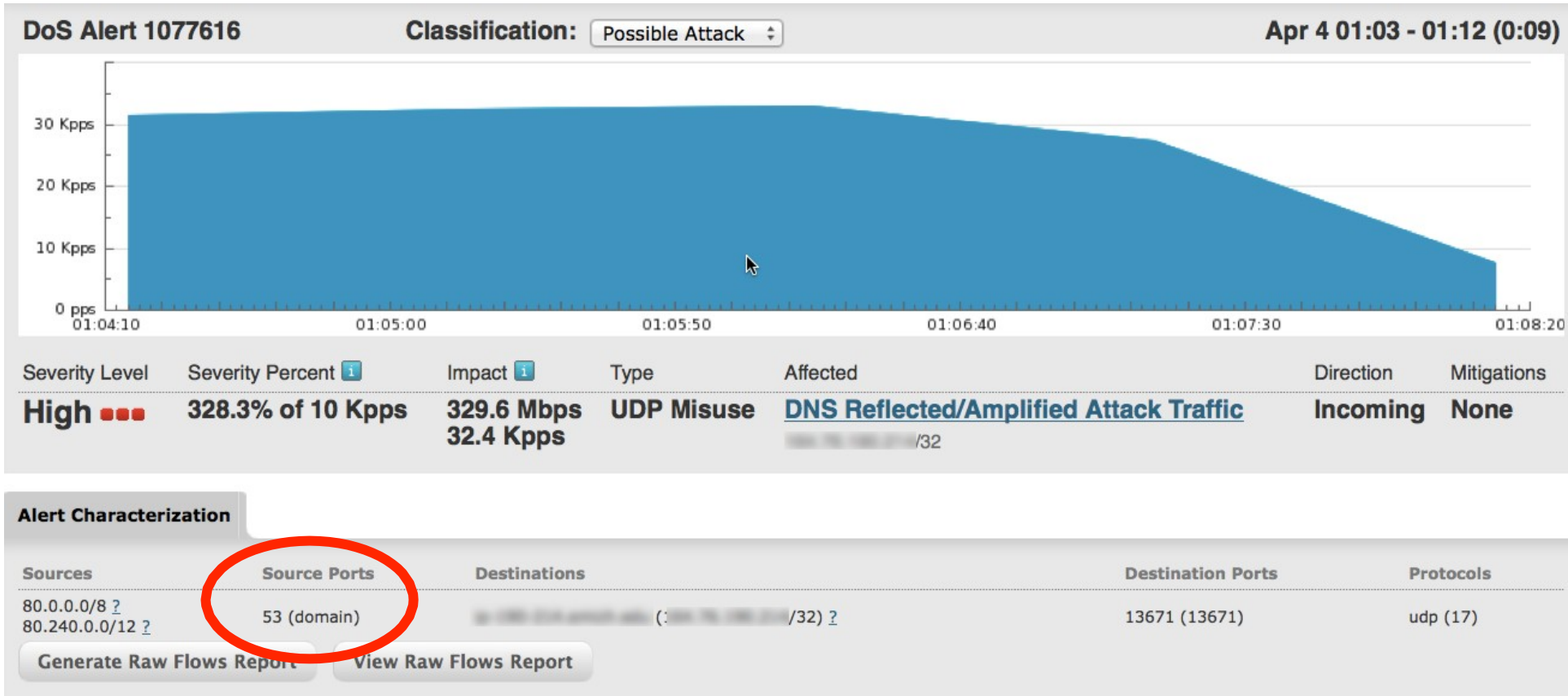
Attaque par réflexion/amplification du DNS - UDP/53



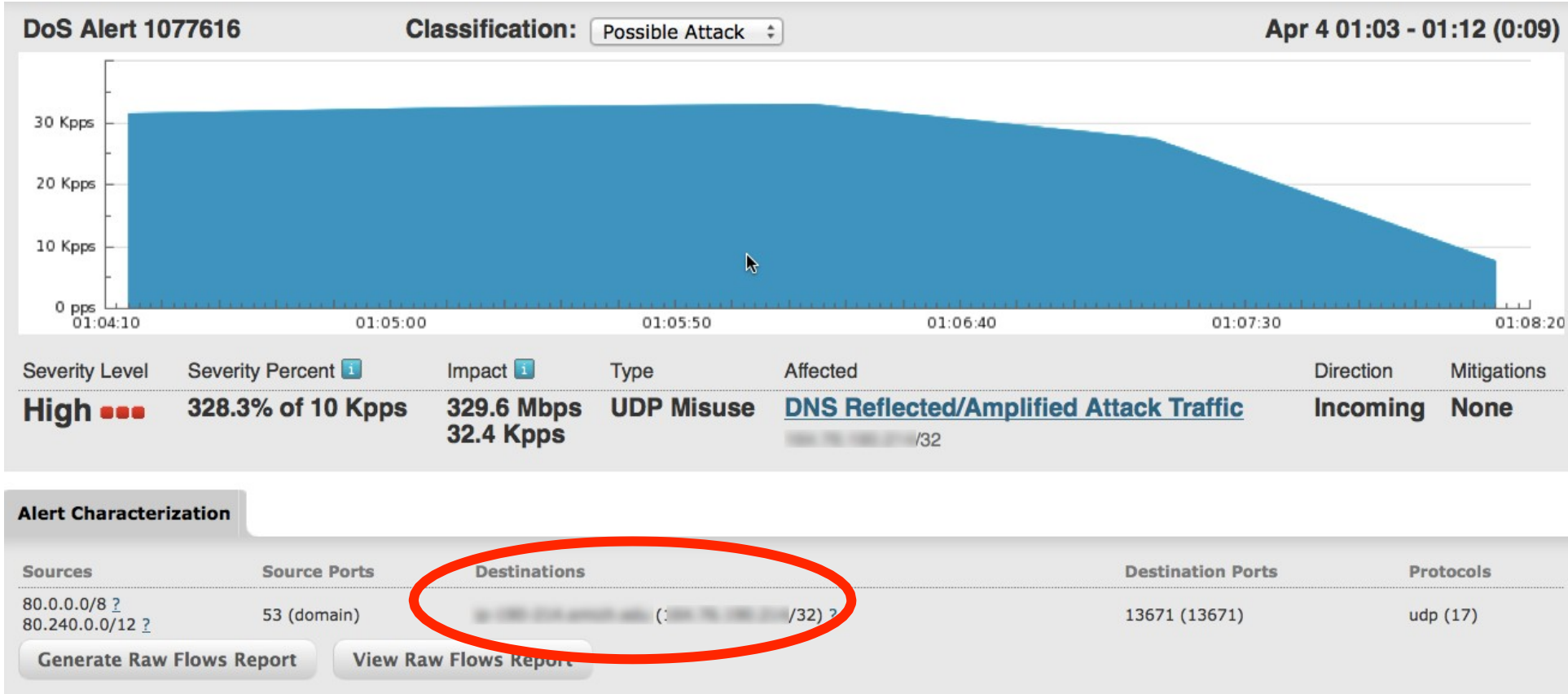
Attaque par réflexion/amplification du DNS - UDP/53



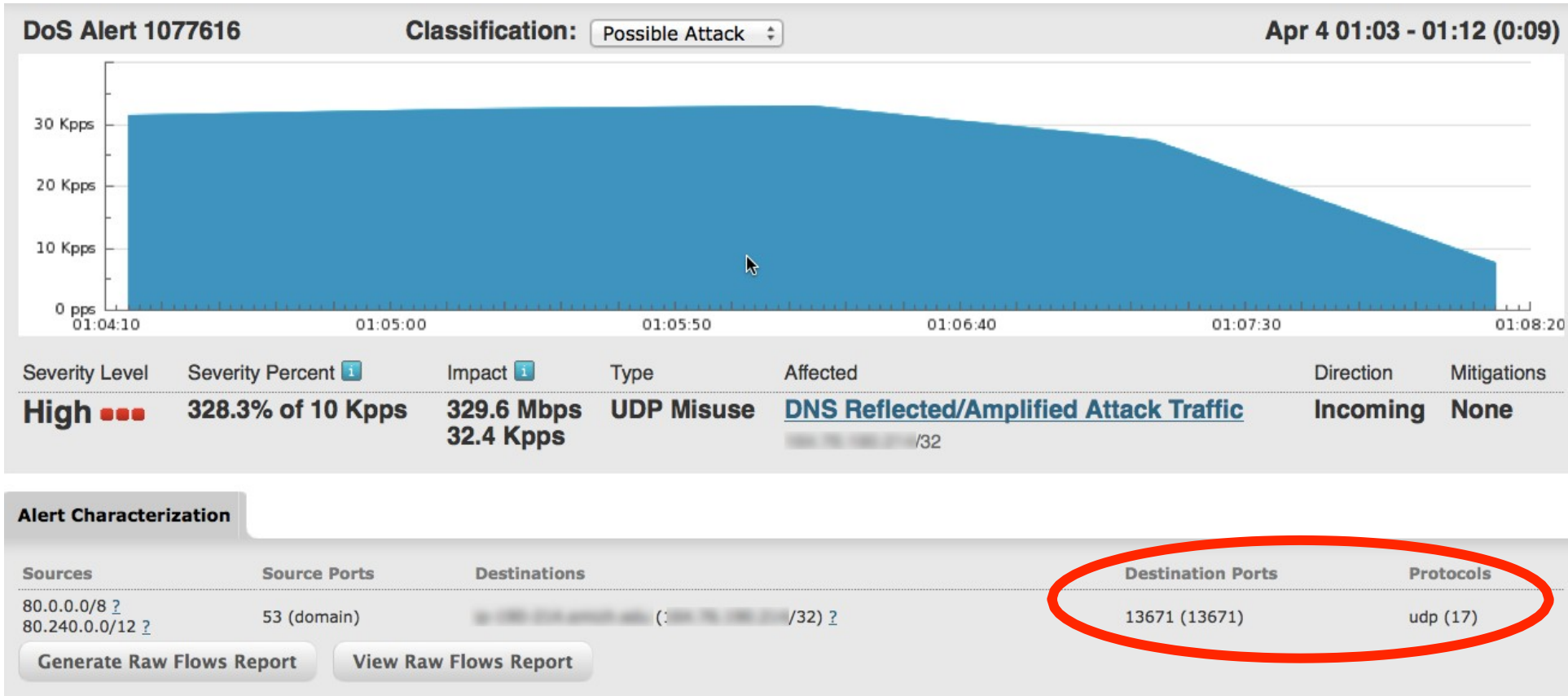
Attaque par réflexion/amplification du DNS - UDP/53



Attaque par réflexion/amplification du DNS - UDP/53



Attaque par réflexion/amplification du DNS - UDP/53



Attaque par réflexion/amplification du DNS - UDP/53

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	5.00 Kpps	326.82 Mbps	168.71 Mbps	32.73 Kpps	16.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	4.59 Mbps	3.21 Mbps	433.00 pps	305.56 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	4.33 Mbps	2.95 Mbps	516.00 pps	366.67 pps	Details
Interface (SNMP 521) xe-5/1/0.106		-	203.42 Mbps	101.67 Mbps	20.15 Kpps	10.10 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	114.55 Mbps	83.22 Mbps	11.63 Kpps	8.37 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

Attaque par réflexion/amplification du DNS - UDP/53

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	5.00 Kpps	326.82 Mbps	168.71 Mbps	32.73 Kpps	16.88 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	4.59 Mbps	3.21 Mbps	433.00 pps	305.56 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	4.33 Mbps	2.95 Mbps	516.00 pps	366.67 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	203.42 Mbps	101.67 Mbps	20.15 Kpps	10.10 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	114.55 Mbps	83.22 Mbps	11.63 Kpps	8.37 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

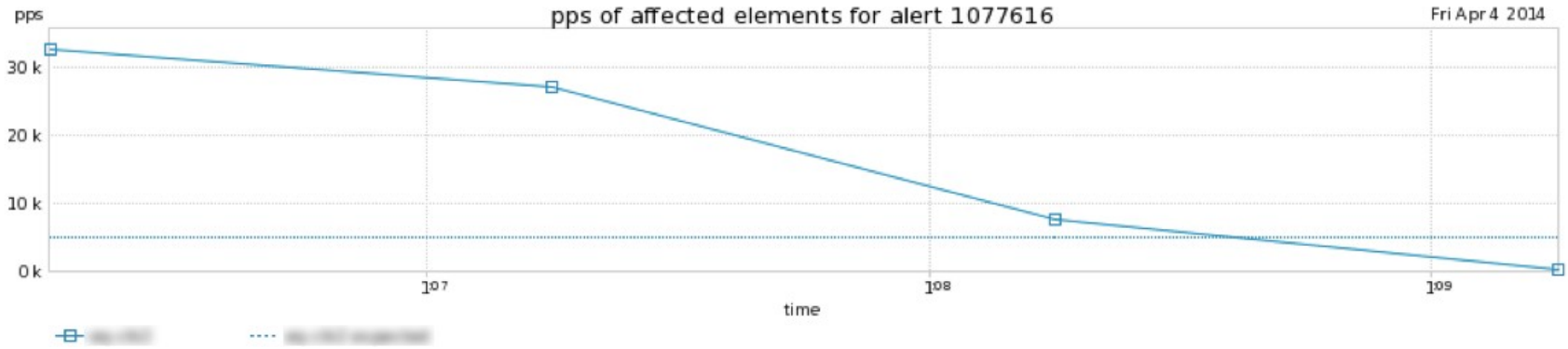
Attaque par réflexion/amplification du DNS - UDP/53

DoS Alert 1077616 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1077616	High 328.3% Of 10.0 Kpps	329.64 Mbps 32.39 Kpps	0:09 (Ended)	Fri, Apr 4 2014, 01:03:14	Incoming	UDP (Misuse)	DNS Reflected/Amplified Attack Traffic [redacted]/32 DNS Reflected/Amplified Attack Traffic



Attaque par réflexion/amplification du DNS - UDP/53

Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	5.00 kpps	326.82 M	168.71 M	32.73 k	16.88 k

Change Timeframe

Timeframe:

Other (*Interval*) | 2014-04-04 01:06:15 (*Start*) | 2014-04-04 01:09:15 (*End*) | Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
5.06 G	4.05 M	1.25 k	168.71 M	16.88 k

Attaque par réflexion/amplification du DNS - UDP/53

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	997.64 M	826.00 k	1.21 k	33.25 M	3.44 k	20.40	☑
80.240.0.0/12 ?	888.50 M	705.00 k	1.26 k	29.62 M	2.94 k	17.41	☑
80.64.0.0/11 ?	888.15 M	647.00 k	1.37 k	29.60 M	2.70 k	15.98	☑
80.64.0.0/10 ?	438.96 M	385.00 k	1.14 k	14.63 M	1.60 k	9.51	☑
80.128.0.0/9 ?	359.47 M	265.00 k	1.36 k	11.98 M	1.10 k	6.54	☑
80.80.0.0/12 ?	344.24 M	256.00 k	1.34 k	11.47 M	1.07 k	6.32	☑
80.48.0.0/13 ?	350.93 M	247.00 k	1.42 k	11.70 M	1.03 k	6.10	☑
80.12.0.0/14 ?	251.94 M	246.00 k	1.02 k	8.40 M	1.02 k	6.07	☑
0.0.0.0/0 ?	276.77 M	241.00 k	1.15 k	9.23 M	1.00 k	5.95	☑
60.0.0.0/10 ?	264.85 M	232.00 k	1.14 k	8.83 M	966.67	5.73	☑

Attaque par réflexion/amplification du DNS - UDP/53

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	997.64 M	826.00 k	1.21 k	33.25 M	3.44 k	20.40	☑
80.240.0.0/12 ?	888.50 M	705.00 k	1.26 k	29.62 M	2.94 k	17.41	☑
80.64.0.0/11 ?	888.15 M	647.00 k	1.37 k	29.60 M	2.70 k	15.98	☑
80.64.0.0/10 ?	438.96 M	385.00 k	1.14 k	14.63 M	1.60 k	9.51	☑
80.128.0.0/9 ?	359.47 M	265.00 k	1.36 k	11.98 M	1.10 k	6.54	☑
80.80.0.0/12 ?	344.24 M	256.00 k	1.34 k	11.47 M	1.07 k	6.32	☑
80.48.0.0/13 ?	350.93 M	247.00 k	1.42 k	11.70 M	1.03 k	6.10	☑
80.12.0.0/14 ?	251.94 M	246.00 k	1.02 k	8.40 M	1.02 k	6.07	☑
0.0.0.0/0 ?	276.77 M	241.00 k	1.15 k	9.23 M	1.00 k	5.95	☑
60.0.0.0/10 ?	264.85 M	232.00 k	1.14 k	8.83 M	966.67	5.73	☑

Attaque par réflexion/amplification du DNS - UDP/53

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	997.64 M	826.00 k	1.21 k	33.25 M	3.44 k	20.40	☑
80.240.0.0/12 ?	888.50 M	705.00 k	1.26 k	29.62 M	2.94 k	17.41	☑
80.64.0.0/11 ?	888.15 M	647.00 k	1.37 k	29.60 M	2.70 k	15.98	☑
80.64.0.0/10 ?	438.96 M	385.00 k	1.14 k	14.63 M	1.60 k	9.51	☑
80.128.0.0/9 ?	359.47 M	265.00 k	1.36 k	11.98 M	1.10 k	6.54	☑
80.80.0.0/12 ?	344.24 M	256.00 k	1.34 k	11.47 M	1.07 k	6.32	☑
80.48.0.0/13 ?	350.93 M	247.00 k	1.42 k	11.70 M	1.03 k	6.10	☑
80.12.0.0/14 ?	251.94 M	246.00 k	1.02 k	8.40 M	1.02 k	6.07	☑
0.0.0.0/0 ?	276.77 M	241.00 k	1.15 k	9.23 M	1.00 k	5.95	☑
60.0.0.0/10 ?	264.85 M	232.00 k	1.14 k	8.83 M	966.67	5.73	☑

Attaque par réflexion/amplification du DNS - UDP/53

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
domain (53)	udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
13671	udp (17)	67.00 k	1.00 k	67.00	2.23 k	4.17	0.02	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Attaque par réflexion/amplification du DNS - UDP/53

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
domain (53)	udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
13671	udp (17)	67.00 k	1.00 k	67.00	2.23 k	4.17	0.02	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Attaque par réflexion/amplification du DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Attaque par réflexion/amplification du DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Attaque par réflexion/amplification du DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-[illegible]/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Attaque par réflexion/amplification du DNS - UDP/53

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

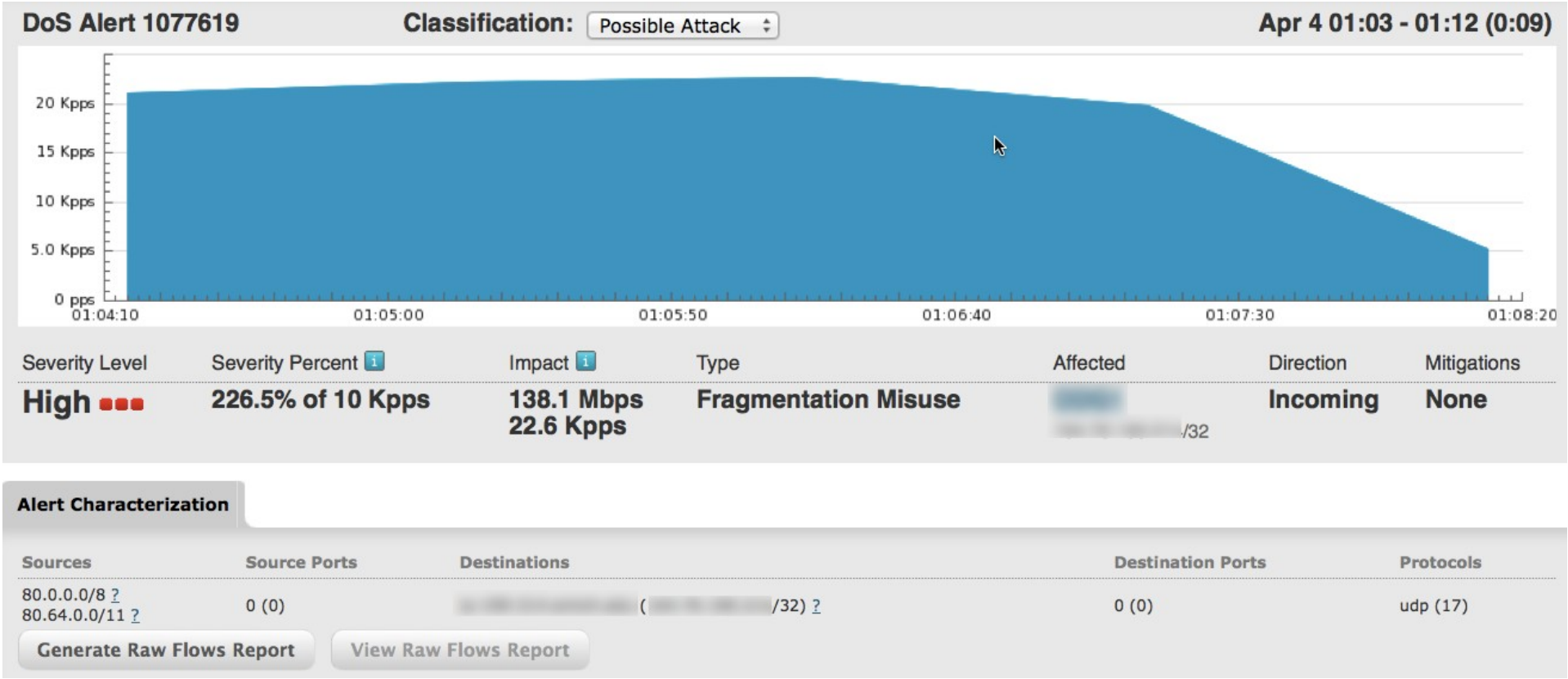
Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.106	521	3.05 G	2.42 M	1.26 k	101.67 M	10.10 k	59.83	☑
xe-4/0/0.104	584	1.87 G	1.51 M	1.24 k	62.42 M	6.28 k	37.19	☑
xe-5/0/1.584	518	66.48 M	66.00 k	1.01 k	2.22 M	275.00	1.63	☐
xe-4/0/1.386	516	72.22 M	55.00 k	1.31 k	2.41 M	229.17	1.36	☐

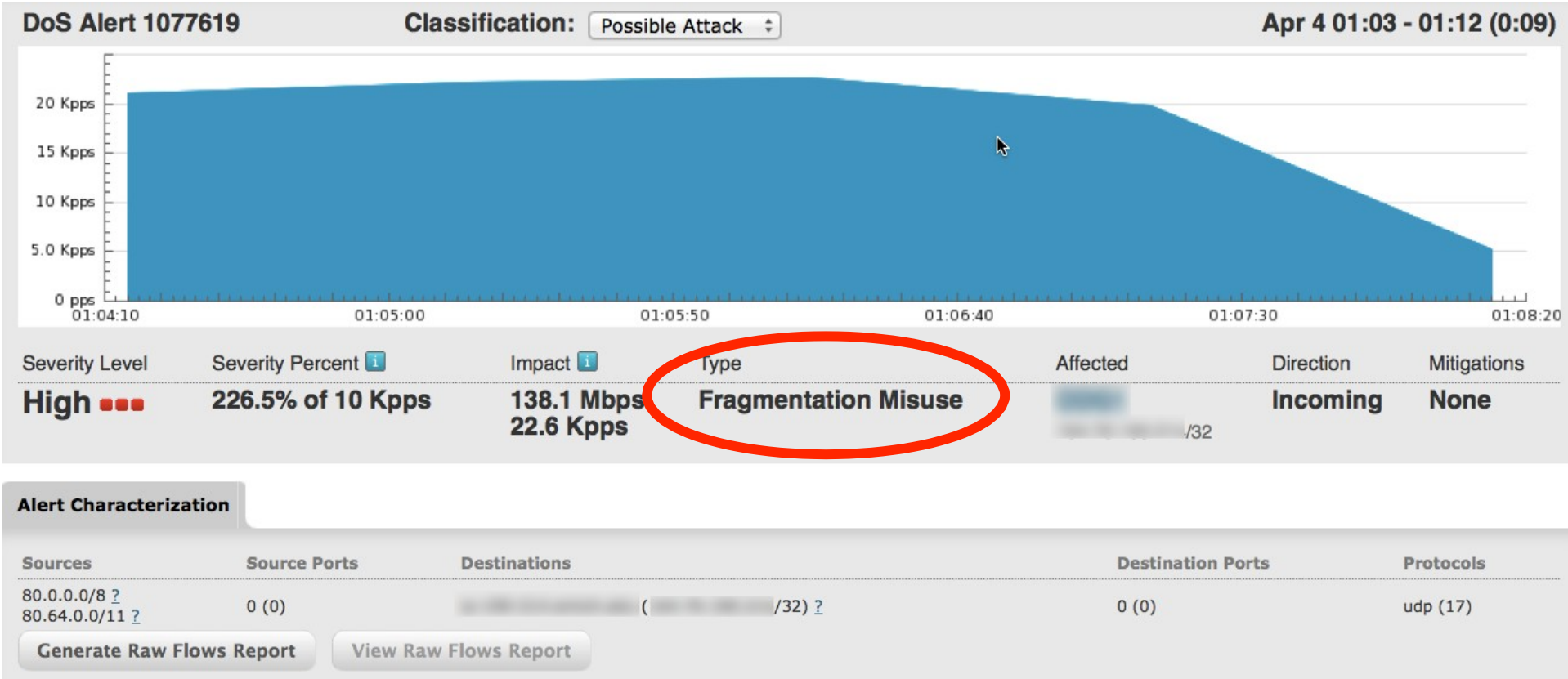
Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	5.06 G	4.05 M	1.25 k	168.71 M	16.88 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux



Attaque par réflexion/amplification du DNS - Fragments non initiaux



Attaque par réflexion/amplification du DNS - Fragments non initiaux

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router [redacted]	High	2.00 Kpps	137.70 Mbps	96.15 Mbps	22.58 Kpps	15.86 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	55.11 Mbps	40.16 Mbps	8.92 Kpps	6.58 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [redacted]	High	2.00 Kpps	137.70 Mbps	96.15 Mbps	22.58 Kpps	15.86 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	55.11 Mbps	40.16 Mbps	8.92 Kpps	6.58 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router [redacted]	High	2.00 Kpps	137.70 Mbps	96.15 Mbps	22.58 Kpps	15[redacted]6 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 [redacted]	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	55.11 Mbps	40.16 Mbps	8.92 Kpps	6.58 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

DNS reflection/amplification attack.

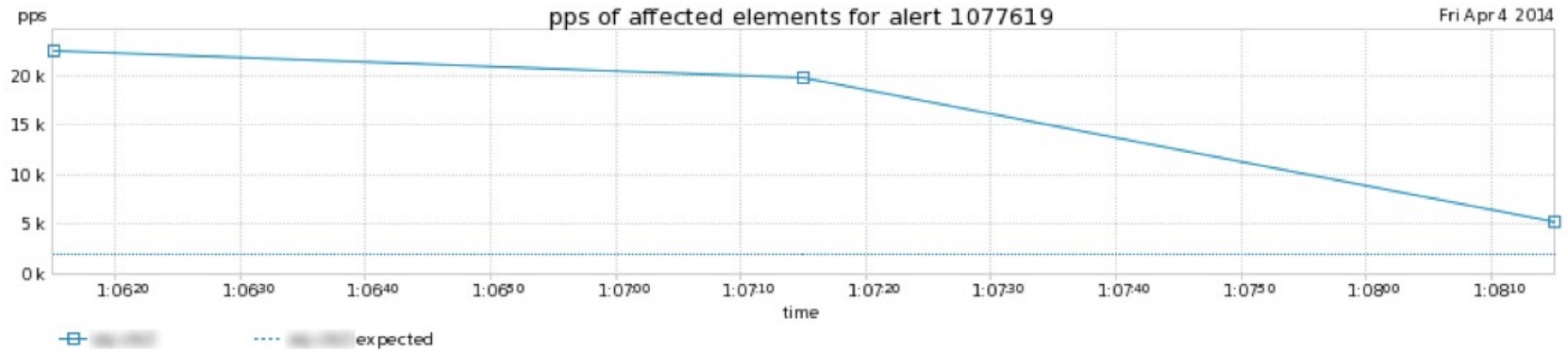
Attaque par réflexion/amplification du DNS - Fragments non initiaux

DoS Alert 1077619 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1077619	High 226.5% Of 10.0 Kpps	138.10 Mbps 22.65 Kpps	0:09 (Ended)	Fri, Apr 4 2014, 01:03:14	Incoming	Fragment (Misuse)	[redacted]/32



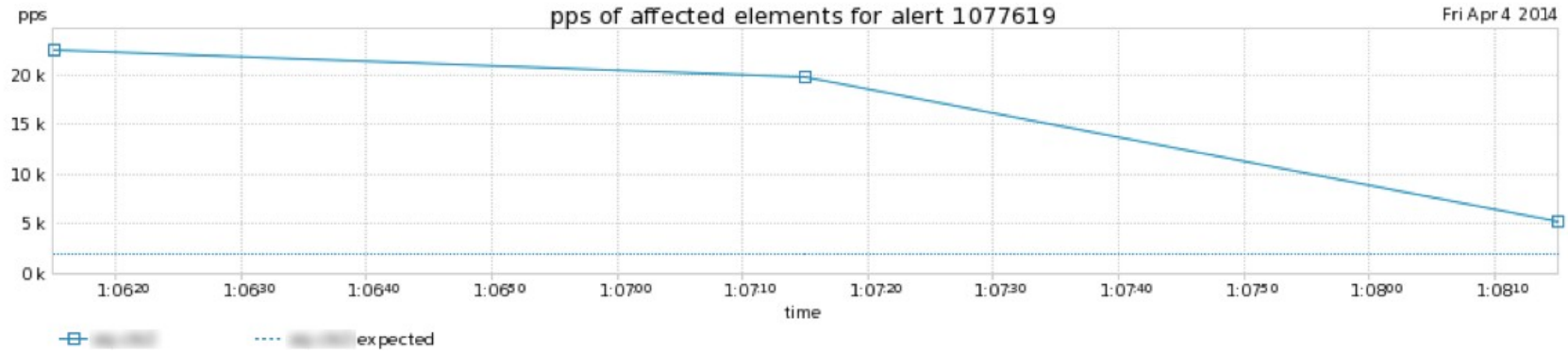
Attaque par réflexion/amplification du DNS - Fragments non initiaux

DoS Alert 1077619 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1077619	High 226.5% Of 10.0 Kpps	138.10 Mbps 22.65 Kpps	0:09 (Ended)	Fri, Apr 4 2014, 01:03:14	Incoming	Fragment (Misuse)	[redacted]/32



Attaque par réflexion/amplification du DNS - Fragments non initiaux

Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	2.00 kpps	137.70 M	96.15 M	22.58 k	15.86 k

Change Timeframe

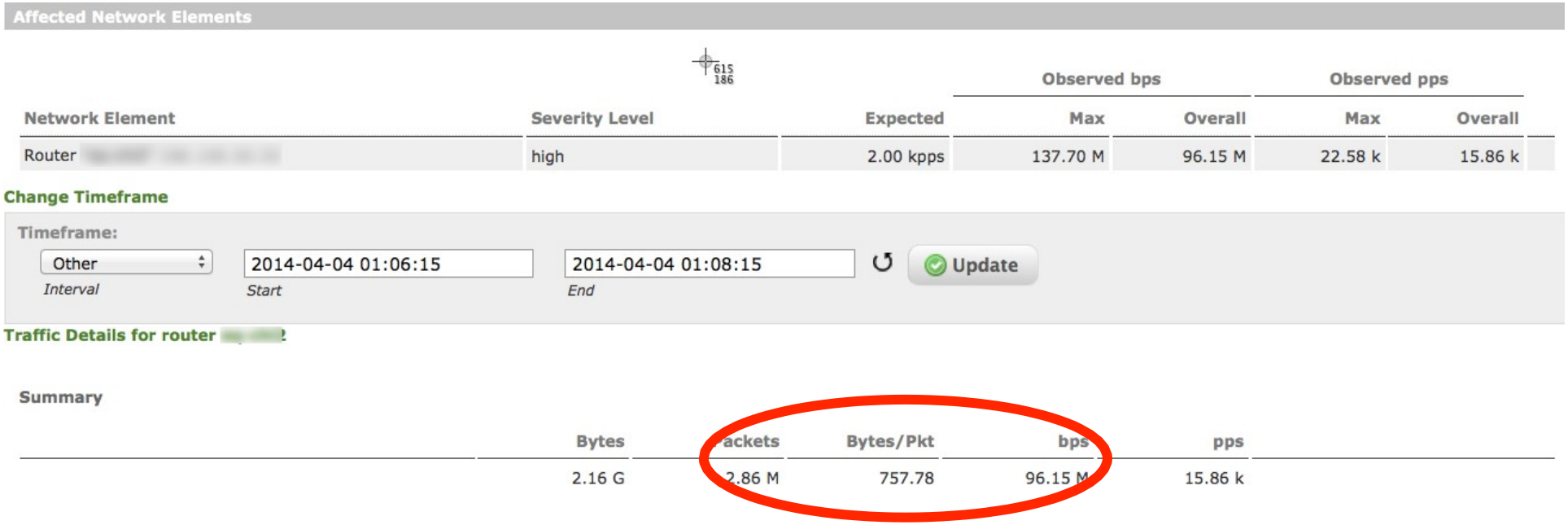
Timeframe: Other (*Interval*) 2014-04-04 01:06:15 (*Start*) 2014-04-04 01:08:15 (*End*) Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
2.16 G	2.86 M	757.78	96.15 M	15.86 k

Attaque par réflexion/amplification du DNS - Fragments non initiaux



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	2.00 kpps	137.70 M	96.15 M	22.58 k	15.86 k

Change Timeframe

Timeframe: Other (*Interval*) 2014-04-04 01:06:15 (*Start*) 2014-04-04 01:08:15 (*End*) Update

Traffic Details for router [redacted]

Summary

	Bytes	Packets	Bytes/Pkt	bps	pps
	2.16 G	2.86 M	757.78	96.15 M	15.86 k

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	432.54 M	612.00 k	706.76	19.22 M	3.40 k	21.44	☑
80.64.0.0/11 ?	385.48 M	467.00 k	825.44	17.13 M	2.59 k	16.36	☑
0.0.0.0/0 ?	290.26 M	424.00 k	684.58	12.90 M	2.36 k	14.85	☑
80.240.0.0/12 ?	281.81 M	399.00 k	706.29	12.52 M	2.22 k	13.98	☑
80.0.0.0/9 ?	303.92 M	379.00 k	801.89	13.51 M	2.11 k	13.27	☑
80.80.0.0/12 ?	206.59 M	244.00 k	846.66	9.18 M	1.36 k	8.55	☑
80.128.0.0/9 ?	128.22 M	170.00 k	754.24	5.70 M	944.44	5.95	☑
80.232.0.0/13 ?	134.64 M	160.00 k	841.51	5.98 M	888.89	5.60	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
80.0.0.0/8 ?	432.54 M	612.00 k	706.76	19.22 M	3.40 k	21.44	☑
80.64.0.0/11 ?	385.48 M	467.00 k	825.44	17.13 M	2.59 k	16.36	☑
0.0.0.0/0 ?	290.26 M	424.00 k	684.58	12.90 M	2.36 k	14.85	☑
80.240.0.0/12 ?	281.81 M	399.00 k	706.29	12.52 M	2.22 k	13.98	☑
80.0.0.0/9 ?	303.92 M	379.00 k	801.89	13.51 M	2.11 k	13.27	☑
80.80.0.0/12 ?	206.59 M	244.00 k	846.66	9.18 M	1.36 k	8.55	☑
80.128.0.0/9 ?	128.22 M	170.00 k	754.24	5.70 M	944.44	5.95	☑
80.232.0.0/13 ?	134.64 M	160.00 k	841.51	5.98 M	888.89	5.60	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted] (/32) ?	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0	udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.	521	1.20 G	1.60 M	751.39	53.43 M	8.89 k	56.04	☑
xe-4/0/0.104	584	903.70 M	1.19 M	762.62	40.16 M	6.58 k	41.51	☑
xe-5/0/1.584	518	29.06 M	36.00 k	807.34	1.29 M	200.00	1.26	☐
xe-4/0/1.386	516	28.47 M	34.00 k	837.36	1.27 M	188.89	1.19	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.	521	1.20 G	1.60 M	751.39	53.43 M	8.89 k	56.04	☑
xe-4/0/0.104	584	903.70 M	1.19 M	762.62	40.16 M	6.58 k	41.51	☑
xe-5/0/1.584	518	29.06 M	36.00 k	807.34	1.29 M	200.00	1.26	☐
xe-4/0/1.386	516	28.47 M	34.00 k	837.36	1.27 M	188.89	1.19	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Attaque par réflexion/amplification du DNS - Fragments non initiaux

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/1/0.	521	1.20 G	1.60 M	751.39	53.43 M	8.89 k	56.04	☑
xe-4/0/0.104	584	903.70 M	1.19 M	762.62	40.16 M	6.58 k	41.51	☑
xe-5/0/1.584	518	29.06 M	36.00 k	807.34	1.29 M	200.00	1.26	☐
xe-4/0/1.386	516	28.47 M	34.00 k	837.36	1.27 M	188.89	1.19	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

Reflection/Amplification SNMP

Facteur d'amplification - SNMP

Abréviation	Protocole	Ports	Facteur d'amplification	# Serveurs abusifs
CHARGEN	Protocole de génération de caractères	UDP / 19	18x/1000x	Des dizaines de milliers (90K)
DNS	Système de nom de domaine	UDP / 53	160x	Millions (27M)
NTP	Protocole de temps réseau	UDP / 123	1000x	Plus de cent mille (119K)
SNMP	Protocole de gestion de réseau simple	UDP / 161	880x	Millions (5M)
SSDP	Protocole de découverte de service simple	UDP /1900	20x/83x	Millions (2M)

Caractéristiques d'une attaque par réflexion/amplification

- L'attaquant usurpe l'adresse IP de la cible de l'attaque et envoie une requête SNMP *GetBulkRequest* à des services SNMP abusifs fonctionnant sur des dispositifs CPE domestiques, des routeurs de grands FAI et d'entreprises, des serveurs, etc. etc. Ces paquets ont généralement une longueur de etc. 60 à 102 octets.
- L'attaquant choisit le port UDP qu'il souhaite cibler - il peut s'agir de n'importe quel port de son choix - et l'utilise comme sourceport . Le port de destination est UDP/ 161.
- Les services SNMP "répondent" à la cible de l'attaque par des flux de paquets de 423 à 1560 octets provenant de UDP/161 ; le port de destination est le port source choisi par l'attaquant lors de la génération des requêtes SNMP.

Caractéristiques d'une attaque par réflexion/amplification (suite)

- Lorsque ces multiples flux de réponses SNMP convergent, le volume de l'attaque peut être très important - la plus grande attaque vérifiée de ce type à ce jour dépasse les 60gb/sec. 20-30 gigaoctets/seconde ; les attaques sont monnaie courante.
- En raison du volume des attaques, la bande passante de transit Internet de la cible, ainsi que la bande passante principale des pairs/amonts de la cible, de même que la bande passante principale des réseaux intermédiaires entre les divers services SNMP utilisés de manière abusive et la cible, sont saturées.
- Les attaquants plus avisés énuméreront les différents identifiants d'objet SNMP (OID) sur les services SNMP abusifs, et énuméreront chacun d'entre eux avec des queries lots SNMP usurpés parallèles itératifs queries de fragments non initiaux dans ce scénario, à la DNS.
- Dans la plupart des attaques, entre ~2 000 et 4 000 services SNMP abusifs sont exploités par attackers. Jusqu'à 10 000 services SNMP ont été observés dans certaines attaques.

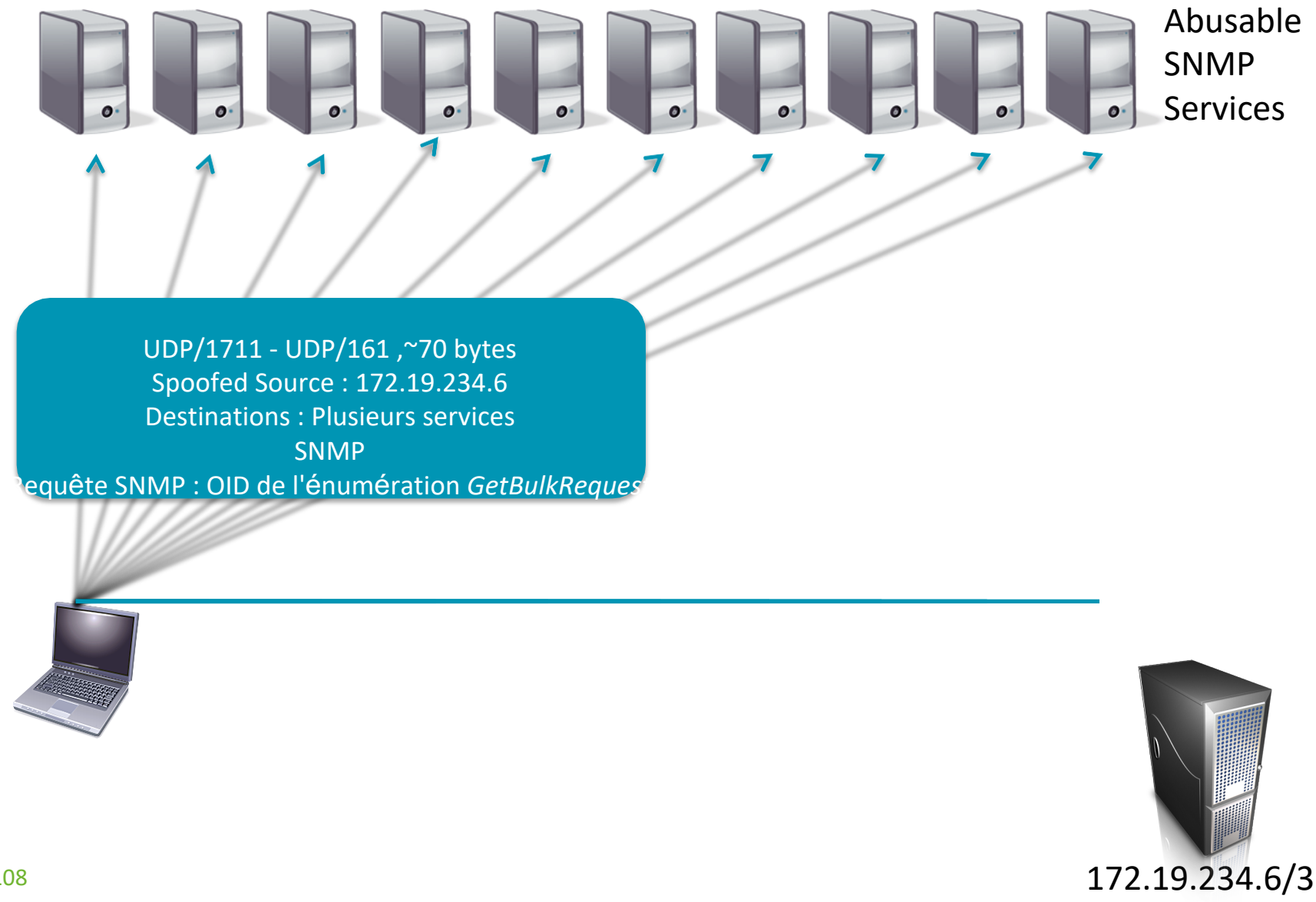
Méthodologie d'attaque par réflexion/amplification

Abusable
SNMP
Services

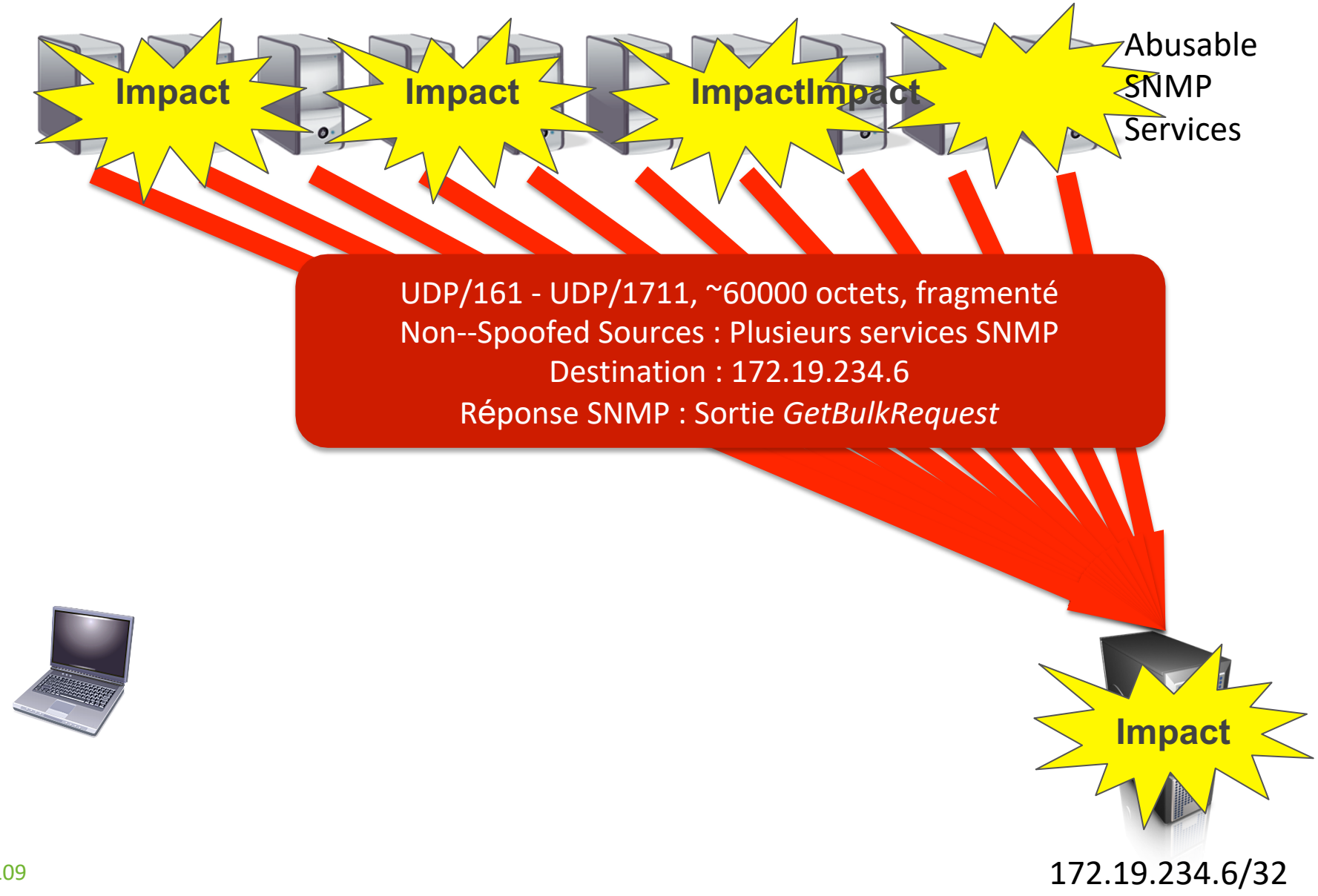
Serveurs accessibles par Internet, routeurs, dispositifs CPE domestiques, etc.

172.19.234.6/32

Méthodologie d'attaque par réflexion/amplification



Méthodologie d'attaque par réflexion/amplification



Reflection/Amplification de la charge

Facteur d'amplification - chargen

Abréviation	Protocole	Ports	Facteur d'amplification	# Serveurs abusifs
CHARGEN	Protocole de génération de caractères	UDP / 19	18x/1000x	Des dizaines de milliers (90K)
DNS	Système de nom de domaine	UDP / 53	160x	Millions (27M)
NTP	Protocole de temps réseau	UDP / 123	1000x	Plus de cent mille (119K)
SNMP	Protocole de gestion de réseau simple	UDP / 161	880x	Millions (5M)
SSDP	Protocole de découverte de service simple	UDP /1900	20x/83x	Millions (2M)

Caractéristiques d'une attaque par réflexion/amplification

- L'attaquant usurpe l'adresse IP de la cible de l'attaque, envoie des paquets remplis d'au moins 18 octets de données utiles (tous les zéros ; paquet de 70 octets) à plusieurs services de charge abusifs fonctionnant sur des serveurs, des imprimantes, des dispositifs CPE domestiques, etc.
- L'attaquant choisit le port UDP qu'il souhaite cibler - il peut s'agir de tout port supérieur à 1023 - et l'utilise comme sourceport. Le port de destination est UDP/19.
- Les services chargen "répondent" à la cible de l'attaque avec des paquets de ~1000 à ~1500 octets provenant d'UDP/19 vers la cible ; le port de destination est le port source choisi par l'attaquant lorsqu'il a généré le chargen queries. La plupart des services chargen génèrent un paquet de réponse pour chaque paquet de requête, mais certains services chargen non conformes à la RFC envoient plus de paquets par requête.

Caractéristiques d'une attaque par réflexion/amplification (suite)

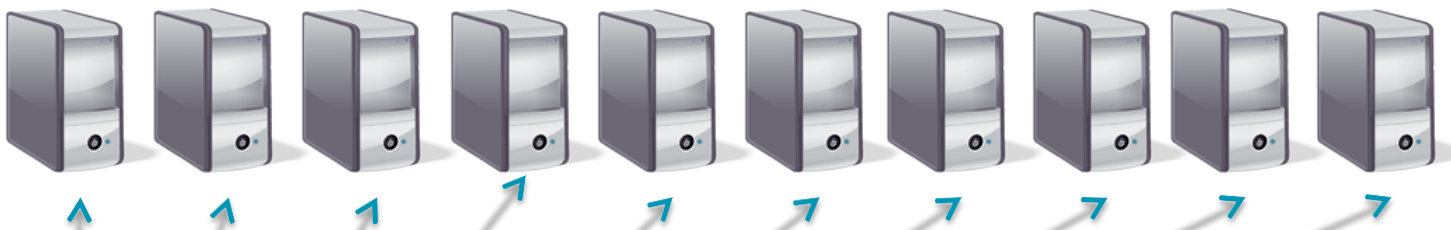
- Au fur et à mesure que ces multiples flux de réponses chargées convergent, le volume de l'attaque peut être assez important - la plus grande attaque vérifiée de ce type jusqu'à présent est supérieure à 137gb/sec 2-5gb/sec ; les attaques sont monnaie courante.
- En raison du volume des attaques, la bande passante de transit Internet de la cible, ainsi que la bande passante principale des pairs/amonts de la cible, de même que la bande passante principale des réseaux intermédiaires entre les divers services de charge utilisés et la cible, peuvent être saturées.
- Les services de charge non conformes au RFC peuvent fournir un facteur d'amplification allant jusqu'à 1000:1 (la plupart sont de 18:1).
- Dans la plupart des attaques, entre ~20 et ~2 000 services chargents abusifs sont exploités par les services chargents. Jusqu'attackers à 5 000 services chargents ont été observés dans certaines attaques.

Méthodologie d'attaque par réflexion/amplification des charognes

Services de chargements abusifs

172.19.234.6/32

Méthodologie d'attaque par réflexion/amplification des charognes



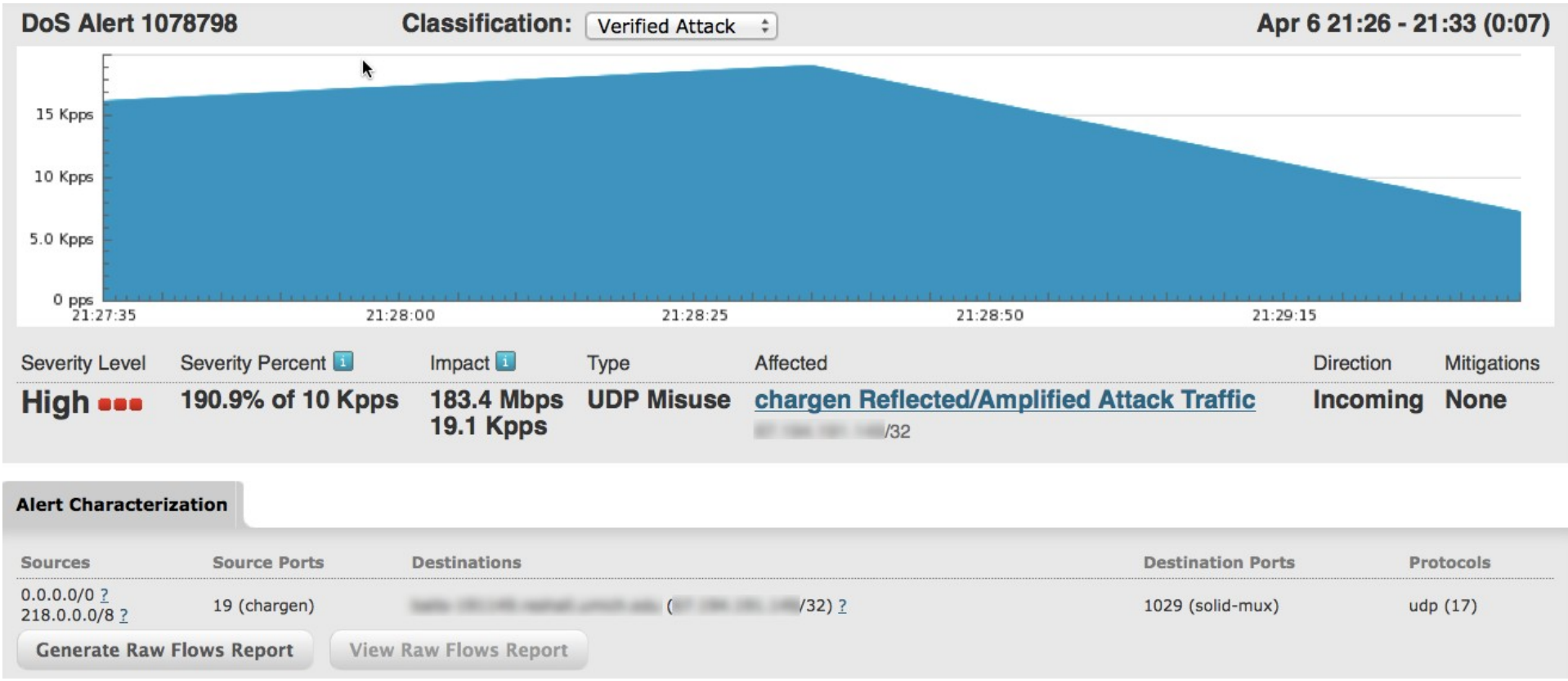
Services de chargements abusifs

UDP/21880- UDP/19 ,~70 bytes Spoofed
Source : 172.19.234.6 Destinations :
Plusieurs services charges Requête
Chargen : 18 octets de bourrage de crâne

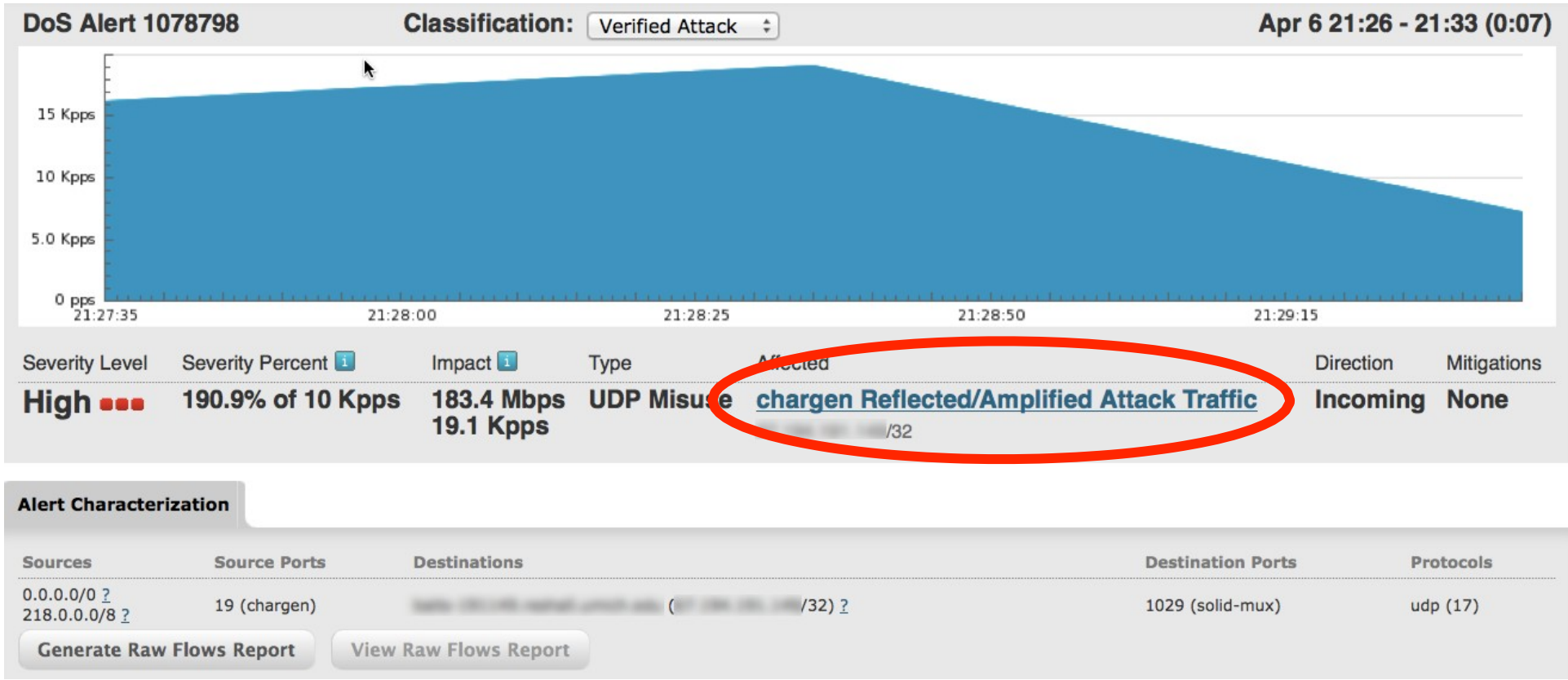
172.19.234.6/32

Méthodologie d'attaque par réflexion/amplification des charognes

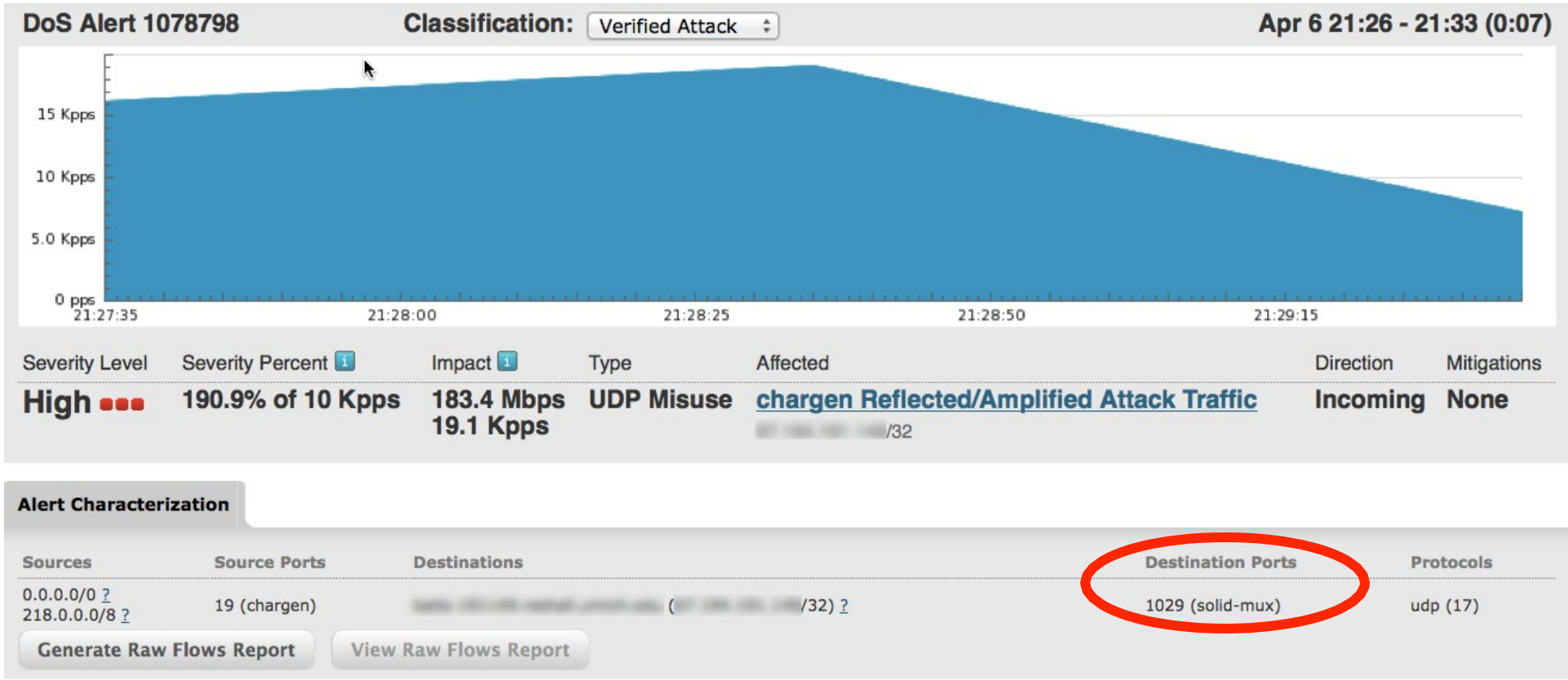
Attaque par réflexion/amplification du logiciel - UDP/19



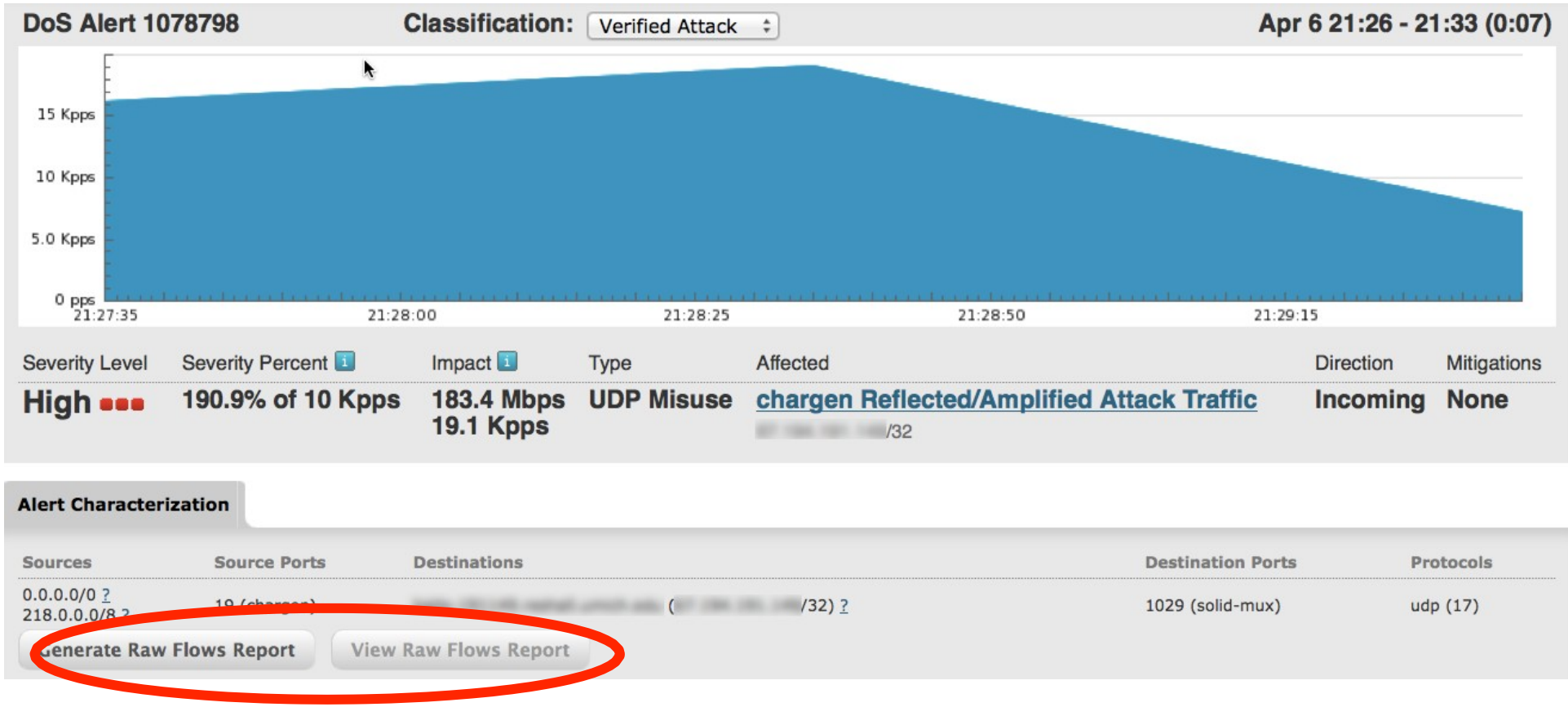
Attaque par réflexion/amplification du logiciel - UDP/19



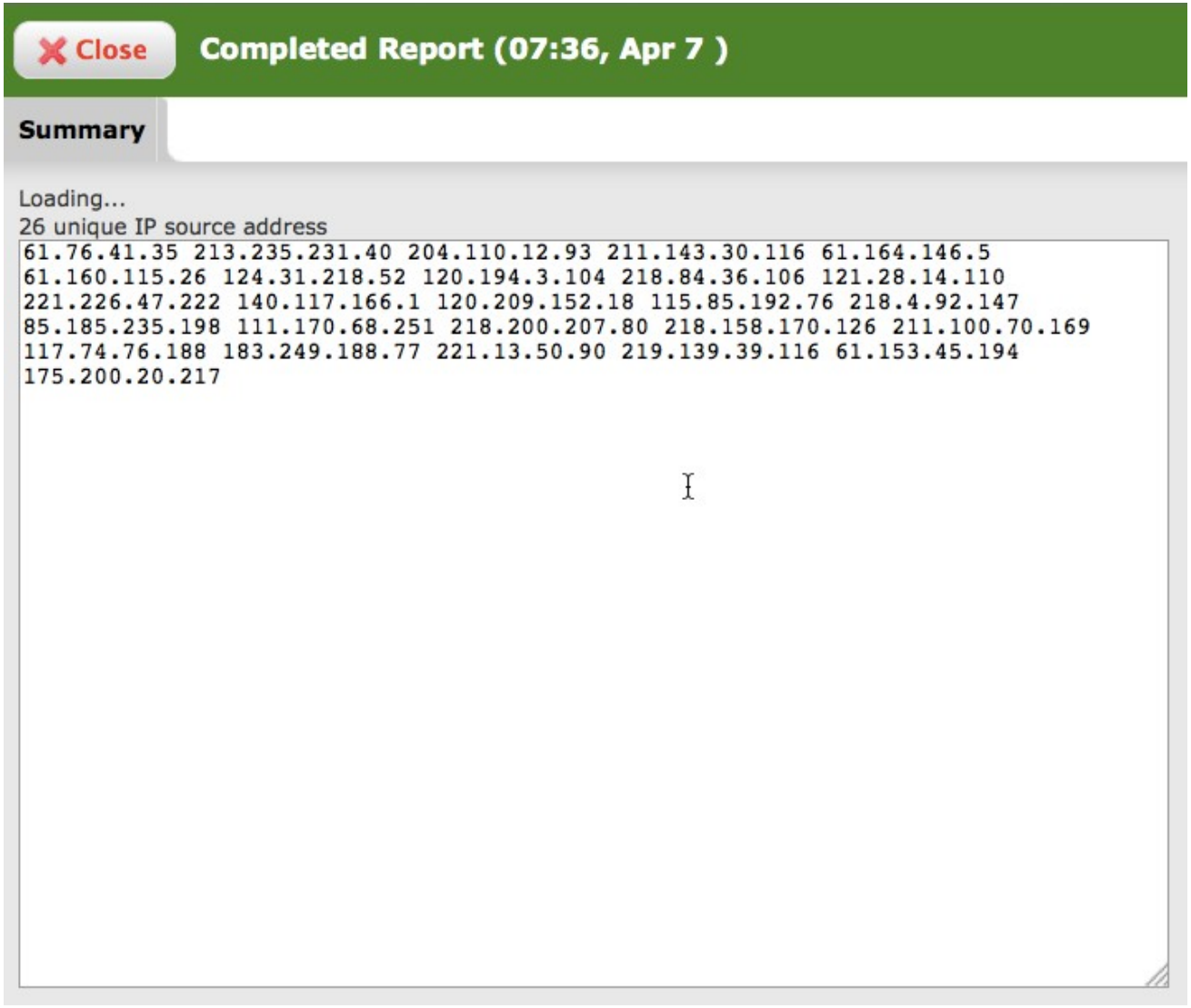
Attaque par réflexion/amplification du logiciel - UDP/19



Attaque par réflexion/amplification du logiciel - UDP/19



Attaque par réflexion/amplification du logiciel - UDP/19



Attaque par réflexion/amplification du logiciel - UDP/19

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router eq-chi2	High	5.00 Kpps	147.33 Mbps	73.92 Mbps	15.45 Kpps	7.76 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386		-	500.13 Kbps	500.14 Kbps	50.00 pps	50.00 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	76.11 Mbps	38.15 Mbps	8.12 Kpps	4.07 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106		-	49.96 Mbps	25.13 Mbps	5.10 Kpps	2.57 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	20.76 Mbps	10.38 Mbps	2.18 Kpps	1.10 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

chargen reflection/amplification attack.

Attaque par réflexion/amplification du logiciel - UDP/19

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router eq-chi2 [redacted]	High	5.00 Kpps	147.33 Mbps	73.92 Mbps	15.45 Kpps	7.[illegible]6 Kpps	Details
Interface (SNMP 516) xe-4/0/1.386 [redacted]		-	500.13 Kbps	500.14 Kbps	50.00 pps	50.00 [illegible]ps	Details
Interface (SNMP 518) xe-5/0/1.584 [redacted]		-	76.11 Mbps	38.15 Mbps	8.12 Kpps	4.07 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106 [redacted]		-	49.96 Mbps	25.13 Mbps	5.10 Kpps	2.57 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [redacted]		-	20.76 Mbps	10.38 Mbps	2.18 Kpps	1.10 Kpps	Details

Annotations

Add Comment

Escalated

This alert has been escalated to the security group and mitigated efficiently!

chargen reflection/amplification attack.

Attaque par réflexion/amplification du logiciel - UDP/19

DoS Alert 1078798 Traffic Details

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
1078798	High 190.9% Of 10.0 Kpps	183.38 Mbps 19.09 Kpps	0:07 (Ended)	Sun, Apr 6 2014, 21:26:36	Incoming	UDP (Misuse)	chargen Reflected/Amplified Attack Traffic [redacted]/32 chargen Reflected/Amplified Attack Traffic

Attaque par réflexion/amplification du logiciel - UDP/19

Affected Network Elements

Network Element	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall
Router [redacted]	high	5.00 kpps	147.33 M	73.92 M	15.45 k	7.76 k

Change Timeframe

Timeframe:

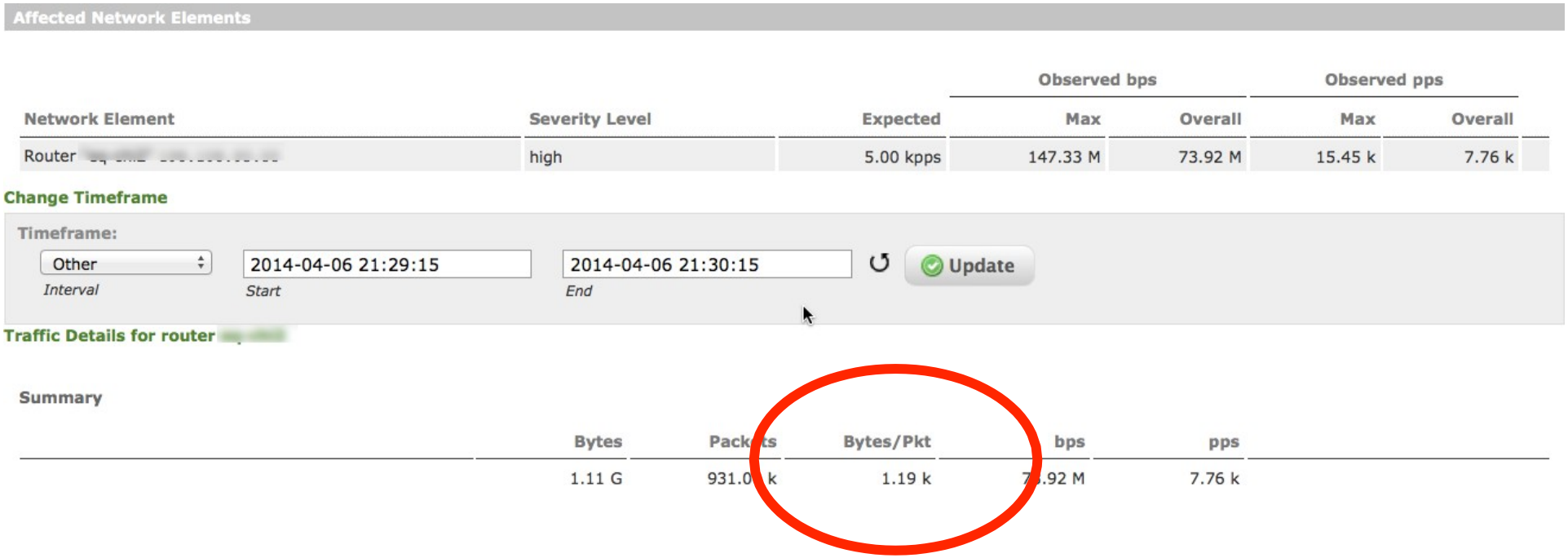
Other (*Interval*) 2014-04-06 21:29:15 (*Start*) 2014-04-06 21:30:15 (*End*) Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
1.11 G	931.00 k	1.19 k	73.92 M	7.76 k

Attaque par réflexion/amplification du logiciel - UDP/19



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [redacted]	high	5.00 kpps	147.33 M	73.92 M	15.45 k	7.76 k

Change Timeframe

Timeframe:

Other (*Interval*) | 2014-04-06 21:29:15 (*Start*) | 2014-04-06 21:30:15 (*End*) | Update

Traffic Details for router [redacted]

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
1.11 G	931.0 k	1.19 k	73.92 M	7.76 k

Attaque par réflexion/amplification du logiciel - UDP/19

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	940.18 M	792.00 k	1.19 k	62.68 M	6.60 k	85.07	☑
218.0.0.0/8 ?	108.55 M	91.00 k	1.19 k	7.24 M	758.33	9.77	☑
61.128.0.0/10 ?	60.03 M	48.00 k	1.25 k	4.00 M	400.00	5.16	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32) ?	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
chargen (19)	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1029	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Attaque par réflexion/amplification du logiciel - UDP/19

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	940.18 M	792.00 k	1.19 k	62.68 M	6.60 k	85.07	☑
218.0.0.0/8 ?	108.55 M	91.00 k	1.19 k	7.24 M	758.33	9.77	☑
61.128.0.0/10 ?	60.03 M	48.00 k	1.25 k	4.00 M	400.00	5.16	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32) ?	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
chargen (19)	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1029	udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Attaque par réflexion/amplification du logiciel - UDP/19

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/0/1.584	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
xe-4/0/0.104	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-4/0/1.386	516	3.75 M	3.00 k	1.25 k	250.07 k	25.00	0.32	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Attaque par réflexion/amplification du logiciel - UDP/19

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/0/1.584	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
e-4/0/0.104	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-1/0/1.386	516	3.75 M	3.00 k	1.25 k	250.07 k	25.00	0.32	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Attaque par réflexion/amplification du logiciel - UDP/19

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-5/0/1.584	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
xe-4/0/0.104	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-4/0/1.386	516	3.75 M	3.00 k	1.25 k	250.07 k	25.00	0.32	☐

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
xe-4/1/1.76	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

Reflection/Amplification du SSDP

Facteur d'amplification - SSDP

Abréviation	Protocole	Ports	Facteur d'amplification	# Serveurs abusifs
CHARGEN	Protocole de génération de caractères	UDP / 19	18x/1000x	Des dizaines de milliers (90K)
DNS	Système de nom de domaine	UDP / 53	160x	Millions (27M)
NTP	Protocole de temps réseau	UDP / 123	1000x	Plus de cent mille (119K)
SNMP	Protocole de gestion de réseau simple	UDP / 161	880x	Millions (5M)
SSDP	Protocole de découverte de service simple	UDP /1900	20x/83x	Millions (2M)

Caractéristiques d'une attaque par réflexion/amplification

- L'attaquant usurpe l'adresse IP de la cible de l'attaque, envoie une requête SSDP *M-Search* aux services SSDP abusifs fonctionnant sur les appareils CPE domestiques et certains anciens Windows XP systems Ces paquets ont généralement une longueur de ~118 octets.
- L'attaquant choisit le port UDP qu'il souhaite cibler - il peut s'agir de n'importe quel port au choix de l'attaquant - et l'utilise comme sourceport. Le port de destination est UDP/1900.
- Les services SSDP "répondent" à la cible de l'attaque par des flux de paquets de 1360 à 9800 octets provenant de UDP/1900 ; le port de destination est le port source choisi par l'attaquant lors de la génération du SSDP. queries. Ces paquets se composent de fragments queries. UDP initiaux et non initiaux.

Caractéristiques d'une attaque par réflexion/amplification (suite)

- Lorsque ces multiples flux de réponses SSDP convergent, le volume de l'attaque peut être très important - la plus grande attaque vérifiée de ce type à ce jour est supérieure à 42gb/sec. 10-35 gigaoctets/seconde ; les attaques sont monnaie courante.
- En raison du volume des attaques, la bande passante de transit Internet de la cible, ainsi que la bande passante principale des pairs/amonts de la cible, de même que la bande passante principale des réseaux intermédiaires entre les divers services SSDP utilisés de manière abusive et la cible, sont saturées.
- Les attaquants plus avisés identifieront les services SSDP individuels disponibles sur les appareils SSDP abusifs et les énuméreront avec des queries lots SSDP parallèles itératifs et usurpés de queries fragments non initiaux dans ce scénario, à la DNS.
- Dans la plupart des attaques, entre ~4 000 et 6 000 services SSDP abusifs sont exploités par attackers. Jusqu'à 10 000 services attackers. SSDP abusifs ont été observés dans certaines attaques.

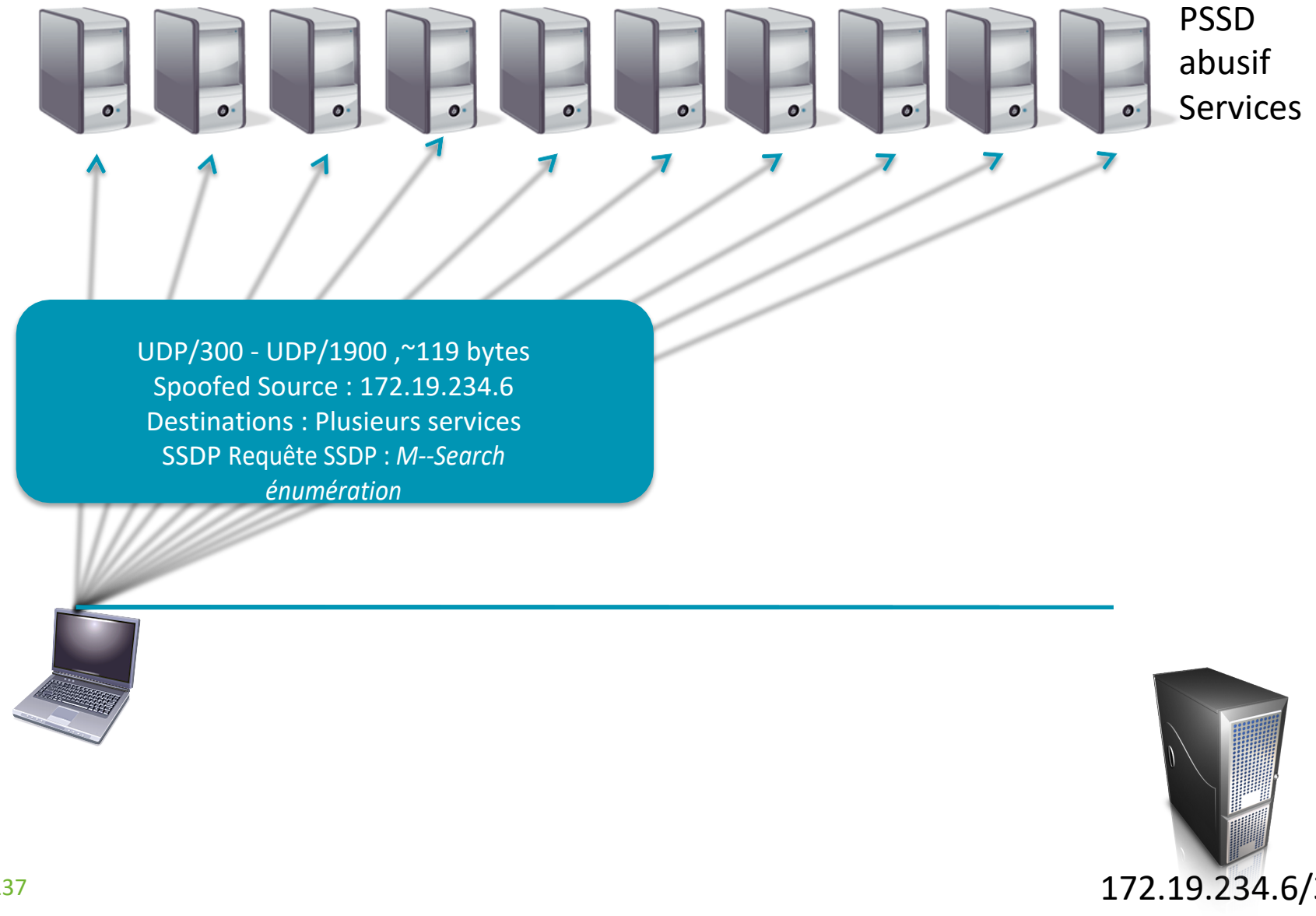
Méthodologie d'attaque par réflexion/amplification du SSDP

PSSD
abusif
Services

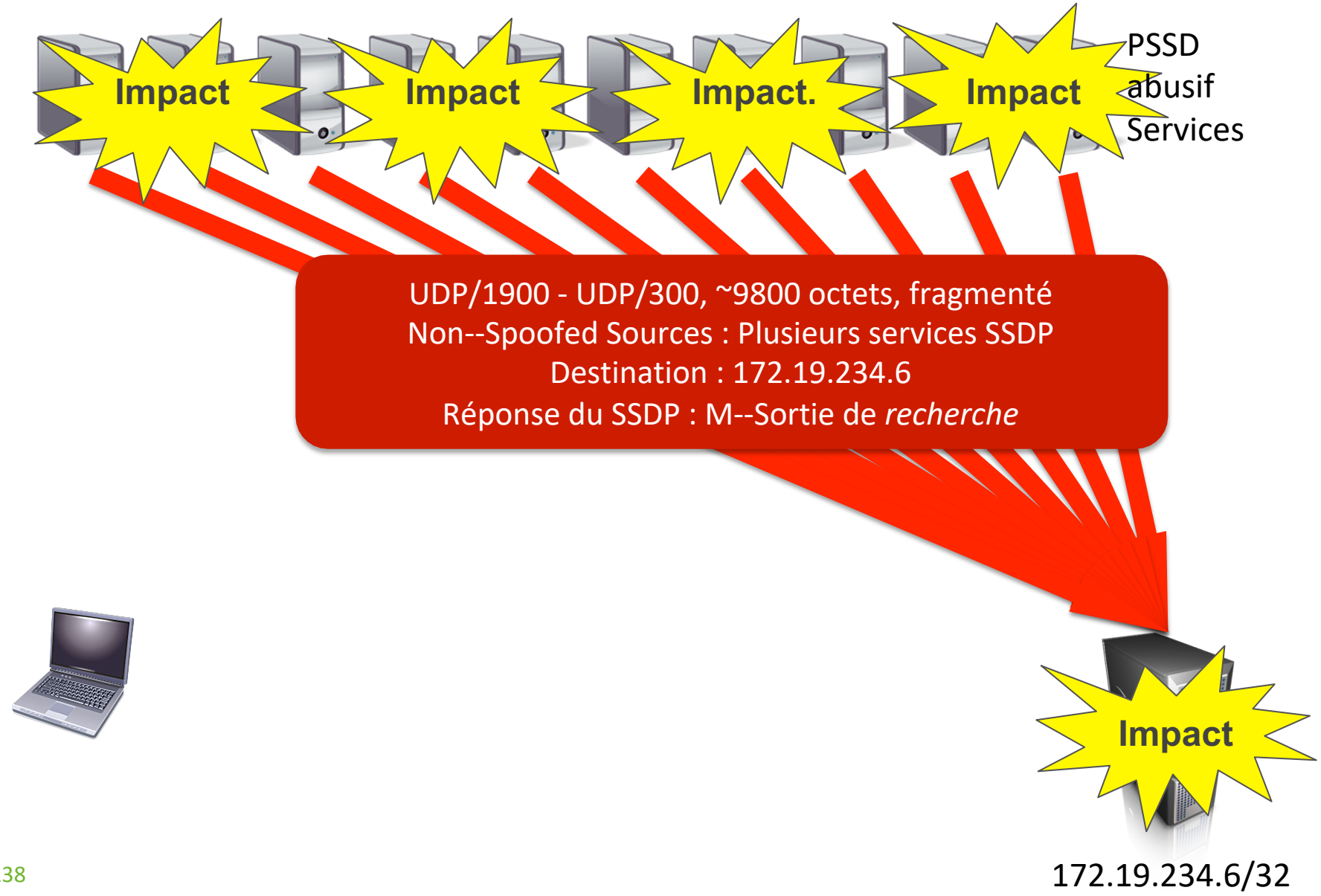
Dispositifs CPE accessibles par Internet, vieilles boîtes Windows XP, etc.

172.19.234.6/32

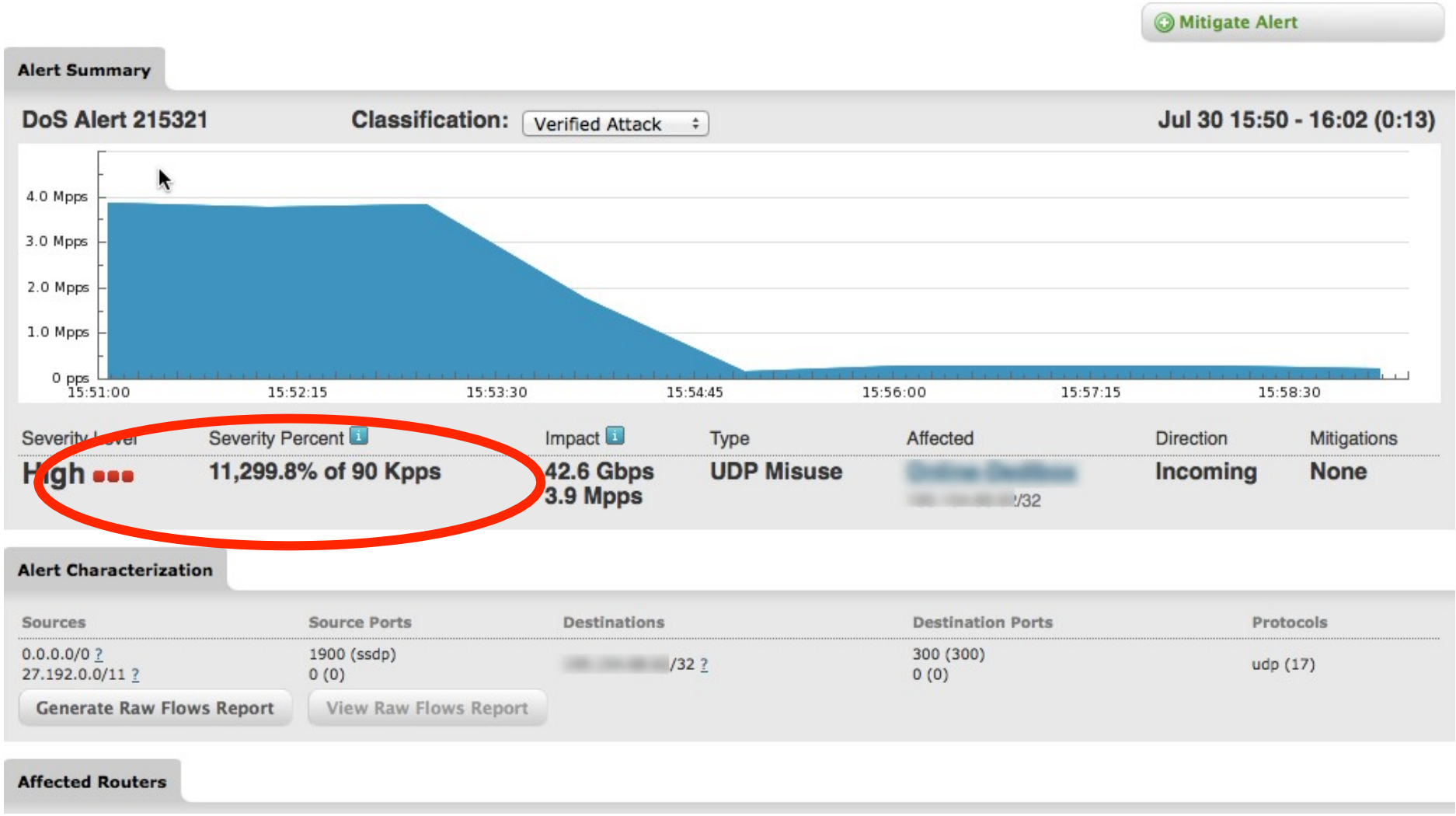
Méthodologie d'attaque par réflexion/amplification du SSDP



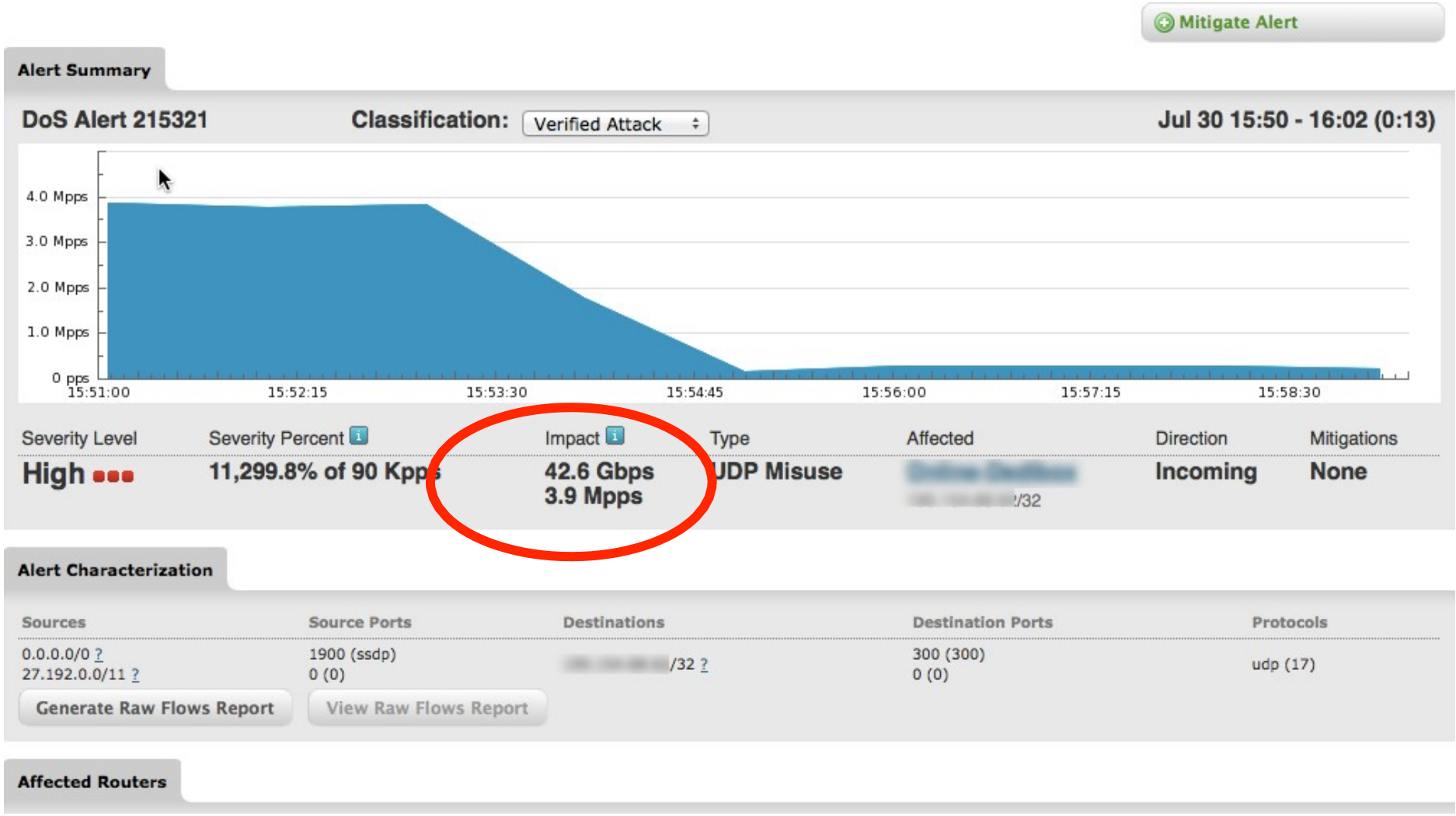
Méthodologie d'attaque par réflexion/amplification du SSDP



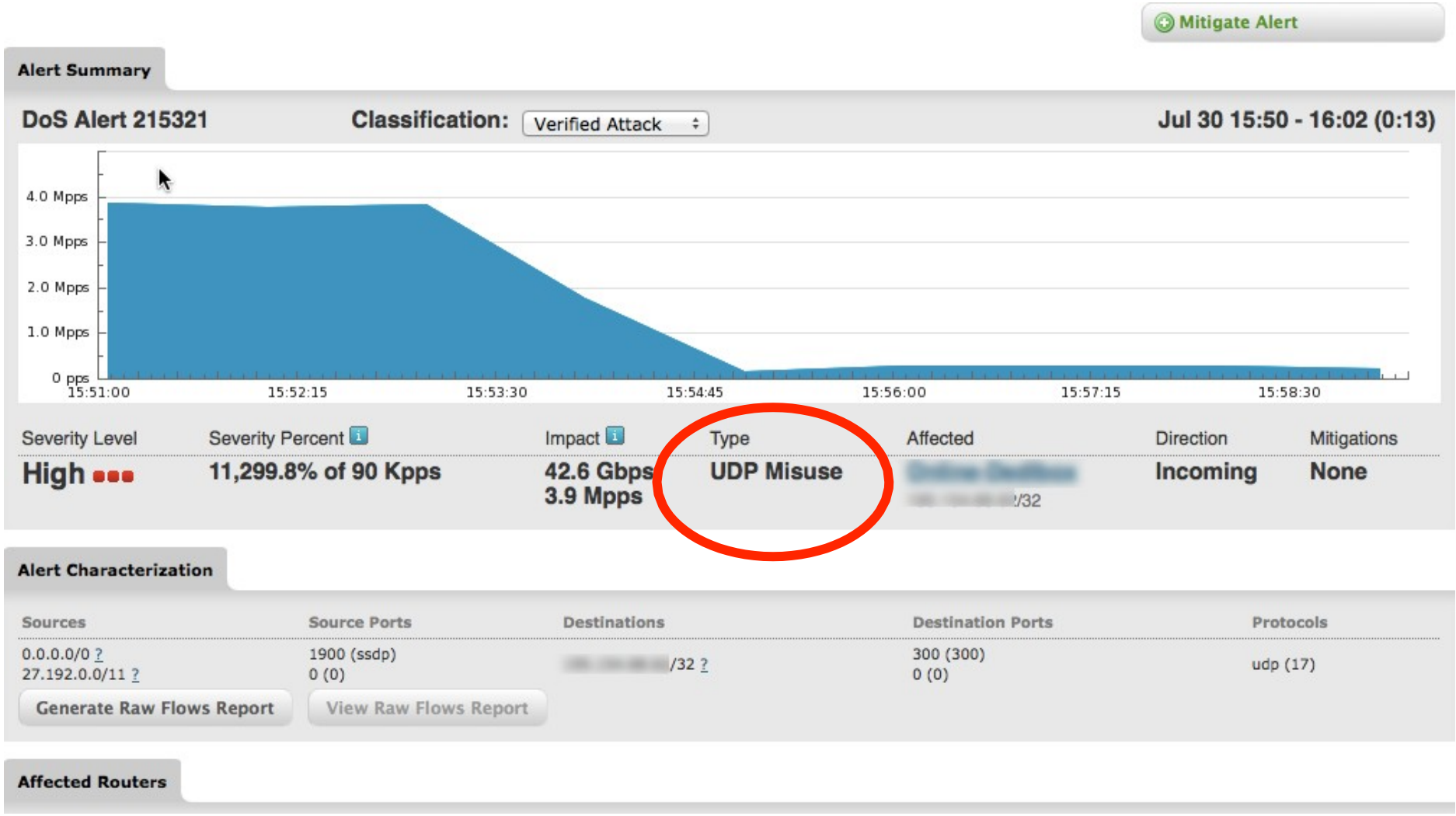
Attaque par réflexion/amplification du SSDP



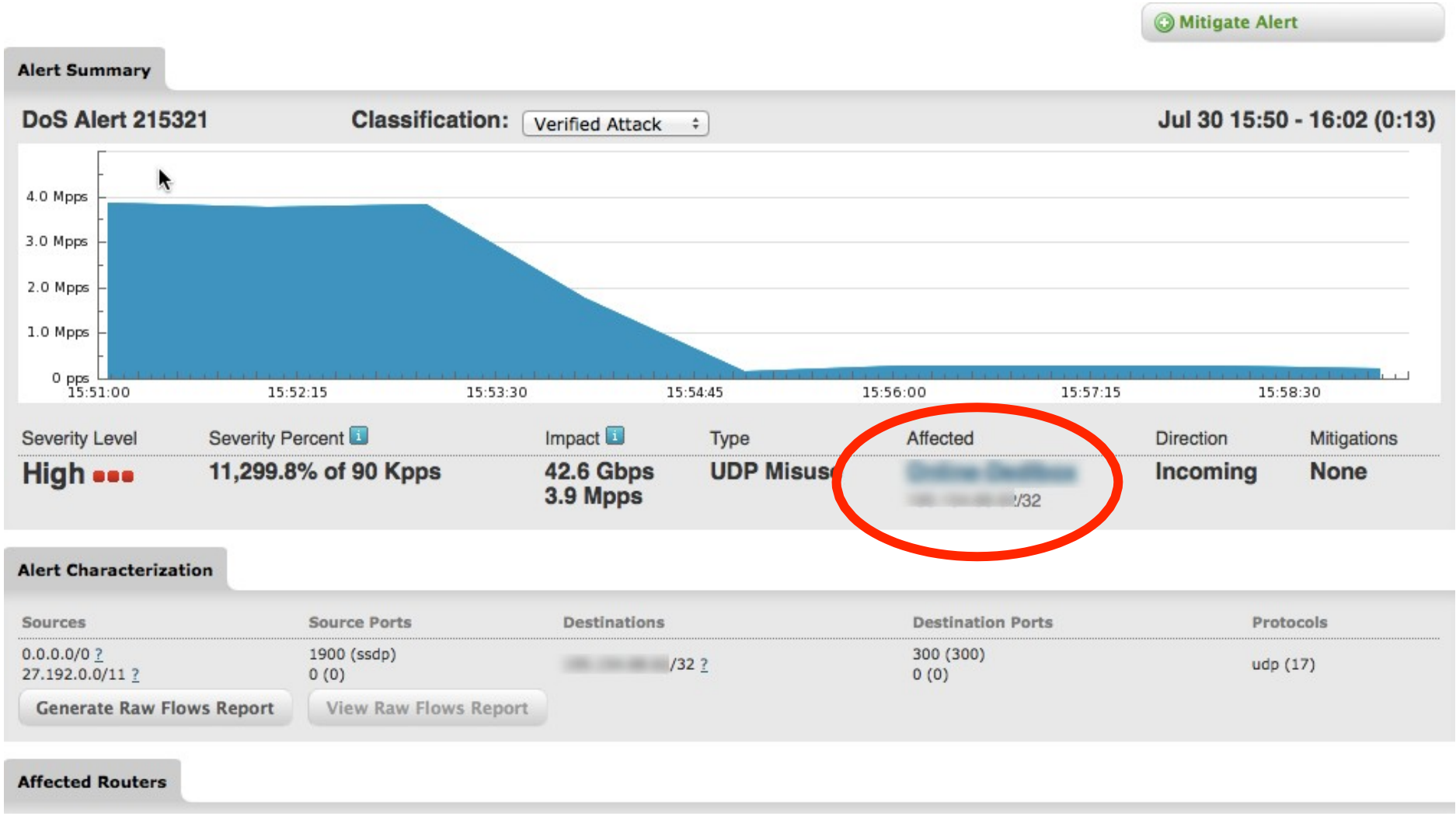
Attaque par réflexion/amplification du SSDP



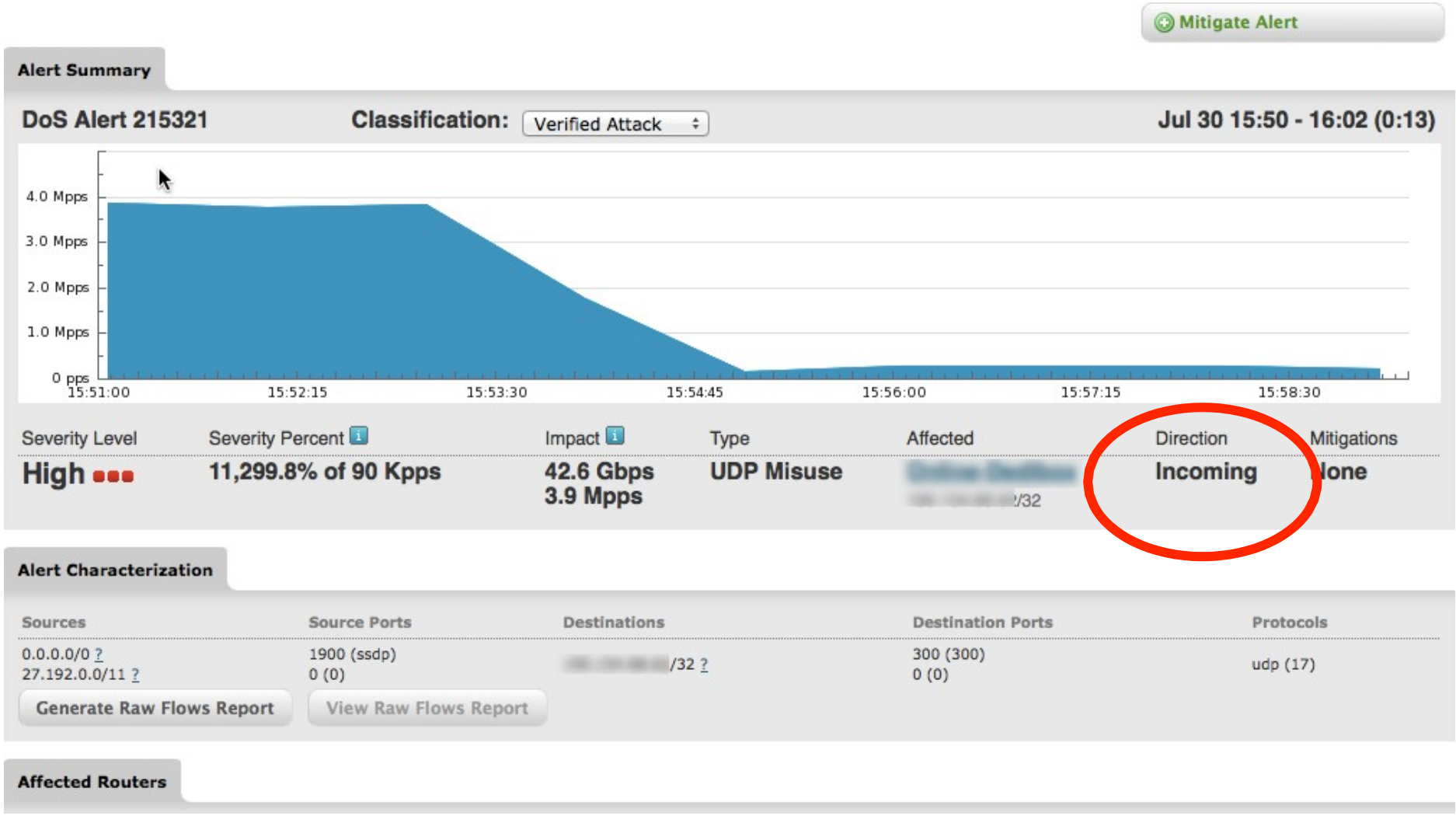
Attaque par réflexion/amplification du SSDP



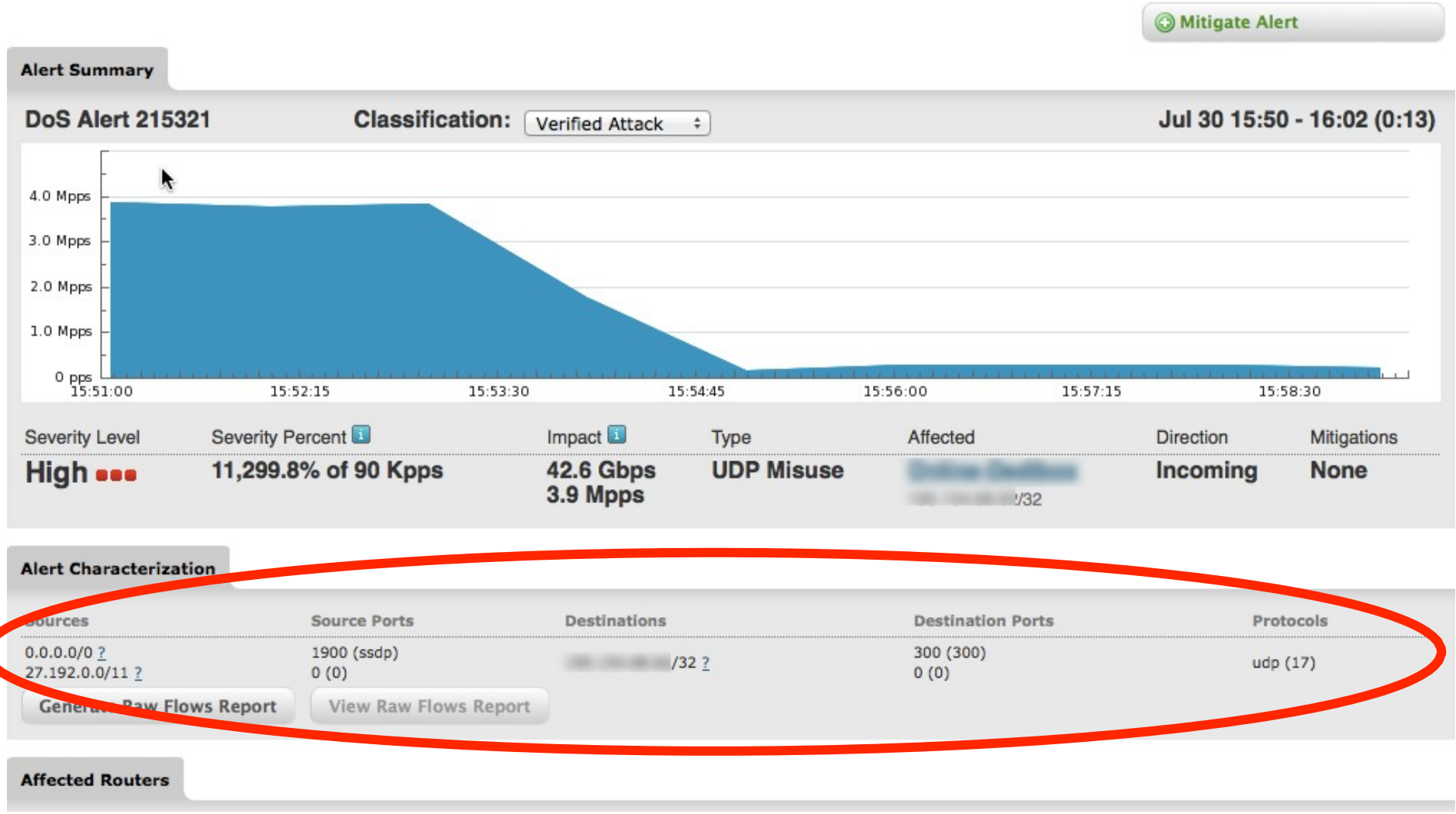
Attaque par réflexion/amplification du SSDP



Attaque par réflexion/amplification du SSDP



Attaque par réflexion/amplification du SSDP



Attaque par réflexion/amplification du SSDP

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	50.00 Kpps	40.14 Gbps	20.25 Gbps	9.94 Mpps	4.79 Mpps	Details
Interface (SNMP 315) Bundle-Ether2.1013		-	1.20 Gbps	549.60 Mbps	287.47 Kpps	166.81 Kpps	Details
Interface (SNMP 344) Bundle-Ether100.2002		-	3.89 Mbps	2.15 Mbps	1.48 Kpps	757.14 pps	Details
Interface (SNMP 299) Bundle-Ether6453		-	10.62 Gbps	3.70 Gbps	965.25 Kpps	559.58 Kpps	Details
Interface (SNMP 478) Bundle-Ether44530		-	5.40 Mbps	5.22 Mbps	533.00 pps	505.56 pps	Details
Interface (SNMP 480) Bundle-Ether1299		-	22.46 Gbps	14.26 Gbps	8.52 Mpps	3.83 Mpps	Details
Interface (SNMP 569) Bundle-Ether3356		-	4.96 Gbps	1.81 Gbps	448.37 Kpps	295.68 Kpps	Details
Interface (SNMP 626) Bundle-Ether3.4090		-	2.11 Gbps	792.03 Mbps	191.38 Kpps	90.91 Kpps	Details
Router	High	50.00 Kpps	2.24 Gbps	934.88 Mbps	294.82 Kpps	178.77 Kpps	Details
Interface (SNMP 88) TenGigE0/0/0/17		-	2.22 Mbps	1.78 Mbps	200.00 pps	155.56 pps	Details
Interface (SNMP 274) TenGigE0/0/0/11.4080		-	2.49 Mbps	1.76 Mbps	233.00 pps	161.11 pps	Details
Interface (SNMP 361) Bundle-Ether44530		-	12.51 Mbps	5.46 Mbps	1.12 Kpps	891.44 pps	Details
Interface (SNMP 445) Bundle-Ether3.4080		-	2.09 Gbps	787.81 Mbps	189.22 Kpps	90.86 Kpps	Details
Interface (SNMP 470) TenGigE0/4/0/20.4		-	634.94 Mbps	298.68 Mbps	244.43 Kpps	105.23 Kpps	Details

Attaque par réflexion/amplification du SSDP

Affected Routers

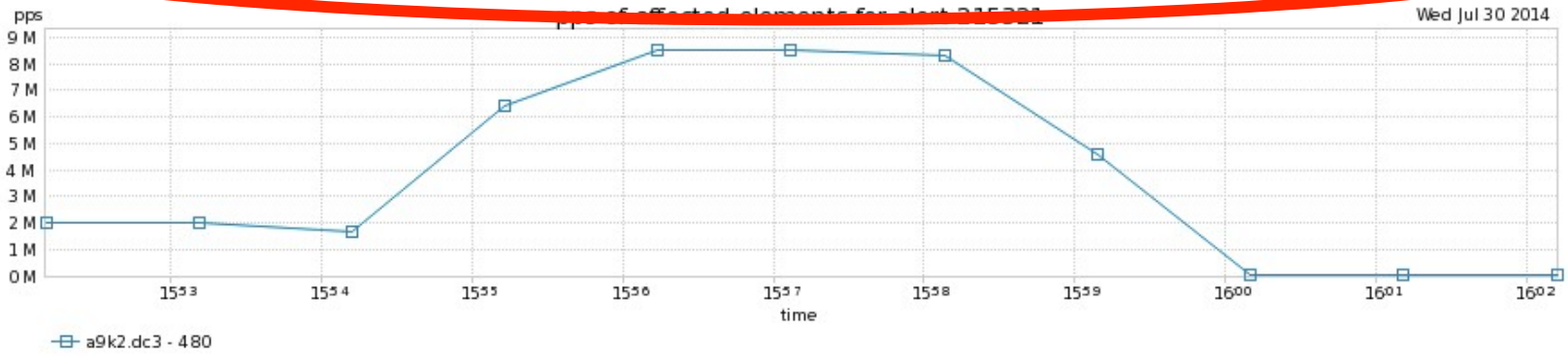
	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	50.00 Kpps	40.14 Gbps	20.25 Gbps	9.94 Mpps	4.7[illegible] Mpps	Details
Interface (SNMP 315) Bundle-Ether2.1013		-	1.20 Gbps	549.60 Mbps	287.47 Kpps	166.81 Kpp[illegible]	Details
Interface (SNMP 344) Bundle-Ether100.2002		-	3.89 Mbps	2.15 Mbps	1.48 Kpps	757.14 pps	Details
Interface (SNMP 299) Bundle-Ether6453		-	10.62 Gbps	3.70 Gbps	965.25 Kpps	559.58 Kpps	Details
Interface (SNMP 478) Bundle-Ether44530		-	5.40 Mbps	5.22 Mbps	533.00 pps	505.56 pps	Details
Interface (SNMP 480) Bundle-Ether1299		-	22.46 Gbps	14.26 Gbps	8.52 Mpps	3.83 Mpps	Details
Interface (SNMP 569) Bundle-Ether3356		-	4.96 Gbps	1.81 Gbps	448.37 Kpps	295.68 Kpps	Details
Interface (SNMP 626) Bundle-Ether3.4090		-	2.11 Gbps	792.03 Mbps	191.38 Kpps	90.91 Kpps	Details
Router	High	50.00 Kpps	2.24 Gbps	934.88 Mbps	294.82 Kpps	178.77 Kpps	Details
Interface (SNMP 88) TenGigE0/0/0/17		-	2.22 Mbps	1.78 Mbps	200.00 pps	155.56 pps	Details
Interface (SNMP 274) TenGigE0/0/0/11.408[illegible]		-	2.49 Mbps	1.76 Mbps	233.00 pps	161.11 pps	Details
Interface (SNMP 361) Bundle-Ether44530		-	12.51 Mbps	5.46 Mbps	1.12 Kpps	891.44 pps	Details
Interface (SNMP 445) Bundle-Ether3.4080		-	2.09 Gbps	787.81 Mbps	189.22 Kpps	90.86 Kpps	Details
Interface (SNMP 470) TenGigE0/4/0/20.4		-	634.94 Mbps	298.68 Mbps	244.43 Kpps	105.23 Kpps	Details

Attaque par réflexion/amplification du SSDP

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	[illegible]
215321	High 11,299.8% Of 90.0 Kpps	42.62 Gbps 3.86 Mpps	0:13 (Ended)	Wed, Jul 30 2014, 15:50:04	Incoming	UDP (Misuse)	[illegible]



Affected Network Elements

Network Element	Severity Level	Expected	Observed bps		Observed pps	
			Max	Overall	Max	Overall
Router [illegible]	high	50.00 kpps	40.14 G	20.25 G	9.94 M	4.79 M
Interface 480 Bundle-Ether1299 [illegible]		-	22.46 G	14.26 G	8.52 M	3.83 M

Attaque par réflexion/amplification du SSDP

Summary

	Bytes	Packets	Bytes/Pkt	bps	pps
	1.18 T	2.53 G	465.76	14.26 G	3.83 M

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	721.81 G	1.11 G	647.97	8.75 G	1.69 M	44.12	☑
27.192.0.0/11 ?	138.49 G	428.31 M	323.35	1.68 G	648.95 k	16.96	☑
117.0.0.0/9 ?	99.91 G	311.60 M	320.63	1.21 G	472.12 k	12.34	☑
218.0.0.0/9 ?	84.05 G	259.96 M	323.32	1.02 G	393.88 k	10.30	☑
180.96.0.0/11 ?	68.35 G	213.31 M	320.45	828.54 M	323.19 k	8.45	☑
27.128.0.0/9 ?	63.46 G	197.93 M	320.62	769.22 M	299.89 k	7.84	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]'32 ?	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1900	udp (17)	703.33 G	2.18 G	322.31	8.53 G	3.31 M	86.42	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	145.17 M	1.33 M	108.91	1.76 M	2.02 k	0.05	☐

Destination Ports

Attaque par réflexion/amplification du SSDP

Summary

Bytes	Packets	Bytes/Pkt	bps	pps
1.18 T	2.53 G	465.76	14.26 G	3.83 M

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	721.81 G	1.11 G	647.97	8.75 G	1.69 M	44.12	☑
27.192.0.0/11 ?	138.49 G	428.31 M	323.35	1.68 G	648.95 k	16.96	☑
117.0.0.0/9 ?	99.91 G	311.60 M	320.63	1.21 G	472.12 k	12.34	☑
218.0.0.0/9 ?	84.05 G	259.96 M	323.32	1.02 G	393.88 k	10.30	☑
180.96.0.0/11 ?	68.35 G	213.31 M	320.45	828.54 M	323.19 k	8.45	☑
27.128.0.0/9 ?	63.46 G	197.93 M	320.62	769.22 M	299.89 k	7.84	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1900	udp (17)	703.33 G	2.18 G	322.31	8.53 G	3.31 M	86.42	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	145.17 M	1.33 M	108.91	1.76 M	2.02 k	0.05	☐

Destination Ports

Attaque par réflexion/amplification du SSDP

Summary

	Bytes	Packets	Bytes/Pkt	bps	pps
	1.18 T	2.53 G	465.76	14.26 G	3.83 M

Source Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
0.0.0.0/0 ?	721.81 G	1.11 G	647.97	8.75 G	1.69 M	44.12	☑
27.192.0.0/11 ?	138.49 G	428.31 M	323.35	1.68 G	648.95 k	16.96	☑
117.0.0.0/9 ?	99.91 G	311.60 M	320.63	1.21 G	472.12 k	12.34	☑
218.0.0.0/9 ?	84.05 G	259.96 M	323.32	1.02 G	393.88 k	10.30	☑
180.96.0.0/11 ?	68.35 G	213.31 M	320.45	828.54 M	323.19 k	8.45	☑
27.128.0.0/9 ?	63.46 G	197.93 M	320.62	769.22 M	299.89 k	7.84	☑

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[redacted]/32 ?	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Source Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
1900	udp (17)	703.33 G	2.18 G	322.31	8.[illegible] G	3.31 M	86.42	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 [illegible]	514.87 k	13.46	☑
0 - 32767	udp (17)	145.17 M	1.33 M	108.91	1.76 M	2.02 k	0.05	☐

Destination Ports

Attaque par réflexion/amplification du SSDP

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
300	udp (17)	703.57 G	2.18 G	322.31	8.53 G	3.31 M	86.45	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
[illegible] - 32767	udp (17)	29.05 M	21.00 k	1.38 k	352.14 k	31.82	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
Bundle-Ether1299 [illegible]	480	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
TenGigE0/7/0/20 [illegible]	143	793.91 G	2.25 G	353.08	9.62 G	3.41 M	89.05	☑
TenGigE0/0/0/10.409[illegible]	705	359.31 G	261.05 M	1.38 k	4.36 G	395.53 k	10.34	☑
Index:0	0	6.89 G	4.68 M	1.47 k	83.55 M	7.09 k	0.19	☐

Attaque par réflexion/amplification du SSDP

Destination Ports

Port Range	Protocol	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
300	udp (17)	703.57 G	2.18 G	322.31	8.53 G	3.31 M	86.45	☑
0	udp (17)	470.92 G	339.82 M	1.39 k	5.71 G	514.87 k	13.46	☑
0 - 32767	udp (17)	29.05 M	21.00 k	1.38 k	352.14 k	31.82	0.00	☐

IP Protocol

Type	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
udp (17)	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Ingress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
Bundle-Ether1299	480	1.18 T	2.53 G	465.76	14.26 G	3.83 M	100.00	☑

Egress Interfaces

Name	ifIndex	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
TenGigE0/7/0/20	143	793.91 G	2.25 G	353.08	9.62 G	3.41 M	89.05	☑
TenGigE0/0/0/10.409	705	359.31 G	261.05 M	1.38 k	4.36 G	395.53 k	10.34	☑
index:0	0	6.89 G	4.68 M	1.47 k	83.55 M	7.09 k	0.19	☐

How Much Spoofed Traffic Yieldsa 100gb/sec DDoS Attack ?

Quelle quantité de trafic usurpé permet de réaliser une attaque DDoS de 100 Go/sec ?

- **DNS - facteur d'amplification de 160:1**
  - **625mb/sec** de requêtes DNS usurpées pour une attaque de **100gb/sec.**
  - La plus grande observée en 2014 - 104gb/sec, 125gb/sec signalée.
- **ntp - facteur d'amplification 1000:1**
  - **100mb/sec** de requêtes ntp usurpées pour une attaque de **100gb/sec**
  - Le plus grand observé en 2014 - 325gb/sec, 450gb/sec rapporté
- **chargen - facteur d'amplification 18:1 / 1000:1**
  - **100mb/sec - 5.5gb/sec** de requêtes chargen usurpées pour une attaque de **100gb/sec**
  - La plus grande observée en 2014 - 96gb/sec, 120gb/sec signalée.
- **SNMP - Facteur d'amplification de 880:1 pour une attaque optimisée**
  - **114mb/sec** de requêtes SNMP itérées et usurpées pour une attaque de **100gb/sec.**
  - La plus grande observée en 2014 - 18gb/sec, 60gb/sec signalée.
- **SSDP - facteur d'amplification 20:1 / 83:1**
  - **1.2gb/sec - 5gb/sec** de requêtes SSDP usurpées pour une attaque de **100gb/sec**
  - Le plus grand observé en 2014 - 131gb/sec.
- **Service de réplication MS SQL, alias SQL Slammer-on-Demand - facteur d'amplification 173:1 - 473:1**
  - **211mb/sec - 578mb/sec** de requêtes MS SQL RS usurpées pour une attaque de **100gb/sec**
  - Le plus grand observé en 2014 - N/A

Atténuation de la Reflection / Amplification des attaques DDoS

Ce qu'il *ne faut pas* faire !

- ***Ne*** bloquez ***pas*** sans discernement UDP/123 sur vos réseaux !
- ***Ne*** bloquez ***pas*** sans discernement UDP/53 sur vos réseaux !
- ***Ne pas*** bloquer les paquets UDP/53 de plus de 512 octets !
- ***Ne*** bloquez ***pas*** TCP/53 sur vos réseaux !
- ***Ne*** bloquez ***pas*** sans discernement UDP/161 sur vos réseaux !
- ***Ne*** bloquez ***pas*** sans discernement UDP/19 sur vos réseaux !
- ***Ne*** bloquez ***pas*** sans discernement UDP/1900 sur vos réseaux !
- ***Ne*** bloquez ***pas*** sans discernement les fragments sur vos réseaux !
- ***Ne*** bloquez ***pas*** tous les ICMP sur votre réseau. networks! Au minimum, autorisez les ICMP Type-3/Code-4, requis pour PMTU-D.
  Si vous faites ces choses, vous allez ***casser l'Internet*** pour vos clients/utilisateurs !

Ne faites pas partie du problème !

- Déployez un **système anti-spoofing** à ***tous les*** bords du réseau.
  - **uRPF Loose-Mode/Feasible-Mode** à la périphérie du peering
  - **uRPF Strict Mode** au bord de l'agrégation du client
  - **ACLs** au bord de l'agrégation du client
  - **uRPF Strict-Mode** et/ou **ACLs** au bord de l'agrégation du Centre de Données Internet (IDC)
  - **DHCP Snooping** (fonctionne aussi pour les adresses statiques) et **IP Source Verify** au bord de l'accès au réseau local de l'IDC.
  - **PACLs** & VACLs **au** bord de l'accès au LAN de l'IDC
  - **Câble IP Source Verify**, etc. au CMTS
  - **Autres** mécanismes DOCSIS et DSL
- Si vous avez la réputation d'être un réseau favorable au spoofing, vous serez **dé-perçu/dé-transité** et/ou **bloqué** !

Ne faites pas partie du problème !

- ***Recherchez*** et corrigez de ***manière proactive les*** services abusifs ***sur votre réseau*** et sur les ***réseaux des clients/utilisateurs***, y compris en bloquant le trafic vers/depuis les services abusifs si nécessaire afin d'atteindre la conformité.
- Consultez http://www.openntpproject.org pour savoir si des services NTP abusifs ont été identifiés sur vos réseaux et/ou sur les réseaux de vos clients/utilisateurs.
- Consultez http://www.openresolverproject.org pour voir si des récurseurs DNS ouverts abusifs ont été identifiés sur votre réseau ou sur les réseaux des clients/utilisateurs.
- Les ***dommages collatéraux*** de ces attaques sont considérables - si des services abusifs sont présents sur vos réseaux ou sur les réseaux de vos clients/utilisateurs***, ces derniers subiront des pannes*** et des problèmes de performance ***importants***, et votre service d'assistance s'allumera !

Détection/Classification/Trackback/Mitigation

- Utiliser la **télémétrie des flux** (NetFlow, cflowd/jflow, etc.) exportée à partir du site Web de l'entreprise. *tous les* bords du réseau pour la détection/classification/retour en arrière des attaques De nombreux outils open-source sont disponibles, vous n'avez aucune excuse pour ne pas vous lancer !
- Appliquer des **politiques d'accès au réseau standard** devant les serveurs/services via des listes de contrôle d'accès sans état dans les routeurs/commutateurs de niveau 3 basés sur le matériel.
- Assurez-vous que les serveurs DNS récursifs **ne peuvent pas être interrogés** depuis l'Internet public - uniquement par vos clients/utilisateurs.
- Assurez-vous que **SNMP est désactivé/bloqué** sur les infrastructures/serveurs publics.
- Refuser les **requêtes NTP de niveau 6/-7** depuis l'Internet public.
- Désactivez tous les **services inutiles** tels que chargen.
- **Auditer régulièrement l'**infrastructure du réseau et les serveurs/services.

Détection/Classification/Traceback/Mitigation (suite)

- Déployer des techniques de réaction/atténuation basées sur l'infrastructure du réseau, telles que **S/RTBH** et **flowspec,** à ***toutes les*** extrémités du réseau.
- Déployez des systèmes intelligents d'atténuation des attaques DDoS (IDMS) dans des centres d'atténuation situés à des points topologiquement appropriés de vos réseaux pour atténuer les attaques.
- Assurer une ***capacité d'atténuation et une bande passante de déviation/réinjection suffisantes*** - S/RTBH, flowspec, IDMS envisager des liens de centre d'atténuation OOB à partir des routeurs de périphérie pour garantir une bande passante de IDMS "nettoyage".
- Les entreprises/ASP devraient s'abonner aux services d'atténuation DDoS "**Clean Pipes**" des ISP/MSSP.
- Les opérateurs de haut débit grand public devraient envisager des **ACL par défaut minimales** pour limiter l'impact des abus de service sur les réseaux des clients.
- Utilisez la **puissance de l'appel d'offres** pour spécifier des configurations par défaut sécurisées pour les dispositifs PE et CPE - et vérifiez-les par des tests.
- **Sachez qui contacter** chez vos pairs/transitions pour obtenir de l'aide.
- **Participer à la** communauté mondiale de la sécurité opérationnelle.

Détection/Classification/Traceback/Mitigation (suite)

- Les FAI doivent envisager de déployer des mécanismes de **qualité de service (QoS)** à toutes les extrémités du réseau afin de réduire le trafic NTP non synchronisé à un niveau approprié (c'est-à-dire 1 mb/sec).
  - Les paquets NTP timesync ont une longueur de 76 octets (toutes les tailles sont moins la trame de la couche 2).
  - Les réponses NTP monlist sont d'une longueur de 468 octets.
  - Les requêtes NTP monlist utilisées dans ces attaques ont une longueur de 50, 60 et 234 octets.
  - **Option 1** - contrôler tout le trafic UDP/123 autre que 76 octets (source, destination, ou les deux) jusqu'à 1 mb/sec. Cela permet de contrôler le trafic source d'attaque - réflecteur/amplificateur ainsi que le trafic réflecteur/amplificateur - cible.
  - **Option 2** - contrôler tout le trafic UDP/123 de 400 octets ou plus (source) jusqu'à 1 Mo/sec. Cela ne contrôlera que le trafic du réflecteur/amplificateur - cible.
  - Le trafic NTP timesync ne sera pas affecté.
  - Les fonctions administratives supplémentaires (rarement utilisées) de NTP, telles que *ntptrace,* ne seront affectées que lors d'une attaque.
- Les entreprises/ASP ne doivent autoriser que les requêtes/réponses NTP vers/depuis des **services NTP spécifiques**, et interdire tous les autres.

Évolution de la capacité d'atténuation - 4 tb/sec et au-delà

- Le système intelligent d'atténuation des attaques DDoS (IDMS) le plus performant actuellement en vente - 40 Go/s
- 16-IDMS (limite CEF/ECMP) = 640gb/sec par cluster
- Plusieurs clusters peuvent être "anycasted".
- Le plus grand nombre d'IDMS par déploiement est actuellement de 100 = 4 tb/sec de capacité d'atténuation par déploiement, soit 10 fois plus que le plus grand DDoS à ce jour.
- Déployer des IDMS dans des centres d'atténuation aux limites - dans/hors des dispositifs de limite.
- Déployez des IDMS dans des centres d'atténuation régionaux ou centralisés avec des liaisons dédiées de grande capacité pour la déviation/réinjection OOB. Une largeur de bande suffisante pour la déviation/réinjection est essentielle !
- S/RTBH & flowspec exploitent le matériel de routeur/commutateur, des centaines de mpps, gb/secL. 'infrastructure de réseau est nécessaire en raison du rapport entre les volumes d'attaque et les capacités de peering et de liaison centrale !

Conclusion

Réflexion/Amplification Résumé de l'attaque DDoS

- Les services abusifs sont largement mis en œuvre ou mal configurés sur l'internet.
- Grands pools de serveurs/services abusifs
- Lacunes en matière d'anti-spoofing à la périphérie des réseaux
- Rapports d'amplification élevés
- Faible difficulté d'exécution
- Outils d'attaque facilement disponibles
- Impact extrêmement fort - "Le ciel nous tombe sur la tête".
- Risque important pour les cibles potentielles et les réseaux intermédiaires/les passants.

Sur les origines du trafic pirate

- NAT est laid, casse des choses, et n'a aucune valeur de sécurité inhérente.
- Toutefois, la prédominance des NAT sur les réseaux d'accès à large bande a eu un effet secondaire bénéfique : l'anti-spoofing (il est généralement impossible d'usurper le trafic derrière un NAT, à moins qu'il ne soit cassé).
- Nous pensons qu'une grande partie du trafic usurpé utilisé pour lancer des attaques DDoS par réflexion/amplification provient de serveurs contrôlés par des attaquants dans des centres de données Internet (IDC) d'hébergement/de co-location/VPS/de "nuage" qui n'appliquent pas la validation de l'adresse source.
- Les serveurs peuvent être compromis ; il peut s'agir de VPS loués par des attaquants ; ils peuvent être hébergés par des fournisseurs "à l'épreuve des balles".
- Les outils de collecte et d'analyse de la télémétrie des flux permettent de retracer automatiquement le trafic usurpé jusqu'aux points d'entrée du réseau, mais uniquement dans le cadre de son propre contrôle administratif.

Que faut-il faire ?

- Lancer un projet de location d'instances shell/VPS dans le monde entier, exécuter un code de type Spoofer Project sur les instances VPS, compiler les rapports des IDCs/hosters/co-locateurs qui permettent le spoofing. C'est un début, au moins.
- Discuter de la possibilité d'inclure la fonctionnalité du projet Spoofer dans les systèmes d'exploitation avec les fournisseurs/organisations concernés (Microsoft, Apple, Google, distros Linux, distros *BSD, fournisseurs de consoles, Cisco, Juniper, Linksys, Asus, etc.)
- Mécanisme d'apprentissage pour la fonctionnalité de type IP Source Guard ou pACL/vACL activée par défaut sur les ports de commutateurs de couche 2 configurés comme ports d'accès - fournisseurs d'infrastructure réseau. La couche d'accès d'IDC est un domaine relativement restreint, avec une marge de manœuvre réduite pour les résultats indésirables et une plus grande probabilité de réussite.
- Auto-provisionnement "SDN" des mécanismes de validation de l'adresse de source > cringe<
- Améliorer la classification du trafic usurpé, les capacités de traçage coopératif entre opérateurs - fournisseurs d'outils de collecte/analyse de télémétrie des flux.
- Travailler avec les compagnies d'assurance pour les aider à comprendre les risques non garantis, développer des capacités d'audit.

Sommes-nous condamnés ?

- Le No! déploiement d'outils/techniques/BCP No! existants et bien connus permet d'améliorer considérablement la sécurité et d'obtenir des résultats mesurables.
- L'évolution des défenses contre ces attaques montre qu'un changement positif est possible - les organisations ciblées et les ISP/MSSP qui les défendent ont modifié leurs architectures, leurs techniques d'atténuation, leurs processus et leurs procédures afin d'atténuer ces attaques avec succès.
- Les capacités d'atténuation s'adaptent pour répondre et dépasser les volumes d'attaques - l'architecture de déploiement, la bande passante de déviation/réinjection, l'exploitation de l'infrastructure réseau sont essentielles.
- L'automatisation est une bonne chose, mais elle ne remplace pas une architecture résiliente, une planification perspicace et un personnel de sécurité opérationnelle intelligent, qui sont plus importants que jamais !

Discussion

Cette présentation - http://bit.ly/1lHksUH

Nous remercions tout particulièrement Gary Sockrider et Ben Fischer d'Arbor Networks pour leur contribution à cette présentation.

Merci !

Roland Dobbins < rdobbins@arbor.net>
Analyste ASERT senior